PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA

"ESTUDIO DE APLICACIÓN DE MECANISMO DE SEGURIDAD INFORMÁTICA PARA LA TRANSMISIÓN DE VIDEO STREAMING EN UN SISTEMA DE TELE VIGILANCIA"

CRISTIAN ALEJANDRO DÍAZ VILLENA

INFORME FINAL DEL PROYECTO
PARA OPTAR AL TÍTULO PROFESIONAL DE
INGENIERO CIVIL EN INFORMÁTICA

MARZO 2011

Pontificia Universidad Católica de Valparaíso

Facultad de Ingeniería

Escuela de Ingeniería Informática

"ESTUDIO DE APLICACIÓN DE MECANISMO DE SEGURIDAD INFORMÁTICA PARA LA TRANSMISIÓN DE VIDEO STREAMING EN UN SISTEMA DE TELE VIGILANCIA"

CRISTIAN ALEJANDRO DÍAZ VILLENA

Profesor Guía: **Jaime Briggs Luque.**

Profesor Co-referente: **Cristian Alexandru Rusu**.

Carrera: **Ingeniería Civil en Informática**

Marzo 2011

Dedicatoria

Agradezco a mis padres, familia por todo el cariño y esfuerzo entregado en este proceso académico y a mí novia por su gran amor e incondicional apoyo profesional.

Resumen

El presente documento da cuenta de la problemática situada en la transmisión de contenido multimedia a través de Internet, la cual se basa en la probabilidad de que este contenido pueda ser vulnerado o accesado por entidades que no correspondan, todo esto en el marco de los sistemas de tele vigilancia.

Por ello que se describe el proceso utilizado para la aplicación de los mecanismos de seguridad, en la transmisión de video streaming para un sistema de tele vigilancia. Con esto se propone un modelo con mecanismos de seguridad para contrarrestar dicha problemática antes mencionada.

Asimismo se dan a conocer los resultados y análisis, en relación al prototipo obtenido, dando cuenta de que esta investigación evidencia que la utilización de técnicas de seguridad puede ser aplicada en pos de mantener una buena calidad de servicio.

Palabras Claves: Streaming, Tele Vigilancia, Calidad de Servicio, Seguridad.

Abstract

This report describes security problems on media streaming over the Internet, which arise with the probability of unauthorized access to content for a third party in the context of remote systems monitoring.

It is described the process used to implement the security mechanisms on video streaming transmission. This thesis proposes models and security mechanisms to counter attack the problems mentioned above.

We present results and analysis in relation to progress achieved, realizing that this research evidence that the use of security techniques can be applied towards maintaining a good Quality of Service.

Keywords: Streaming, Tele Monitoring, Quality of Service, Security.

Tabla de Contenidos

Glosario de Términos

Streaming: Técnica utilizada para la visualización de contenido multimedia a través de Internet en tiempo real, sin la descarga completa previamente del contenido.

HTTPS: (Hyper Text Transfer Protocol Secure) es idéntico a HTTP excepto en una diferencia clave, los datos transferidos se cifran con Capa de sockets seguros (SSL) o Seguridad de la capa de transporte (TLS). Este método de seguridad aplica el cifrado a los propios datos, lo que permite la visualización segura de vídeo en un navegador Web. Sin embargo, el uso de HTTPS puede ralentizar el enlace de comunicación y, en consecuencia, la frecuencia de imagen del vídeo.

Estándar IEEE 802.1X: establece una conexión punto a punto o impide el acceso desde el puerto de la LAN si la autenticación es errónea. También evita el denominado "porthi-jacking", es decir, el acceso de un equipo no autorizado a una red mediante una toma de red del interior o del exterior de un edificio.

PTZ: características de las cámaras, que significa que pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto de forma manual o automática.

Lista de Abreviaturas o Siglas

RTP: Real Time Protocol o Protocolo de Tiempo Real.

RTSP: Real Time Streaming Protocol.

RTMO: Real Time Messaging Protocol.

RTCP: Real Time Control Protocol

SRTP: El Secure Real-time Transport Protocol.

SIP: Session Initiation Protocol.

IPSEC: Internet Protocol Security.

VPN: Virtual Private Network.

Lista de Figuras

Lista de Tablas

1 Introducción

1.1 Introducción

Hoy en día, el concepto de seguridad, está plasmado en distintos ámbitos y campos de la vida humana, como deportes, empresas, ciudadanía, entre otros, y ha sido uno de los tópicos más controversiales, frente a las nuevas generaciones y épocas, donde las vulnerabilidades e inseguridades existentes frente a la inteligencia de la delincuencia, convierten a los espacios privados y públicos en focos de ataques. Así, se puede definir "Seguridad" , como la protección de objetos de cierto valor, personas y de su entorno, mediante elementos como cámaras para vigilancia, cerraduras de alta seguridad, cristales y puertas blindadas entre otros sistemas.

La seguridad perimetral o del entorno que deben tener los espacios, tanto públicos como privados, generan la necesidad de implementar soluciones de Tele Vigilancia, en pos de que en los últimos años la percepción de victimización e inseguridad frente a los delitos a aumentado.. Por ejemplo sólo en la región de Valparaíso, la ciudadanía percibe que la delincuencia ha aumentado o mantenido en los últimos doce meses [1].

Por otra parte, se puede definir un Sistema de Tele Vigilancia, como el conjunto de elementos e instalaciones necesarias para proporcionar a las personas y bienes materiales, existentes en un espacio físico determinado, protección frente a robo, atracos o sabotajes, entre otras. Así, los sistemas de Tele Vigilancia pueden ser variables según las necesidades del lugar a proteger y del presupuesto disponible para ello. En el mercado existe un gran abanico de soluciones, con características técnicas y calidades diversas, que hacen que no se pueda elegir una en particular, a la hora de implementar un sistema de seguridad.

Es por esto, que en este documento se realizará un estudio de las distintas herramientas, dispositivos y protocolos de comunicación para un Diseño de un Sistema de Tele Vigilancia Seguro, por lo que, en los próximos capítulos se detallará en profundidad los tópicos más relevantes relacionados con este Diseño.

Por lo tanto, esta investigación tendrá como núcleo central, 3 directrices relevantes para este diseño, Sistemas de Tele Vigilancia actuales, Tecnología Streaming y Seguridad Informática relacionada a la transmisión de video, que se abordarán a lo largo de este documento.

1.2 Objetivos

1.2.1 Objetivo General

Proponer una solución de diseño con aplicación de mecanismo de seguridad informática en la transmisión de video Streaming para un sitema de Tele Vigilancia.

1.2.2 Objetivos Específicos

- Establecer marco teórico de mecanismo de Seguridad Informática aplicados a la tecnología Streaming y productos asociados a un Sistema de Tele Vigilancia.
- Establecer el modelo de comunicación segura para la transmisión de video streaming.
- Validar modelo de comunicación segura a través de un prototipo funcional.

1.3 Plan de Trabajo

El plan de trabajo contempla las siguientes actividades para proyecto 1 y 2.

Tabla 1 – Plan de Trabajo.

Mes	Actividad
Agosto-Septiembre	Desarrollo del marco teórico de los tópicos relacionados con Tele Vigilancia, Streaming y enlaces Seguros.
Septiembre-Octubre	Estudio y análisis de tópicos relacionados con Tele Vigilancia para Diseño a proponer.
Octubre-Noviembre	Diseño de Sistema de Tele Vigilancia utilizando Streaming y Conectividad Segura.
Marzo-Abril-Mayo	Adquisición de dispositivos y Codificación de prototipo aplicando mecanismos de seguridad.
Mayo-Junio	Test y correcciones de prototipo.
Junio-Julio	Evaluación, refinamiento y término de prototipo.

1.4 Metodología

Esta investigación se enmarca en el estudio de los mecanismos de seguridad informática, en conjunto con la tecnología streaming y sistemas de Tele Vigilancia. Por ello esta investigación tiene un enfoque cuantitativo, donde a continuación se define cada una de las etapas fundamentales para este estudio.

1.4.1 Idea

Nace de la inquietud de mejorar la transmisión y calidad de servicios de los sistemas de tele vigilancia, apoyándose en nuevas tecnologías y técnicas que mejoren la comunicación y disminuyan los retardos de comunicación. Además, existen variadas técnicas, métodos y mecanismos de seguridad informática que se aplican en distintos ámbitos tecnológicos, pero resulta limitada la investigación que se hacen en relación a la problemática que existe entre la aplicación de seguridad informática v/s calidad de servicio.

1.4.2 Planteamiento del Problema

La problemática se enmarca en aplicar mecanismos de seguridad informática en la transmisión de video streaming para los sistemas de Tele Vigilancia. Por ello, el desarrollo de este estudio se realizará acorde a los objetivos expuestos en el capítulo anterior.

1.4.3 Desarrollo marco teórico

A través de este documento se desarrolla el marco teórico referente al estudio de los mecanismos de seguridad informática aplicados a streaming de video y Tele vigilancia.

1.4.4 Visualización del alcance del estudio

Este estudio es de tipo exploratorio y se basa en indagar la problemática de seguridad en video streaming, con el fin de evaluar y observar el comportamiento de la aplicación de cada uno de los mecanismos de seguridad propuestos, con el fin de verificar su impacto en la calidad de servicio y transmisión a través de la red IP.

1.4.5 Desarrollo del Diseño

Al final del documento, se propone un modelo de diseño que aplica mecanismos de seguridad en la comunicación entre un usuario y un servidor, a través de la utilización de un sistema de Tele Vigilancia, con transmisión de video streaming. Por ello, que a través del diseño propuesto se realizaran las actividades según el plan de trabajo propuesto en los capítulos anteriores.

1.4.6 Obtención y Análisis de Datos

Realizar, obtener y recopilar datos a través de pruebas de distinta índole, que validen el diseño, como así demuestren su ventaja y utilidad en los sistemas de televigilaqncia.

1.4.7 Resultados

Análisis y comparación de los datos obtenidos, verificando el impacto producido por la aplicación de mecanismos de seguridad informática, en los enlaces de comunicación, para la transmisión de video en un sistema de Tele Vigilancia.

1.5 Organización del Texto

El presente informe se encuentra dividido en 4 capítulos, los cuales representan el marco teórico para el desarrollo de este proyecto.

El primer Capítulo expone la introducción del proyecto, además de la definición de los objetivos generales, específicos y el plan de trabajo. En el segundo capítulo, se presentan las distintas tecnologías de Tele Vigilancia y cámaras existentes en el mercado. En el Tercer capítulo, se describen los distintos protocolos y aspectos de seguridad utilizados en los sistemas de Tele Vigilancia. Finalmente, en el cuarto Capítulo, se describen los aspectos y tópicos relevantes relacionados con la tecnología Streaming.

2 Tecnología de Tele Vigilancia

2.1 Sistemas de Tele Vigilancia

2.1.1 Introducción

Los Sistemas de Tele Vigilancia son cada día más requeridos, debido a la necesidad de una mayor seguridad. Hasta hace unos años, sólo se instalaban sistemas de seguridad en lugares concretos, para hacer frente a robos, atracos o incendios. Hoy en día, se utilizan en hogares, pequeños negocios, fábricas, además de lugares de alto riesgo, como bancos y joyerías.

Frente a la diversidad de necesidades, se han desarrollado una variedad de herramientas y soluciones, con el fin de obtener una mayor seguridad y calidad de productos, cuyo objetivo es satisfacer las distintas necesidades de costos, seguridad, envergadura, calidad de servicio, entre otras.

En los siguientes ítems, se presentará una breve reseña histórica del concepto de Sistemas de Tele vigilancia. Para luego abordar las distintas tecnologías relacionadas que actualmente se pueden encontrar en el mercado.

2.1.2 Reseña Conceptual

La expresión “Sistemas de Tele Vigilancia”, comúnmente parece estar alineada con la de “Cámaras contra Robos”. Pues bien, decir esto resulta ser una expresión muy simple y deteriorada de lo que en realidad es un “Sistema de Tele Vigilancia”.

A través de toda la historia, el hombre se ha visto en la necesidad de proteger sus pertenecías, por motivos de robos por parte de otros individuos, o bien por las acciones normales de la naturaleza. Hasta hace poco tiempo, la forma de protección, era bien sencilla. El propio individuo como ser humano, se encargaba de vigilar o establecía mecanismos naturales de protección, para así evitar desagradables sorpresas, que por desgracia siempre se han producido.

La aparición de la electrónica y la era de las Tecnologías de Información (Tics), ha permitido un rápido progreso en lo que se refiere al concepto de seguridad, ya que ha proporcionado una variedad de posibilidades en los sistemas de seguridad, cada día más amplia y eliminando de ésta forma viejos conceptos y formas de vida.

Los Sistemas de Tele Vigilancia existen desde hace 25 años. Comenzaron siendo sistemas analógicos al 100% y paulatinamente se fueron digitalizando. Los Sistemas de hoy en día, han avanzado mucho desde la aparición de las primeras cámaras.

La aplicación de estos Sistemas ha permitido la realización de los procesos y actividades de forma protegida frente a eventualidades. Estos sistemas tienen como finalidad ser utilizados para controlar, supervisar y monitorear tanto en tiempo real como en forma diferida, las eventualidades almacenadas o grabadas en un mismo lugar o desde lugares remotos.

Los Sistema de Tele Vigilancia no sólo sirven para proteger los bienes e inmuebles, resguardan a las personas, ahorran tiempo y dinero y en los procesos domésticos y empresariales.

Algunos ejemplos de su aplicación:

- Seguridad en vivienda.
- Seguridad en bancos.
- Seguridad en cárceles, centrales nucleares, etc.
- Seguridad empresarial.
- Entre otros.

En la actualidad, estos sistemas utilizan diversos dispositivos, como cámaras, servidores de computadores, para la grabación de vídeo, en un sistema digitalizado. Sin embargo, existen también los sistemas análogos, que frente a los anteriormente mencionados, existen algunas diferencias, como también existe una integración de ambas tecnologías. Es por ello que en los siguientes capítulos se darán referencias a estos tipos de sistemas y sus características más relevantes, que se tomarán como base para el futuro Diseño de Tele Vigilancia que se desea proponer a través de este documento.

2.1.3 Sistema Análogo

Un Sistema Análogo o Analógico es aquel que utiliza un VCR (grabador de vídeo) que se representa a través de un sistema completamente análogo, formado por cámaras análogas con salida coaxial, conectadas a un VCR para grabar.

El VCR utiliza el mismo tipo de cintas que una grabadora doméstica, sin embargo este dispositivo es especialmente fabricado para vigilancia y no de uso doméstico. El vídeo no se comprime y, se graba a una velocidad de imagen completa. Existen diversas versiones de grabadores, pudiendo incluso grabar hasta 960 horas en una cinta. Pero en realidad, 960 horas grabando una imagen analógica cada 9 segundos, no siendo despreciable considerando que ésta tecnología tiene más de 20 años [2].

En sistemas mayores, se puede conectar un quad o un multiplexor entre la cámara y el VCR. El quad/multiplexor permite grabar el vídeo procedente de varias cámaras en un sólo grabador, pero con el inconveniente que tiene una menor velocidad de imagen. Para monitorear el vídeo, es necesario un monitor analógico.

Este Sistema se representa en el siguiente esquema.

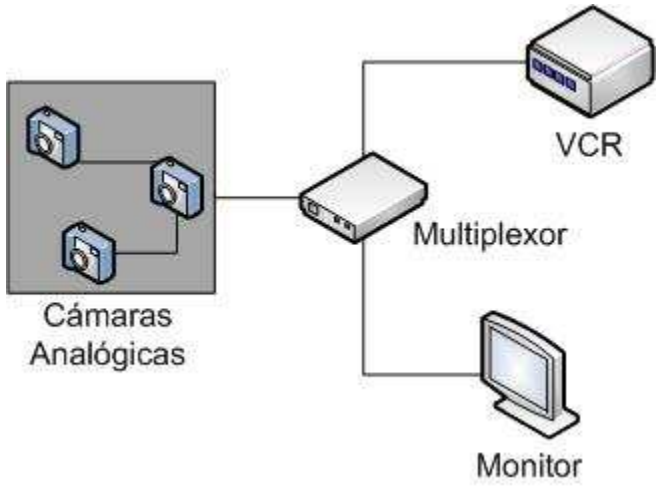

Figura 1 – Sistema Análogo.

En la figura 2.1 se aprecia un Sistema Análogo, en donde la señal de vídeo de cada cámara, a través del cable coaxial es conectada al multiplexor. A su vez, un cable coaxial es conectado desde el multiplexor hasta la entrada de vídeo del monitor. Otro cable es conectado desde la salida del multiplexor hasta el grabador. El sistema se programa desde el panel de control del grabador. El monitor nos sirve para visualizar la programación del sistema y las imágenes grabadas por las cámaras de vigilancia. El modo de reproducción del grabador, nos facilitará simultáneamente todas las imágenes grabadas.

2.1.4 Sistema Digital Basado en Computador o Completamente Digital

Un Sistema Completamente Digital es un sistema de vídeo IP que utiliza servidores de vídeo que incluye un servidor de vídeo, un conmutador de red y un computador con software de gestión de vídeo. La cámara se conecta al servidor de vídeo, el cual digitaliza y comprime el vídeo. A continuación, el servidor de vídeo se conecta a una red y transmite el vídeo a través de un conmutador de red a un computador, donde se almacena en discos duros [3].

Este Sistema se representa en el siguiente esquema.

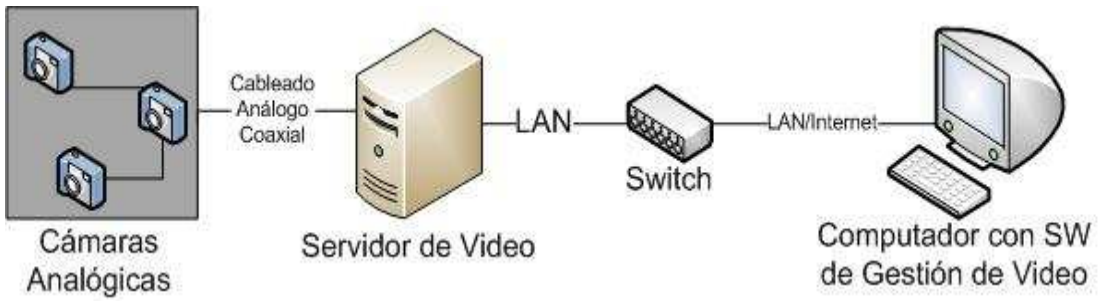

Figura 2 – Sistema Digital con Cámaras Análogas.

Además, existe también un Sistema que utiliza una cámara IP que combina una cámara y un computador en una unidad, lo que incluye la digitalización y la compresión del vídeo así como un conector de red. El vídeo se transmite a través de una red IP, mediante los conmutadores o switch de red y se graba en un computador estándar con software de gestión de vídeo.

Este Sistema se representa en el siguiente esquema.

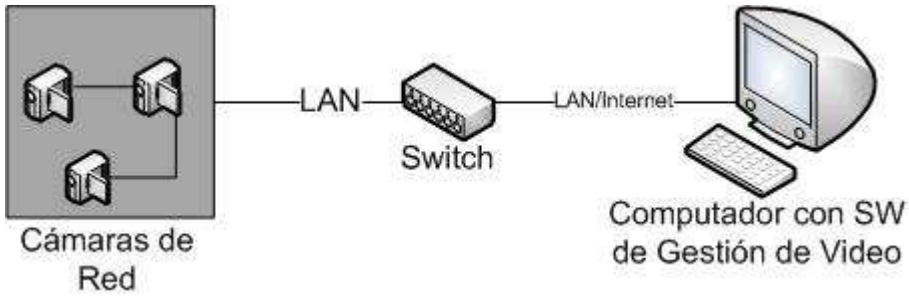

Figura 3 – Sistema Digital con Cámaras de Red.

Además de las topologías antes expuestas, se puede tener un esquema como lo muestra la siguiente figura.

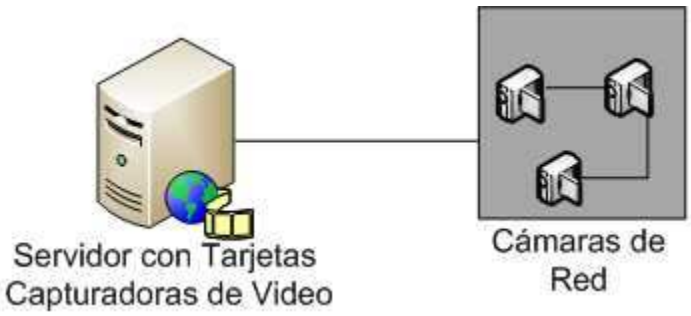

Figura 4 – Sistema Digital Basado en Computador.

Este esquema básicamente es un Sistema Digital Basado en un Computador, compuesto de un computador básicamente, una o varias tarjetas capturadotes de video y un programa de gestión de video especifico. Proporciona una excelente calidad de imagen.

2.1.5 Sistema Digital Integral o Parcialmente Digital

Un Sistema Digital Integral o Parcialmente Digital utiliza un DVR (grabador de vídeo digital), es un sistema analógico con grabación digital. En un DVR, la cinta de vídeo se sustituye por discos duros para la grabación de vídeo, y es necesario que el vídeo se digitalice y comprima para almacenar la máxima cantidad de imágenes posible.

Con los primeros DVR, el espacio del disco duro era limitado, por tanto, la duración de la grabación era limitada, o debía usarse una velocidad de imagen inferior. El reciente desarrollo de los discos duros significa que el espacio deja de ser el principal problema. La mayoría de los DVR disponen de varias entradas de vídeo, normalmente 4, 9 ó 16, lo que significa que también incluyen la funcionalidad de los quads y multiplexores.

Este Sistema se representa en el siguiente esquema.

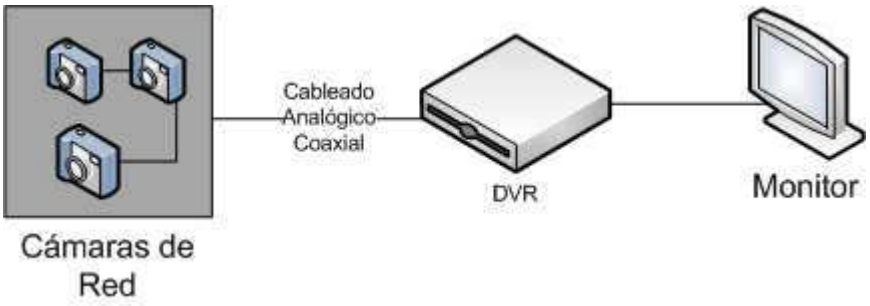

Figura 5 – Sistema Digital Integral.

Además existe un Sistema Digital Integral o Parcialmente Digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. Como el vídeo se digitaliza y comprime en el DVR, se puede transmitir a través de una red, para que se monitorice en un computador, en una ubicación remota.

Algunos sistemas pueden monitorizar, tanto vídeo grabado como en directo, mientras otros sólo pueden monitorizar el vídeo grabado. Además, algunos sistemas exigen un usuario especial para monitorizar el vídeo, mientras que otros utilizan un navegador Web estándar, lo que flexibiliza la monitorización remota.

Este Sistema se representa en el siguiente esquema.

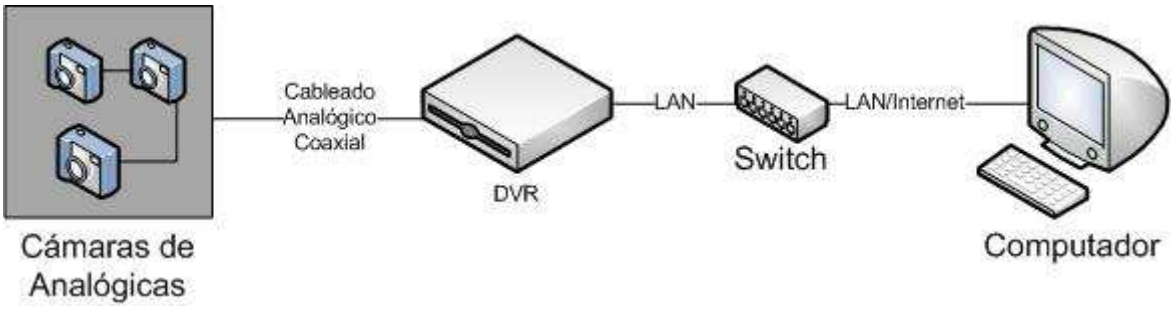

Figura 6 – Sistema Digital con DVR IP.

2.1.6 Ventajas y Limitaciones

A continuación se presentan las Ventajas y Limitaciones de cada una de las Tecnologías de Tele Vigilancia expuestas anteriormente.

Tabla 2 – Sistema Análogo.

Tipo Tecnología	Sistema Análogo
Ventajas	• El sistema es estable, con una tecnología muy antigua.
Limitaciones	• La calidad de las imágenes es muy "pobre" comparada con los sistemas digitales. • La cinta tiene que ser cambiada cada 3 días o menos incluso. • El sistema necesita ser limpiado con mucha frecuencia e incluso está sometido al desgaste de las cabezas grabadoras. • Las imágenes de vídeo se van degradando con el tiempo. • El sistema no tiene la posibilidad de poder visualizarse en remoto, a través de Internet o de poder comandar las cámaras vía Web como en los sistemas digitales.

Tabla 3 – Sistema Digital Integral.

Tipo Tecnología	Sistema Digital Integral o Parcialmente Digital
Ventajas	El sistema DVR añade las siguientes ventajas: • No es necesario cambiar las cintas • Calidad de imagen constante El sistema DVR IP añade las siguientes ventajas: • Monitorización remota de vídeo a través de un computador. • Funcionamiento remoto del sistema.
Limitaciones	• Muchas conversiones analógicas a digital y viceversa. • Degradación por la conversión. • Problemas con almacenamiento por pérdida de calidad o degradación.

Tabla 4 –Sistema Completamente Integral.

Tipo Tecnología	Sistema Digital Basado en Computador o Completamente Digital
Ventajas	Un Sistema Completamente Digital que utiliza servidores de vídeo añade las ventajas siguientes: • Utilización de red estándar y hardware como servidor o computador para la grabación y gestión de vídeo. • El sistema es escalable en ampliaciones de una cámara cada vez. • Es posible la grabación fuera de las instalaciones. • Preparado para el futuro, ya que este sistema puede ampliarse fácilmente incorporando cámaras IP. Un Sistema que utiliza cámaras IP añade las ventajas siguientes: • Cámaras de alta resolución (megapíxel). • Calidad de imagen constante. • Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica • Funciones de Pan/tilt/zoom, audio, entradas y salidas digitales a través de IP, junto con el vídeo. • Flexibilidad y escalabilidad completas. Un Sistema Digital Basado en un Computador añade las ventajas siguientes: • Grabación en alta resolución. • Flexibilidad y facilidad de uso. • Gran capacidad de almacenamiento pudiendo almacenar muchos días de grabaciones. • Pequeño o mínimo mantenimiento. • Fácil integración en las redes de la empresa o de Internet. • En caso de avería o daños, el sistema podrá estar listo en tiempo récord, ya que son infinitos y variados los componentes para su reparación (placas madre, discos duros, tarjetas de vídeo etc.).
Limitaciones	• El sistema adopta el sistema operativo del computador, con lo que el usuario debe tener cierta destreza en el manejo de estos dispositivos. No obstante, se puede simplificar muchísimo. Asimismo, los sistemas de Tele Vigilancia basados en Computador están adoptando últimamente sistemas operativos más simples como Linux.

2.2 Cámaras

2.2.1 Introducción

Una cámara es un elemento que se encarga de transformar las variaciones ópticas o imágenes, en variaciones de tensión. Las variaciones de tensión son amplificadas y tratadas, para más tarde llevarlas a los monitores, donde de nuevo son transformadas en las primitivas imágenes. Están constituidas por las carcasas de protección, soportes, entre otros, además de los propios dispositivos de captación de imágenes.

Las cámaras utilizadas en Tele Vigilancia se pueden clasificar en función si están diseñadas únicamente para su uso en interiores o exteriores tanto alámbrica como inalámbricas. Asimismo, pueden poseer reguladores de luz, sensores, carcasas de protección, entre otras. En toda la gama de cámaras que se definirán a continuación, existe una gran variedad de medidas, estilos y colores.

En las siguientes secciones se presentan las distintas tecnologías relacionadas con Cámaras de Tele Vigilancia, que actualmente se pueden encontrar en el mercado [4].

2.2.2 Fijas

Una Cámara fija, que puede colocarse hacia un objetivo fijo, es una cámara que dispone de un campo de vista fijo una vez situada en algún lugar específico. Una cámara fija, es el tipo de cámara tradicional en el que la cámara y la dirección en la que apunta son claramente visibles. Este tipo de cámara es la mejor opción en aplicaciones en las que resulta útil que la cámara esté bien visible. Normalmente, las cámaras fijas permiten que se cambien sus objetivos o puntos de grabación. Pueden adaptarse carcasas diseñadas para su uso en instalaciones interiores o exteriores [6].

2.2.3 Domo

Una cámara domo, también conocida como mini domo, consta básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar el punto seleccionado en cualquier dirección. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara.

Uno de los inconvenientes que presentan las cámaras domo es que normalmente no disponen de objetivos intercambiables, y en el caso de poder intercambiarse, la selección de objetivos está limitada por el espacio dentro de la carcasa domo. Para compensarlo, a menudo se proporciona un objetivo que permita realizar ajustes en el campo de visión de la cámara [5].

2.2.4 PTZ(Pan, Tilt, Zoom)

Las cámaras PTZ pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto de forma manual o automática. Todos los comandos PTZ se envían a través del mismo cable de red que la transmisión de vídeo [5].

Algunas de las funciones que se pueden incorporar a una cámara PTZ incluyen:

- **Estabilización electrónica de imagen (EIS).** En instalaciones exteriores, las cámaras PTZ con factores de zoom superiores a los 20x son sensibles a las vibraciones y al movimiento causado por el tráfico o el viento. La estabilización electrónica de la imagen (EIS) ayuda a reducir el efecto de la vibración en un vídeo. Además de obtener vídeos más útiles, EIS reducirá el tamaño del archivo de la imagen comprimida, de modo que se ahorrará un valioso espacio de almacenamiento.

- **Máscara de privacidad.** La máscara de privacidad, permite bloquear o enmascarar determinadas áreas de la escena frente a visualización o grabación. En este tipo de cámara, la funcionalidad es capaz de mantener la máscara de privacidad incluso en caso de que el campo de visualización de la cámara cambie debido al movimiento de la máscara con el sistema coordinado.

- **Posiciones predefinidas.** Muchos modelo de cámaras PTZ permiten programar posiciones predefinidas, normalmente entre 20 y 100. Una vez las posiciones predefinidas se han configurado en la cámara, se puede cambiar de una posición a otra de forma muy rápida.

- **E-flip.** En caso de que la cámara PTZ se monte por ejemplo en un techo y se utilice para realizar el seguimiento de una persona, se producirán situaciones en las que el individuo en cuestión pasará justo por debajo de la cámara. Sin la funcionalidad E-flip, las imágenes de dicho seguimiento se verían al revés. En estos casos, E-flip gira las imágenes 180 grados de forma automática. Dicha operación se realiza automáticamente y no será advertida por el usuario.

- **Auto-flip.** Gracias a la función Auto-flip, una cámara de red PTZ puede girar al instante 180 grados su cabezal y seguir realizando el movimiento horizontal más allá de su punto cero. De este modo, la cámara puede continuar siguiendo el objeto o la persona en cualquier dirección.

- **Autoseguimiento.** El autoseguimiento es una función de vídeo inteligente que detecta automáticamente el movimiento de una persona o vehículo y lo sigue dentro de la zona de cobertura de la cámara. Esta función resulta especialmente útil en situaciones de Tele Vigilancia no controlada humanamente, en las que la presencia ocasional de personas o vehículos requiere especial atención. La funcionalidad recorta notablemente el costo de un sistema de supervisión, puesto que se necesitan menos cámaras para cubrir una escena. Asimismo, aumenta la efectividad de la solución, debido a que permite que las cámaras PTZ graben áreas de una escena en actividad.

2.2.5 Nocturnas

Es una novedad dentro del campo de Tele Vigilancia. Suelen ser cámaras infrarrojos. Existen además cámaras de color durante el día que conmutan a blanco y negro cuando decae la luz. En blanco y negro nos permite una mayor resolución e incluso mucha más velocidad cuando se trata de transmitir a través de Internet. Una vez que se restaura los niveles de luz, vuelven a cambiar a color [5].

2.2.6 Ocultas

Cada día se fabrican cámaras más pequeñas y versátiles. Esto nos permite poder disimular cámaras en los más diversos objetos, techos, paredes, etc. Existen módulos sueltos que nos permitirán alojar una cámara prácticamente en cualquier sitio. Asimismo, se comercializan ya cámaras integradas en sensores de detección de movimiento para alarmas, detectores de humos, libros, etc. Son las mismas cámaras que se utilizan para una instalación convencional pero sin carcasas ni añadidos exteriores [6].

2.2.7 IP

La combinación de los avances tecnológicos que se han venido produciendo en torno a los dispositivos de grabación de vídeo, la robótica y la posibilidad de transmitir imágenes y sonido a través de Internet ha dado lugar a una nueva tecnología: Tele Vigilancia por IP. Simplemente es montar una cámara, configurar IP y conectar a un router. La diferencia con el resto de las cámaras es su facilidad de funcionamiento [5].

2.2.8 Aspectos Técnicos

Existen distintos aspectos a la hora de elegir una cámara, con el fin de situarla en un determinado lugar. Casi todas las cámaras actuales, cumplen con las características normales para cualquier instalación de Tele Vigilancia. No obstante, a continuación se presentan algunas especificaciones técnicas que hacen distinguir un tipo de cámara de otra [7].

2.2.8.1 Sensibilidad Lumínica

La sensibilidad lumínica se especifica en términos de lux, que corresponde a un nivel de iluminación bajo el que una cámara produce una imagen aceptable. Cuanto más baja es la especificación de lux, mejor es la sensibilidad lumínica de la cámara. Normalmente, es necesario un mínimo de 200 lux para iluminar un objeto de manera que se pueda obtener una imagen de buena calidad.

En general, cuanta más luz reciba el sujeto, mejor será la imagen. Con poca luz, será difícil realizar el enfoque y la imagen resultará granulada y/u oscura.

Para capturar imágenes de buena calidad en condiciones de poca luz u oscuridad, es necesaria una cámara con visión diurna/nocturna que aproveche la luz próxima al espectro infrarrojo. Condiciones lumínicas diferentes ofrecen una iluminancia diferente. Muchas escenas naturales tienen una iluminación bastante compleja, con sombras y puntos destacados que producen lecturas de lux diferentes en distintas partes de la escena.

Por ello es importante tener presente que una lectura de lux no indica la condición de iluminación de una escena en su conjunto. Muchos fabricantes especifican el nivel mínimo de iluminación necesario para que una cámara produzca una imagen aceptable.

Aunque estas especificaciones son útiles a la hora de realizar comparaciones de sensibilidad lumínica para cámaras del mismo fabricante, es posible que no sea tan útil utilizar dichas cifras para comparar cámaras de fabricantes diferentes.

Esto se debe a que cada fabricante utiliza un método diferente y tiene un criterio distinto sobre lo que es una imagen aceptable. Para poder comparar adecuadamente el rendimiento de dos cámaras diferentes en condiciones de poca luz, las cámaras deben situarse una al lado de la otra y visualizar un objeto en movimiento con poca luz [7].

Tabla 5 — Iluminancia.

Iluminancia	Condición de Iluminación
100000 lux	Luz solar intensa
10000 lux	Luz del día
500 lux	Luz en oficina
100 lux	Habitación con poca luz

2.2.8.2 Elementos del Objeto

Un objetivo o conjunto de objetivos de una cámara, realiza varias funciones. Algunas son:

- Definir el campo de visión, es decir, definir la parte de una escena y el nivel de detalle que se capturará.
- Controlar la cantidad de luz que atraviesa el sensor de imagen, para que una imagen quede expuesta correctamente.
- Enfocar ajustando los elementos internos del conjunto de objetivos o la distancia entre el conjunto de objetivos y el sensor de imagen.

2.2.8.2.1 Campo de Visión

Área de cobertura y el grado de detalle que se visualizará. El campo de visión viene determinado por la longitud focal del objetivo y el tamaño del sensor de imagen, ambos se especifican en una hoja de datos de la cámara. La longitud focal del objetivo, se define como la distancia entre el objetivo de entrada (o un punto específico en un conjunto de objetivo complejo) y el punto en el que convergen todos los rayos de luz hacia un punto (normalmente el sensor de imagen de la cámara). Cuanto mayor es la longitud focal, más estrecho es el campo de visión [7].

2.2.8.2.2 Número F y Exposición

En situaciones con poca luz, especialmente en entornos interiores, un factor importante que hay que tener en cuenta para una cámara es la capacidad para recoger la luz. Ésta se puede determinar por el número F del objetivo, también conocido como F-stop. Un número F, define la cantidad de luz que puede atravesar un objetivo.

Un número F, es la relación entre la longitud focal del objetivo y el diámetro de la apertura o diámetro del iris, es decir, número F = longitud focal/apertura. Cuanto menor sea el número F (longitud focal corta relativa a la apertura o apertura grande relativa a la longitud focal), mejor será la capacidad de recogida de luz del objetivo, es decir, podrá pasar más luz por el objetivo hasta el sensor de imagen. En situaciones de poca luz, un número F menor producirá por lo general una mejor calidad de imagen. No obstante, pueden haber algunos sensores que tal vez no puedan aprovechar un número F menor en situaciones de poca luz debido a la forma en que están diseñados. Normalmente, un objetivo con un número F más bajo es más caro que un objetivo con un número F alto [7].

2.2.8.3 Sensores de Imagen

A medida que la luz atraviesa un objetivo, ésta se enfoca en el sensor de imagen de la cámara. Un sensor de imagen está compuesto de muchos fotositos y cada fotosito corresponde a un elemento de la imagen, comúnmente conocido como "píxel", en un sensor de imagen.

Cada píxel de un sensor de imagen registra la cantidad de luz a la que se expone y la convierte en un número de electrones correspondiente. Cuanto más brillante es la luz, más electrones se generan [7]. Existen dos tecnologías principales que pueden utilizarse para el sensor de imagen:

- **CCD** (dispositivo de acoplamiento de carga): Los sensores CCD llevan utilizándose en las cámaras desde hace más de 30 años y presentan muchas cualidades ventajosas. Por regla general, siguen ofreciendo una sensibilidad lumínica ligeramente superior y producen menos ruido que los sensores CMOS. Esta mayor sensibilidad lumínica se traduce en mejores imágenes en condiciones de poca luz. Sin embargo, los sensores CCD son más caros y más complejos de incorporar a una cámara. Un sensor CCD también puede consumir hasta 100 veces más energía que un sensor CMOS equivalente

- **CMOS** (semiconductor de óxido metálico complementario). Los recientes avances en los sensores CMOS los están acercando a sus homólogos CCD en términos de calidad de la imagen. Los sensores CMOS reducen el coste total de las cámaras, ya que contienen todas las funciones lógicas necesarias para fabricar cámaras para ellos. En comparación con los sensores CCD, los sensores CMOS permiten mayores posibilidades de integración y más funciones. Los sensores CMOS también tienen un tiempo menor de lectura (lo que resulta una ventaja cuando se requieren imágenes de alta resolución), una disipación de energía menor a nivel del chip, así como un tamaño menor del sistema.

Para finalizar, en el desarrollo de un sistema de Tele Vigilancia, es necesario seleccionar la cámara de acuerdo, a las necesidades y lugares a los que se desea observar, por ello, se muestran a continuación, un detalle técnico de las consideraciones al momento de seleccionar alguna de ellas, centrándose en las cámaras de red, por su versatilidad y manejo para sus diferentes usos en la red como es Internet [53].

Tabla 6 –Aspectos Técnicos Cámaras Red.

Ítem	Característica Técnica
Sensor de Imagen	• CMOS • CMD • Barrido progresivo de 1/3" a ¼" • 1.3 a 3 megapíxel
Objetivo	• De 2.7 a 119 mm / F de 1.0 a 2.0 • Iris fijo o DC • Iris automático • Enfoque automático • Auto foco • Zoom óptico hasta 35x • Zoom digital hasta 12x • Montura CS • Vari focal
Día/ Noche	• Automático • Configurable • Lámpara IR integrada
Sensibilidad Lumínica (Lux)	• De 0.005 a 10000 • B/N o color • LED encendido o apagado
Compresión de Video	• MPEG-4 • H.264
Resolución Máxima de video (Pixeles)	• 640 x 480 • 1280 x 1024 • 1600 x 900 • 1600 x 1200 • NTSC • PAL • 4CIF • HDTV 1080i 1929 x 1080 • HDTV 720p 1280 x 720
Imágenes por Segundo	12 a 60 (640 x 480 a 1600 x 1200)
Soporte de audio	• Monodireccional • Bidireccional • Micrófono integrado • Altavoz integrado
Pan/Tilt/Zoom	• Posiciones predefinidas hasta 100 • 360° Pan • 180° Tilt • Guard tour • Auto slip •
Entradas / Salidas	1 o varias
Video Inteligente	• Detección de movimiento • Detección de audio • Alarma antimanipulación • Gate Keeper

Seguridad	• Auto tracking • Contraseña multinivel • Filtro de direcciones ip • Cifrado HTTPS
Red	• IPv4 • IPv6 • Q&S
POOE	• Disponible clase 1 a 3 • C/S calentador
Conectores serie	• Rs-232 • Rs-485 • Rs-422 • Rs-485
Otros	• IEEE inalámbrica 802.11 b/g • Ranuras tarjetas sd/sdhc • Salida de video analógico • Uso interior exterior • Certificación IP66 • Movimiento continuo 24/7 • Auto slip • E slip • Amplio rango dinámico • Estabilizador de imagen

2.2.8.4 Medio de Comunicación

El medio de transmisión físico para una red por cable implica cables, principalmente de par trenzado, o bien, fibra óptica. Un cable de par trenzado consiste en ocho cables que forman cuatro pares de cables de cobre trenzados, y se utiliza con conectores RJ-45 y sockets. La longitud máxima de un cable de par trenzado es de 100 m, mientras que para la fibra, el máximo varía entre 10 km y 70 km, dependiendo del tipo. En función del tipo de cables de par trenzado o de fibra óptica que se utilicen, actualmente las velocidades de datos pueden oscilar entre 100 Mbit/s y 10.000 Mbit/s.

2.2.8.5 Alimentación por Ethernet

La Alimentación a través de Ethernet (PoE) permite proveer de energía a los dispositivos conectados a una red Ethernet usando el mismo cable que para la comunicación de datos. Su uso es frecuente en teléfonos IP, puntos de acceso inalámbricos y cámaras de red conectadas a una LAN. La principal ventaja de PoE es el ahorro de costos que conlleva. No es necesario contratar a un electricista ni instalar una línea de alimentación separada. Esto supone una ventaja, sobre todo en zonas de difícil acceso. El hecho de que no sea necesario instalar otro cable de alimentación puede suponer un ahorro, dependiendo de la ubicación de la cámara. PoE también facilita el hecho de cambiar la ubicación de la cámara o añadir otras cámaras al sistema de Tele Vigilancia. Además, aumenta la seguridad del sistema de video. Un sistema de Tele Vigilancia con PoE se puede alimentar desde una sala de servidores los cuales están protegidos en la mayoría de los casos UPS. Esto significa que el sistema de Tele Vigilancia puede funcionar incluso durante un corte eléctrico. Por las ventajas que tiene PoE, se recomienda usarla en tantos dispositivos como sea posible. La energía de un switch o midspan

con PoE debería ser suficiente para los dispositivos conectados, y éstos deberían admitir la potencia necesaria.

2.2.8.6 Norma 802.3af

Hoy en día, la mayoría de dispositivos PoE cumplen con la norma IEEE 802.3af, que se publicó en 2003. Esta norma utiliza cables estándares Cat-5 o superiores y asegura que la transferencia de datos no se vea afectada. En dicha norma, al dispositivo que proporciona la energía se le llama equipo de suministro eléctrico (PSE). Éste puede ser un conmutador u otro dispositivo habilitado para PoE.

El dispositivo que recibe la energía se conoce como dispositivo alimentado (PD). Esta función normalmente está integrada en un dispositivo de red, como una cámara, o en otro dispositivo independiente.

La norma incluye un método para identificar automáticamente si un dispositivo es compatible con PoE, y sólo se le proporciona energía una vez que se ha confirmado dicha compatibilidad. Esto también implica que el cable Ethernet conectado a un conmutador PoE no proporcionará energía alguna si no está conectado a un dispositivo habilitado para PoE, lo cual elimina el riesgo de una descarga eléctrica al instalar una red o renovar la instalación. En un cable de par trenzado hay cuatro pares de cables trenzados. PoE puede utilizar dos pares de cables "de recambio" o bien superponer el actual a los pares de cables usados para la transmisión de datos. Los switch con PoE integrada a menudo proporcionan la electricidad por medio de los dos pares de cables utilizados para la transmisión de datos.

A continuación la siguiente tabla muestra la clasificación de potencia según IEEE 802.3af.

Tabla 7– Clasificación de Potencia.

Clase	Nivel de potencia mínimo en PSE	Nivel de potencia máximo de un PD	Uso
0	15.4 W	0.44 w- 12.95 w	Predeterminado
1	4.0 W	0.44 w -3.84 w	opcional
2	7.0 W	3.84 w – 6.49 w	opcional
3	15.4 W	6.49 w - 12.95 w	opcional
4	15.4 W	----------	reservado

2.2.8.7 Ancho de Banda y Almacenamiento

Los requerimientos de ancho de banda y almacenamiento del contenido multimedia son aspectos importantes en un sistema de Tele Vigilancia. Entre los factores que se incluyen el número de cámaras, la resolución de imagen utilizada el tipo y relación de compresión, frecuencias de imagen y complejidad escenas.

Esto depende de los siguientes factores:

- Numero de cámaras: menos de 5
- Tipo de grabación: continua
- Tiempo de grabación: 24/7.
- Compresión: h.264
- Resolución: 1.3 megapíxeles.

2.2.8.8 Requisito de Ancho de Banda

En este tipo de sistema con menos de 5 cámaras, se puede utilizar un switch básico con 100 megabits (Mbits) sin tener que considerar limitaciones de ancho de banda, sin embargo dejar por lo menos un 40% del ancho de banda dedicado seria considerable para este sistema. Por ello los dispositivos deben soportar Q&S, con DSCP, tanto switch, routers y cámaras de video.

2.2.8.9 Cálculo de Almacenamiento

Como se ha mencionado anteriormente, el tipo de compresión de video utilizado es uno de los factores que afectan a los requerimientos de almacenamiento. El formato de compresión H.264 es lejos la técnica de compresión de video más eficiente que existe actualmente. Sin asegurar calidad de imagen, un codificador H.264 puede reducir el tamaño de un archivo de video digital en más de un 80% comparado con el formato MPEG-4 y en más de un 50% con el estándar MPEG-4 (Parte 2). Esto significa que se necesita mucho menos ancho de banda y espacio de almacenamiento para un archivo de video H.264. A causa de diversas variables que afectan a los niveles de frecuencia de bits, los cálculos no son tan triviales ni claros para los formatos H.264. Cálculo en H.264:

Velocidad binaria aprox./8 (bits en un byte) x 3.600s = KB por hora/1.000 = MB por hora

MB por hora x horas de funcionamiento diarias/1.000 = GB por día

GB por día x periodo de almacenamiento solicitado = Necesidades de almacenamiento

A continuación la siguiente tabla muestra el cálculo para este diseño.

Tabla 8– Cálculo de Almacenamiento.

N° cámaras	Resolución	Velocidad Binaria (Kbps)	Imágenes por segundo	Mb/ hora	Hora de funcionamiento	Gb/día
5	CIF	110	5	49,5	24	1.19

Capacidad total de 5 cámaras por 30 días = 35.64 GB mensual app.

2.2.9 Ventajas frente a las Cámaras Análogas o Convencionales

A continuación, se dan algunos de los motivos, de las ventajas en la utilización de cámaras de red, para sistemas de Tele Vigilancia.

- Acceso remoto a video en directo y grabado en cualquier momento, desde cualquier lugar y cualquier computador autorizado.
- Imágenes de calidad digital para lograr una visualización perfecta.
- Imágenes nítidas de objetos y personas en movimiento gracias al barrido progresivo.
- Escalables y preparadas para el futuro, basadas en estándares IP abiertos.
- Integración sencilla con otros sistemas, como por ejemplo, el control de acceso.
- Gestión centralizada eficaz y reducción de los costos de mantenimiento.
- Escalables, flexibles y bajo costo.

3 Aspectos de Seguridad

3.1 Introducción

Para cualquier sistema seguro, es necesario considerar cuatro criterios importantes y relevantes a la hora de aplicar y utilizar técnicas de seguridad, los cuales son los siguientes:

- **Confidencialidad o Privacidad:** Los datos que son transmitidos a través del sistema, deben estar disponibles solo para las personas autorizadas.
- **Confiabilidad o integridad:** Los datos transferidos no se deben poder cambiar entre el remitente y el receptor.
- **Disponibilidad:** Los datos transferidos deben estar disponibles cuando son necesarios.
- **No Repudio:** Para evitar que una vez firmado un documento el emisor se retracte o niegue haberlo redactado.

Estos cuatro aspectos son relevantes a la hora de decidir los mecanismos o técnicas a utilizar en un sistema u otro. Por ello que se utilizan diversos protocolos para proporcionar las numerosas ventajas respecto a la seguridad de un sistema a través de Internet. Para enviar datos entre un dispositivo conectado por ejemplo a una red de área local a otro conectado a otra LAN se requiere una vía de comunicación estándar, ya que es posible que las redes de área local utilicen distintos tipos de tecnologías. Esta necesidad lleva al desarrollo de un sistema de direcciones IP y protocolos basados en IP para comunicarse a través de Internet, que conforma un sistema global de redes interconectadas. Las LAN también pueden utilizar direcciones y protocolos IP para comunicarse dentro de una red de área local, aunque el uso de las direcciones MAC es suficiente para la comunicación interna.

En los siguientes capítulos se abordarán los aspectos de seguridad y comunicación más relevantes y necesarias en la transmisión de video para un Sistema de Tele Vigilancia.

3.2 Direcciones IP

Cualquier dispositivo que quiera comunicarse con otros dispositivos a través de Internet debe tener una dirección IP única y adecuada. Las direcciones IP sirven para identificar a los dispositivos emisores y receptores. Actualmente existen dos versiones IP: IP versión 4 (IPV4) e IP versión 6 (IPV6). La principal diferencia entre ellas es que una dirección IPV6 tiene una longitud mayor (128 bits, en comparación con los 32 bits de una dirección IPV4). Hoy en día, las direcciones IPV4 son las más comunes.

3.2.1 Direcciones IPV4

Las direcciones IPV4 se agrupan en cuatro bloques, cada uno se separa con un punto. Cada bloque representa un número entre 0 y 255, por ejemplo: 192.168.12.23. Algunos bloques de direcciones IPV4 se han reservado exclusivamente para uso privado. Estas direcciones IP privadas son 10.0.0.0 hasta 10.255.255.255, 172.16.0.0 hasta 172.31.255.255 y 192.168.0.0 hasta 192.168.255.255. Este tipo de direcciones sólo se pueden utilizar en redes privadas y no está permitido reenviarlas a Internet a través de un enrutador.

Todos los dispositivos que quieran comunicarse a través de Internet deben tener su propia dirección IP pública. Una dirección IP pública es una dirección asignada por un proveedor de servicios de Internet. Un ISP (Proveedor de Servicios de Internet) puede asignar direcciones IP dinámicas, que pueden cambiar durante una sesión, o direcciones estáticas, que normalmente implican un costo adicional [8].

3.2.2 Direcciones IPV6

Las direcciones IPV6 se escriben en notación hexadecimal y constan de ocho bloques de 16 bits cada uno, divididos por dos puntos. Por ejemplo, 2001:0da8:65b4:05d3:1315:7c1f: 0461:7847. Entre las principales ventajas de IPV6, además de disponer de una gran cantidad de direcciones IP, se incluye la posibilidad de habilitar un dispositivo para que configure automáticamente su dirección IP mediante la dirección MAC.

En la comunicación a través de Internet, el Host solicita y recibe del enrutador el prefijo necesario del bloque de la dirección pública, así como información adicional. Se utilizan el prefijo y el sufijo del Host, de modo que con IPV6 ya no es necesario el protocolo DHCP para la asignación de direcciones IP ni la definición manual de las mismas. También deja de ser necesario el reenvío de puertos. Otras ventajas de IPV6 son la renumeración para simplificar el cambio de redes corporativas entre proveedores, un enrutamiento más rápido, el cifrado punto a punto según IPSec y la conectividad mediante la misma dirección al cambiar de red (Mobile IPV6) [9].

3.3 Puertos

Un número de puerto define un servicio o aplicación concretos para que el servidor receptor (por ejemplo una cámara IP) sepa cómo procesar los datos entrantes. Cuando un computador envía datos vinculados a una aplicación concreta, normalmente añade el número de puerto a una dirección IP sin que el usuario lo sepa. Los números de puerto pueden ir del 0 al 65535. Algunas aplicaciones utilizan los números de puerto que les ha preasignado. Por ejemplo, un servicio Web vía http se suele asignar al puerto 80 de una cámara IP [10].

3.4 Protocolo de Transporte de Datos

El Protocolo de control de transmisión (TCP, Transmission Control Protocol) y el Protocolo de datagramas de usuario (UDP, User Datagram Protocol) son los protocolos basados en IP que se utilizan para enviar datos. Estos protocolos de transporte actúan como portadores para muchos otros protocolos. Por ejemplo, HTTP (Hyper Text Transfer Protocol), que se utiliza para visualizar páginas Web en servidores de todo el mundo a través de Internet, se realiza en TCP. TCP proporciona un canal de transmisión fiable basado en la conexión. Gestiona el proceso de división de grandes bloques de datos en paquetes más pequeños y garantiza que los datos enviados desde un extremo se reciban en el otro.

La fiabilidad de TCP en la retransmisión puede producir retrasos significativos, por lo que en general se utiliza cuando la fiabilidad de la comunicación prevalece sobre la latencia del transporte. UDP es un protocolo sin conexión que no garantiza la entrega de los datos enviados, dejando así todo el mecanismo de control y comprobación de errores a cargo de la propia aplicación. No proporciona transmisiones de pérdida de datos, por lo que no provoca retrasos adicionales.

En el siguiente esquema se presentan protocolos y puertos utilizados para la transmisión de video a través de la red.

Tabla 9 — Protocolos de Transporte de Datos.

Protocolo	Protocolo de Transporte	Puerto	Uso Típico	Uso en video a través de una red
FTP	TCP	21	Transferencia de archivos a través de Internet/Intranets.	Transferencia de imágenes o video desde una cámara a un servidor o una aplicación.
SMTP	TCP	25	Envío de mensajes de correo electrónico.	Una cámara puede enviar imágenes o notificaciones de alarma utilizando su cliente de correo electrónico integrado.
HTTP	TCP	80	Se utiliza para navegar por la red, por ejemplo, para recuperar páginas Web de servidores.	Es el modo más habitual para transferir video de una cámara, en el que el dispositivo de video en red funciona como servidor Web que pone el video a disposición de un usuario o de un servidor de aplicaciones que lo solicite.
HTTPS	TCP	443	Acceso seguro a páginas Web con tecnología de cifrado.	Transmisión segura de video procedente de una cámara.
RTP (Real Time Protocol)	UDP/TCP	No definido	Formato de paquete RTP estandarizado para la entrega de audio y de video a través de Internet (A menudo utilizado en sistema de transmisión multimedia o videoconferencia).	Modo habitual de transmisión de video en red basado en H.264/MPEG y de sincronizar video y audio, ya que RTP proporciona la numeración y la datación secuencial de paquetes de datos, lo que permite volver a unirlos en el orden correcto. La Transmisión se puede realizar mediante unidifusión o multidifusión.
RTSP (Protocolo de transmisión en tiempo real)	TCP	554	Utilizado para configurar y controlar sesiones multimedia a través de RTP.	Utilizado para configurar y controlar sesiones multimedia a través de RTP

3.4.1 RTP

RTP (Real Time Protocol) define un formato estándar para la entrega de paquetes de audio y video a través de Internet. Es utilizado ampliamente en sistemas de comunicación y de entretenimiento que implican transmisión de medios, tales como telefonía, aplicaciones de videoconferencia basada en Web, entre otras.

Está diseñado para la transferencia de extremo a extremo de datos multimedia en tiempo real. El protocolo proporciona las facilidades para la compensación y la detección de la secuencia de la llegada de los datos, que son comunes durante las transmisiones en una red IP. RTP soporta transferencia de datos a múltiples destinos a través de multicast. RTP es considerado como el principal estándar para el transporte de audio/video en redes IP [11].

3.4.2 RTSP

El protocolo de flujo de datos en tiempo real (Real Time Streaming Protocol) establece y controla uno o muchos flujos sincronizados de datos, ya sean de audio o de video. El RTSP actúa como un mando a distancia mediante la red para servidores multimedia.

RTSP es un protocolo no orientado a conexión, en lugar de esto el servidor mantiene una sesión asociada a un identificador, en la mayoría de los casos RTSP usa TCP para datos de control del reproductor y UDP para los datos de audio y vídeo aunque también puede usar TCP en caso de que sea necesario. En el transcurso de una sesión RTSP, un usuario puede abrir y cerrar varías conexiones de transporte hacia el servidor por tal de satisfacer las necesidades del protocolo. Además es utilizado para controlar dispositivos de grabación y reproducción como cámaras de video IP RTSP [12].

De forma intencionada, el protocolo es similar en sintaxis y operación a HTTP de forma que los mecanismos de expansión añadidos a HTTP pueden, en muchos casos, añadirse a RTSP. Sin embargo, RTSP difiere de HTTP en un número significativo de aspectos:

- RTSP introduce nuevos métodos y tiene un identificador de protocolo diferente.
- Un servidor RTSP necesita mantener el estado de la conexión al contrario de HTTP
- Tanto el servidor como el usuario pueden lanzar peticiones.
- Los datos son transportados por un protocolo diferente.

El protocolo soporta las siguientes operaciones:

- **Recuperar contenidos multimedia del servidor.** El usuario puede solicitar la descripción de una presentación por HTTP o cualquier otro método. Si la presentación es multicast, la descripción contiene los puertos y las direcciones que serán usados. Si la presentación es unicast el usuario es el que proporciona el destino por motivos de seguridad.

- **Invitación de un servidor multimedia a una conferencia.** Un servidor puede ser invitado a unirse a una conferencia existente en lugar de reproducir la presentación o grabar todo o una parte del contenido. Este modo es útil para aplicaciones de enseñanza distribuida dónde diferentes partes de la conferencia van tomando parte en la discusión.

• **Adición multimedia a una presentación existente.** Particularmente para presentaciones en vivo, útil si el servidor puede avisar al usuario sobre los nuevos contenidos disponibles.

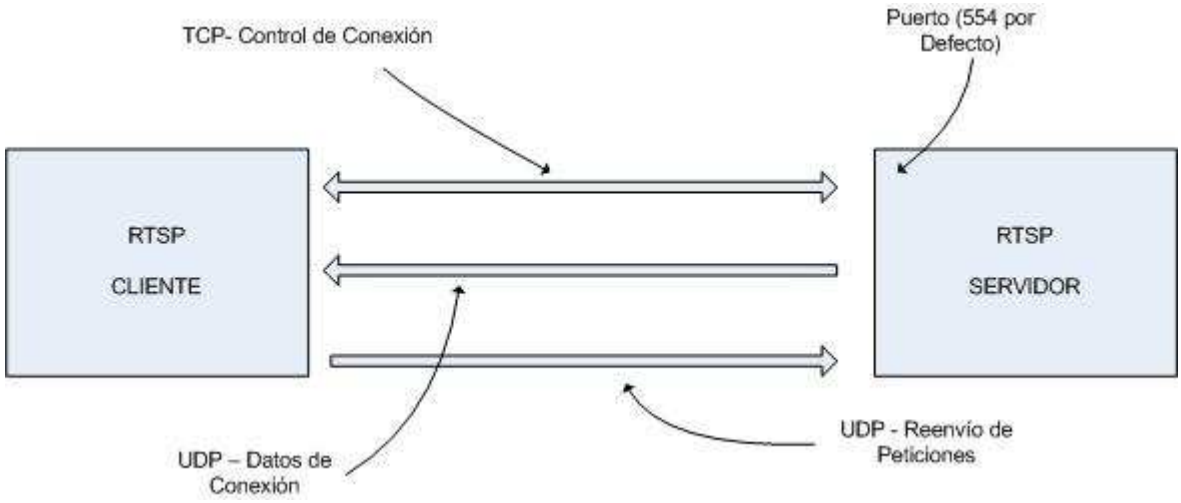

Figura 7 – Representación RTSP.

3.4.3 RTMP

Real Time Messaging Protocol (RTMO) es un protocolo desarrollado por Adobe Systems para Streaming de audio, video y datos a través de Internet, entre un reproductor Flash y un servidor [13]. Si bien la principal motivación de RTMP es dar funcionalidades a Flash, se utiliza también en otras aplicaciones como Adobe LiveCycle Data Services ES.

Este protocolo tiene tres variantes:

- Funciona a través de TCP y utiliza un puerto específico 1935.
- Está encapsulado dentro de peticiones HTTP frente a los cortafuegos transversales.
- RTMPS funciona como RTMP, pero sobre una conexión HTTPS segura.

3.4.4 RTCP

Es un protocolo de comunicación, que proporciona información de control, que está asociado con un flujo de datos para una aplicación multimedia (flujo RTP). Trabaja junto con RTP en el transporte y empaquetado de datos multimedia, pero no transporta ningún dato por sí mismo. Se usa habitualmente para transmitir paquetes de control a los participantes de una sesión multimedia de Streaming. La función principal de RTCP es informar de la calidad de servicio proporcionada por RTP.

Este protocolo recoge estadísticas de la conexión y también información como por ejemplo bytes enviados, paquetes enviados, paquetes perdidos o jitter, entre otros. Una aplicación puede usar esta información para incrementar la calidad de servicio (QoS), ya sea limitando el flujo o usando un códec de compresión más bajo. En resumen, RTCP se usa para informar de la QoS (Quality of Service). RTCP por sí mismo no ofrece ninguna clase de cifrado de flujo o de autenticación. Para tales propósitos se puede usar SRTCP [14].

3.4.5 SRTCP

El Secure Real-time Transport Protocol (SRTP) define un perfil de RTP (Real-time Transport Protocol), con la intención de proporcionar cifrado, autenticación del mensaje e integridad, y protección contra reenvíos a los datos RTP en aplicaciones unicast y multicast.

Dado que RTP está muy relacionado con RTCP (RTP Control Protocol), que puede ser usado para controlar una sesión RTP, SRTP también tiene un protocolo homologo llamado Secure RTCP (o SRTCP). SRTCP proporciona las mismas características relacionadas con la seguridad a RTCP, al igual que hace SRTP con RTP [15].

El empleo de SRTP o SRTCP es opcional al empleo de RTP o RTCP, pero incluso utilizando SRTP/SRTCP, todas las características que estos protocolos proporcionan (tales como cifrado y autenticación) son opcionales y pueden ser habilitadas o deshabilitadas por separado. La única excepción a esto último es la autenticación de los mensajes, que es obligatoria cuando se está usando SRTCP.

3.4.6 SIP

Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones) es un protocolo desarrollado con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como video, voz, mensajería instantánea, juegos online y realidad virtual.

La sintaxis de sus operaciones se asemeja a las de HTTP y SMTP, los protocolos utilizados en los servicios de páginas Web y de distribución de e-mails respectivamente. Esta similitud es natural, ya que SIP fue diseñado para que la telefonía se vuelva un servicio más en la Internet [16].

3.5 VLAN

Al diseñar un sistema de Tele Vigilancia, existe la intención de mantener la red sin contacto con otras redes por motivos tanto de seguridad como de rendimiento. Por lo que, la elección obvia sería construir una red independiente. Aunque esto simplificaría el diseño, los costos, instalación y mantenimiento probablemente serían más elevados que si se utilizara otra tecnología como una red virtual de área local (VLAN).

VLAN es una tecnología que segmenta las redes de forma virtual, una funcionalidad que admiten la mayoría de switch. Esto se consigue dividiendo los usuarios de la red en grupos lógicos. Sólo los usuarios de un grupo específico pueden intercambiar datos o acceder a determinados recursos en la red. Si un sistema de Tele Vigilancia se segmenta en una VLAN, sólo los servidores ubicados en dicha LAN podrán acceder a las cámaras de red.

Normalmente, las VLAN conforman una solución mejor y más económica que una red independiente. El protocolo que se utiliza principalmente al configurar VLAN es IEEE 802.1Q, que etiqueta cada marco o paquete con bytes adicionales para indicar a qué red virtual pertenece [17].

3.6 Calidad de Servicio

Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y Tele Vigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red, para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores o router y los conmutadores o switch de red, funcionen de maneras distintas para cada tipo de servicio (voz, datos y vídeo) del tráfico de la red. Al utilizar la Calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red, sin consumir cada una el ancho de banda de las otras.

El término Calidad de servicio hace referencia a una cantidad de tecnologías, como DSCP (Differentiated Service Codepoint), que pueden identificar el tipo de datos que contiene un paquete y dividir los paquetes en clases de tráfico para priorizar su reenvío. Las ventajas principales de una red sensible a la QoS, son la priorización del tráfico, para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación y, por lo tanto, la competencia entre aplicaciones en el uso del ancho de banda.

Ejemplo “Red ordinaria (sin QoS)”. En este ejemplo, PC1 está reproduciendo dos secuencias de vídeo de las cámaras 1 y 2. Cada cámara transmite a 2,5 Mbit/s. En algún instante, PC2 inicia una transferencia de archivos desde PC3. En este escenario, la transferencia de archivos intentará utilizar la capacidad total de 10 Mbit/s entre los enrutadores 1 y 2, mientras que las secuencias de vídeo intentarán mantener su total de 5 Mbit/s. Así, ya no se puede garantizar la cantidad de ancho de banda destinada al sistema de Tele Vigilancia y probablemente se reducirá la frecuencia de imagen de vídeo. En el peor de los casos, el tráfico del FTP consumirá todo el ancho de banda disponible.

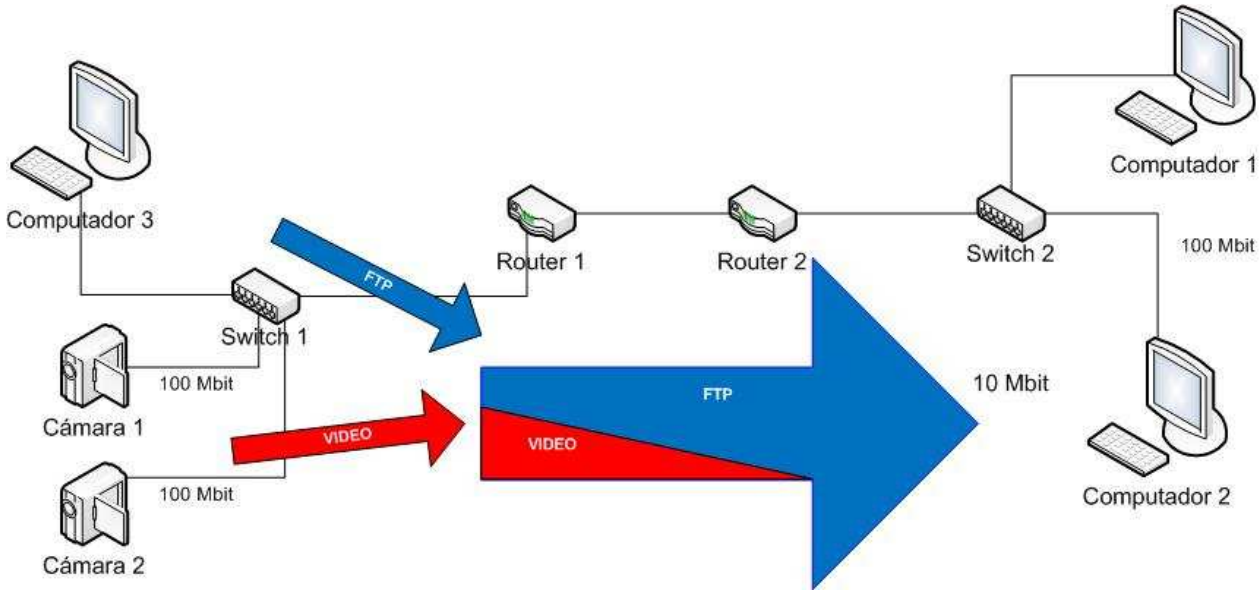

Figura 8 – Red Ordinaria.

Ejemplo "Red con QoS". En este escenario, se ha configurado el enrutador o router 1 para dedicar hasta 5 Mbit/s de los 10 disponibles a la transmisión de vídeo. El tráfico del FTP puede utilizar un máximo de 2 Mbit/s, y HTTP, junto con el resto del tráfico, pueden utilizar un máximo de 3Mbit/s. Con esta división, las transmisiones de vídeo siempre tendrán disponible el ancho de banda que necesitan. Las transferencias de archivos se consideran menos importantes y, por lo tanto, obtienen menor ancho de banda; sin embargo, aún quedará ancho de banda disponible para la navegación Web y el resto del tráfico. Hay que tener en cuenta que estos valores máximos sólo se aplican en caso de congestión en la red. El ancho de banda disponible que no se use se podrá utilizar por cualquier tipo de tráfico.

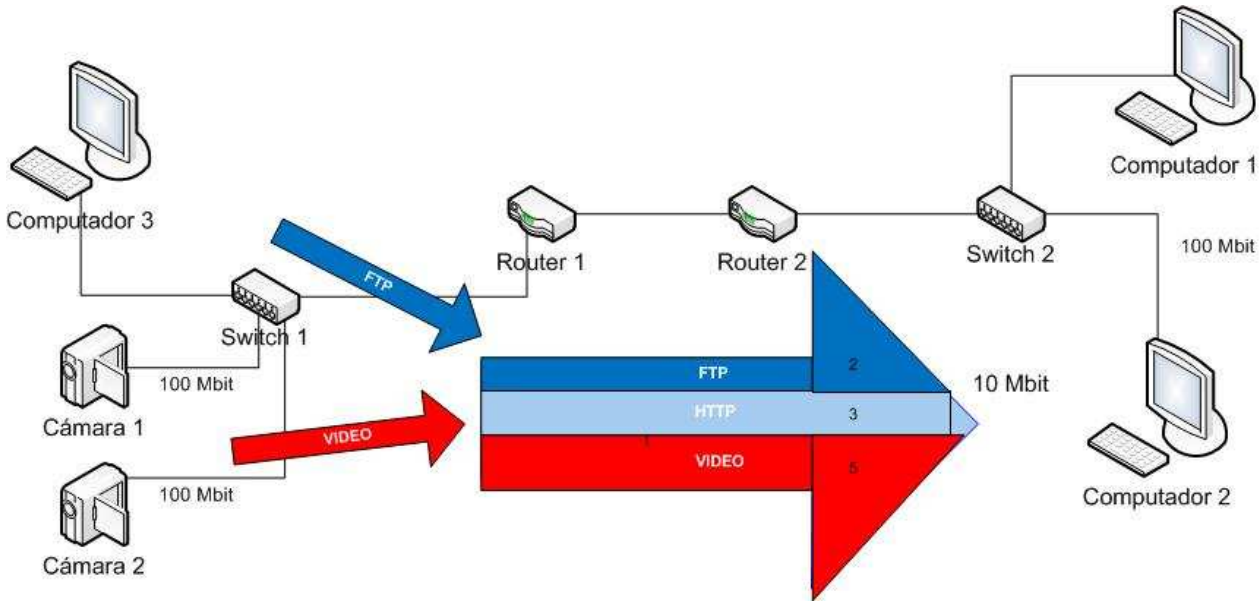

Figura 9 – Red con QoS.

Además se deben tener en cuenta distintos aspectos que pueden afectar directamente QoS, entre los que se encuentran:

- Ancho de banda.
- Latencia.
- Jitter.
- Tiempo de procesamiento utilizando medidas de seguridad.
- Arquitecturas de red.
- Entre otros.

3.7 Seguridad de Video en la Red

Existen varios niveles de seguridad, para proteger la información que se envía a través de las redes IP. El primer nivel es la autenticación y la autorización. El usuario o dispositivo se identifica en la red y en el extremo remoto con un nombre de usuario y una contraseña, que se verifican antes de permitir que el dispositivo entre en el sistema.

Se puede conseguir seguridad adicional cifrando los datos para evitar que otros usuarios los utilicen o los lean. Los métodos más habituales son HTTPS (también conocido como SSL/TLS), VPN y WEP o WPA en redes inalámbricas. El uso del cifrado puede disminuir la velocidad de las comunicaciones en función del tipo de implementación y cifrado utilizados.

3.7.1 Filtro de Direcciones IP

Concede o deniega los derechos de acceso a las direcciones definidas previamente. Una de las configuraciones habituales de las cámaras de red es la de permitir que únicamente la dirección IP del servidor que hospeda el software de gestión de video pueda acceder a los productos de video en la red.

3.7.2 IEEE 802.1X

El estándar IEEE 802.1X establece una conexión punto a punto o impide el acceso desde el puerto de la LAN si la autenticación es errónea. También evita el denominado "porthi-jacking", es decir, el acceso de un equipo no autorizado a una red mediante una toma de red del interior o del exterior de un edificio.

IEEE 802.1X resulta útil en aplicaciones de vídeo en red, ya que a menudo las cámaras de red están colocadas en espacios públicos en los que una toma de red accesible puede suponer un riesgo para la seguridad [18]. En las redes de las empresas de hoy en día, el estándar IEEE 802.1X se está convirtiendo en un requisito básico para establecer cualquier conexión a una red.

En un sistema de vídeo en red, IEEE 802.1X funciona como se indica a continuación:

- Una cámara de red envía una solicitud de acceso a la red, a un conmutador o punto de acceso.

- El conmutador o punto de acceso reenvía la consulta a un servidor de autenticación, por ejemplo, un servidor RADIUS (Remote Authentication Dial-In User Service) como Microsoft Internet Authentication Service.
- Si la autenticación se realiza correctamente, el servidor indica al conmutador o punto de acceso que abra el puerto para permitir el paso de los datos procedentes de la cámara por el conmutador y así enviarlos a través de la red.

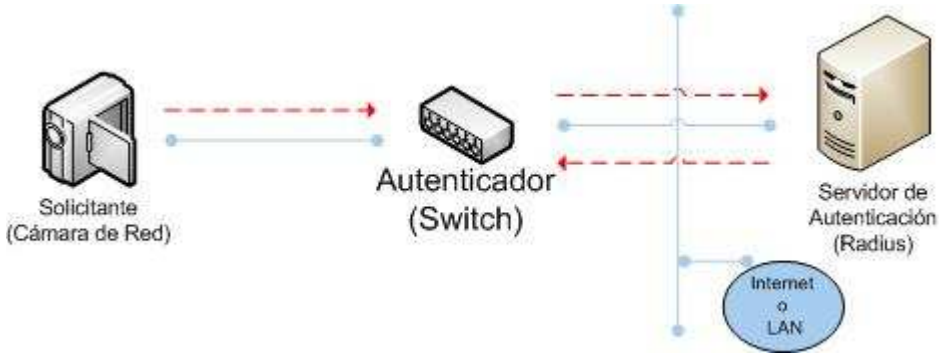

Figura 10 – Sistema de video con IEEE 802.1x.

3.7.3 HTTPS O SSL/TLS

El protocolo HTTPS (Hyper Text Transfer Protocol Secure) es idéntico a HTTP excepto en una diferencia clave, los datos transferidos se cifran con Capa de sockets seguros (SSL) o Seguridad de la capa de transporte (TLS). Este método de seguridad aplica el cifrado a los propios datos, lo que permite la visualización segura de vídeo en un navegador Web. Sin embargo, el uso de HTTPS puede ralentizar el enlace de comunicación y, en consecuencia, la frecuencia de imagen del vídeo [19].

3.7.4 VPN

Con una VPN se puede crear un "túnel" de comunicación seguro entre dos dispositivos y, por lo tanto, una comunicación segura a través de Internet. En esta configuración, se cifra el paquete original, incluidos los datos y su cabecera, que puede contener información como las direcciones de origen y destino, el tipo de información que se envía, el número de paquete en la secuencia y la longitud del paquete.

A continuación, el paquete cifrado se encapsula en otro paquete que sólo muestra las direcciones IP de los dos dispositivos de comunicación, es decir, los enrutadores o router. Esta configuración protege el tráfico y su contenido del acceso no autorizado, y sólo permite que trabajen dentro de la VPN, los dispositivos con la clave correcta. Los dispositivos de red entre un usuario y el servidor no podrán acceder a los datos ni visualizarlos [20].

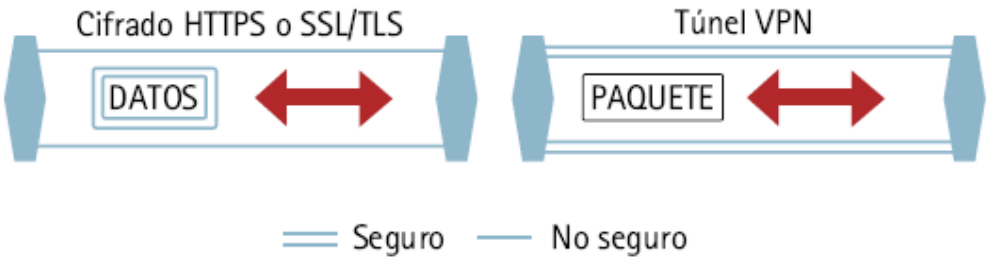

Figura 11 – Representación de HTTPS y VPN.

La diferencia entre HTTPS (SSL/TLS) y VPN es que en HTTPS sólo se cifran los datos reales de un paquete. Con VPN se puede cifrar y encapsular todo el paquete para crear un "túnel" seguro. Ambas tecnologías se pueden utilizar en paralelo, aunque no se recomienda, ya que cada tecnología añadirá una carga adicional que puede disminuir el rendimiento del sistema.

Para poder utilizar una VPN, es necesario comprender a través del modelo OSI el proceso de encriptación y desencriptación de la información, la cual se puede realizar en cualquier punto del flujo de información, sólo con la restricción de realizar los procesos referidos en las mismas capas equivalentes.

Por consiguiente, atendiendo al modelo OSI, se puede apreciar en el mismo dos grandes zonas: Hardware y Software. El término Hardware se refiere al sistema de interconexión física de los dos equipos (capa física), mientras que el término Software se aplica al resto de capas del modelo OSI. Dado que la encriptación y desencriptación se puede realizar en los puntos que se quiera, siempre y cuando sean capas equivalentes, se puede seleccionar estos dos puntos definidos, VPN por Hardware y VPN por Software.

Una VPN por Hardware:

- Depende de una tecnología externa y cerrada.
- El firmware de los sistemas es cerrado y depende del fabricante para poder cambiarlo.
- Los sistemas de encriptación suelen ser cerrados y el fabricante suele utilizar un único tipo.
- En la mayoría de las ocasiones los elementos hardware de los extremos que componen la red privada virtual, que deben ser iguales o por lo menos del mismo fabricante. No siendo posible que sean intercambiables por los de otros fabricantes.
- Sólo sirven para realizar conexiones VPN dentro de la misma red (intranet) o sólo fuera de la red, pero no pueden realizar simultáneamente las dos opciones, aunque esto es algo que pudiera cambiar en el futuro.
- La seguridad sólo se implementa desde los dos extremos de la VPN, siendo inseguro el camino que recorre la información desde el ordenador hasta el dispositivo VPN.

3.7.4.1 VPN por Software

Cada día se está imponiendo más la utilización de Redes Privadas Virtuales por software. La explicación radica en la necesidad que cada vez más tienen los medianos y pequeños usuarios, de implementar sistemas de seguridad en el acceso a sus máquinas. Como además son sistemas que tienden a crecer de forma rápida, es mucho mas barato la utilización de Redes Privadas Virtuales por software que por hardware.

Las ventajas que puede presentar este tipo de redes son:

- Existe una gran variedad de Redes Privadas Virtuales desarrolladas por software, donde elegir y que están continuamente mejorando sus prestaciones.
- El número de usuarios de este tipo de red es mucho mayor que el número de usuarios de VPNs realizadas por hardware, con lo que la posibilidad de encontrar documentación y ayuda para estos elementos es mayor.
- Pueden dar cobertura tanto a redes internas (intranet) como redes externas.
- La seguridad puede cubrir de máquina a máquina, donde se encuentren colocados los extremos de la VPN.

Las desventajas que puede presentar este tipo de redes son:

- Es necesario instalar el software en una máquina, pudiendo ser necesario, si la carga de información es muy grande, tener que dedicar una máquina para este trabajo.
- El sistema de claves y certificados están en máquinas potencialmente inseguras, que pueden ser atacadas.
- Si el software es de libre distribución, éste puede estar modificado y contener puertas traseras.

De todos los tipos disponibles, se puede citar por ser los más utilizados:

- IPSec
- PPTP
- L2TP
- VPNs SSL/TLS
- OpenVPN

3.7.4.1.1 IPSec

Es una extensión al protocolo IP. Añade los servicios de autenticación y cifrado. IPSec actúa dentro del modelo OSI en la capa 3 (capa de red). No está ligado a ningún algoritmo de encriptación o autenticación, tecnología de claves o algoritmos de seguridad específico. De hecho es un estándar que permite que cualquier algoritmo nuevo se pueda introducir. Por sus características es considerado como el protocolo estándar para la construcción de redes privadas virtuales.

IPSec cuenta con dos protocolos diferentes, de forma que se empleará uno u otro en función de lo que se interese proteger y el modo en que se realizen las comunicaciones.

- **Cabecera de Autenticación (Authentication Header, AH).** Se trata de una nueva cabecera que obtenemos de la básica IP y que se añade a los resúmenes criptográficos ("hash") de los datos e información de identificación.
- **Encapsulado de Seguridad (Encapsulating Security Payload, ESP).** Permite reescribir los datos en modo cifrado. No considera los campos de la cabecera IP por lo que sólo garantiza la integridad de los datos.

Ambos protocolos controlan el acceso y distribuyen las claves criptográficas. No pueden ser aplicados los dos a la vez. Lo que sí se permite es aplicarlos uno después de otro, es decir, a un datagrama IP aplicarle un protocolo y al paquete resultante aplicarle otro. Si se hace esto el orden de aplicación es: ESP-AH Cada uno de estos protocolos pueden funcionar en dos modos distintos:

- **Modo Transporte.**
- **Modo Túnel.**

El modo transporte es el que usa un anfitrión que genera los paquetes. En modo transporte, las cabeceras de seguridad se añaden antes que las cabeceras de la capa de transporte (TCP, UDP), antes de que la cabecera IP sea añadida al paquete.

El modo Túnel se usa cuando la cabecera IP extremo-a-extremo ya ha sido adjuntada al paquete, y uno de los extremos de la conexión segura es solamente una pasarela.

IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

3.7.4.1.2 PPTP

PPTP (Point to Point Tunneling Protocol) es un protocolo desarrollado por Microsoft. La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de VPN. La utilidad ASLEAP puede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN. Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo. El fallo de PPTP es causado por errores de diseño en la criptografía en los protocolos handshake o apretón de manos LEAP de Cisco y MSCHAP-v2 de Microsoft y por las limitaciones de la longitud de la clave en MPPE. La actualización de PPTP para las plataformas Microsoft viene por parte de L2TP o IPsec. Su adopción es lenta porque PPTP es fácil de configurar, mientras L2TP requiere certificados de clave pública, e IPsec es complejo y poco soportado por plataformas antiguas como Windows 98 y Windows Me.

3.7.4.1.3 L2TP

L2TP (Layer 2 Tunneling Protocol) fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.

Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.

L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.

A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

A causa de estos inconvenientes se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP.

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

3.7.4.1.4 VPNs SSL/TLS

SSL/TLS Secure Sockets Layer/Transport Layer Security existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" se aplica a ambos protocolos a menos que el contexto indique lo contrario. SSL proporciona autentificación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autentificado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autentificar. La autentificación mutua requiere un despliegue de infraestructura de claves públicas (PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente y mantener la integridad del mensaje.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Encriptación del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
- Con funciones hash: MD5 o de la familia SHA.

TLS/SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC).
- Protección contra varios ataques conocidos (incluidos ataques man in the middle attack), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.
- La función seudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.
- SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS.
- SSL también puede ser usado para hacer un túnel en una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

3.7.4.1.5 OpenVPN

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación, jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas entre otras. Está publicado bajo licencia de código-libre (Open Source).

Algunas de sus ventajas son :

- **Implementación de la VPN en la capa 2 y la capa 3 del modelo OS**I: OpenVPN ofrece dos modos básicos, que funcionamiento como la capa 2 o capa 3. Así los túneles de OpenVPN pueden también transportar tramas de Ethernet, los paquetes del IPX, y los paquetes del navegador de la red de Windows (NETBIOS), que son un problema en la mayoría de las otras soluciones de VPN.
- **Protección de sesión con el cortafuego interno**: Una sesión conectada con la o_cina central de su compañía con un túnel VPN puede cambiar el setup de su red en su ordenador portátil, para enviar todo su tráfico de la red a través del túnel. Una vez que OpenVPN haya establecido un túnel, el cortafuego central en la oficina central de la compañía puede proteger el ordenador portátil, aún cuando él no sea una máquina local. Solamente un puerto de la red se debe abrir en local para trabajar la sesión. El cortafuego central protege al empleado siempre que él o ella esté conectado a través del VPN.
- **Las conexiones de OpenVPN pueden ser establecidas a través de casi cualquier cortafuego**: Si tienes acceso a Internet y si puedes tener acceso a la Web, los túneles de OpenVPN deben de trabajar.
- **Soporte de Proxy y configuraciones**: OpenVPN tiene soporte de Proxy y se puede configurar para funcionar como un servicio de TCP o de UDP, y como servidor o cliente. Como servidor, OpenVPN espera simplemente hasta que un cliente solicita una conexión, mientras que como cliente, intenta establecer una conexión según su configuración.
- **Apertura de un solo puerto en el cortafuego para permitir conexiones entrantes:** Desde OpenVPN 2.0, el modo especial del servidor permite conexiones entrantes múltiples en el mismo puerto del TCP o del UDP, mientras que todavía usa diversas configuraciones para cada conexión.
- **Los interfaces virtuales permiten reglas muy específicas del establecimiento de una red y del cortafuego**: Todas las reglas, restricciones, mecanismos de la expedición, y conceptos como NAT se pueden utilizar con los túneles de OpenVPN.
- **Alta flexibilidad con posibilidades extensas de lenguaje interpretado (scripting)**: OpenVPN ofrece numerosos puntos durante la conexión para la ejecución de los scripts individuales. Estos script se pueden utilizar para una gran variedad de propósitos de la autentificación, recuperación en caso de fallos (failover) y más.

- **Soporte transparente y alto rendimiento para IPs dinámicas**: Si se usa OpenVPN, no hay necesidad de utilizar más IPs estáticas de cualquier lado del túnel. Ambas puntos finales del túnel pueden tener acceso barato de ADSL con el IPs dinámicas y los usuarios no notarán un cambio del IP de cualquier lado. Las sesiones del Terminal Server de Windows y las sesiones seguras de Shell (SSH) parecerán congeladas solamente por algunos segundos, pero no terminarán y continuarán con la acción solicitada después de una corta pausa.
- **Ningún problema con NAT:** El servidor y los clientes de OpenVPN pueden estar dentro de una red usando solamente direcciones privadas del IP. Cada cortafuego se puede utilizar para enviar el trá_co del túnel al otro punto final del túnel.
- **Instalación simple en cualquier plataforma:** La instalación y el uso son increíblemente simples. Especialmente, si ha intentado instalar IPsec con diversas con_guraciones, se apreciará la facilidad de instalación de OpenVPN.
- **Diseño modular:** El diseño modular con un alto grado de simplicidad en seguridad y establecimiento de una red es excepcional. Ninguna otra solución de VPN puede ofrecer la misma gama de posibilidades a este nivel de seguridad.

Además con la versión 2.0 se incorporó las siguientes mejoras:

- **Soporte Multi-cliente**: OpenVPN ofrece un modo de conexión especial, donde proporcionan a los clientes TLS-autenticados al estilo DHCP de IPs en el establecimiento de la red (túnel). De esta manera, varios túneles (hasta 128) pueden comunicarse sobre el mismo puerto del TCP o del UDP. Obviamente, es necesario activar un switch para activar el modo servidor.
- **Opciones de Envío/Recepción:** La configuración de la red de clientes puede ser controlada por el servidor. Después de la configuración correcta del túnel, el servidor puede decir al cliente (Windows y Linux) que utilice una configuración diferente de red instantáneamente.
- **Interfaz de control (Telnet):** Se ha añadido una interfaz de control vía Telnet.
- **El driver y el software de Windows se han mejorado extensamente.**

3.7.4.1.6 Comparación entre OpenVPN y VPN IPSec

Aun cuando IPSec es el estándar de facto, existen muchos argumentos para usar OpenVPN. La siguiente tabla muestra argumentos para seleccionar OpenVPN, los puntos precedidos por "+" son ventajas y puntos precedidos por "-" son las desventajas.

Tabla 10 – Comparación OpenVpn e IpSec.

IPSec VPN	OpenVPN
+ Es la tecnología estándar de VPN.	- Todavía es algo desconocido, no es compatible con IPSec.
+ Plataformas de hardware (dispositivos, aplicaciones)	- Solamente se puede instalar en los computadores. Pero en todos los sistemas operativos. La excepción al párrafo anterior, es cuando se tiene dispositivos donde está ejecutándose OpenWRrt basado en Unix y similares.
+ Tecnología bien conocida.	- Nueva tecnología, todavía creciendo y aumentando.
+ Existen muchos GUIs para su administración.	- No hay ningún GUI profesional, sin embargo hay algunos proyectos interesantes y prometedores.
- Modificación compleja de la pila del IP.	+ Tecnología simple.
- Es necesario una modificación crítica del núcleo.	+ Interfaces y paquetes estandarizados de red.
- Son necesario privilegios de administrador.	+ El software de OpenVPN puede funcionar en el espacio de usuario, y puede ser chroot-ed.
- Diversas implementaciones de IPSec de diversos fabricantes pueden ser incompatibles.	+ Usa tecnología estandarizada de cifrado.
- Configuración compleja, tecnología compleja.	+ Tecnología fácil, bien estructurada, modular, configuración fácil.
- Curva grande de aprendizaje para los novatos.	+ Fácil de aprender, éxito rápido para los novatos.
- Son necesarios varios puertos y protocolos en el cortafuego.	+ Solamente es necesario un puerto en el cortafuego.
- Problemas con direcciones dinámicas en ambos lados.	+ DynDNS trabaja enteramente, vuelve a conectar más rápidamente.
- Problemas de la seguridad con las tecnologías de IPSec.	+ SSL/TLS como capa criptográfica estándar industrial.
	+ Traffic Shaping.
	+ Velocidad (hasta 20 Mbps en un computador con 1 Ghz).
	+ Compatibilidad con los cortafuegos y proxies.
	+ Ningún problema al realizar NAT. (ambos lados pueden estar en las redes de Naced)
	+ Posibilidades de la configuración del viajante.

Como se puede apreciar en la tabla comparativa, para esta investigación se ha utilizado OpenVPN por muchas razones que se muestran en la tabla, como así también por las siguientes razones:

- Fácil de instalación y configuración.
- Es una aplicación de libre distribución (licencia Open Source).
- Es de Código Abierto.
- El sistema de criptografía se basa en OpenSSL.

Es multiplataforma, corriendo en los sistemas: Linux, Windows, FreeBSD, OpenBSD, Mac, Solaris, entre otros.

3.7.5 Cifrado

Existe diversos tipos y técnicas de cifrado que se pueden utilizar en la transmisión de video streaming, a continuación se describen alguno de ellos.

3.7.5.1 Red y la capa de transporte de cifrado

Los protocolos de red actuales, como IPSec o Seguridad Capa Transporte (TLS) pueden ser usados para cifrar un flujo de bits independientemente de la infraestructura de servidor de streaming, para minimizar los requisitos de diseño del sistema. IPSec es una solución de la capa IP que proporciona seguridad de transmisión entre dos hosts IPsec permitidos, a menudo utilizado para las redes privadas virtuales o VPN sobre redes IP públicas. En un video streaming, IPSec sería instalado en el servidor de transmisión o de su enrutador [30,31].

Todo el tráfico sería cifrado, ya que deja el acceso al contenido almacenado y se descifra en el computador de destino. Aunque IPSec es compatible con todas las propiedades intelectuales de software existente, es poco adecuado para su uso con video streaming. IPSec tiene un procesamiento complejo, lo que da problemas de escalabilidad y la limitación del número máximo de streams concurrentes que pueden acceder, es un factor que convierte a IPSec en una herramienta de seguridad poco utilizada en video streaming. Otro aspecto importante, es que el servidor de contenido almacena el contenido de video en texto plano, haciendo que el servidor sea atractivo y objetivo de intentos de robo de contenido [32,33].

Además, el descifrado de paquetes puede ser capturado fácilmente por la capa IP en el cliente. IPSec fue diseñado originalmente para las comunicaciones seguras con confianza entre las partes. Sin embargo, un servicio de video streaming requiere la distribución de contenidos de una parte de confianza (la del servidor central) a una parte que no se confía (el cliente).

TLS se basada en la aplicación original de Netscape de la Secure Sockets Layer (SSL) y corresponde a una capa de sockets seguro que proporciona comunicaciones seguras entre dos aplicaciones que se ejecutan a través de capa IP. Como SSL se ejecuta encima de TCP / IP, una sesión SSL puede ser transmitido por cualquier enrutador IP de la red. SSL se utiliza típicamente para proporcionar servicios Web seguros, tales como banca por Internet.

SSL no es apto para la transmisión de video, con similares características de escalabilidad y los problemas de seguridad como IPsec. Además, debido a que SSL proporciona comunicaciones seguras a través de TCP, otros utilizan UDP o RTP basados en contenido de aplicaciones de streaming, esto exigiría modificaciones al utilizar SSL, por lo tanto otro factor que evidencia que SSL no es apto para video streaming [34].

3.7.5.2 SECMPEG

El sistema de cifrado SECMPEG, se aplica de acuerdo a cada uno de los cuatro algoritmos que se mencionan a continuación: cifrar todas las cabeceras, en cooperación de los coeficientes DC de I macro bloques, Cifrar todos los cuadros I e I macro bloques en marcos P y B, Cifrar todo el bitstream. Los datos seleccionados se cifran usando algún algoritmo de encriptación como DES. Las cabeceras son aumentadas con información extra que permite el descifrado correcto en una siguiente etapa [35].

SECMPEG no es apto para el video streaming. Los cambios en la cabecera son incompatibles con los actuales estándares de Streaming en relación a MPEG. Tampoco es posible el indexado en el flujo de bits, debido a la falta de resincronización del sistema de cifrado utilizado. SECMPEG con video cifrado sólo puede ser descifrado de principio a fin con una velocidad normal de reproducción, lo que impide la aplicación de indexados o modos de alta velocidad de reproducción [36].

3.7.5.3 Zig-Zag Algoritmo de Permutación

En un formato MPEG de secuencia de video, cada bloque de 8x8 píxeles en un macro bloque, se codifica mediante una transformación discreta del coseno llamada DCT y procesados en un patrón zig-zag. El algoritmo divide el coeficiente DC para ocultar relativamente el largo del valor entre los pequeños coeficientes AC.

La misma lista de permutación se aplica a todos los macro bloques [37]. Tang sugiere modificaciones adicionales. Uno consiste en la seudo selección al azar de una de las dos listas a través de permutación criptográficamente segura generando bits aleatorios, y el otro se aplica el algoritmo de cifrado como AES a los bloques de 8 coeficientes DC.

Como el sistema de cifrado sólo modifica el contenido de macro bloque, el bitstream puede ser procesado por un servidor de streaming y todos los modos de reproducción son compatibles. La resincronización del cifrado en el indexado y el modo de alta velocidad de la reproducción no es necesaria porque cada fotograma se cifra con la misma lista. Sin embargo, si la lista de permutación es pseudo seleccionada al azar, el generador de bits aleatorios debe ser resincronizado [33,37].

Este cifrado es vulnerable a un ataque de texto conocido. Se propone un decodificador con un sistema de cifrado incorporado en un módulo, permitiendo que la lista de permutación al azar que se aplicará después del coeficiente, haya sido extraída del acceso indirecto, pero antes de que se decodificarán en valores de píxel individual. Sin embargo, la incorporación del algoritmo de cifrado en el descodificador se opone a la utilización de terceros descodificadores en MPEG.

3.7.5.4 Algoritmo de Cifrado de Video

VEA cifra cuadros individuales de todos los datos en la capa de imagen, dentro de la secuencia de video son seleccionados los cuadros para el cifrado. La capa de imagen está codificada por:

- Una subdivisión de datos en bloques de un número par de bytes. Aleatoriamente se dividen cada bloque en dos listas de igual longitud.
- Las dos listas aplican XOR para formar una tercera lista.
- Los bloques de cifrado se construyen a partir de la tercera lista y la segunda lista encriptada mediante cifrado como el AES.

Desencriptado implica el descifrado de la segunda lista a la que se le aplica un XOR con la tercera lista para recuperar la primera lista original. El flujo de texto plano original se reconstruirá. El formato de imagen para la capa de flujo de bits, utiliza un nuevo bloque de cabecera de codificación del número y la duración del trozo con la de la imagen, acortando en lugar de alargar el flujo de bits [38].

VEA es seguro y el cifrado consiste en una libreta de un texto cifrado y una copia cifrada de otra libreta. VEA es tan seguro como el sistema de cifrado utilizado para proteger la segunda lista. Sin embargo, VEA no es adecuado para el video streaming, el formato de la capa de imagen se ha modificado [38], y el modo de alta velocidad de reproducción no puede ser aplicado desde cuadros individuales I, porque no pueden ser extraídos desde la secuencia de bitstream.

3.7.5.5 Algoritmo de cifrado de video - Número 2

En su versión inicial, el sistema cifra el signo de los bits de todos los coeficientes AC y DC en el flujo de bits. Cada bit de una clave binaria hace un XOR con los bits de signo. Cuando se agotan los bits de la clave, se vuelve a utilizar la clave [39].

Los autores sugieren resincronización regular en el comienzo de cada grupo de imágenes (GOP) por la reactivación de cifrado desde el principio de la clave. La cifra fue posteriormente modificada también cifrando los bits de signo del vector de movimiento [40].

En ambos algoritmos la clave se utiliza directamente en la operación XOR (aunque es posible utilizar un generador de bits aleatorio). El cifrado es susceptible a un ataque de texto conocido. Un atacante extrae la señal correspondiente de los flujos de bits cifrados, determinando la secuencia pseudo aleatoria de bit (común para cada GOP) y descifran el flujo de bits completo [41].

3.7.5.6 Dominio de Frecuencia del Algoritmo de Codificación (FDSA)

La frecuencia de codificación de dominio de cifrado propuesto, opera en la información codificada en la capa de macro bloque, en particular, los coeficientes de DCT [42]. El cifrado se ve reforzado por considerar también:

- Refinamiento del cifrado de bits dentro de los coeficientes: El refinamiento (o menos significativos) de los bits de los coeficientes tienden a tener una distribución uniforme y se pueden cifrar sin afectar a la tasa de compresión.
- Bloque de arrastre: Divide el bitstream en una serie de bloques que se barajan con una mesa de cambio. Sólo las posiciones de los macro bloques dentro del stream son cambiados, por consiguiente una compresión alta.
- Bloque de rotación: macro bloques se rotan pseudo aleatoriamente. Los valores reales de píxeles no se modifican y la relación de compresión no se ve afectada.

El cifrado es seguro y el contenido codificado puede ser atacado y sólo los macro bloque son modificados, manteniendo [43] así la información de cabecera requerido por los servidores para proporcionar un indexado y alta velocidad de transmisión [44].

3.7.5.7 Un sistema de Cifrado Único

Acá se proponen un algoritmo único para la protección de video distribuido. Un proceso de Poisson se utiliza para seleccionar bytes de la secuencia de bits en intervalos aleatorios. Los bytes seleccionados forman un nuevo flujo de bits que está cifrado. Correspondientes bytes de la secuencia de bits original se dañan, utilizando octetos para calcular un valor estadísticamente similar [45].

El descifrado se realiza mediante la adquisición de la segunda secuencia de bits de los bytes dañados o corrompidos y vuelven a insertarlos en el flujo de bits dañados. Este sistema funciona bien en una forma como "descargar ahora y a utilizar", pero no funciona en una aplicación de video streaming [45]. Existentes servidores de streaming que pueden no ser capaces de manejar el flujo de bits al azar corrompidos.

3.7.5.8 Encriptación Multicapas

Se modifica el sistema de cifrado VEA, rompiendo los 64 coeficientes DCT en tres capas diferentes. Más abajo (más importantes), la gama media y alta frecuencia de coeficientes se asignan en la capa base, media y mejor respectivamente. Cada capa recibe diferentes características del transporte garantizando la entrega de la capa base, alta probabilidad de entrega de la capa media y baja prioridad para la capa mejor (debido a su bajo contenido de la información) [46]. Las tres corrientes se recombinan en el destino o cliente antes de la decodificación y visualización. Sólo se cifran la capa base y media. Esto permite la entrega segura a través de redes con capacidad limitada, las capas inferiores pueden ser descifradas y se muestra de forma independiente de las capas superiores, dando lugar a una peor calidad de video en lugar de discontinuidades en la reproducción. Desafortunadamente, las múltiples capas de cifrado no son adecuadas para la transmisión de video, sufriendo los mismos problemas que el algoritmo de VEA original [47].

3.7.5.9 Selectiva macro bloque cifrado (SME)

Se propone un conjunto de cuatro cifras que operan en los macro bloques en el MPEG de la secuencia de video. Los datos seleccionados se cifran mediante por ejemplo AES, asegurando que el contenido de video es seguro contra todo [48].

Los autores recomiendan reiniciar el conteo para determinar el enésimo bloque al inicio de cada sector (asegurando la correcta selección del macro en un tramo en caso de pérdida de datos), así como cambiar periódicamente la clave AES para atacar este cifrado es imposible. Esta cifra no es adecuada para la transmisión de video [49]. Mientras que los servidores podrían escuchar el flujo de bits codificado en todos los modos de reproducción, la resincronización de cifrado AES en los modos de reproducción no es posible, ya que no se puede determinar qué marco se está reproduciendo actualmente.

3.7.5.10 AEGIS

Se propone AEGIS, que cifra el contenido de los cuadros I y las cabeceras de secuencia de video. Ellos cambian el flujo de bits mediante la inclusión extra en la información y el punto final de ubicación. AEGIS no es adecuado para la transmisión de video [50]. Ya que existente servidores de streaming que no pueden manejar su falta de flujo de bits en formato estándar. Además, aunque los autores sugieren que la codificación de los cuadros I sólo garantiza el video entero, otros han demostrado que también es necesario considerar el cifrado de los marcos P y B.

3.7.5.11 Comparación con otros Métodos de Cifrado

A continuación se presenta una tabla resumen respecto a distintos métodos de encriptación en video Streaming.

Tabla 11 —Métodos de Encriptación de Video Streaming.

Cifrado	Escalable Concurrente	Cifrado sincronizado para el cliente durante indexación en reproducción	Cifrado sincronizado para el cliente durante indexación en alta velocidad de reproducción	Cifrado implementado MPEG externamente e implementación de codificación	Cifrado seguro frente a ataques
IPSec	x	x	x	x	x
SSL	x	x	x	x	x
Encriptación completa	x	x	x	x	x
SECMPEG	ok	x	x	ok	ok
ZIG-ZAG	ok	ok	ok	x	x
VEA	ok	x	x	ok	ok
VEA-2	ok	x	x	x	x
FDSA	ok	x	x	x	ok
Único cifrado	ok	x	v	ok	ok
Muli capa	ok	x	x	ok	ok
SME	ok	x	x	ok	ok
AEGIS	ok	x	x	ok	x

3.7.6 Autenticación

3.7.6.1 Autenticación Mediante Nombre de Usuario y Contraseña

La autenticación mediante nombre de usuario y contraseña es el método más básico para proteger los datos en una red IP. Este método debería ser suficiente en escenarios que no requieran niveles de seguridad elevados o en los que la red de vídeo esté separada de la red principal y los usuarios no autorizados no puedan acceder físicamente a ella. Las contraseñas se pueden cifrar o descifrar cuando se envían. La primera opción es la más segura.

Se pueden proporcionar varios niveles de protección por contraseña dependiendo de los usuarios y nivel de información al que ellos pueden acceder.

3.7.6.2 Cifrado Autenticación

En una tarea de cifrado, el emisor y el receptor, deben conocer el conjunto de reglas que rigen el mecanismo como tal. Las llaves son usadas para transformar la información original en una resultante llamada texto cifrado. Como ambas partes conocen el cifrado, cualquiera de ellas puede reversar el proceso para abstraer el texto original.

El cifrado se basa en dos componentes: un algoritmo y una llave. Un algoritmo criptográfico es una función matemática que combina texto plano o cualquier otra información inteligible con una cadena de dígitos llamada key (llave) para producir un texto cifrado o no inteligible. Tanto la llave como el algoritmo son cruciales en un proceso de cifrado. El cifrado basado en un sistema de llaves ofrece una gran ventaja, los algoritmos criptográficos son difíciles de idear por lo cual sería traumático usar un nuevo algoritmo cada vez que una parte se quiera comunicar de manera privada con una nueva. Usando una llave, un usuario podría utilizar el mismo algoritmo para comunicarse con diferentes usuarios remotos y todo lo que se debería hacer sería utilizar una diferente llave con cada uno de ellos.

El número de llaves posibles que tiene cada algoritmo depende del número de bits de la llave. El número de posibles llaves viene dado por la fórmula 2n, donde n es el número de bits de la llave. Por ejemplo, una llave de 64 bits permite 264 posibles combinaciones numéricas o llaves. Es decir, 18’446.744’073.709’551.616 claves. El gran número de posibles claves dificulta los ataques de fuerza bruta en donde se examinan todas las posibles combinaciones. Por lo tanto la fortaleza del cifrado depende de la longitud de a llave.

3.7.6.2.1 Criptografía de Llaves Públicas

La criptografía de llaves públicas se basa en el manejo de una pareja de llaves. Cada llave puede encriptar información que sólo la otra puede desencriptar. La llave privada, únicamente es conocida por su propietario, la llave pública, se pública abiertamente, pero sigue asociada al propietario. Los pares de llaves tienen una característica única: los datos encriptados con una llave sólo pueden desencriptarse con la otra llave del par. En otras palabras, no tiene importancia que se use la llave privada o la pública para encriptar un mensaje, ya que el receptor puede usar la otra llave para desencriptarlo.

Las llaves se pueden usar de dos maneras diferentes: para garantizar confidencialidad al mensaje y para probar la autenticidad del emisor de un mensaje. En el primer caso, el emisor usa la llave pública del receptor para encriptar un mensaje, de manera que el mensaje continúe siendo confidencial hasta que sea decodificado por el receptor con la llave privada. En el segundo caso, el emisor encripta un mensaje usando la llave privada, una llave a la cual sólo tiene acceso él.

La llave pública del receptor asegura la confidencialidad; la llave privada del emisor verifica la identidad del mismo. Por ejemplo, para crear un mensaje confidencial, una persona necesita conocer primero la llave pública de su receptor, después deberá usar la misma para encriptar el mensaje y enviarlo. Como el mensaje se encriptó con la llave pública del receptor, sólo éste con su llave privada puede desencriptar el mensaje.

Aunque una persona puede encriptar un mensaje con una llave pública o con una llave secreta, usar la llave pública presenta ciertas ventajas. Por ejemplo, la llave pública de la pareja de llaves se puede distribuir en un servidor sin temor de que esto comprometa el uso de la llave privada. Por ello, no se necesita enviar una copia de la llave pública a todos los receptores, ya que ellos la pueden obtener desde un servidor de llaves, o a través de un proveedor de servicios. La figura 5.2.4.1.1 muestra el esquema con el cual un emisor encripta su mensaje por medio de la llave pública del destinatario y como este último con su llave privada desencripta el mensaje cifrado que le ha llegado.

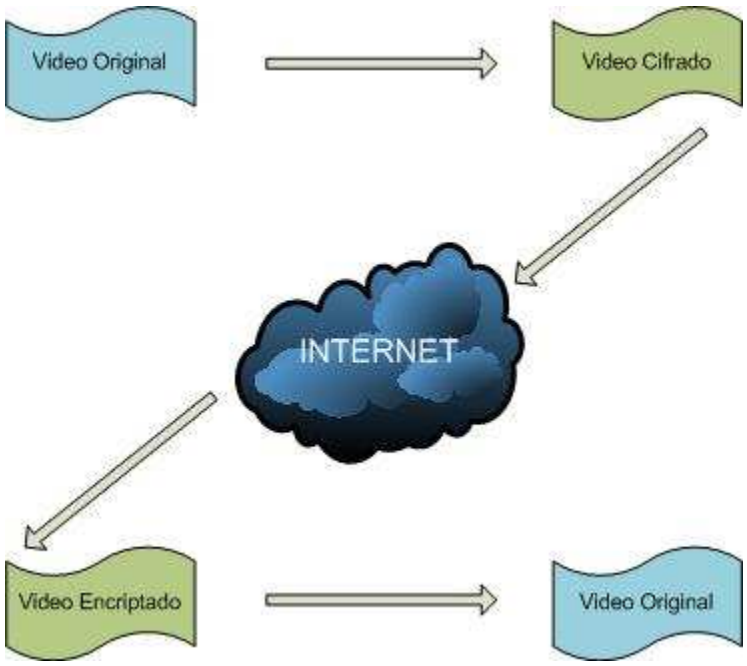

Figura 12 – Cifrado Clave Pública.

Colocar una llave pública en una red la vuelve fácilmente accesible, y no se pone en peligro la llave privada correspondiente. Otra ventaja de la criptografía con llave pública es que permite que el receptor autentifique al originador del mensaje.

La idea básica es la siguiente, ya que el emisor es la única persona que puede encriptar algo con su llave privada, todo aquel que use la llave pública del mismo para desencriptar el mensaje, puede estar seguro de que el mensaje proviene de él. Así, el uso de su llave privada en un documento electrónico es similar a la firma en un documento de papel. Pero hay que recordar que aunque el receptor puede estar seguro de que el mensaje proviene del emisor, no hay forma de garantizar que alguien más lo haya leído con anterioridad.

Usar algoritmos criptográficos de llaves públicas para encriptar mensajes es computacionalmente lento, así que se ha descubierto una manera para generar con rapidez una representación corta y única del mensaje, llamada "resumen" (message digest), que se puede encriptar y después usar como firma digital.

Algunos algoritmos criptográficos populares y veloces para generar resúmenes se conocen como funciones de dispersión (hash) de un solo sentido. Una función de dispersión (hash) de un solo sentido no usa una llave, simplemente es una fórmula para convertir un mensaje de cualquier longitud en una sola cadena de dígitos, llamada "resumen".

Cuando se usa una función de dispersión (hash) de 16 bits, el texto procesado con dicha función produciría 16 bits de salida (un mensaje podría dar como resultado la cadena CBBV235ndsAG3D67, por ejemplo). Cada mensaje produce un resumen de mensaje al azar. Para obtener una firma digital solo basta con encriptar dicho resumen con su llave privada.

Por ejemplo, suponiendo que el emisor, A, calcula un resumen para un mensaje, y encripta dicho resumen con su llave privada, luego envía esa firma digital junto con un mensaje de texto simple a B. Después de que B usa la llave pública de A para desencriptar la firma digital, B tiene una copia del resumen del mensaje que A calculó. Dado que B pudo desencriptar la firma digital con la llave pública de A, sabe que A lo creó, autentificando así al originador. B usa entonces la misma función de dispersión (que se acordó de antemano) para calcular su propio resumen del mensaje de texto simple de A. Si su valor calculado y el que A envió son iguales, entonces B puede estar seguro de que la firma digital es auténtica, lo que significa que A no sólo envió el mensaje, sino que el mensaje no fue alterado.

3.7.6.2.2 Algoritmos Importantes de Llaves Públicas

Existe un amplia variedad de algoritmos criptográficos para llaves públicas, los más importantes utilizados en esta investigación han sido: Diffie-Hellman y RSA.

3.7.6.2.2.1 Diffie-Hellman

El protocolo Diffie-Hellman permite a dos usuarios intercambiar una llave secreta sobre un medio inseguro sin tener acuerdos preestablecidos. Diffie-Hellman no se usa para encriptar datos, como se piensa generalmente. Se usa para intercambiar de forma segura las llaves que encriptan los datos. Esto lo logra generando un “secreto compartido”, también llamado “llave de cifrado de la llave” entre las dos partes. Este secreto compartido luego encripta la llave simétrica (usando AES) que asegura la transmisión.

Los sistemas de llaves asimétricas (la base de la infraestructura de llaves públicas) usan dos llaves, la llave privada y la llave pública, desafortunadamente estos sistemas tornan lenta la transmisión de datos. Lo práctico hoy en día, es usar un sistema simétrico para encriptar los datos y un sistema asimétrico para cifrar las llaves a usar en el proceso de cifrado de los datos.

Inicialmente, cada lado de la comunicación tiene su llave privada y la llave pública del otro lado. Diffie-Hellman tiene la capacidad de generar llaves compartidas idénticamente iguales en ambos lados de la comunicación con la llave privada local y la llave pública del lado remoto.

Una vez, cada lado de la comunicación tiene su secreto compartido idéntico al remoto, se inicia un proceso de cifrado de datos simétrico que es mucho más liviano que un mecanismo asimétrico, por tanto no disminuye sensitivamente la velocidad del enlace. Se tiene que hacer especial énfasis en el hecho que la llave compartida nunca se trasmite de un lado a otro, lo cual es muy importante.

El intercambio de llaves usando Diffie-Hellman es vulnerable a ataques tipo "hombre en el medio", ya que el intruso podría interceptar la comunicación, hacerse pasar por el lado remoto y enviarle al emisor su llave pública haciéndose pasar por el receptor. La solución para evitar este problema es usar firmas digitales que aseguren que la persona con la cual se está estableciendo la comunicación es efectivamente quien dice ser.

3.7.6.2.2.2 RSA

RSA es un sistema de cifrado de llaves públicas que se usa tanto para cifrado de datos como para autenticación de llaves públicas.

La dificultad para poder obtener la llave privada a partir de la pareja radica en el tamaño tan grande de las llaves, que en la actualidad son del orden de los 512 a 2048 bits de tamaño. Cuanto más grande se escojan estos números mayor será el tiempo que se tome un intruso en calcular las llaves privadas de las partes que se comunican.

3.7.6.2.3 Infraestructura de Llaves Públicas

La criptografía de llaves públicas ofrecen una gran herramienta matemática para facilitar la autenticidad, pero surge un gran problema y es el cómo manejar y publicar dichas llaves para cada persona o entidad que las necesiten.

Una infraestructura de llaves públicas (Public Key Infrastructure - PKI) es el conjunto de servicios y políticas que rigen el esquema de vinculación de una identidad con una llave pública y la posterior redistribución de ese vínculo.

Una PKI tiene tres procesos básicos: certificación, validación y la revocación de certificados. La certificación es la vinculación de una identidad a una llave pública. La llave pública y la identidad o atributos son puestos dentro de un documento digital llamado certificado. Un tercer participante confiable firma el certificado digitalmente, dando fe de la validez del contenido. El tercer participante en una PKI es llamado una Autoridad de Certificación (CA).

La validación es el proceso de comprobar la autenticidad del certificado, por tanto de asegurar que el contenido del mismo es confiable. Esto requiere la verificación de la firma del CA usando la llave pública del mismo y chequeando el certificado contra una lista de revocación de certificados (CRL). Una CRL contiene una lista de certificados que han sido revocados anteriormente por la CA indicando que ese vínculo no es válido. La validación también involucra chequear el periodo de validez contenido en el certificado mismo.

La revocación de un certificado es el proceso de desconocer un certificado previamente emitido antes de su fecha de expiración. Esto sucede cuando algunos aspectos de la información contenidos en el certificado cambian, quizás porque la identidad del usuario ha cambiado o porque la llave privada del usuario ha sido comprometida. El CA es responsable de emitir una CRL actualizada.

Un aspecto fundamental de las PKI es el grado de confianza que deposita en las CAs. Sin tal confianza los certificados digitales emitidos por cada CA perderían valor.

3.7.6.2.4 Arquitectura de una Infraestructura de Llaves Públicas

Una PKI incluye la autoridad certificadora (CA) y todos los otros componentes que permiten la certificación, validación y revocación. La figura 5.2.4.1.4 muestra los principales componentes de una PKI: El usuario, el validador, la autoridad de registro RA, la autoridad de certificación CA, el certificado y un depósito de CRLs. Todos estos componentes interactúan para facilitar la adquisición y uso de certificados digitales.

Las CAs, las RAs y el depósito de CRLs son entidades de manejo o administración dado que ellos son responsables de la generación, distribución, almacenamiento y revocación de certificados digitales. Los usuarios y los validadores son entidades de usuario dado que ellos usan los certificados y las funciones de la PKI para lograr sus propósitos. Las entidades de usuarios realizan requerimientos a las entidades de manejo, bien sea para adquirir un certificado o validar alguno que haya presentado otra entidad de usuario.

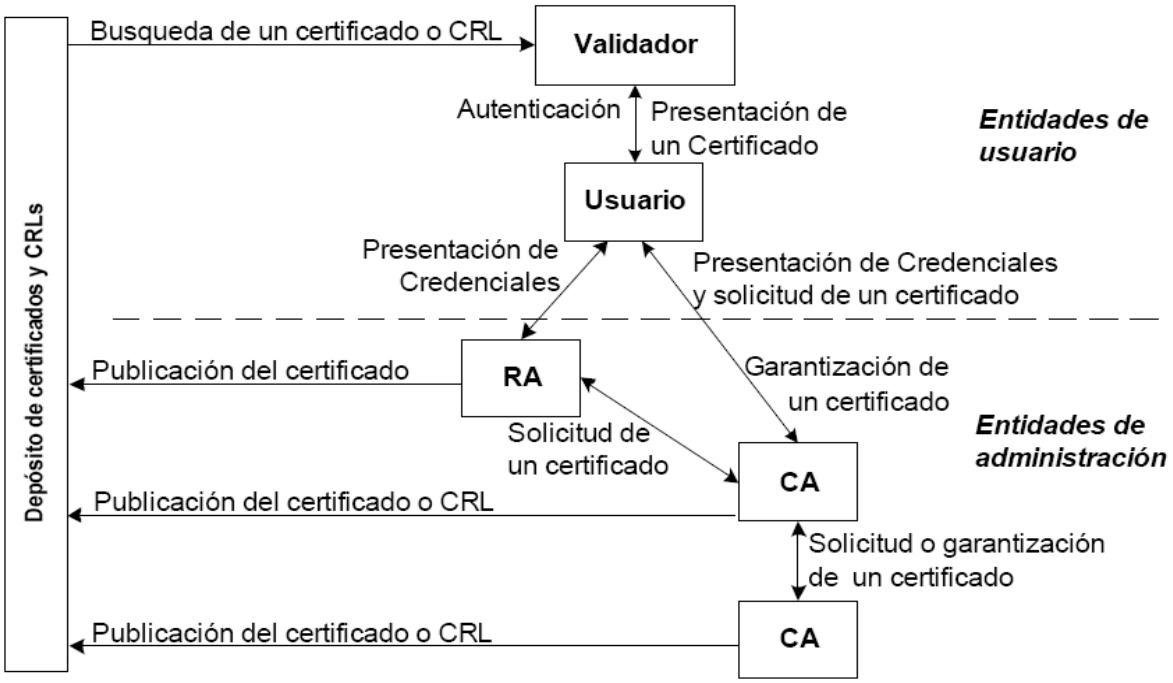

Figura 13– Cifrado Clave Pública.

Después que las credenciales son certificadas y verificadas, un certificado es emitido al usuario y publicado en el depósito. Cuando un validador necesita autenticar un usuario, usa la llave pública válida contenida en el certificado para verificar un mensaje firmado por la llave privada del usuario. Las CAs también publican las CRLs en el depósito, por tanto el validador puede chequear si el certificado del usuario es todavía válido.

3.7.6.2.5 Certificación

La certificación es el proceso de vincular un usuario con su información. Para asegurar la autenticidad e integridad de tal vínculo, la CA firma el documento usando su llave privada. El proceso de certificación toma varios pasos. Primero, el CA debe verificar que la información contenida en el certificado digital es auténtica y precisa. Esto implica un cierto nivel de seguridad en el canal que se usa para hacer este requerimiento y un especial cuidado del personal autorizado para insertar la información de la entidad dentro de un certificado. En algunas ocasiones la parte que entra la información no es el usuario a certificar. El siguiente paso es la generación del par de llaves. La llave pública del usuario deberá ser incluida en el certificado. Algunas veces el usuario genera el par de llaves y pasa solamente la llave pública a la CA, por tanto solo él conoce su llave privada.

Después, la CA firma el certificado con su llave privada. Esto tiene dos objetivos: Que el certificado sea garantizado por la CA y que la integridad del certificado sea protegida. Después que el certificado digital es creado y firmado por la CA, el usuario puede recuperarlo desde ella. El proceso de recuperación del certificado comienza con la presentación de una credencial por una única y primera vez a la CA, usualmente es un número de referencia y un código de autorización dado al usuario por otro medio (preferiblemente seguro). En algunos casos es tan simple como un e-mail que envía la CA al usuario.

3.7.6.2.6 Validación

Un certificado debe ser validado antes de poder ser usado para brindar confiabilidad, la validación del certificado comprende los siguientes pasos:

- La integridad del certificado es chequeada verificando la firma digital por medio de la llave pública de la CA.
- El intervalo de validación del certificado digital es chequeado.
- La CRL de la CA es chequeada para asegurarse que el certificado no ha sido rechazado.

3.7.6.2.7 Revocación del Certificado

Un certificado puede ser revocado antes de su fecha de expiración si pierde su validez de alguna manera, por ejemplo cuando la longitud de la información contenida en el no es válida. Así como con el proceso de certificación, el requerimiento para revocar un certificado deberá ser recibido por medio de un canal seguro y examinado detenidamente.

La CA revoca un certificado incluyéndolo en la lista de certificados revocados o CRL (Certificate Revocation List). Una CRL usualmente contiene solo los números seriales de los certificados revocados. La inclusión de toda la información de los certificados revocados dentro de la CRL resultaría innecesaria y de un tamaño de archivo muy grande. La CA garantiza la integridad de la CRL firmando la misma con su propia llave privada.

La CA da a conocer la CRL publicándola en su depósito. LA CRL es actualizada frecuentemente (por ejemplo cada ocho horas). La entidad de validación puede realizar un requerimiento de la CRL actualizada cuando la misma en su posesión ha expirado.

En algunas ocasiones la CA proactivamente entrega su CRL a las entidades de validación más grandes cuando una nueva revocación ha sucedido, de esta manera el efecto se torna inmediato.

3.7.6.2.8 Formatos de Certificados Digitales

Un certificado digital, como ya se había dicho anteriormente, vincula la identidad de una entidad a su llave pública. La autenticidad de la información es garantizada por la firma digital de la CA emisora. Varios estándares describen la información que debe estar contenida en el certificado, cómo debe ser organizada dentro del mismo y cómo se firma el certificado. Entre los formatos más usados se encuentran el X.509 el utilizado en esta investigación y el PGP.

3.7.6.2.8.1 Certificado X.509

La X.509 define los lineamientos de los certificados de llaves públicas, incluyen una especificación de los certificados usados para vincular un nombre con una llave pública, y una especificación de revocación para los certificados emitidos que no sean confiables. El estándar X.509 no especifica una infraestructura de llaves públicas (PKI) en su totalidad, solo provee las bases sobre las cuales una PKI puede ser construida.

X.509 define el formato de certificados de llaves públicas más ampliamente usado. Un certificado digital X.509 es un documento firmado que garantiza el vínculo de un nombre y una llave pública, por lo tanto, debe contener al menos un nombre y una llave pública.

3.7.6.2.9 Sistemas de Administración de Certificados

La interacción de todos los componentes de una PKI que manejan la creación, renovación, mantenimiento y revocación de certificados digitales es conocida como el Sistema de Administración de Certificados (Certificate Management System). Esos componentes incluyen:

- Autoridad de certificación
- Autoridad de registro
- Depósito de certificados y CRL
- Algunas veces todos los tres componentes residen en el mismo computador.

3.7.6.2.10 Autoridad De Certificación (CA)

La CA es la entidad que emite y revoca los certificados, entre sus funciones están:

- Creación y administración de las llaves públicas y privadas de la propia CA
- Creación de parejas de llaves públicas y privadas para los usuarios que así las necesitan.
- Creación de un certificado vinculando la llave pública del usuario a la identidad del mismo.
- Revocación de certificados.
- Creación de la lista de certificados revocados.
- Administración de una base de datos de información segura donde reside la historia de los certificados emitidos y revocados.
- Manejo de un completo registro (log) de mensajes para propósitos de auditoría.

3.7.6.2.11 Autoridad de Registro (RA)

Una CA es responsable de dos cosas: La verificación de la información del usuario y la emisión del certificado. La emisión de un certificado requiere acceso a la llave privada de la CA para que ella misma lo firme. Lo ideal es mantener la llave privada de la CA en un pequeño número de sitios. La verificación de la información de un usuario, el requerimiento de un certificado, la generación de la llave y el almacenamiento de la misma, son aspectos que hace la CA sin requerir accesar la llave privada del usuario. Uno o más autoridades de registro (RA) son empleadas para realizar estas funciones.

Una CA puede tener muchas RAs estratégicamente localizadas para proveer una alta disponibilidad. Dado que la población de usuarios crece continuamente, más y más RAs deben ser adicionadas para mantener estable el nivel de servicio.

Una desventaja obvia de tener más y más RAs es que se incrementa la complejidad del mantenimiento de la seguridad; ya que cada RA debe ser certificada por la CA y debe comunicarse con la misma y con las otras RAs que tienen que ver con la verificación y revocación de los certificados que ella maneja.

3.7.6.2.12 Depósitos de Certificados y de CRLs

Cuando un certificado es emitido a un usuario, la CA puede también publicar una copia de dicho certificado en un depósito. De la misma manera cuando es necesario invalidar un certificado antes de su fecha de expiración, la CA debe publicar la revocación publicándola en su CRL. Lo más conveniente es mantener la CRL en la lista de certificados en el mismo depósito.

Un certificado no puede ser declarado válido hasta no ser chequeado contra la CRL, por lo tanto, es vital que un depósito de CRLs tenga siempre un fácil acceso. Sin embargo, el facilitar este acceso también puede hacer que el depósito sea vulnerable a varios tipos de ataques DOS (Denial-Off- Service). Medidas de seguridad apropiadas deben ser tomadas para reducir este riesgo e incrementar la robustez de la PKI. Algunas veces es de utilidad tener múltiples depósitos redundantes.

4 Tecnología Streaming

4.1 Introducción

La tecnología Streaming es una técnica de transferencia de datos, la cual permite procesar de forma inmediata y continua un conjunto de información. Esta tecnología posibilita incrementar en forma importante las posibilidades de Internet de visualizar grandes cantidades de información multimedia; para ello debe existir un visualizador cliente capaz de leer este tipo de archivos o conectar el plugin adecuado. La tecnología Streaming puede ser de cliente o de servidor-cliente.

Hasta el momento la mayoría de los contenidos de audio y video, almacenados en los sitios Web son descargables. Esto significa que el contenido multimedia debe ser transmitido a través de la Web y copiado en el computador del usuario antes de poder reproducirlo. Para los usuarios era poco atractivo bajar archivos de música y videos que eran de su interés por las largas demoras que significaba esperar la descarga de éstos para después poder disfrutarlos.

La tecnología Streaming vendría a suplir tal defecto. Permite oír o ver el archivo inmediatamente después de haberle hecho un doble clic en él. Para el usuario es un cambio radical ya que no necesita bajarlo completamente para saber si es de su interés o no, evitando frustraciones y ahorrando tiempo.

Esta tecnología se refiere al contenido multimedia digital que ha sido comprimido y codificado en un formato tal que se subdivide en paquetes de información, los cuales fluyen a través de la red hacia el destinatario, el que los comienza a reproducir en cuanto llena su búfer.

Este proceso dura muy poco tiempo después de iniciado el flujo y continúa reproduciendo los paquetes a medida que siguen llegando y llenando el búfer. Los paquetes sólo se guardan el tiempo necesario para ser reproducidos, por lo tanto el archivo no queda almacenado en el disco duro. Se logra de esta manera con este sistema una reproducción fluida.

4.2 Formatos de Video

Para hacer llegar a cada usuario la información, hace falta un formato determinado que aplique, o no, compresión y que será el que almacene la información en un fichero.

4.2.1 Quicktime

El formato Quicktime (ficheros MOV) fue creado por Apple para el uso en computadoras Macintosh, aunque se ha extendido a otras plataformas. Es un software que le permite reproducir y editar video digital, así como otros tipos de archivos, en el computador. Quicktime no es en sí ninguna aplicación, sino una tecnología que permite a las aplicaciones llevar a cabo diversas funciones. Consta de una serie de elementos de software que amplían la capacidad del sistema operativo para gestionar archivos dinámicos [22].

4.2.2 Video para Windows

Los ficheros AVI (Audio y Video Intercalado) son el formato estándar de video que fue desarrollado por Microsoft Windows y por lo tanto uno de los más populares. "Intercalado" significa que en un fichero AVI los datos de audio y video son almacenados consecutivamente en capas, o sea, un segmento de datos de video es seguido inmediatamente por otro de audio. Es el formato más extendido para el manejo de datos multimedia en un computador. Un AVI no es más que un formato de archivo que puede guardar datos en su interior codificados de diversas formas y con la ayuda de diversos códecs que aplican diversos factores de compresión. También existe la posibilidad de almacenar los ficheros en un formato AVI "raw" (crudo), es decir, sin compresión [23].

4.2.3 Real Video

Es un flujo de datos continuo que permite a un archivo estándar de video, tal como puede ser MPEG, ser visualizado a través de Internet. Esto quita la necesidad de transmitir el archivo entero antes para visualizarlo. Desarrollado por RealNetworks compatible con varias plataformas como Windows, Mac, Linux, Solaris y una variedad de teléfonos móviles [24].

Se reproduce a través de un archivo RealMedia o por medio de la red utilizando RTSP, este último sólo utilizado para crear y gestionar la conexión. Los datos de video son enviados a través del protocolo RDT (Transporte de Datos Real).

4.2.4 Windows Media Video

El formato WMV (Windows Media Video) es una extensión que no tiene diferencia con los archivos ASF. Estos usan el formato de fichero estándar de Windows Media. Los ficheros con extensión ASF normalmente son utilizados en contenidos basados en Windows Media usando las Herramientas Windows Media [25].

El video WMV se empaqueta normalmente en algún contenedor multimedia, como pueden ser AVI o ASF. Los archivos resultantes reciben la extensión .AVI si el contenedor es de solo video o .ASF si se trata de un contenedor con contenido de audio y video.

4.2.5 Formato Avanzado de Secuencias

ASF fue desarrollado por Microsoft en 1996, es uno de los primeros formatos de ficheros designados específicamente para el streaming. Este formato está optimizado para enviar secuencias multimedia a través de una red, es el recomendado para ello, pues, tiene la capacidad de adaptarse a anchos de bandas variables y cambios en las condiciones de la red, es un estándar abierto que admite la entrega de datos a través de una gran variedad de protocolos y redes. También es posible utilizar cualquier códec para codificar las secuencias ASF. Se utiliza para ordenar, organizar y sincronizar los datos multimedia que se transmitirán por las redes. Sin embargo, puede utilizarse para especificar el formato de las presentaciones en directo y es también adecuado para la reproducción local [26].

Es un formato de alta flexibilidad que contiene una descripción y una representación digital comprimida de audio, video, imágenes, subtítulos y eventos. Este formato también puede describir la estructura del dato del flujo en vivo. Cada flujo contiene uno o más flujos media, más comúnmente, uno de audio y uno o más de video, la entrega y presentación de los cuales son sincronizados a una línea de tiempo común.

4.2.6 Flash Video

FLV (Flash Video) es un formato de archivo propietario usado para transmitir video sobre Internet usando Adobe Flash Player (anteriormente conocido como Macromedia Flash Player). Los contenidos FLV pueden ser incrustados dentro de archivos SWF. Entre los sitios más notables que utilizan el formato FLV se encuentran YouTube, Google Video, Reuters.com, Yahoo! Video y MySpace [27].

Flash Video puede ser visto en la mayoría de los sistemas operativos, mediante Adobe Flash Player, un plugin extensamente disponible para navegadores Web, o de otros programas de terceros como MPlayer, VLC media player, o cualquier reproductor que use filtros DirectShow (tales como Media Player Classic, Windows Media Player, y Windows Media Center) cuando el filtro ffdshow está instalado.

4.2.7 Codificación de Video

Para codificar un video hay que considerar distintos aspectos, los cuales se mencionan a continuación.

4.2.7.1 Resolución

En los sistemas digitales, la imagen esta formada por pixeles cuadrados, a diferencia de los videos analógicos que constan de líneas o líneas de TV, puesto que deriva de la tecnología implementada por la televisión. Por eso mismo que a continuación se abordarán las distintas resoluciones orientadas a los videos digitales.

4.2.7.1.1 Resolución VGA

Con los sistemas 100% digitales basados en cámaras de red se pueden proporcionar resoluciones derivadas de la informática y normalizadas en todo el mundo, de modo que la flexibilidad es mayor. VGA (Tabla de Gráficos de Video) es un sistema de pantalla de gráficos para computadoras, desarrollado originalmente por IBM. Esta resolución es de 640 x 480 píxeles, un formato habitual en las cámaras de red que no disponen de megapíxeles. La resolución VGA suele ser más adecuada para cámaras de red, ya que el video basado en VGA produce píxeles cuadrados que coinciden con los de las pantallas de un computador. Los monitores de ordenador manejan resoluciones en VGA o múltiplos de VGA.

A continuación se muestra la tabla de resolución VGA, respecto a pixeles.

Tabla 12 – Resolución VGA.

Formato de visualización	Pixeles
QVGA (SIF)	320X240
VGA	640X480
SVGA	800x600
XVGA	1024x768
4x VGA	1280x960

4.2.7.1.2 Resolución megapíxel

Una cámara de red que ofrece una resolución megapíxel utiliza un sensor megapíxel para proporcionar una imagen que contiene un millón de megapíxeles o más. Cuántos más píxeles tenga el sensor, mayor potencial tendrá para captar más detalles y ofrecer una calidad de imagen mayor.

Con las cámaras de red que tengan resolución megapíxel los usuarios pueden obtener más detalles (ideal para la identificación de personas y objetos) o para visualizar un área mayor del escenario que se desea captar. Esta ventaja evidencia una importante consideración en aplicaciones como es en este caso de Tele Vigilancia.

A continuación se muestra la siguiente tabla, que muestra distintos formatos megapíxel.

Tabla 13 – Resolución Pixeles.

Formato de Visualización	N° Megapíxeles	Pixeles
SXGA	1.3 megapíxeles	1280 X 1024
SXGA + (EXGA)	1.4 megapíxeles	1400 X 1050
UXGA	1.9 megapíxeles	1600 X 1200
WUXGA	2.3 megapíxeles	1920 X 1200
QXGA	3.1 megapíxeles	2048 X 1536
WQXGA	4.1 megapíxeles	2560 x 1600
QSXGA	5.2 megapíxeles	2560 x 2048

La resolución megapíxel es una característica en la que las cámaras de red se distinguen de las analógicas. La resolución máxima que puede proporcionar una cámara analógica convencional tras haber digitalizado la señal de video en una grabadora o codificador de video es D1, es decir, 720 x 480 píxeles (NTSC) o 720 x 576 píxeles (PAL). La resolución D1 corresponde a un máximo de 414.720 píxeles ó 0,4 megapíxeles. En comparación, un formato megapíxel común de 1280 x 1024 píxeles consigue una resolución de 1,3 megapíxeles. Esto es más del triple de la resolución que pueden proporcionar las cámaras analógicas. También existen cámaras de red con resoluciones de 2 megapíxeles y 3 megapíxeles, e incluso superiores.

La resolución megapíxel también consigue un mayor grado de flexibilidad, es decir, es capaz de proporcionar imágenes con distintas relaciones de aspecto. (La relación de aspecto es la relación entre la anchura y la altura de una imagen). Una pantalla de televisión tradicional muestra una imagen con una relación de aspecto de 4:3. Las cámaras de red con resolución megapíxel pueden ofrecer la misma relación, además de otras, como 16:9. La ventaja de la relación de aspecto 16:9 es que los detalles insignificantes, que suelen encontrarse en las partes superior e inferior de una imagen con un tamaño tradicional, no aparecen y, por lo tanto, puede reducirse el ancho de banda y por ende el almacenamiento.

La siguiente figura muestra algunas relaciones de aspecto.

Figura 14– – Relaciones de Aspectos.

4.2.7.2 Compresión de Video

Las técnicas de compresión de video consisten en reducir y eliminar datos redundantes de video para que el archivo de video digital se pueda enviar a través de la red y almacenarlos. Con técnicas de compresión eficaces se puede reducir considerablemente el tamaño del fichero sin que ello afecte muy poco, o en absoluto, la calidad de la imagen. Sin embargo, la calidad del video puede verse afectada si se reduce en exceso el tamaño del fichero aumentando el nivel de compresión dependiendo de la técnica que se utilice.

Existen diferentes técnicas de compresión, tanto patentadas como estándar. Hoy en día, la mayoría de proveedores de video en la red utilizan técnicas de compresión estándar. Los estándares son importantes para asegurar la compatibilidad y la interoperabilidad.

Tienen un papel especialmente relevante en la compresión de video, puesto que éste se puede utilizar para varias finalidades y, en algunas aplicaciones de Tele Vigilancia, debe poderse visualizar varios años después de su grabación. Gracias al desarrollo de estándares, los usuarios finales tienen la opción de escoger entre diferentes proveedores, en lugar de optar a uno solo para un sistema de Tele Vigilancia.

Existen varios estándares de compresión de video distintos como: MPEG-4 Parte 2 (o, simplemente, MPEG-4) y H.264. El H.264 es el estándar de compresión de video más actual y eficaz.

4.2.7.3 Códec de Video

En el proceso de compresión se aplica un algoritmo al video original para crear un archivo comprimido y listo para ser transmitido o almacenado. Para reproducir el archivo comprimido, se aplica el algoritmo inverso y se crea un video que incluye prácticamente el mismo contenido que el video original. El tiempo que se tarda en comprimir, enviar, descomprimir y mostrar un archivo es lo que se denomina latencia. Cuanto más avanzado sea el algoritmo de compresión, mayor será la latencia.

El par de algoritmos que funcionan conjuntamente se denomina códec de video (codificador/ decodificador). Los códecs de video de estándares diferentes no suelen ser compatibles entre sí, es decir, el contenido de video comprimido con un estándar no se puede descomprimir con otro estándar diferente. Por ejemplo, un decodificador MPEG-4 no funcionará con un codificador H.264. Esto ocurre simplemente porque un algoritmo no puede descodificar correctamente los datos de salida del otro algoritmo, pero es posible usar muchos algoritmos diferentes en el mismo software o hardware, que permitirían la coexistencia de varios formatos.

4.2.7.4 Método de Compresión de Vdeo

Los algoritmos de compresión de video como el MPEG-4 y el H.264 utilizan la predicción inter fotograma para reducir los datos de video entre las series de fotogramas. Ésta consiste en técnicas como la codificación diferencial, en la que un fotograma se compara con un fotograma de referencia y sólo se codifican los píxeles que han cambiado con respecto al fotograma de referencia. De esta forma, se reduce el número de valores de píxeles codificados y enviados. Cuando se visualiza una secuencia codificada de este modo, las imágenes aparecen como en la secuencia de video original.

Para reducir aún más los datos, se pueden aplicar otras técnicas como la compensación de movimiento basada en bloques. La compensación de movimiento basada en bloques tiene en cuenta que gran parte de un fotograma nuevo está ya incluido en el fotograma anterior, aunque quizás en un lugar diferente del mismo. Esta técnica divide un fotograma en una serie de macro bloques (bloques de píxeles). Se puede componer o "predecir" un nuevo fotograma bloque a bloque, buscando un bloque que coincida en un fotograma de referencia. Si se encuentra una coincidencia, el codificador codifica la posición en la que se debe encontrar el bloque coincidente en el fotograma de referencia. La codificación del vector de movimiento, como se denomina, utiliza menos bits que si se hubiera codificado el contenido real de un bloque.

A continuación se muestra la figura de compensación de movimiento basada en bloques.

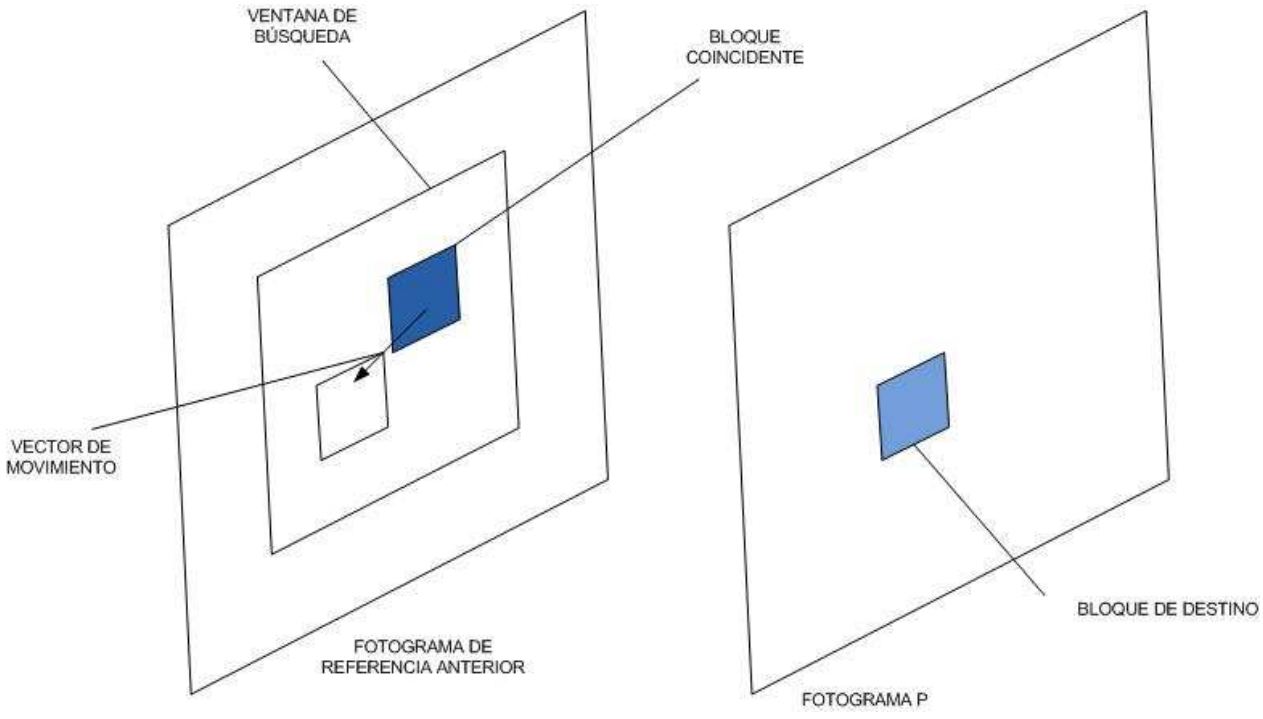

Figura 15 – Compensación de Movimiento.

Con la predicción inter fotograma, cada fotograma de una secuencia de imágenes se clasifica como un tipo de fotograma concreto, como un fotograma I, P o B.

Un fotograma I, o intrafotograma, es una imagen autónoma que se puede codificar de forma independiente sin hacer referencia a otras imágenes. La primera imagen de una secuencia de video es siempre un fotograma I. Los fotogramas I sirven como puntos de inicio en nuevas imágenes o como puntos de resincronización si la transmisión de bits resulta dañada. Los fotogramas I se pueden utilizar para implementar funciones de avance o retroceso rápido o de acceso aleatorio. Un codificador insertará automáticamente fotogramas I a intervalos regulares o a petición de nuevos clientes que puedan incorporarse a la visualización de una transmisión. La desventaja de este tipo de fotogramas es que consumen muchos más bits, pero por otro lado no generan demasiados defectos provocados por los datos que faltan. Un fotograma P (de inter fotograma Predictivo), hace referencia a partes de fotogramas I o P anteriores para codificar el fotograma. Los fotogramas P suelen requerir menos bits que los fotogramas I, pero con la desventaja de ser muy sensibles a la transmisión de errores, debido a la compleja dependencia con fotogramas P o I anteriores. Un fotograma B, o inter fotograma Bipredictivo, es un fotograma que hace referencia tanto a fotogramas anteriores como posteriores. El uso de fotogramas B aumenta la latencia.

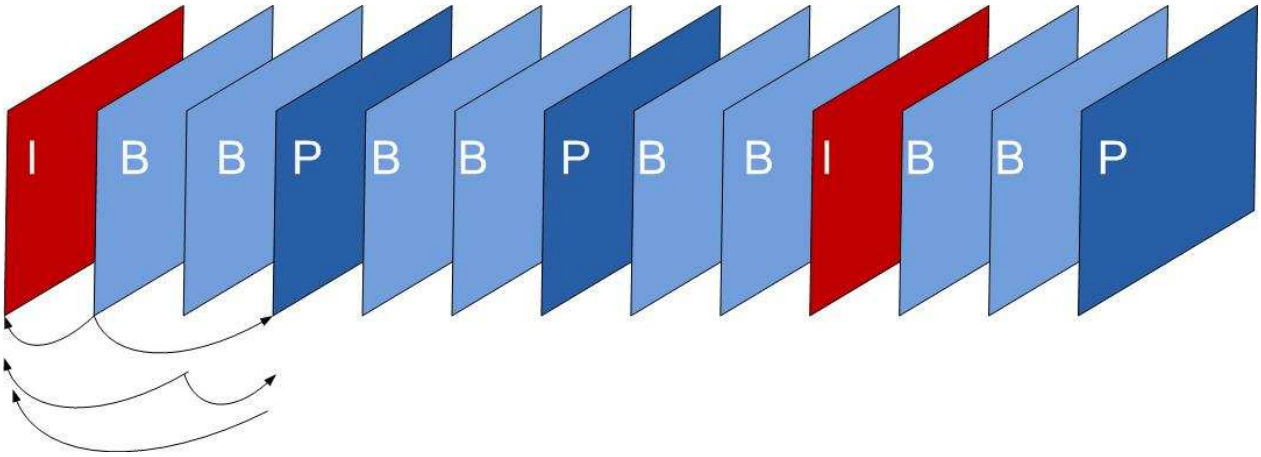

Figura 16 – Fotogramas.

Cuando un decodificador de video restaura un video descodificando la transmisión de bits fotograma a fotograma, la descodificación debe comenzar siempre por un fotograma I. Los fotogramas P y B, en caso de usarse, deben descodificarse junto a los fotogramas de referencia. La longitud de GOV (grupo de video) determina la cantidad de fotogramas P que se deberían enviar antes de realizar el envío de otro fotograma I. La frecuencia de bits se puede disminuir mediante la reducción de la frecuencia de fotogramas I (GOV más largo). Para reducir la latencia no se utilizan fotogramas B. Además de la codificación diferencial y la compensación de movimiento, se pueden emplear otros métodos avanzados para reducir aún más los datos y mejorar la calidad de video. El H.264, por ejemplo, admite técnicas avanzadas como los esquemas de predicción para codificar fotogramas I, la compensación de movimiento mejorada con una precisión inferior a un píxel y el filtro de eliminación de bloques en bucle para suavizar los bordes de los bloques (defectos).

4.2.7.5 Formatos de Compresión

4.2.7.5.1 MPEG-4

Cuando se menciona MPEG-4 en las aplicaciones de Tele Vigilancia, normalmente se refiere a MPEG-4 Parte 2, también conocido como MPEG-4 Visual. Como todos los estándares MPEG (Moving Picture Experts Group), requiere una licencia, es decir, los usuarios deben pagar una licencia. MPEG-4 es compatible con aplicaciones de bajo ancho de banda y aplicaciones que requieren imágenes de alta calidad, sin limitaciones de frecuencia de imagen y con un ancho de banda virtualmente ilimitado.

4.2.7.5.2 H.264

El H.264, también conocido como MPEG-4 Parte 10/AVC para Codificación de Video Avanzado, es el estándar MPEG más actual para la codificación de video. Ello se debe a que, sin comprometer la calidad de la imagen, un codificador H.264 puede reducir el tamaño de un archivo de video digital en más de un 50% más en comparación con el estándar MPEG-4. Esto significa que se requiere menos ancho de banda y espacio de almacenamiento para los archivos de video. Visto de otra manera, se puede lograr mayor calidad de imagen de video para una frecuencia de bits determinada.

En la Tele Vigilancia, H.264 ha encontrado su mayor utilidad en aplicaciones donde se necesiten velocidades y resoluciones altas, como en la de autopistas, aeropuertos y casinos, lugares donde por lo general se usa una velocidad de 30/25 (NTSC/PAL) imágenes por segundo. Es aquí donde las ventajas económicas de un ancho de banda y un almacenamiento reducidos se harán evidentes de forma más clara. Se espera que H.264 acelere también la adopción de cámaras megapíxel, ya que con esta eficiente tecnología de compresión se pueden reducir los archivos de gran tamaño y las frecuencias de bits sin que la calidad de la imagen se vea afectada. En cualquier caso, tiene sus exigencias aunque H.264 permite ahorrar los costos de ancho de banda y almacenamiento, también necesita cámaras de red y dispositivos de control de mejor rendimiento.

4.2.7.6 Frecuencia de Bits Variables

Con MPEG-4 y H.264, se pueden determinar que una transmisión de video codificado tenga una frecuencia de bits variable o constante. La selección óptima dependerá de la aplicación y de la arquitectura de red. Con VBR (frecuencia de bits variable), se puede mantener un nivel predefinido de calidad de imagen independientemente del movimiento o falta de movimiento en una escena. Esto significa que el uso de ancho de banda aumentará cuando haya mucha actividad en una escena, y disminuirá cuando no haya movimiento. A menudo esta opción es ideal para las aplicaciones de Tele Vigilancia que requieren una alta calidad, especialmente si hay movimiento en una escena.

Debido a que la frecuencia de bits puede variar, incluso aunque se haya definido una frecuencia de bits media de destino, la arquitectura de red (ancho de banda disponible) debe poder adaptarse a grandes cantidades de datos. Con un ancho de banda limitado se recomienda utilizar el modo CBR (frecuencia de bits constante), ya que este modo genera una frecuencia de bits que se pueden predefinir. La desventaja que tiene la CBR es que si, por ejemplo, hay mucha actividad en una escena que da como resultado una frecuencia de bits mayor que la velocidad de destino, la restricción para mantener una frecuencia de bits constante conlleva una calidad y frecuencia de imagen inferiores.

4.2.8 Protocolos Transmisión Video

SRTP fuero desarrollado para tratar la seguridad de los flujos de RTP que proporciona confidencialidad, autenticación de mensajes y protección de reproducción para el tráfico de RTP, así como para otros protocolos asociados de control de tráfico en tiempo real, como el protocolo de transferencia de control RTCP. SRTP proporciona los servicios de seguridad básicos necesarios para garantizar transmisión entre un emisor y un receptor, pero no proporciona la capacidad de adaptarse de forma segura los medios de comunicación protegidos, y deja sin resolver la autenticación del emisor, respecto a los cálculo de costos generales de ancho de banda.

Sin embargo, el cifrado se realiza a nivel de contenido en lugar de a nivel de transporte, haciendo que el transporte y su protección sean independiente y por lo tanto seguridad de extremo a extremo. Sin embargo, sólo proporciona autenticidad de integración, y no resuelve la autenticación del emisor. Frente a esto se muestra los distintos protocolos utilizados para la transmisión de video a través de Internet, que apoyan la transmisión de streaming y soportan seguridad para la transmisión de contenido streaming propiamente tal.

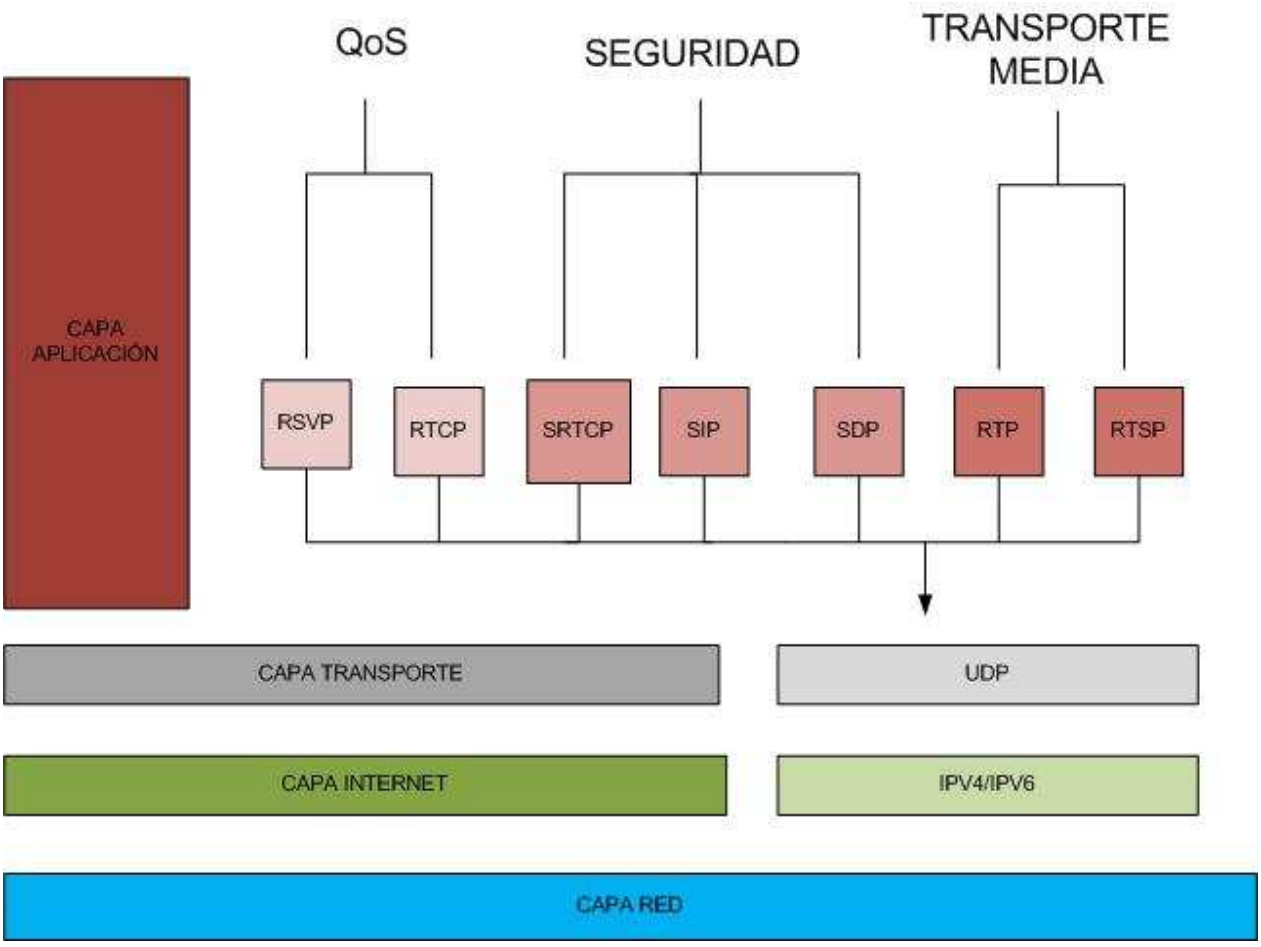

Figura 17 – Protocolos Modelo TCP/IP.

RSVP usado para manejar la calidad de servicio de la comunicación, ya que hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser congestionado. El propósito de RSVP es eliminar aquellas situaciones en las que el video se pierde porque se tiene una congestión de datos en la red. Para ello, éste solicita ancho de banda, divide los paquetes de datos grandes y da prioridad a los paquetes de video cuando hay una congestión en un router. Si bien este protocolo ayudará considerablemente al tráfico multimedia por la red, ayudando a garantizar una pequeña calidad de servicio.

Además, ya se definió RTCP en capítulos anteriores, y se describe como un protocolo de control de RTP orientado a dar información sobre la calidad de servicio en la transmisión de video, por ello que ambos protocolos pueden ayudar a controlar y verificar en cierto porcentaje QoS.

SRTCP como se definió en capítulos anteriores, corresponde a un perfil de RTP, el cual proporciona cifrado, autenticación, integridad y protección contra reenvío de datos, es por ello que la utilización de este protocolo nos proporciona aspectos de seguridad para poder transmitir y visualizar contenido multimedia a través de Internet. Además con SIP podemos iniciar sesiones multimedia, como es en este caso una sesión de Tele Vigilancia, en conjunto con SDP, el cual define o describe las sesiones streaming, el cual puede dar algunas posibilidades en las seguridad en la transmisión y tal vez QoS. Para finalizar RTSP, es un protocolo que utiliza la tecnología streaming y la transporta a través de los enlaces de comunicación de Internet.

4.3 Plataformas

En la actualidad existen cuatro tecnologías de emisión audiovisual en Internet Flash, Windows Media, Real Video y Quicktime. Estas compiten entre sí con diferentes estrategias, pero tienen puntos en común, como puede ser la distribución gratuita del software de reproducción, con el fin de tener el liderazgo del mercado. La más amplia, por ser parte del sistema operativo Windows, es Windows Media. Real Video, de la casa Real Networks, es la segunda más extendida, Flash por Macromedia y Quicktime, el software de Apple, lucha por instalarse como el estándar de video de alta calidad, algo que ya está consiguiendo en determinados segmentos como puede ser el de promociones cinematográficas.

Además es preciso un software que trabaje de acuerdo con ella y genere los ficheros. Para el caso del Quicktime es el Quicktime Pro, para el caso de Flash es Adobe Flash Player, en el caso del Windows Media es Windows Media Encoder y para el Real Server el software se llama Real Producer. Una vez que se obtienen los programas, se necesita un servidor capaz de emitir los videos mediante el proceso de Streaming.

En estos momentos existen tres servidores de video, Quicktime Streaming Server, Windows Media Server y Real Media Server. Cada uno de ellos utiliza un formato de fichero y un programa o plug-in distinto. Para poder visualizar cualquiera de los tipos de streaming media existentes, el cliente debe tener instalado en su sistema algún reproductor. Hay que tener en cuenta que los contenidos que se transmiten con Real Media Server solamente se pueden visualizar con el reproductor Realplayer, los de Windows Media Server únicamente con el Windows Media Player, Adobe Flash Media Server para archivos Flash y los de Quicktime Streaming Server con el reproductor Apple Quicktime Player.

4.4 Tipos de Transmisión

Se distinguen tres tipos de transmisiones: Broadcast, Unicast y Multicast. En los siguientes esquemas se muestra un emisor y cuatro receptores y dos puntos de la red donde no solicitan la transmisión de los datos (los círculos). Los envíos se señalan por medio de flechas.

La Figura representa la transmisión broadcast, donde los datos se distribuyen por todo los segmentos de la red, incluso en aquellas donde no hay receptores del mensaje (los círculos). Una sola copia del mensaje sale del emisor, sin importar el número de receptores que haya. Ejemplo del uso de este tipo de transmisión lo constituyen las emisiones de televisión y Streaming.

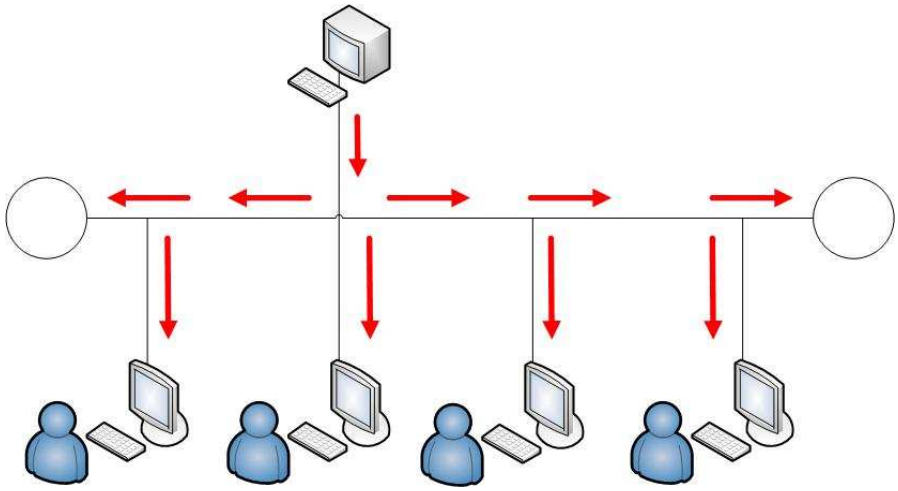

Figura 18 – Transmisión Broadcast.

La Figura siguiente ilustra el tráfico unicast (el más habitual en Internet), donde se envían los datos sólo a aquellas partes de la red donde hayan usuarios interesados en recibirlos. En este sentido es más eficiente que el broadcast. Sin embargo, el emisor tiene que enviar una copia para cada receptor, sobrecargando la red con copias de los mismos datos.

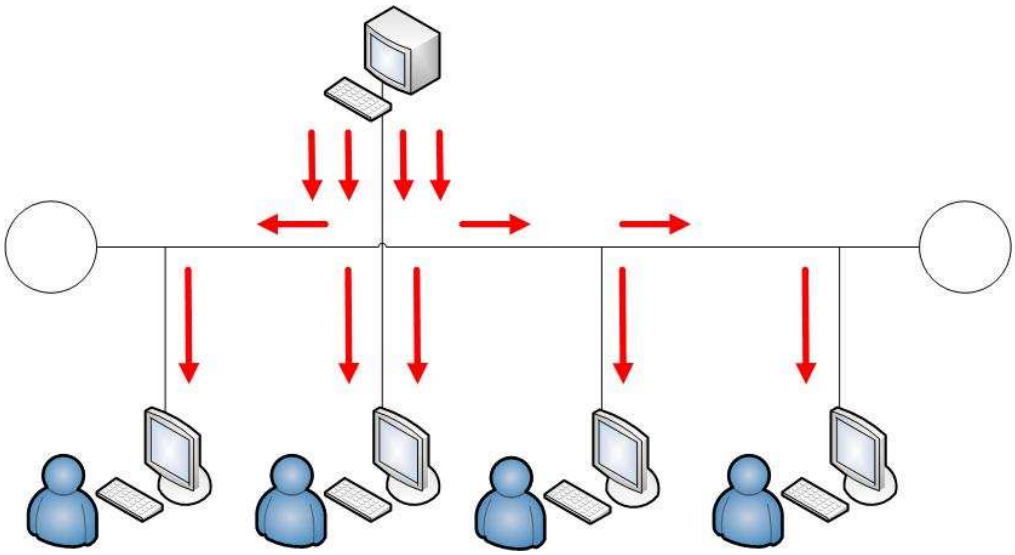

Figura 19 – Transmisión Unicast.

A su vez, como se observa en la Figura, el Multicast combina los mejores aspectos de los dos anteriores. Los datos sólo se envían una vez desde el servidor, sin importar el número de receptores, y estos datos sólo se envían a aquellas partes de la red donde haya usuarios interesados en recibirlos. Por tanto la red no está sobrecargada con un mismo envío [28].

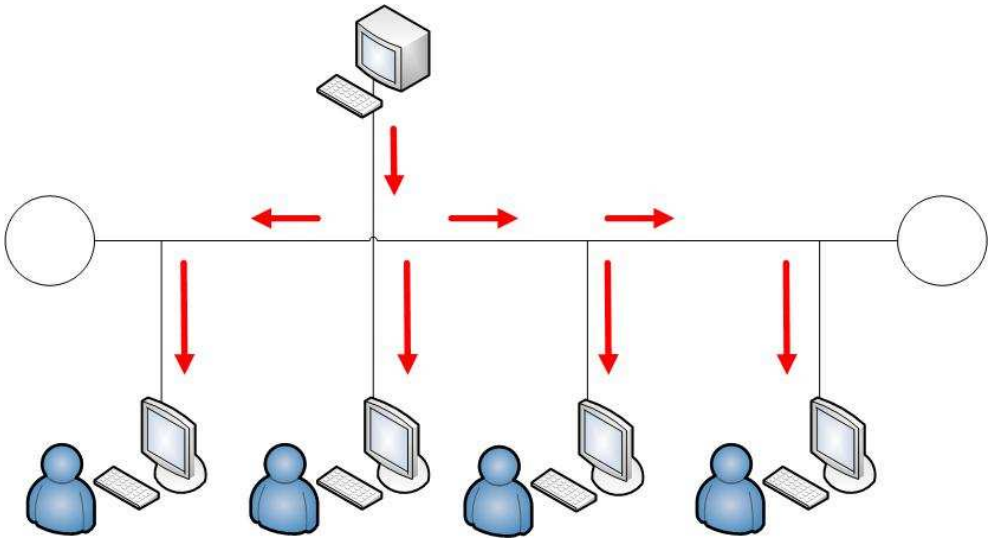

Figura 20 – Transmisión Multicast.

4.5 Secuencia de Transmisión

Para la transmisión de video Streaming se debe seguir la siguiente secuencia.

- **Planificación y Captura.** Consiste en la grabación del evento mediante cámaras de vídeo, recogiendo la mayor cantidad de información. Es necesario revisar las instalaciones del evento y planificar la grabación del video, pruebas de audio y líneas de comunicaciones instalados previamente para el evento.
- **Codificación.** Utilizar el equipo necesario para la codificación y compresión de las imágenes y el audio. Utilizando las aplicaciones más idóneas que actualmente existen en el mercado, para tratar el vídeo y audio para su posterior envío.
- **Envío del vídeo.** Tras la codificación y compresión del vídeo se envía. El envió se va realizando según se va codificando, Los servidores de video Streaming van presentando los eventos en directo a los usuarios de Internet, con un pequeño retraso por la codificación, comunicación y presentación Streaming. El servidor es el componente encargado de almacenar y poner a disposición de los usuarios finales el contenido del vídeo y audio ya sea para la emisión directa o desde la Web.
- **Emisión.** En directo o diferido, según se va recibiendo o sea el caso, se va presentando el video a los usuarios de Internet.

5 Modelo Propuesto

El diseño considera tres partes fundamentales: Sistema de Tele Vigilancia, Video Streaming y Mecanismos de Seguridad. Como se menciono anteriormente, a través de este diseño se pretende demostrar que la utilización de mecanismo de seguridad en la transmisión de video streaming es factible, desde el punto de vista de la calidad de servicio y de que esta no afecta en gran porcentaje al rendimiento y transmisión de video en un sistema de tele vigilancia. Por ello, estos serán explicados a continuación.

5.1 Sistema de Tele Vigilancia

Luego del estudio de las distintas tecnologías asociadas a un sistema de Tele Vigilancia, se propone el siguiente diseño para el desarrollo de esta investigación.

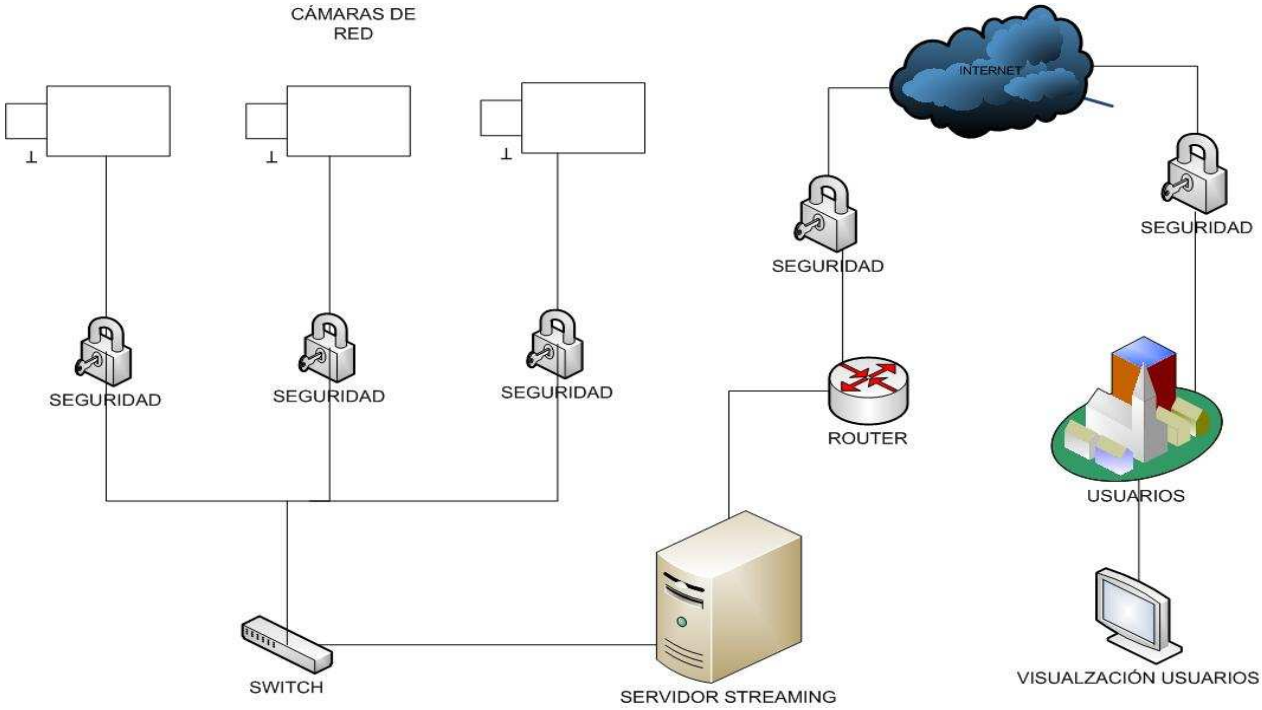

Figura 21 – Modelo General Sistema Tele Vigilancia Seguro.

Los componente básico propuestos en el diseño, se pueden apreciar en la figura, los cuales son cámara de red, Internet, servidor de almacenamiento, codificación y gestión de video, y los usuarios, que pueden acceder a este video generado a través de Internet.

Como se puede apreciar, el modelo de diseño general, se divide en dos partes de seguridad, por un lado está la en las cámaras de Tele Vigilancia, es decir, la seguridad que debería haber desde las cámaras hacia el servidor de Streaming, por otro lado, se encuentra la seguridad de la comunicación que existe desde el servidor, hacia la visualización del usuario final, el cual se conecta por medio de la red de Internet, para poder visualizar el contenido generado por las cámaras de Tele Vigilancia.

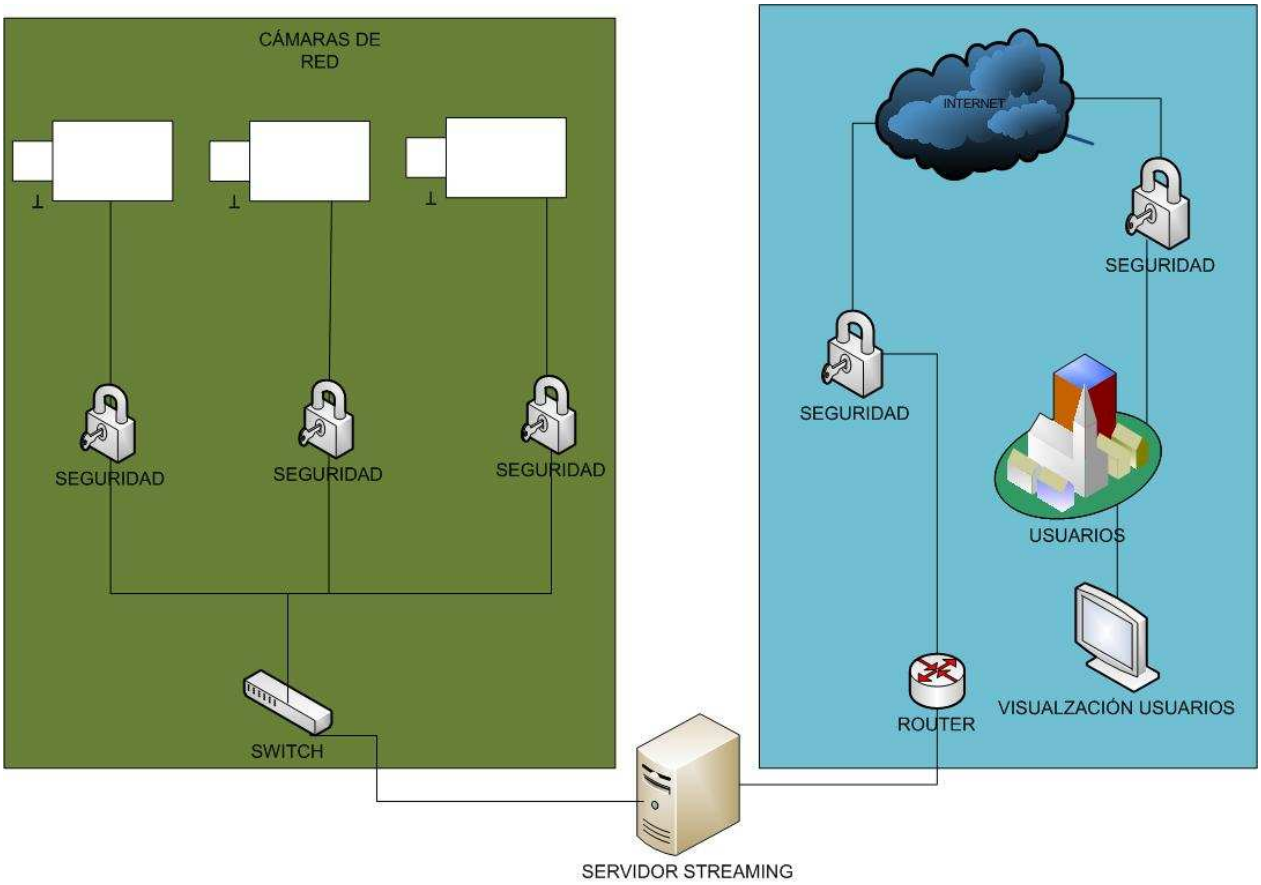

Figura 22 – Áreas de Aplicación de Seguridad.

A continuación se muestran las distintas tecnologías de seguridad aplicadas a las dos áreas que aborda esta propuesta.

5.2 Comunicación Cámara - Servidor

Para mantener la seguridad de comunicación desde las cámaras de red hacia el servidor de Streaming, es necesario considerar también algunos aspectos de seguridad.

Como los dispositivos están dentro del mismo espacio físico, se propone utilizar una VLAN y Filtrado de Direcciones IP.

Al diseñar un sistema de Tele Vigilancia, es necesario mantener las redes separadas por motivos de seguridad. Por lo que, la elección obvia sería construir una red independiente como una red virtual de área local (VLAN). Es por esto, que se han divido los usuarios en grupos segmentados, con el fin de de que las cámaras estén y se comuniquen de forma independiente, respecto a otras conexiones que puedan haber en el ambiente de desarrollo.

Esto se evidencia en la siguiente figura.

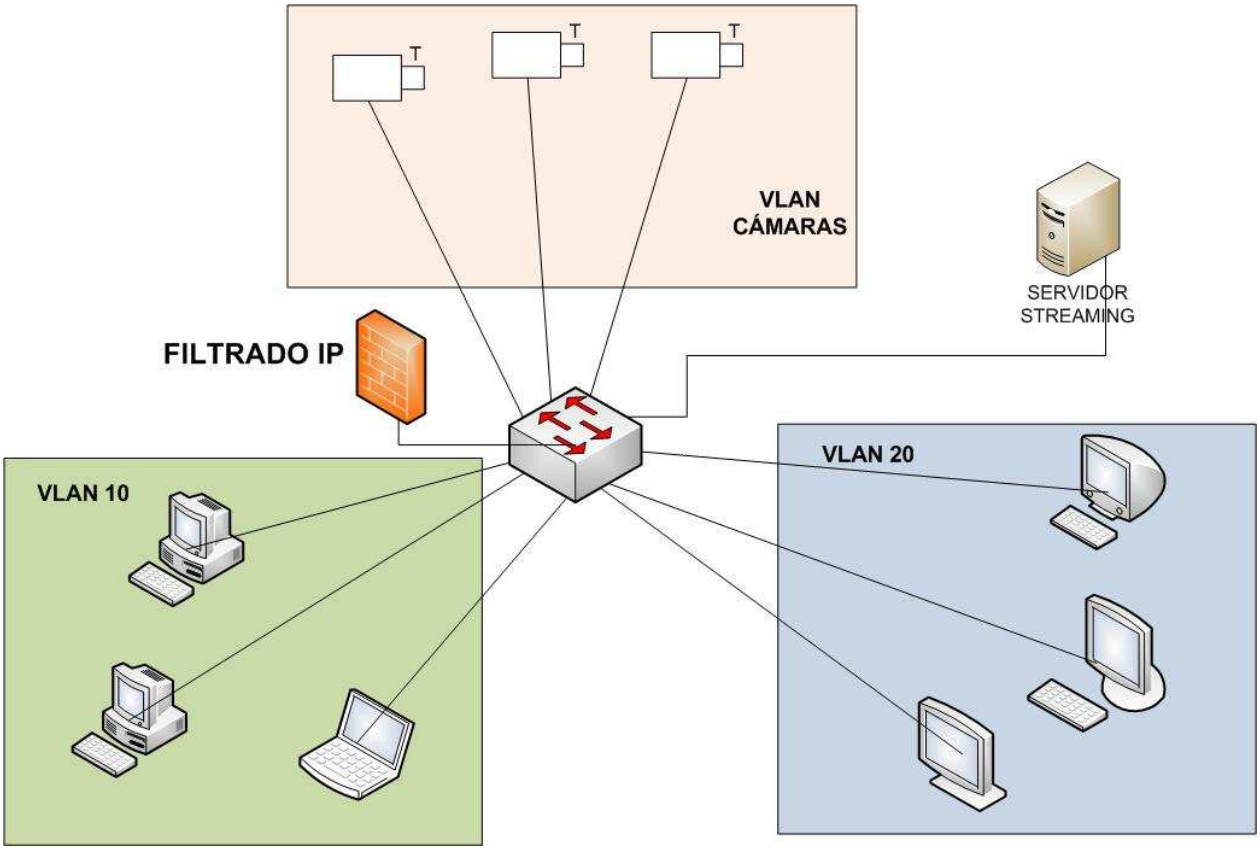

Figura 23 – Mecanismos de Seguridad Aplicados en Comunicación Servidor – Cámaras Red.

Si existe la posibilidad de acceder a la VLAN de las cámaras de red, se ha propuesto utilizar filtrado Ip, para así evitar que otras Ip puedan acceder hacia las cámaras y servidor streaming. Por ello definir las direcciones Ip previamente en cada uno de los dispositivos, será de vital importancia en la seguridad de la transmisión de contenido, entre las cámaras de red y el servidor streaming. A continuación se muestra la figura de representación de filtrado Ip.

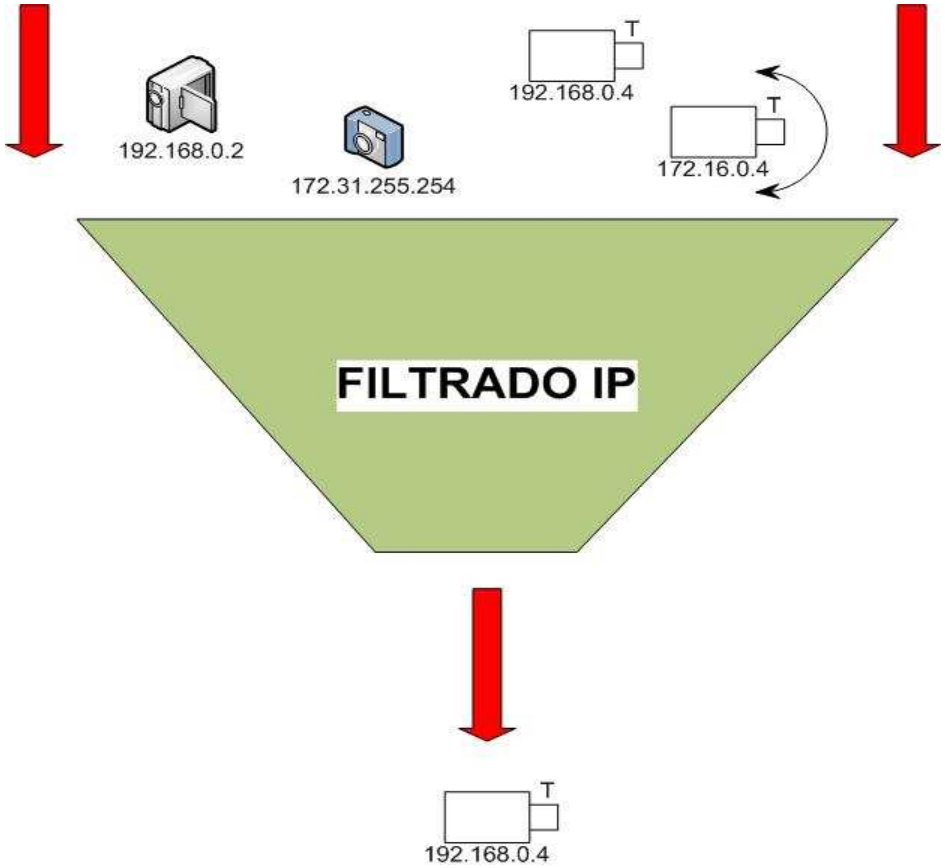

Figura 24 – Filtrado IP Aplicados en Comunicación Servidor – Cámaras Red.

5.3 Comunicación Servidor - Usuario

Para la comunicación entre, el servidor y el usuario final del sistema, se propone la siguiente estructura.

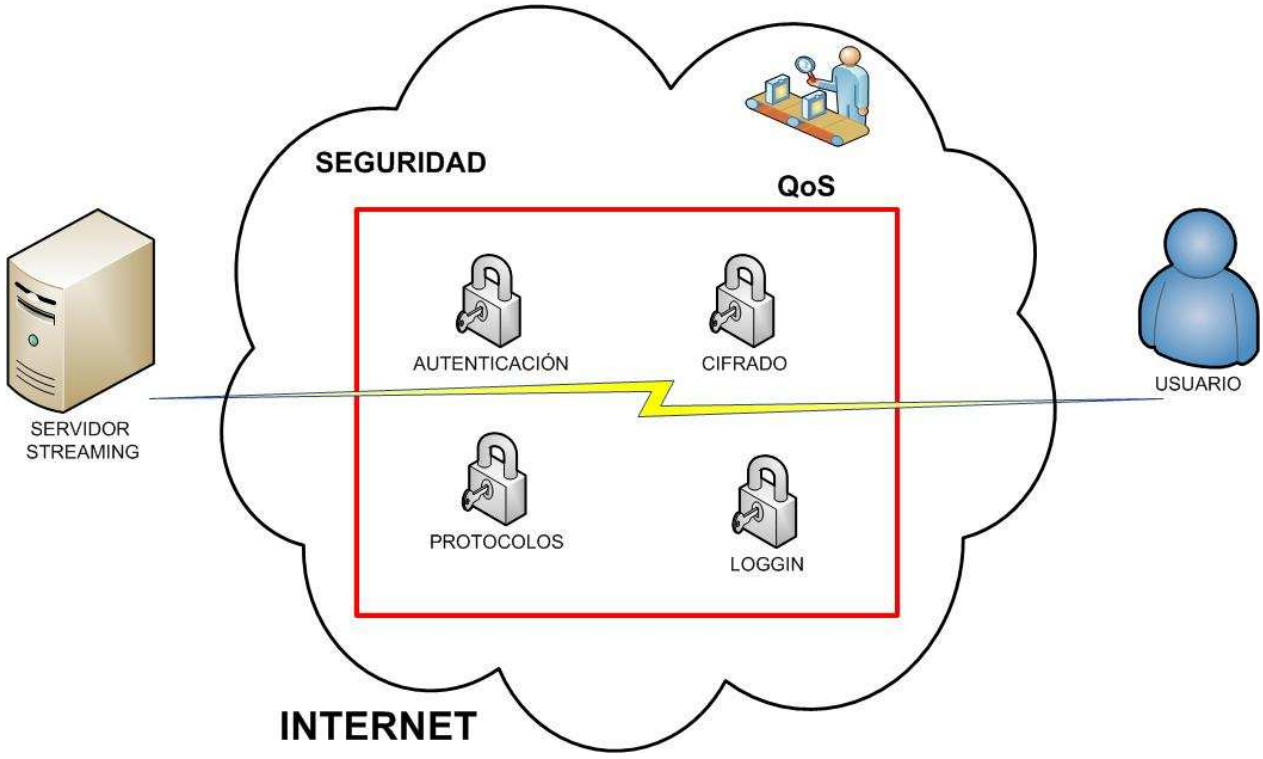

Figura 25 – Mecanismo de Seguridad Aplicados en Comunicación Servidor - Usuario.

En la figura, se aprecian distintos mecanismos, a distintos niveles de seguridad, que pueden ser aplicados en la transmisión de video streaming a través de la red, los cuales serán abordados en los capítulos siguientes.

El proceso propuesto de comunicación segura, se muestra en la siguiente figura.

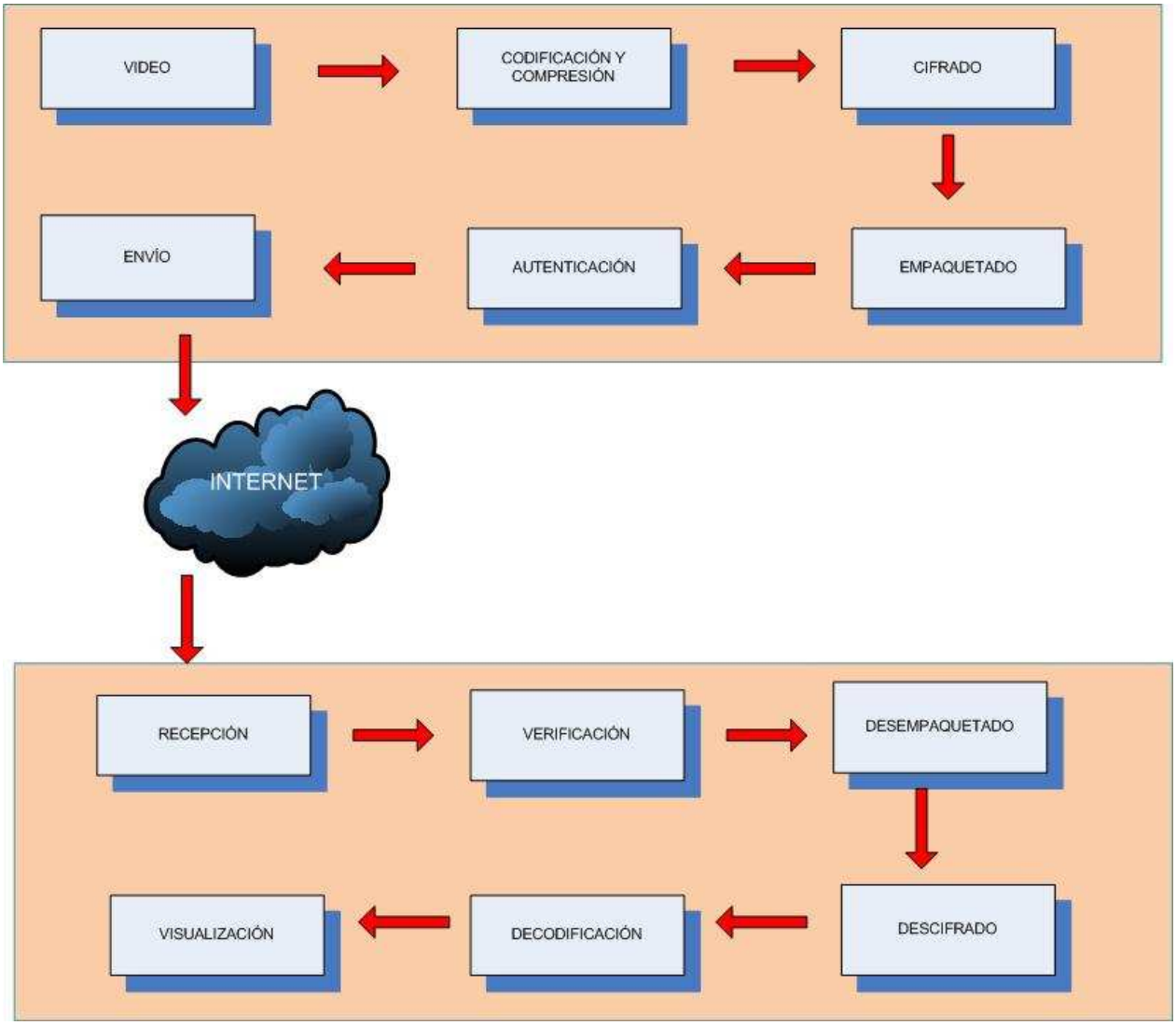

Figura 26 – Proceso de Transmisión de video Streaming Seguro.

Para cualquier sistema seguro, es necesario considerar cuatro criterios importantes y relevantes a la hora de aplicar y utilizar técnicas de seguridad, los cuales son los siguientes:

- **Confidencialidad o Privacidad:** Los datos que son transmitidos a través del sistema, deben estar disponibles solo para las personas autorizadas.
- **Confiabilidad o integridad:** Los datos transferidos no se deben poder cambiar entre el remitente y el receptor.
- **Disponibilidad:** Los datos transferidos deben estar disponibles cuando son necesarios.
- **No Repudio:** Para evitar que una vez firmado un documento el emisor se retracte o niegue haberlo redactado.

Para cumplir estas condiciones en el diseño propuesto, los paquetes IP que se desean transmitir, realizan los siguientes aspectos:

- Se cifran para garantizar la confidencialidad.
- Se firman para garantizar la autenticidad, integridad y no repudio.

El paquete resultante se encapsula en un nuevo paquete IP y se envía a través de la red insegura al otro extremo de la comunicación.

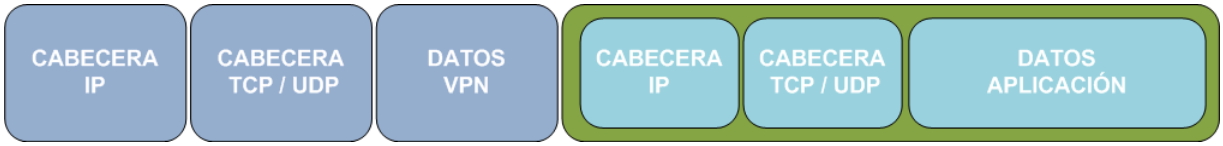

Figura 27 – Encapsulación.

La comunicación entre los dispositivos del diseño de red, se puede lograr a través de la autenticación mutua. La autenticación mutua se visualiza por el intercambio y la verificación de los certificados, que son emitidos por una cierta entidad de certificados CA.

Una vez establecida esta red segura, todos los paquetes se alistan para ser empaquetados en el protocolo elegido para la transmisión, en este caso RTP y otros, el cual lleva el contenido protegido o no protegido, luego debe ser autenticado antes de la transmisión, utilizando un algoritmo de firma digital y la clave privada del emisor .

La firma y un identificador de la transmisión, es decir, un identificador de flujo único global (StreamId), se adjuntan al final de un paquete RTP como un código de autenticación. Aquí, el StreamId es asignado por un certificado de un emisor en particular de la red cuando una sesión de RTP está establecida y que el emisor ha enviado su certificado. Por lo tanto, un StreamId específico es asociado con un certificado de un emisor en particular (en comparación con CertID de un certificado, StreamId es mucho más compacto).

Cuando un paquete RTP llega a un proxy a través de la red, es verificado en el proxy de la red, chequeando si se encuentra el certificado del emisor, indicado por la etiqueta de autenticación, y luego revisar la firma del paquete de RTP con la clave pública del emisor. Si el certificado no se encuentra o falla la verificación, el paquete de RTP será descartado de inmediato. Si la firma es válida, el Host u Proxy decidirá si aprobar en el paquete, mediante la realización de un algoritmo de adaptación de los medios de comunicación. Por lo tanto, los paquetes de RTP con firma falsa o no, tienen ninguna posibilidad de ser transmitidos en la red segura.

Se describen a manera general, los procesos propuestos para una comunicación segura.

- **Codificación:** codificar un flujo de medios de comunicación de una alta tasa de bits a una baja tasa de bits, para satisfacer la restricción de acceso de ancho de banda de un receptor determinado. Este proceso se realiza mediante la eliminación de algunas tramas consideradas como menos importantes según el medio de comunicación, por ejemplo, eliminar marcos P en el flujo de bits. Dado que el flujo de bits, es en video plano, en esta fase, el salto de imágenes es una tarea fácil. Por ello como se ha mencionado anteriormente la codificación y compresión de video con el estándar h.264 será utilizado en esta etapa.
- **Cifrado**: cifrar cada cuadro o algunos fotogramas de la secuencia de bits utilizando un cifrado de flujo o un sistema de cifrado de bloque en modo CTR, AES en modo CTR, con una clave simétrica. Por ello mas detalles de la utilización de AES pueden verse el apartado correspondiente.
- **Empaquetado:** Un marco de medios encriptados, así como información estructural importante en uno o más paquetes RTP utilizando las reglas de empaquetado correspondientes y normas del protocolo correspondiente.
- **Autenticación:** signo de la carga útil de RTP, utilizando un algoritmo de firma digital, en este caso ECDSA, con la clave privada del emisor y luego, añadir la etiqueta de autenticación, es decir, la firma y el StreamId, al final del paquete RTP. Sólo autenticar la carga útil de un paquete de RTP, ya que el encabezado de RTP podría ser modificado durante la transmisión y sólo se quiere garantizar la autenticidad de los medios de comunicación en sí. La autenticación de la carga útil en RTP, la integridad de la información sin encriptación es factible, y cualquier manipulación de las operaciones realizadas a la información sin encriptar, puede ser detectada por la verificación de la firma.
- **Verificación:** verificar la firma de un paquete RTP utilizando el mismo algoritmo de firma digital utilizada por el emisor, con la clave pública del emisor en su certificado digital. Mediante la verificación de la firma, tanto la integridad y la autenticidad del emisor de la carga útil de RTP se puede garantizar.
- **Desempaquetado**: desempaquetar un paquete RTP de acuerdo al empaquetado correspondiente. Dado que el paquete de RTP provee autenticidad, en este paquete RTP se puede confiar y la etiqueta de autenticación puede ser simplemente ignorada.
- **Descifrado:** descifrar el contenido mediante el cifrado de flujo original o cifrado de bloque en el modo CTR y la misma clave que utiliza el proceso de cifrado. Preferiblemente, el descifrado se hace sólo por el receptor de destino, de la información trasmitida como lo exige el requisito del diseño para la seguridad final.
- **Decodificación:** Decodificar un flujo de comunicación de una baja tasa de bits a una alta tasa de bits de acuerdo a la información enviada por las cámaras.

Un objetivo importante del diseño de transmisión seguro, es establecer una red segura a través de Internet. Esta red de seguridad, se compone de distintos aspectos de seguridad, que pueden ser visualizados a través de la figura 25. Es por ello que a continuación se explica cada uno de estos bloques.

5.3.1 Video

El primer paso del proceso de transmisión de video streaming seguro, comienza con la emisión de video por medio de las cámaras IP, luego el video transmitido es enviado al siguiente proceso de codificación y compresión realizado por el servidor streaming, cuyo paso será explicado en el capítulo correspondiente.

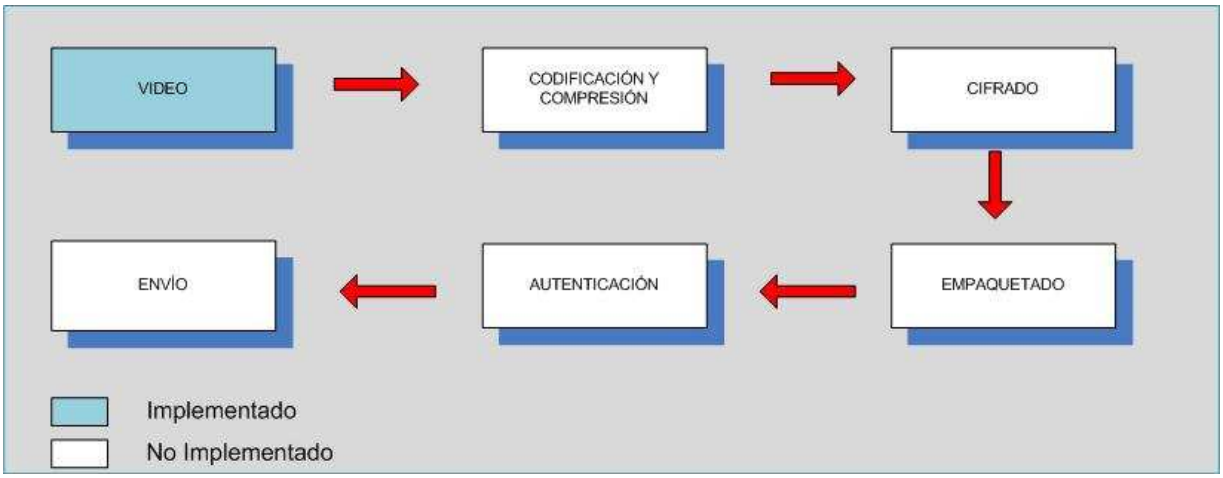

Figura 28 – Video.

5.3.1.1 Cámaras de Red

Los criterios mínimos y necesarios para este modelo, se muestran en la siguiente tabla.

Tabla 14 – Aspectos Relevantes.

Ítem	Característica Técnica
Sensor de Imagen	• CMOS • Barrido progresivo de 1/3” • 1.3 megapíxel
Objetivo	• De 2.7 mm / F de 1.0 • Iris fijo o DC • Auto foco
Día/ Noche	• Configurable
Sensibilidad Lumínica (Lux)	• De 4 a 10000 • color
Compresión de Video	• H.264
Resolución Máxima de video (Pixeles)	• 640 x 480
Imágenes por Segundo	30 (640 x 480)
Pan/Tilt/Zoom	• Posiciones predefinidas
Entradas / Salidas	1 o varias
Seguridad	• Contraseña multinivel • Filtro de direcciones ip • Cifrado HTTPS
Red	• IPv4 • IPv6 • Q&S
POOE	• Disponible clase 1 a 3 • C/S calentador
otros	• IEEE inalámbrica 802.11 b/g • Uso interior exterior • Certificación IP66 • Auto slip • Visibilidad Nocturna

Puede apreciarse simple el modelo, sin embargo con integración de las cámaras de Tele Vigilancia de red, que proveen el formato de video H.264, generan un ahorro de codificación del video a través del servidor de Streaming.

5.3.2 Codificación y Compresión

Como se había explicado anteriormente, la tecnología Streaming funciona de la manera más simple y de bajo consumo de ancho de banda, para visualizar video desde un sitio Web o de otro medio de visualización. Para este método no es necesario ningún tipo especial de página Web, pero si alguna aplicación, para poder visualizar el contenido de acuerdo a los códecs adecuados, según la plataforma seleccionada para su utilización.

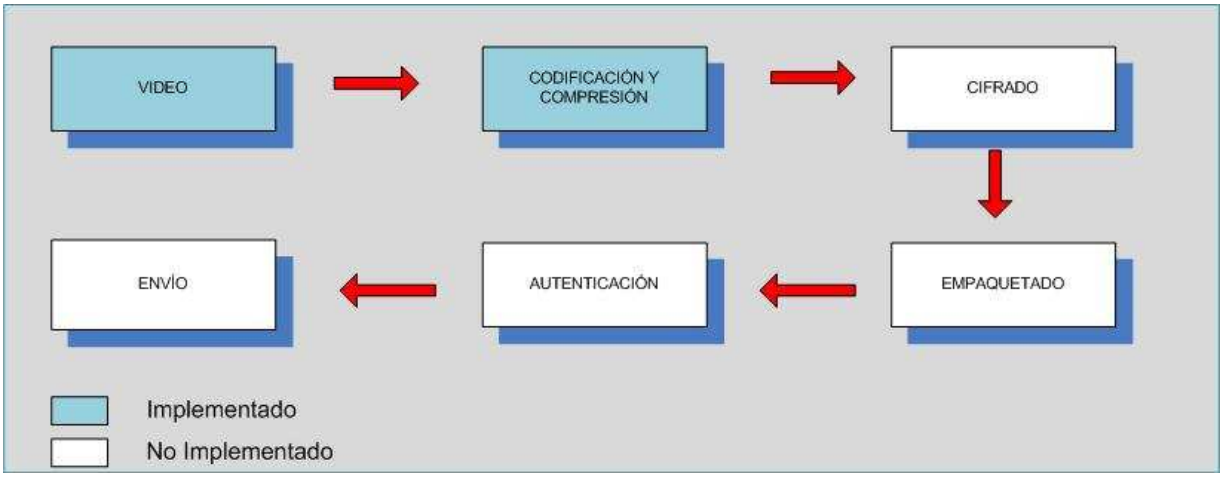

Figura 29 – Codificación y Compresión.

5.3.2.1.1 Funcionamiento

El funcionamiento para poder administrar archivos a través de la tecnología Streaming, se puede visualizar de manera más amplia en la siguiente figura.

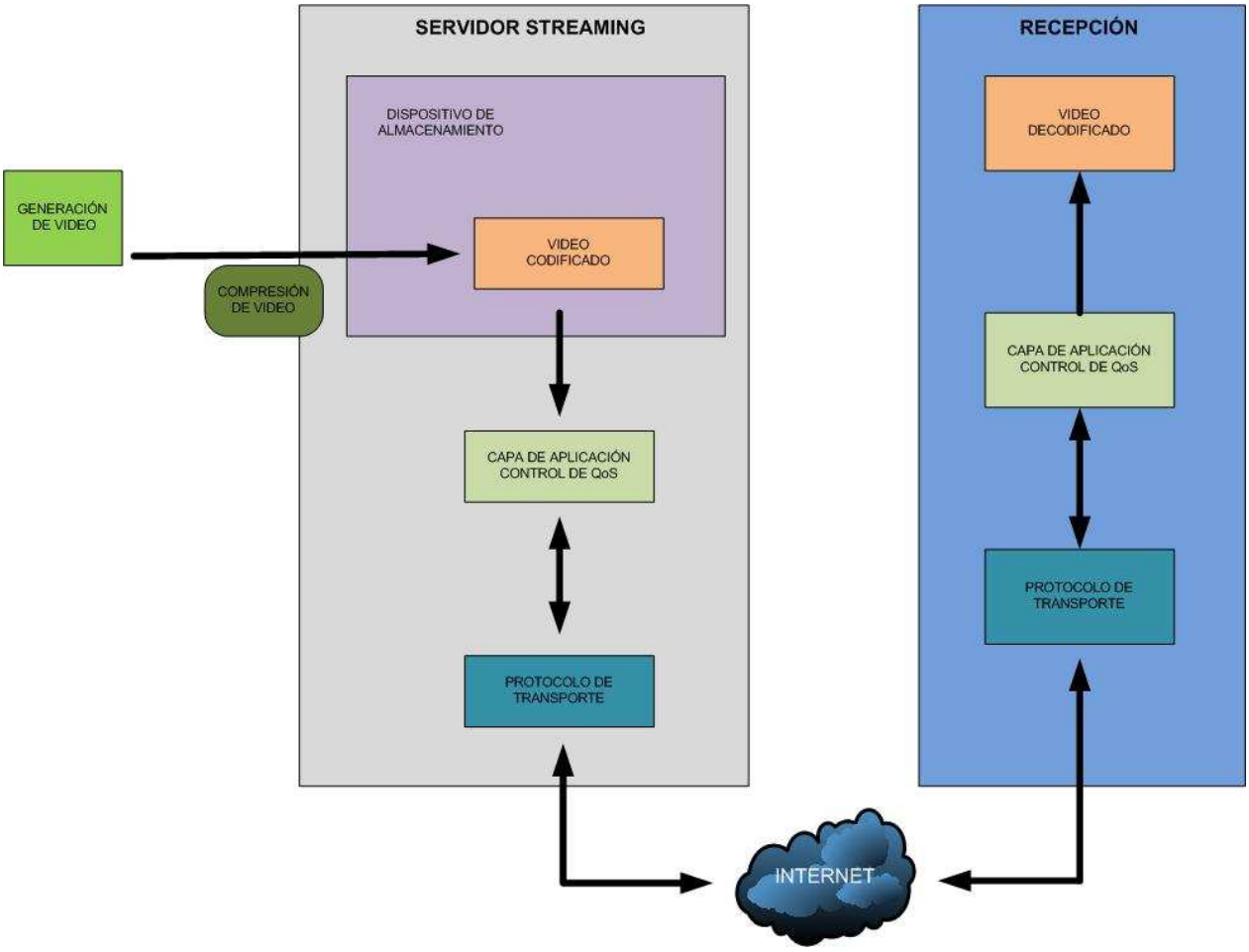

Figura 30 – Proceso de Funcionamiento Streaming.

Para poder clarificar como es el proceso de Streaming dentro del servidor, se visualiza en la siguiente figura.

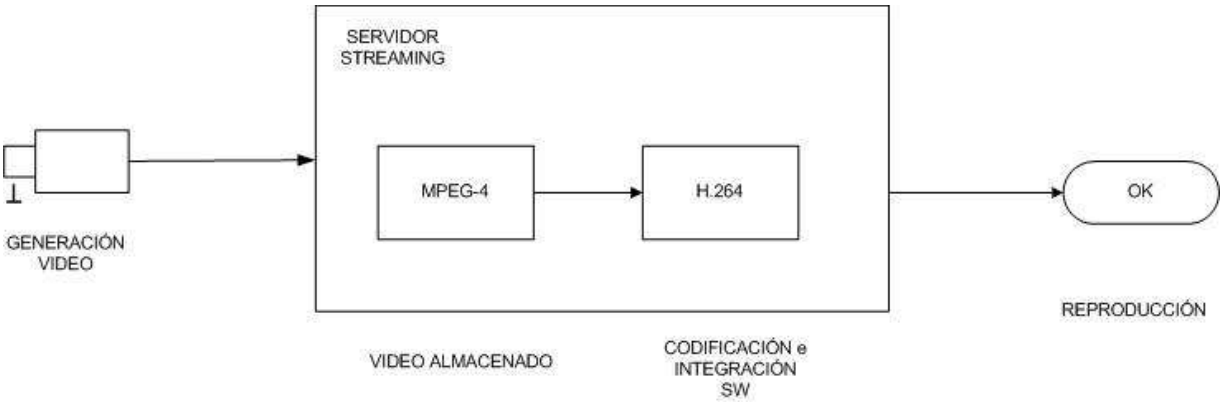

Figura 31 – Proceso Video Streaming Servidor.

5.3.3 Cifrado

Dentro de los distintos tipos de cifrados para la aplicación de streaming video, utilizando la compresión h.264, se ha optado por la utilización por AES, conocido también como Rijndael, cuya elección se baso básicamente por su estabilidad y fiabilidad respecto a otros algoritmos de cifrado como TwoFish, RC6, entre otros. Por ello que la siguiente figura muestra el proceso de cifrado de un contenido de video.

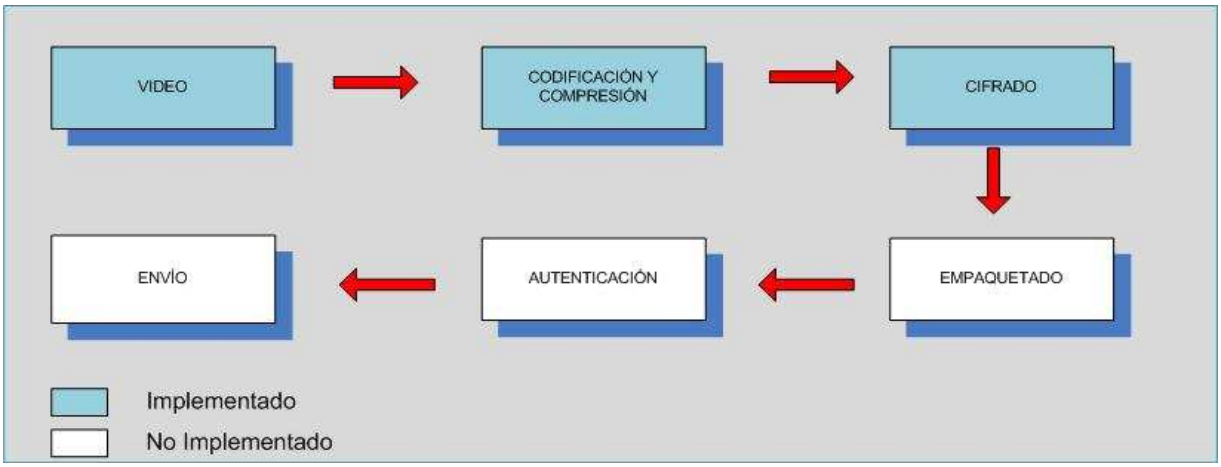

Figura 32 – Cifrado.

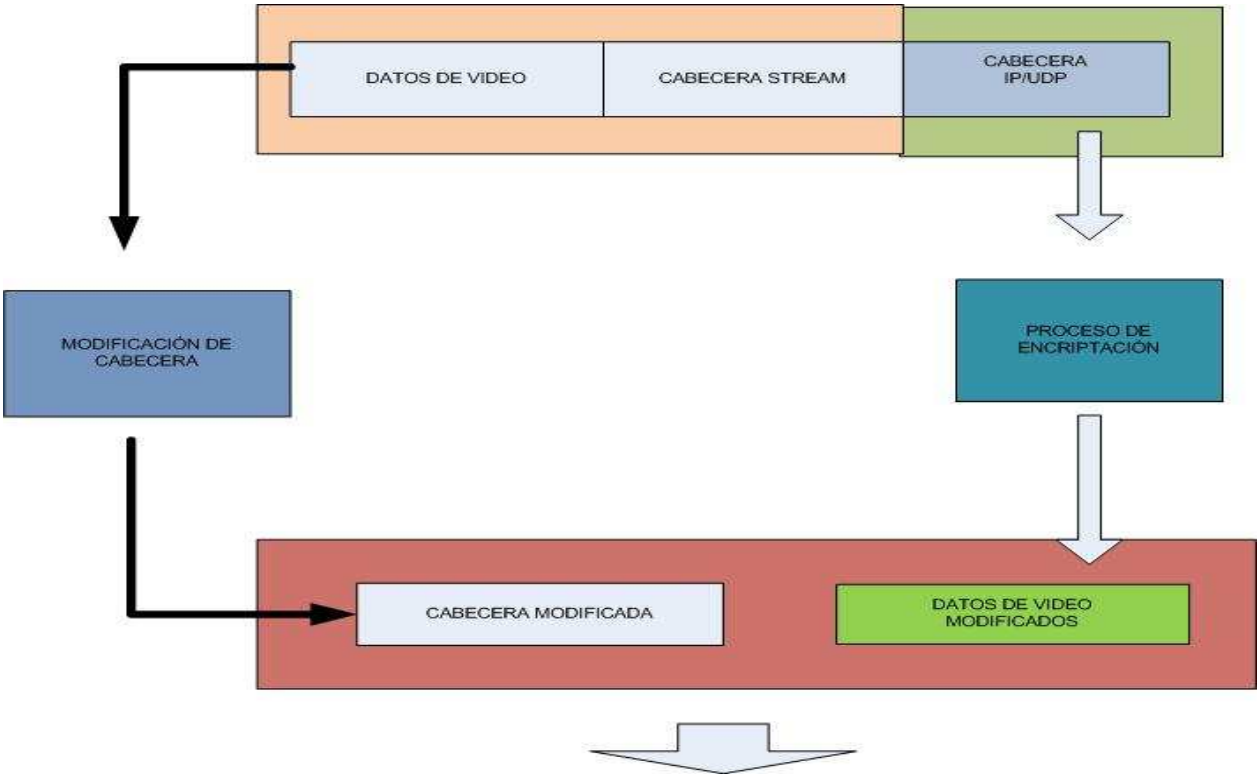

Figura 33 – Proceso General de Cifrado.

Este es un esquema de cifrado de bloques adoptado por un estándar de cifrado llamado AES, siendo uno de los algoritmos más populares de cifrado usados en criptografía. Se caracteriza por ser de dominio público, simétrico y soporta bloques, como mínimo de 128 bits, con calve de cifrado de hasta 256 bits implementable tanto en hardware como software [29].

Su cifrado consta de tres etapas cruciales, una etapa inicial, rondas y una etapa final, cada una de las cuales con sus fases correspondientes, que se pueden apreciar en la siguiente figura.

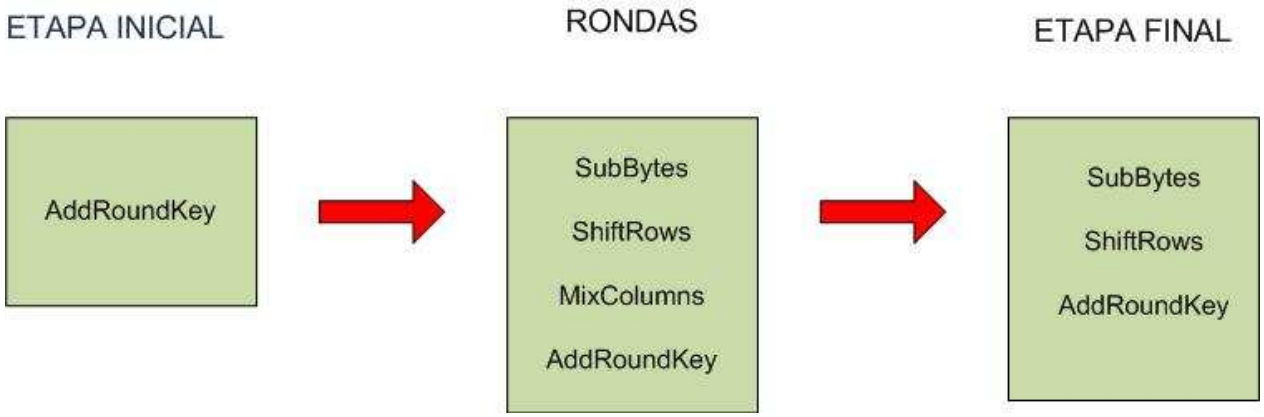

Figura 34 – Etapas Cifrado AES.

A continuación se explica cada una de las etapas correspondientes al cifrado del algoritmo AES.

5.3.3.1 Etapa de SubBytes o Substitución de Bytes

En esta etapa cada byte en la matriz es actualizado usando la caja-S de Rijindel de 8 bits. Esta operación provee la no linealidad en el cifrado. La caja-S utilizada proviene de la función Inversa alrededor del Gf, conocido por tener grandes propiedades de no linealidad. Para evitar ataques basados en simples propiedades algebraicas, la caja-S se construye por la combinación de la función inversa con una transformación afín invertible. La caja-S también se elige para evitar puntos estables y también cualquier punto estable opuestos. Se aprecia en la siguiente figura.

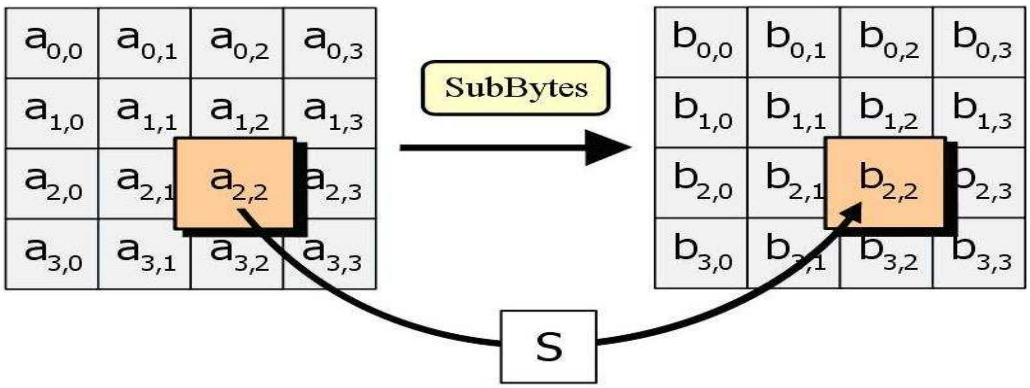

Figura 35 – Etapa SubBytes o Substitución de Bytes.

5.3.3.2 Etapa ShiftRows o Desplazar Filas

El paso `ShiftRows` opera en las filas del state, rota de manera cíclica los bytes en cada fila por un determinado offset. En AES, la primera fila queda en la misma posición. Cada byte de la segunda fila es rotado una posición a la izquierda. De manera similar, la tercera y cuarta filas son rotadas por los offsets de dos y tres respectivamente. De esta manera, cada columna del state resultante del paso `ShiftRows` está compuesta por bytes de cada columna del state inicial. Se aprecia en la siguiente figura.

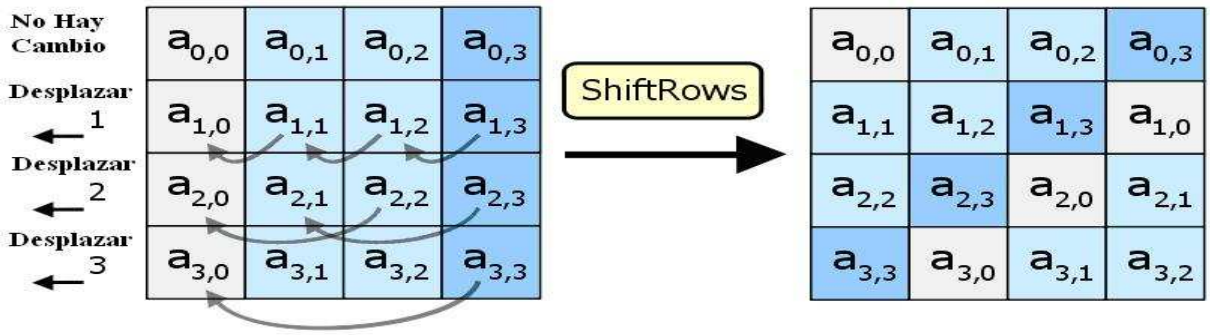

Figura 36 – Etapa ShiftRows o Desplazar Filas.

5.3.3.3 Etapa MixColumns o Mezclar Columnas

En el paso `MixColumns`, los cuatro bytes de cada columna del state se combinan usando una transformación lineal invertible. La función `MixColumns` toma cuatro bytes como entrada y devuelve cuatro bytes, donde cada byte de entrada influye todas las salidas de cuatro bytes. Junto con `ShiftRows`, `MixColumns` implica difusión en el cifrado. Se aprecia en la siguiente figura.

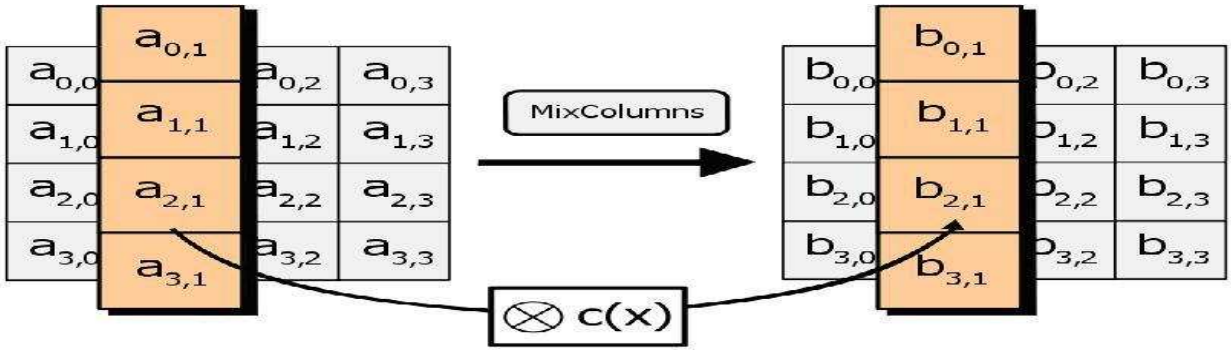

Figura 37 – Etapa MixColumns o Mezclar Columnas.

5.3.3.4 Etapa AddRounKey o Cálculo de las Subclaves

En el paso AddRoundKey, la subclave se combina con el state. En cada ronda se obtiene una subclave de la clave principal, usando la iteración de la clave; cada subclave es del mismo tamaño del state. La subclave se agrega combinando cada byte del state con el correspondiente byte de la subclave usando XOR. Se aprecia en la siguiente figura.

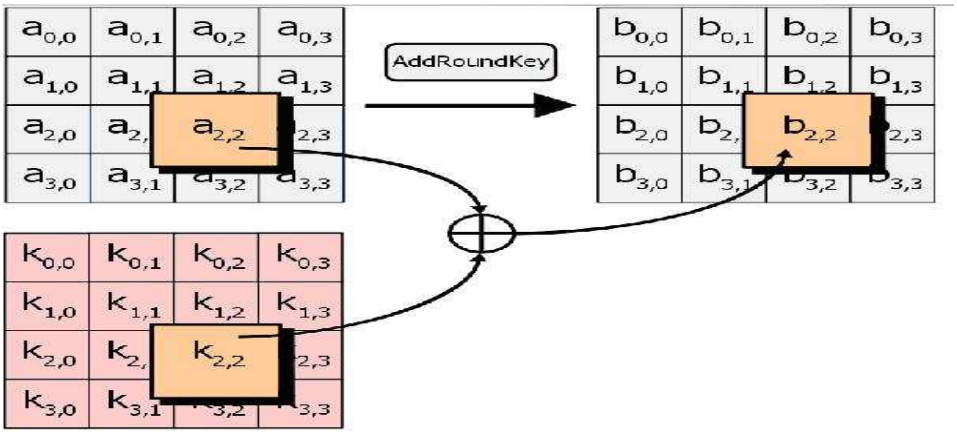

Figura 38 – Etapa AddRounKey o Cálculo de las Subclaves.

Para complementar las fases anteriormente descritas se sintetiza el proceso de cifrado en la siguiente arquitectura.

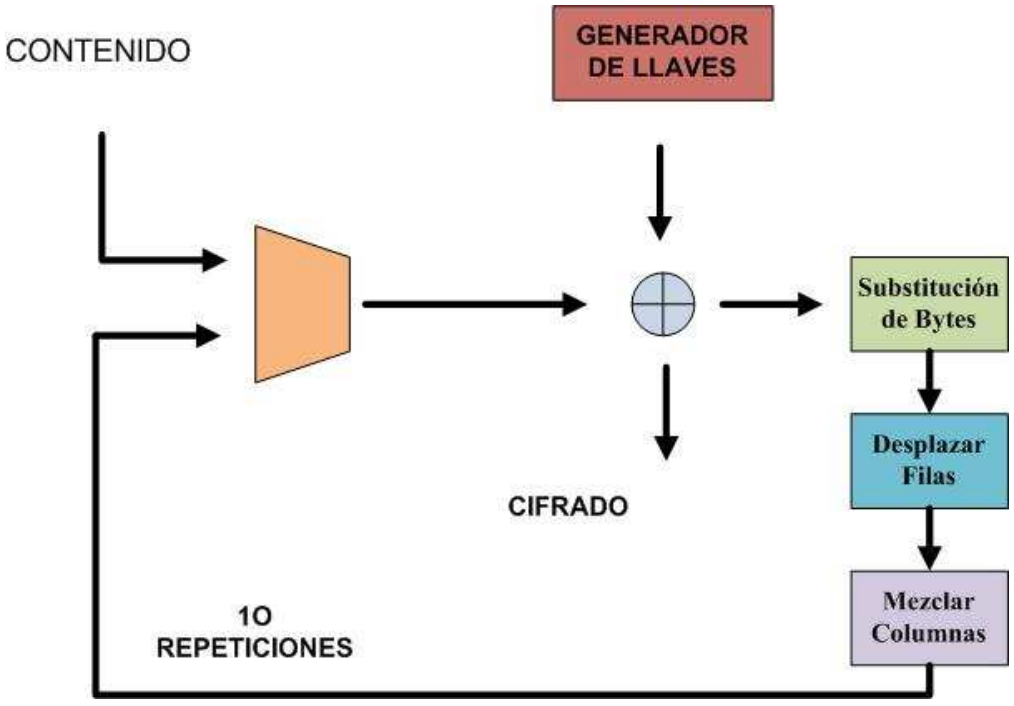

Figura 39 – Proceso Cifrado AES.

5.3.4 Empaquetado

En este proceso, se han utilizado algunos protocolos que están en la dirección de proveer una buena calidad de servicio, con el fin de obtener una fluidez de transmisión, menor retardo de la visualización y mejor calidad de imagen.

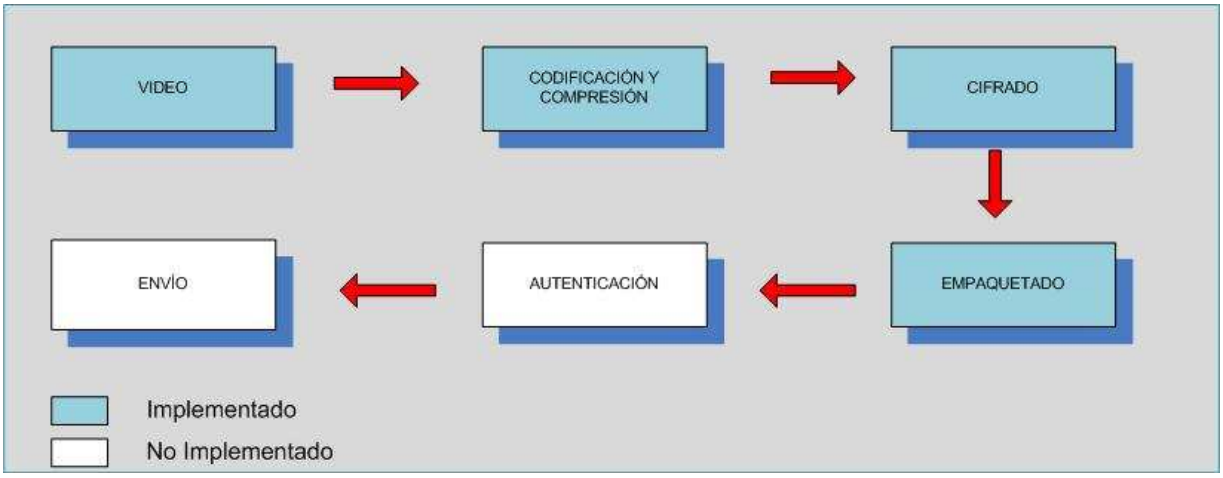

Figura 40 – Empaquetado.

En la siguiente imagen, se muestran los protocolos utilizados en la implementación del diseño de esta propuesta.

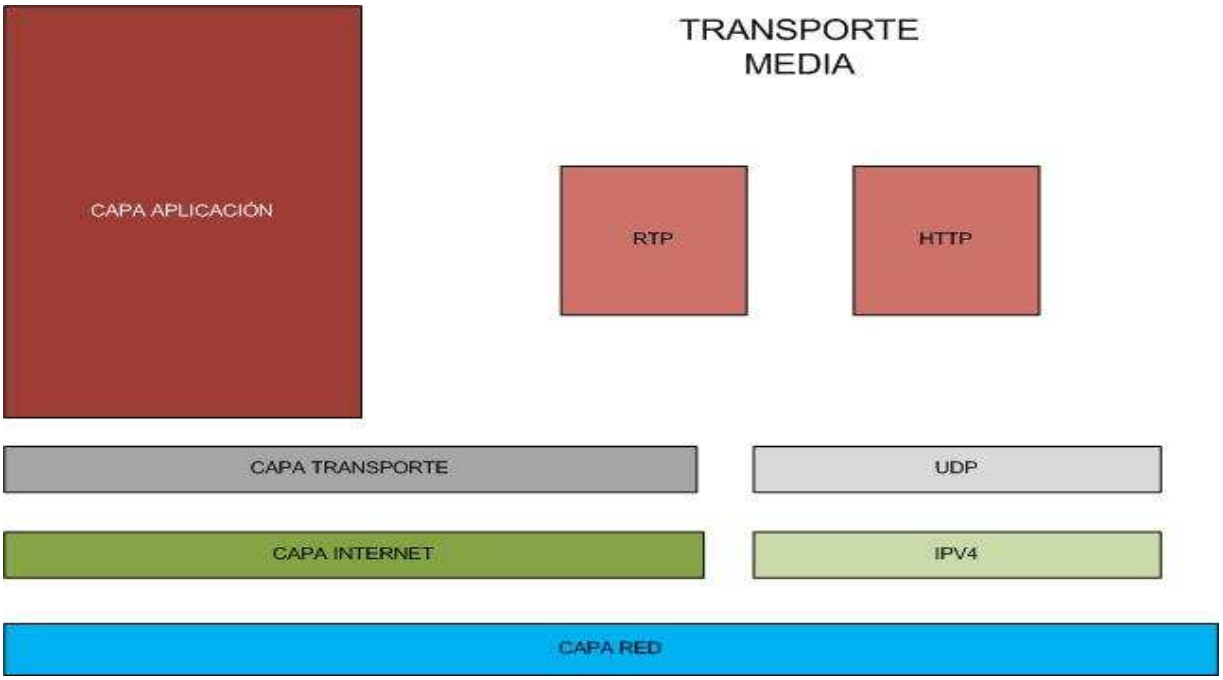

Figura 41 – Aplicación de Empaquetado.

Se ha utilizado en la capa de Internet Ipv4, con el fin de estandarizar y utilizar este protocolo que actualmente es el más utilizado en las aplicaciones multimedia. En la capa de transporte para prevalecer una transmisión fluida y con el menor tiempo de retardo, es que se hace indispensable utilizar el protocolo UDP que provee y es el más utilizado, en las transmisiones multimedia. Para finalizar en la capa de aplicación de han utilizado dos protocolos con el fin de poder realizar prueba y poder evidenciar comparaciones, que demuestran que RTP y RTSP tienen mejores prestaciones que HTTP.

5.3.5 Autenticación

En el sentido de que la autenticación del emisor debe hacerse utilizando por ejemplo medios criptográficos, sin embargo evidencian que en lugar de utilizar nuevas técnicas o protocolos, que son poco sofisticados para abordar la problemática de la autenticación del emisor en los medios de transmisión, es necesario utilizar otras herramientas de seguridad. Sin embargo, la autenticación del emisor es muy crítica para la seguridad de los medios de transmisión. Sin autenticación del emisor, los usuarios puedan estar en peligro por el riesgo de robo del contenido transmitido, que sin duda perjudica los derechos e intereses de todos los usuarios que utilicen el sistema.

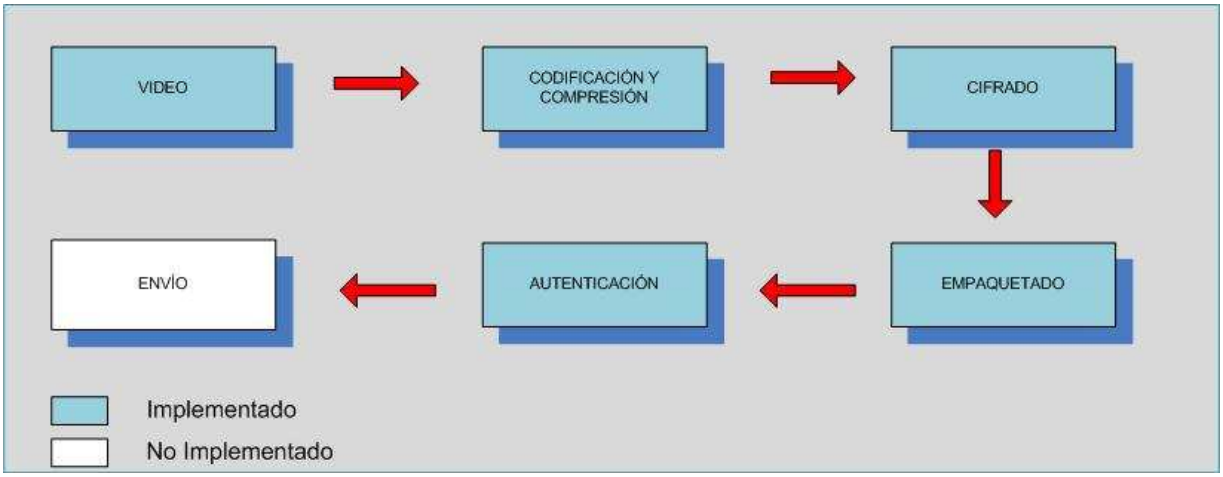

Figura 42 – Autenticación.

Obviamente, mediante el uso de firma digital, la autenticación del emisor se puede lograr, así como la integridad del contenido. La razón de que las técnicas de firma digital no se utilicen o sean elegidas para la autenticación del emisor, es debido principalmente a su alto costo computacional. Sin embargo, se han logrado grandes avances en los últimos años en la informática y transmisión de datos [51].

Debido a su seguridad intrínseca, la utilización de criptografía con clave pública está ganando más y más aplicaciones. Un tema interesante es la criptografía de curvas elípticas ECC que destaca por su alta seguridad y rapidez. Con un módulo de 160 bits, el sistema de curva elíptica ofrece el mismo nivel de seguridad de cifrado que RSA o DSA como con

módulos de 1024 bits. Con pequeño tamaño de las llaves tiene como finalidad pequeño parámetros de sistema, pequeños certificados de clave pública, ahorros de ancho de banda, implementaciones más rápidas, menor consumo de energía y la utilización de procesadores más pequeños de hardware. Por lo tanto, se han aprovechado los algoritmos de firma digital de ECC para cumplir la tarea de la autenticación del emisor en los medios de transmisión segura del sistema propuesto. Además, para las funciones hash se utilizará un algoritmo de cifrado hash seguro como el SHA-1 y un algoritmo asimétrico RSA 2048 bits. Esta propuesta se aprecia en la siguiente figura [52].

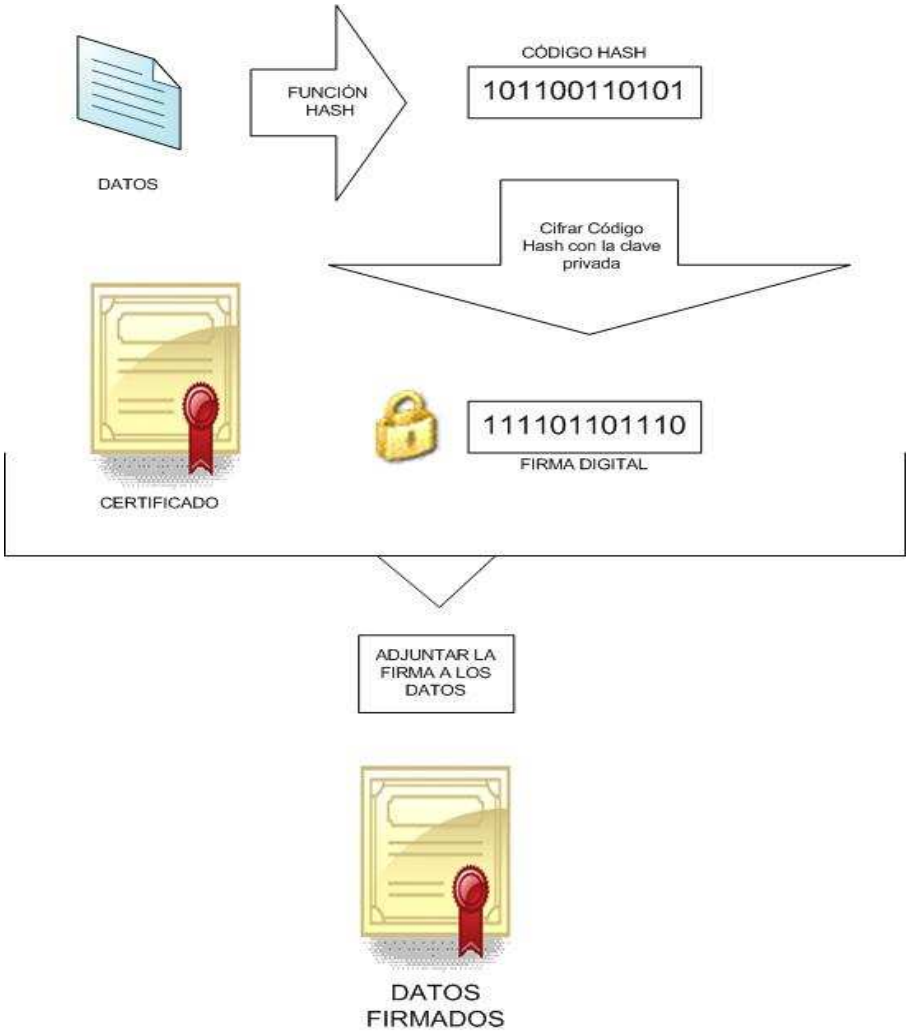

Figura 43 – Firma Digital para Video.

Dese el servidor PfSense se manejan y gestionan las comunicaciones seguras. Además para cada usuario se han creado el certificado digital que sea necesario. Una vez concluida la firma digital, el proceso siguiente es comprobar si esta firma digital corresponde a quien dice ser y esto se verifica de la siguiente manera.

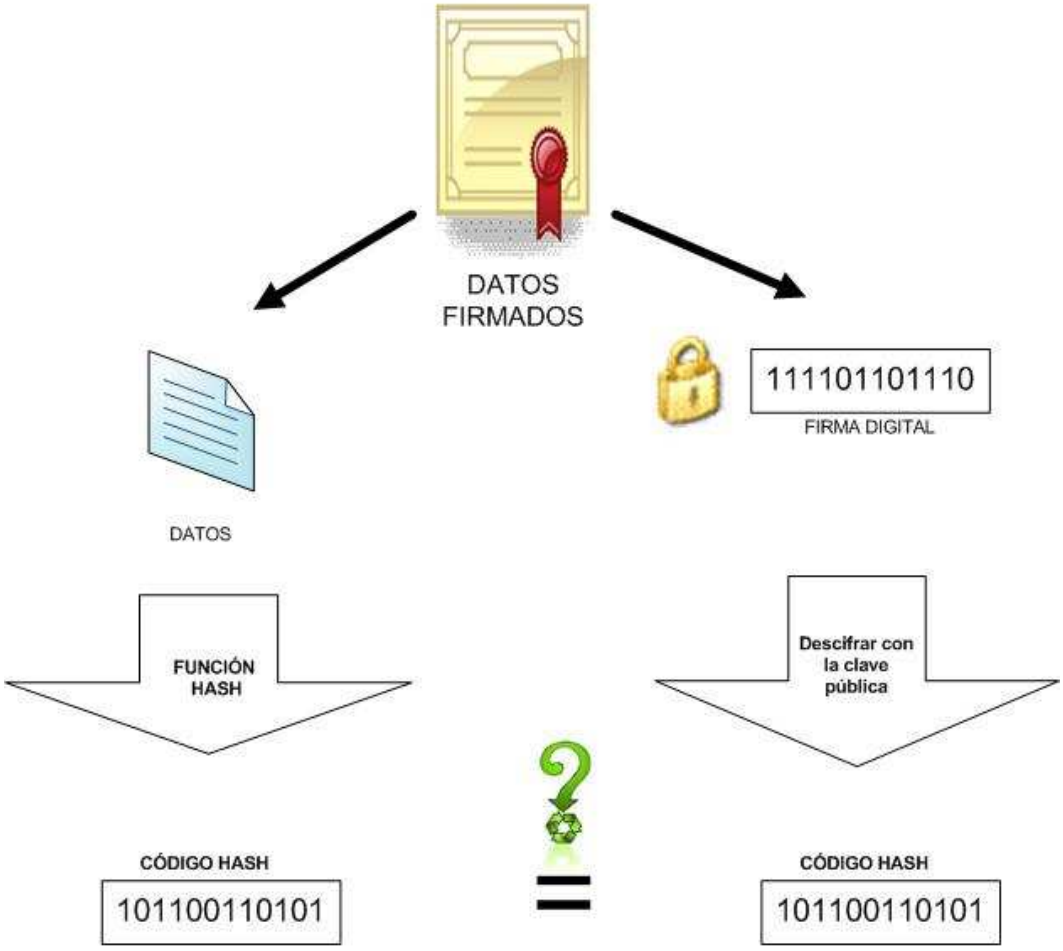

Figura 44 – Verificación Firma Digital.

Por lo tanto, la firma digital sería utilizada en el acceso de identificación y autenticación de usuarios, por la versatilidad y el grado de efectividad que tienen estos métodos de autentificación.

5.3.6 Envío y QoS

Es difícil para los medios de transmisión de contenido, a través de Internet, ofrecer garantías de calidad de servicio debido a que los requisitos de ancho de banda de los servicios de transmisión de contenido, no se puede garantizar, debido a muchas variables, en el tiempo de transmisión a través de Internet.

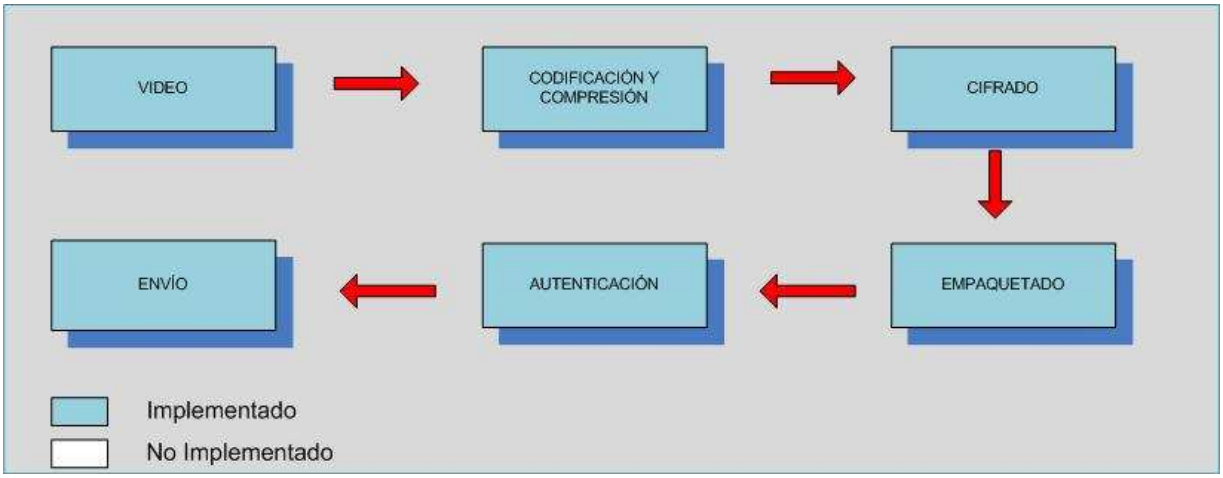

Figura 45 – Envío.

La mayoría de los routers tienen QoS habilitado, pero no se utiliza en absoluto. La razón es que en los routers no se puede establecer la prioridad del tráfico. Sin embargo, para este diseño, se complica permitir una calidad de servicio a través de la red de Internet, frente a ellos, la prioridad de calidad de servicio esta concentrada desde la transmisión de las cámaras hacia el servidor de streaming, por lo tanto, el ancho de banda dedicado, como se dijo anteriormente estará circunscrito entre un 20% y 40% del ancho de banda disponible.

Además, la utilización de algoritmos de cifrado adecuados y protocolos que ayuden a la transmisión de video en tiempo real, utilizando la tecnología streaming, ayudarán a que la transmisión de contenido desde el servidor hacia el usuario pueda ser un éxito.

Pero se podría considerar además, los mecanismos de calidad de servicio adoptados en la comunicación y transmisión de contenido multimedia, desde el servidor y cámaras de red, y viceversa. Para mejorar además los tiempos, es que se ha implementado una VLAN como medida para dar una mejor QoS.

Para mejorar la transmisión de Video se utilizará una técnica denominada “Traffic Shaping” o conocida como catalogación de tráfico, a través de un servidor que otorgue dicha característica. Esta técnica intenta controlar el tráfico en las redes con el fin de optimizar o garantizar un rendimiento, baja latencia y/o un ancho de banda determinado priorizando o catalogando los paquetes que serán transmitidos. Esta técnica utiliza varios criterios como clasificación, colas, imposición de políticas, administración de congestión, calidad de servicio y regulación.

Por ello que esta técnica se convierte en una buena práctica para mejorar la capacidad de servicio en la transmisión de video. Además, esta técnica es utilizada en varios sistemas y plataformas que necesitan proveer buenos servicios. La siguiente figura muestra una transmisión normal de video en un sistema de tele vigilancia.

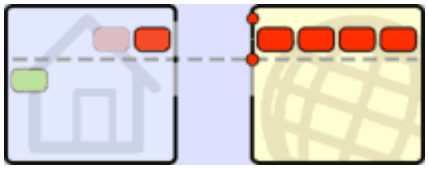

Figura 46 – Transmisión Tradicional de Video.

Como se aprecia en la figura anterior, es posible enviar flujos de video de forma que estos llegan a un usuario final, este envío de información se realiza de manera normal, sin utilizar priorización de tráfico o utilizar streaming para el envío.

Al utilizar el servidor de streaming, que se propone en el diseño, se mejoraría la calidad de servicio, por ende un mayor tráfico de paquetes de datos por cada petición al servidor streaming, teniendo como resultado la siguiente figura.

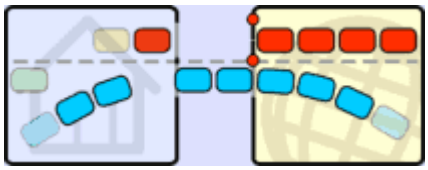

Figura 47 – Transmisión Streming de Video.

Para optimizar la utilización de video streaming, se propone utilizar la técnica antes mencionada denominada "Traffic Shaping", otorgando mejores prestaciones y optimización en el envío de paquetes de datos, aumentando el flujo de envío, etiquetando o marcando cada paquete de dato con mayor prioridad de envío y finalmente catalogando cada paquete y servicio para una mayor eficiencia en cada petición por cada usuario, todo esto evidenciado en ls siguiente figura.

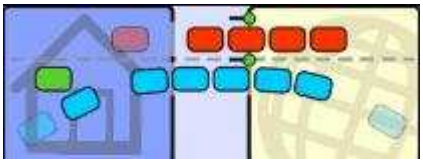

Figura 48 – Transmisión Traffic Shaping de Video.

5.3.7 Recepción

Una vez enviado el contenido multimedia, encriptada a través de Internet, es recepcionado por aquellos usuarios que tienen acceso al sistema de tele vigilancia, con ello realizan el proceso de verificación y autenticación del usuario, con el fin de visualizar la cámara IP.

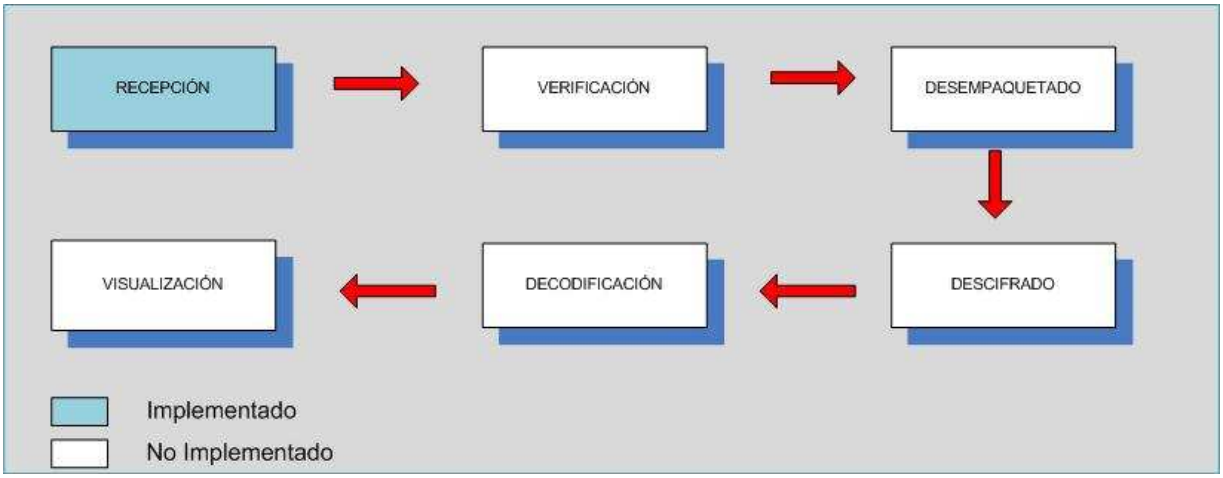

Figura 49 – Recepción.

5.3.8 Verificación Autenticación

Una vez recepcionada la comunicación, el segundo paso es poder generar un canal seguro de comunicación, con ello es necesario realizar una comprobación de la firma digital del usuario que desea conectarse al sistema de televigilancia. Por este motivo, el proceso siguiente es comprobar si esta firma digital corresponde a quien dice ser y esto se verifica de la siguiente manera.

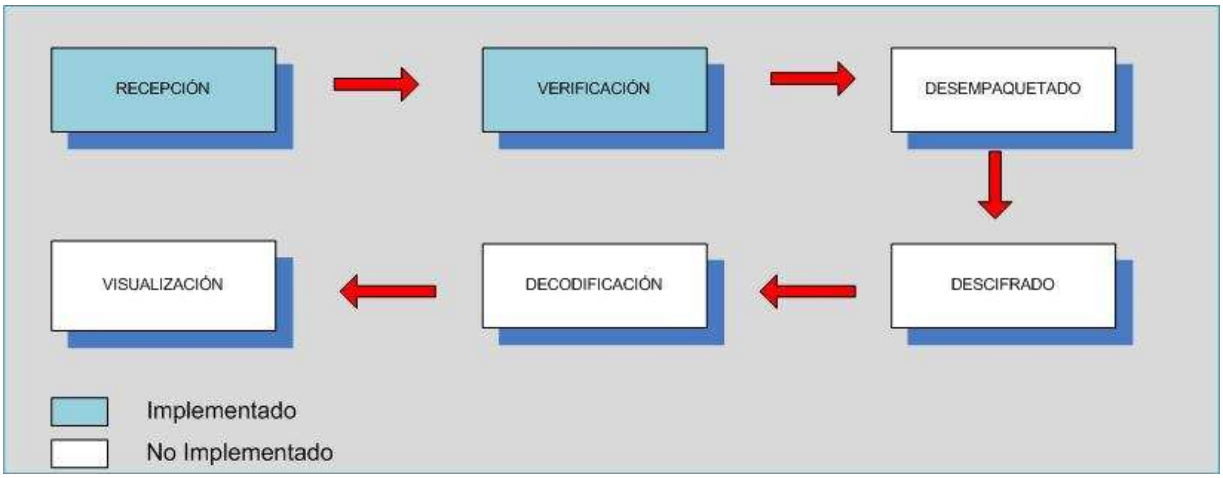

Figura 50 – Verificación.

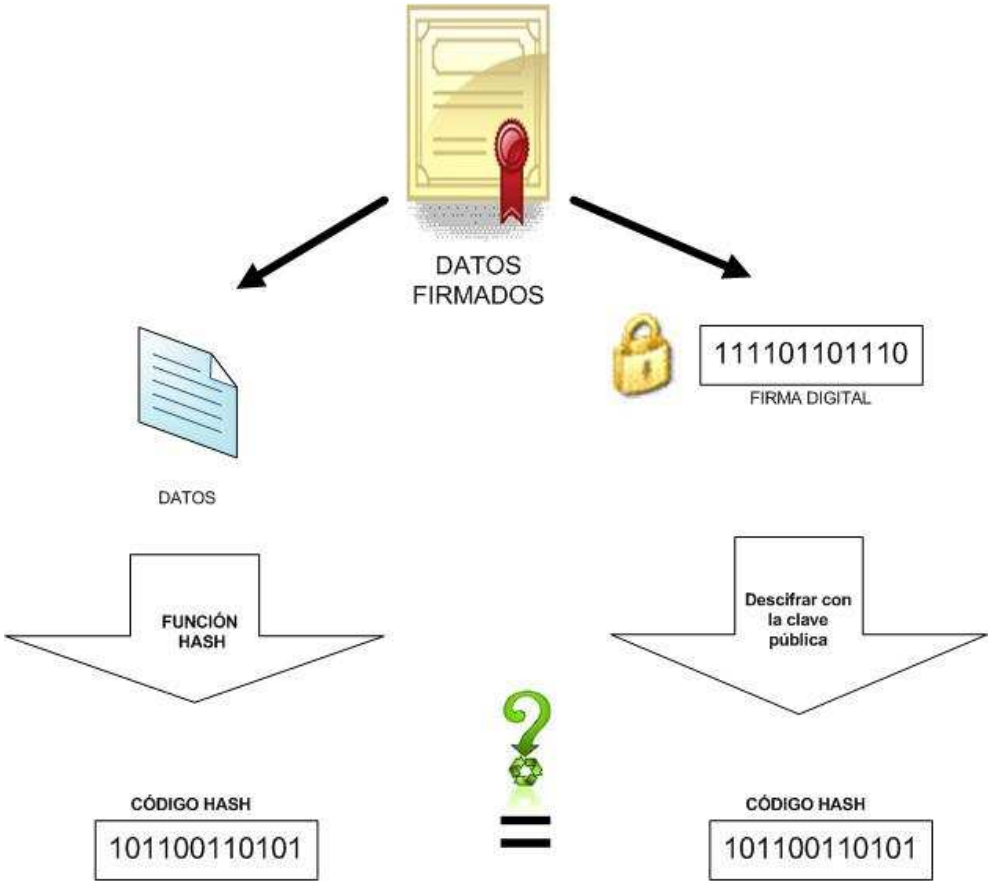

Figura 51 – Verificación Firma Digital.

Por lo tanto, la firma digital sería utilizada en el acceso de identificación y autenticación de usuarios, por la versatilidad y el grado de efectividad que tienen estos métodos de autentificación.

5.3.9 Desempaquetado

Como se menciono anteriormente en este proceso, se han utilizado algunos protocolos que están en la dirección de proveer una buena calidad de servicio, con el fin de obtener una fluidez de transmisión, menor retardo de la transmisión y mejor calidad de imagen.

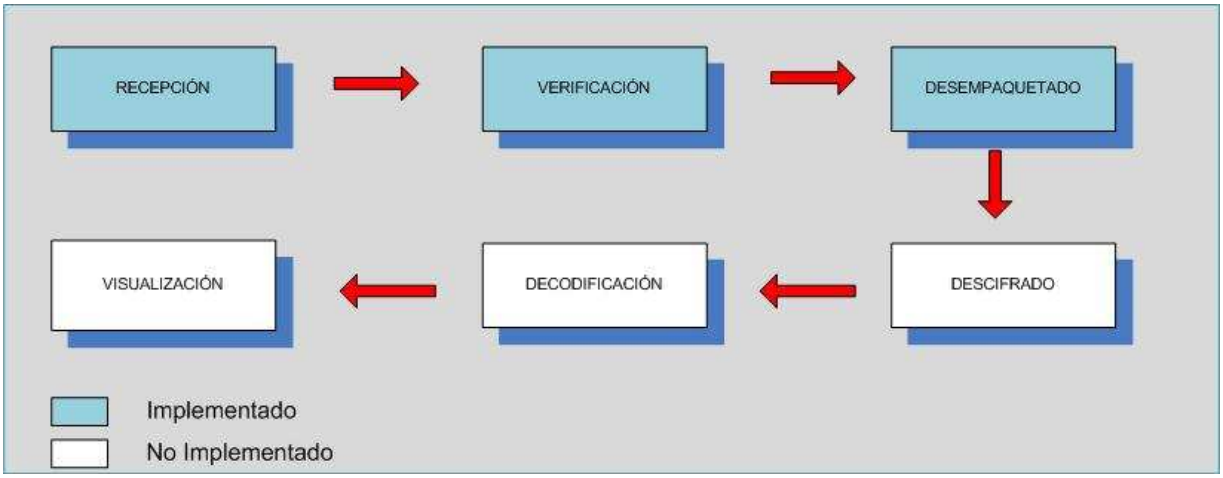

Figura 52 – Desempaquetado.

Además, el usuario recibe los paquetes de datos encapsulados en los protocolos de transmisión de video, los cuales están cifrados,. Una vez recepcionadas son desempaquetados por la máquina del usuario, y luego realizar el proceso de descifrado.

5.3.10 Descifrado

Como se mencionó anteriormente se ha utilizado cifrado AES. Este es un esquema de cifrado de bloques adoptado por un estándar de cifrado, siendo uno de los algoritmos más populares de cifrado usados en criptografía. Para complementar las fases anteriormente descritas se sintetiza el proceso de cifrado en la siguiente arquitectura, donde se descifran los paquetes enviados en el canal seguro para la transmisión de video.

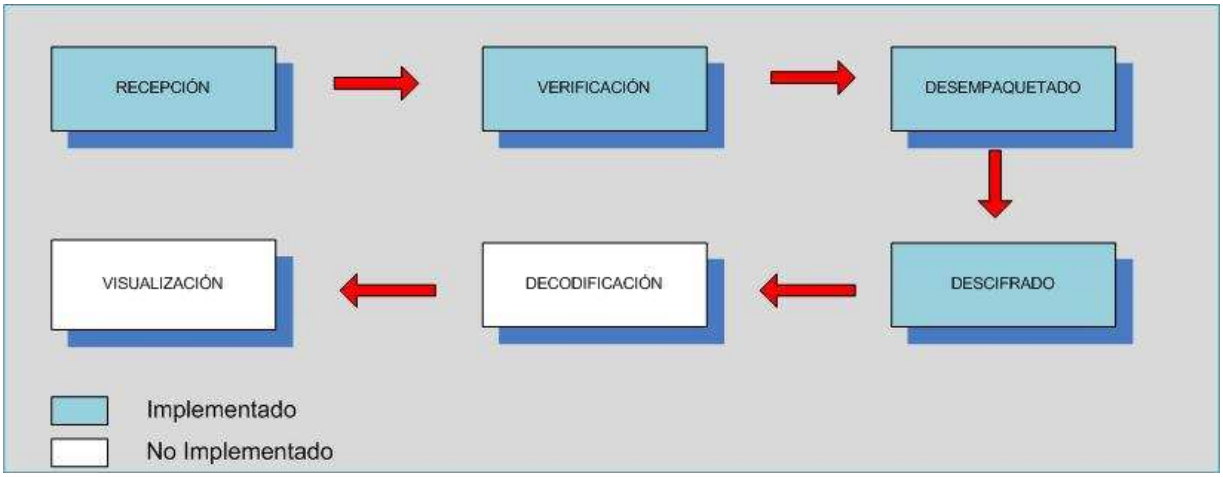

Figura 53 – Descrifrado.

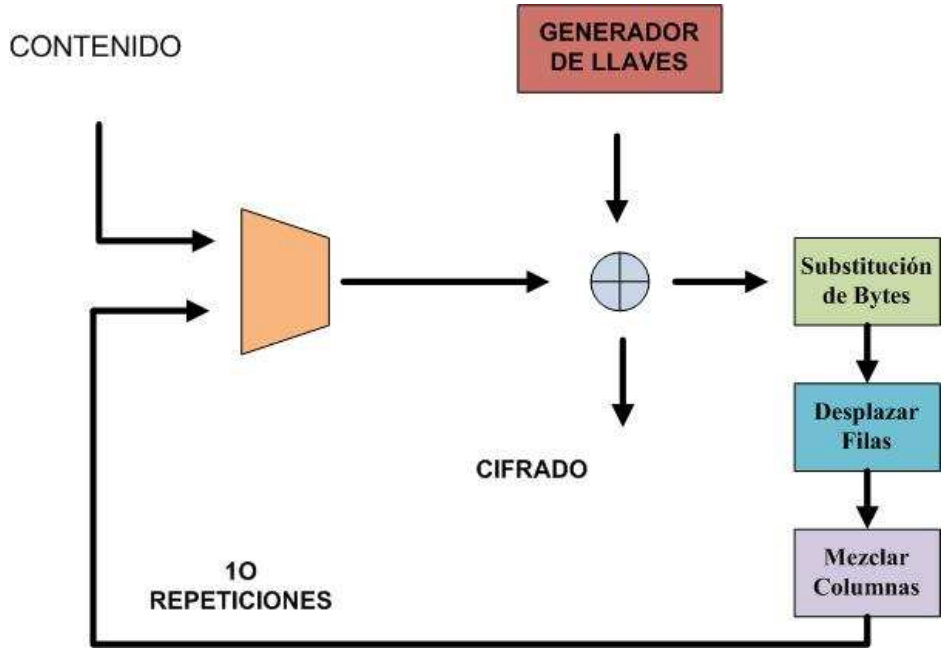

Figura 54 – Proceso Cifrado AES.

5.3.11 Decodificación y Descompresión

Como se explicó anteriormente, la tecnología Streaming funciona de la manera más simple y de bajo consumo de ancho de banda, para visualizar video desde un sitio Web o de otro medio de transmisión. Por ello que una vez descifrado los paquetes es necesario, descodificar y descomprimir los paquetes que son enviados a través del canal seguro que se ha creado para la transmisión de estos paquetes. Finalmente, una vez decodificados y descomprimidos, es posible visualizar el video transmitido al usuario.

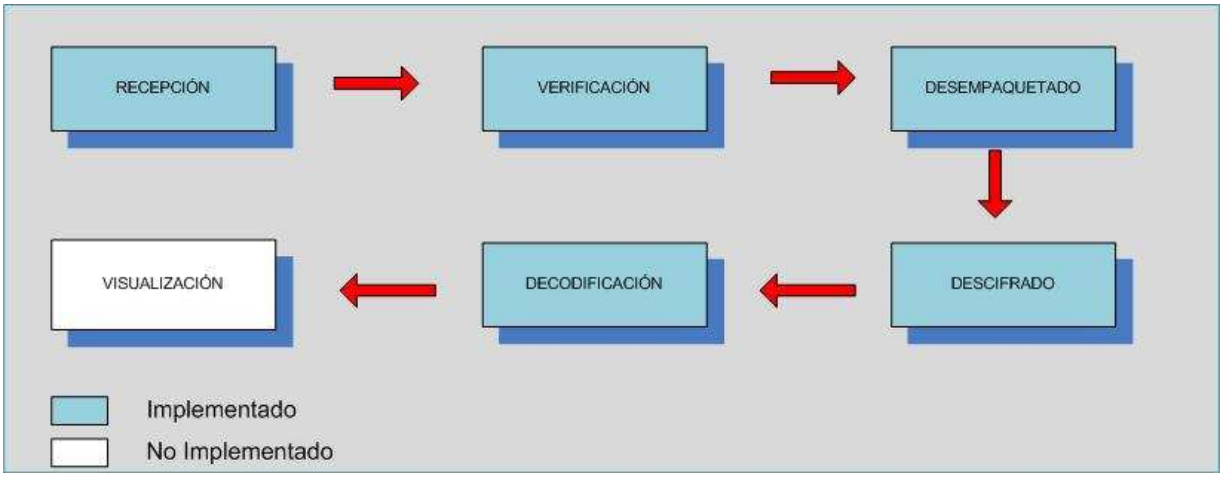

Figura 55 – Decodificación.

5.3.12 Visualización

Finalmente es posible visualizar el video streaming, que ha viajado a través del canal seguro y ha pasado por los procesos antes descritos, con ello el usuario final podrá visualizar el contenido transmitido por las cámaras IP.

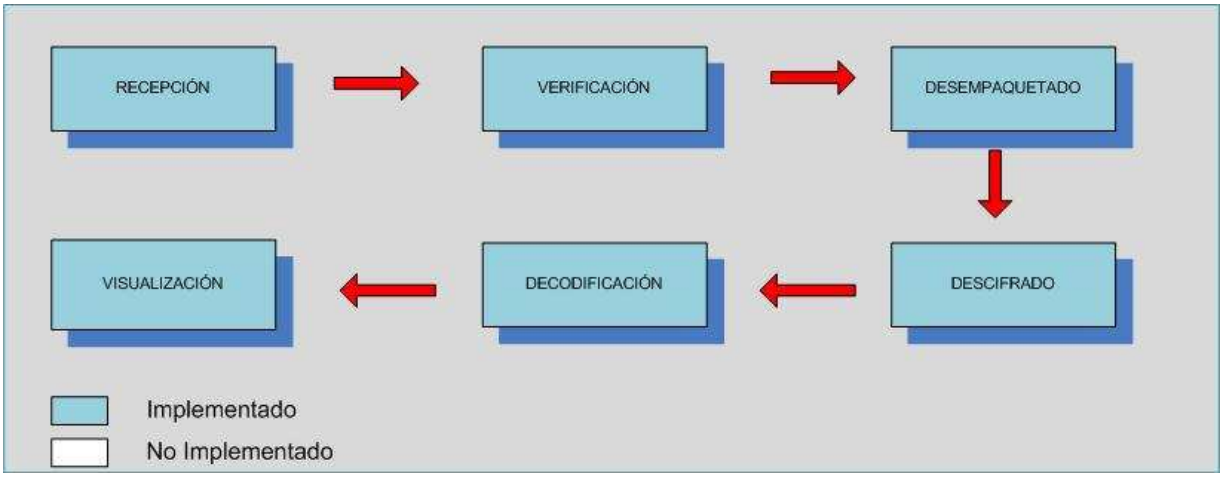

Figura 56 – Visualización.

5.4 Comunicación Sistema Tele Vigilancia

Se muestran los siguientes modelos de comunicación para el sistema de tele vigilancia, que muestran los procesos y aspectos relevantes a considerar en la comunicación segura.

5.4.1 Proceso Comunicación Segura

Se define un proceso de comunicación segura entre servidor y usuario, con el fin de satisfacer las siguientes características: autenticación, confidencialidad, integridad y no repudio.

Con la utilización de cifrado asimétrico se mantiene una comunicación confidencial, debido a que el servidor solo necesita saber las claves públicas de los usuarios, y sólo con la clave privada podrá descifrar el mensaje.

Respecto a la autenticación del usuario, éste cifra previamente el contenido con su clave privada, en este caso no lo está protegiendo, ya que cualquiera que tenga la clave pública podrá descifrarlo, pero sí está garantizando su identidad, ya que nadie más tiene su clave privada.

Para evitar riesgos susceptibles a una alteración del contenido enviado, es necesario que el servidor no cifre todo el mensaje con su clave privada, sino sólo un hash del mismo, obtenido mediante una función criptográfica unidireccional, y añada la firma digital después del contenido enviado. Con estos procesos, es posible enviar el contenido verificando la autenticidad e integridad del contenido.

Como el sistema de vigilancia tiene muchos usuarios, es necesario utilizar la criptografía convencional y asimétrica para cifrar sólo la clave, en vez del contenido completo. Por lo que se distribuye en este caso es un solo mensaje, cifrado con una clave convencional denominada clave de sesión, junto con el resultado de cifrar la clave para cada uno se los usuarios.

A continuación se muestra el diseño que utiliza las técnicas mencionadas anteriormente, que se aplicará en el sistema de tele vigilancia. El cual considera una comunicación segura, entre el usuario y el servidor utilizando los algoritmos de cifrado simétricos AES 256 bits, y cifrado asimétrico RSA 2048 bits para el intercambio de claves y autenticación, y un algoritmo unidireccional hash SHA-1 para la creación de firmas digitales, tal como se muestra en la siguiente figura.

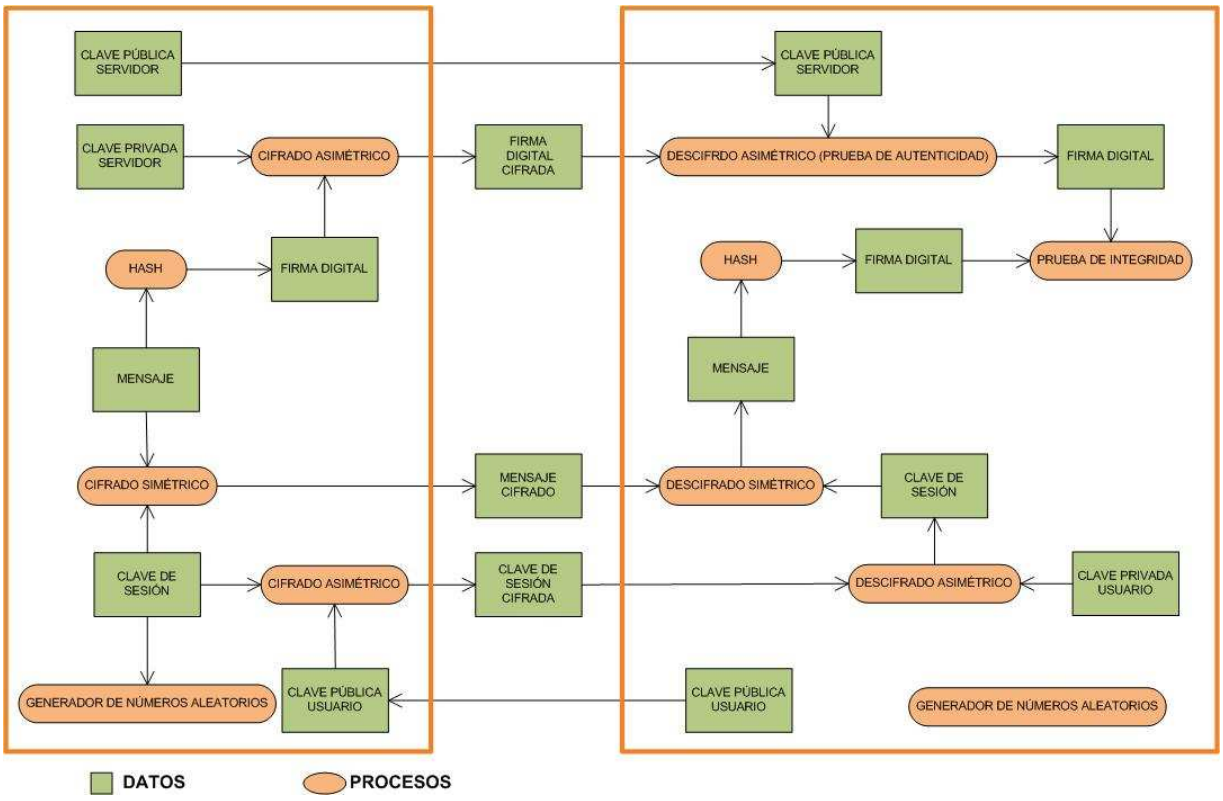

Figura 57 – Proceso Comunicación Segura.

5.4.2 Proceso de Comunicación Servidor – Usuario

Este modelo considera todas aquellas etapas del proceso de comunicación segura entre servidor y usuario. Además muestra de manera conceptual el funcionamiento de esta propuesta a nivel funcional.

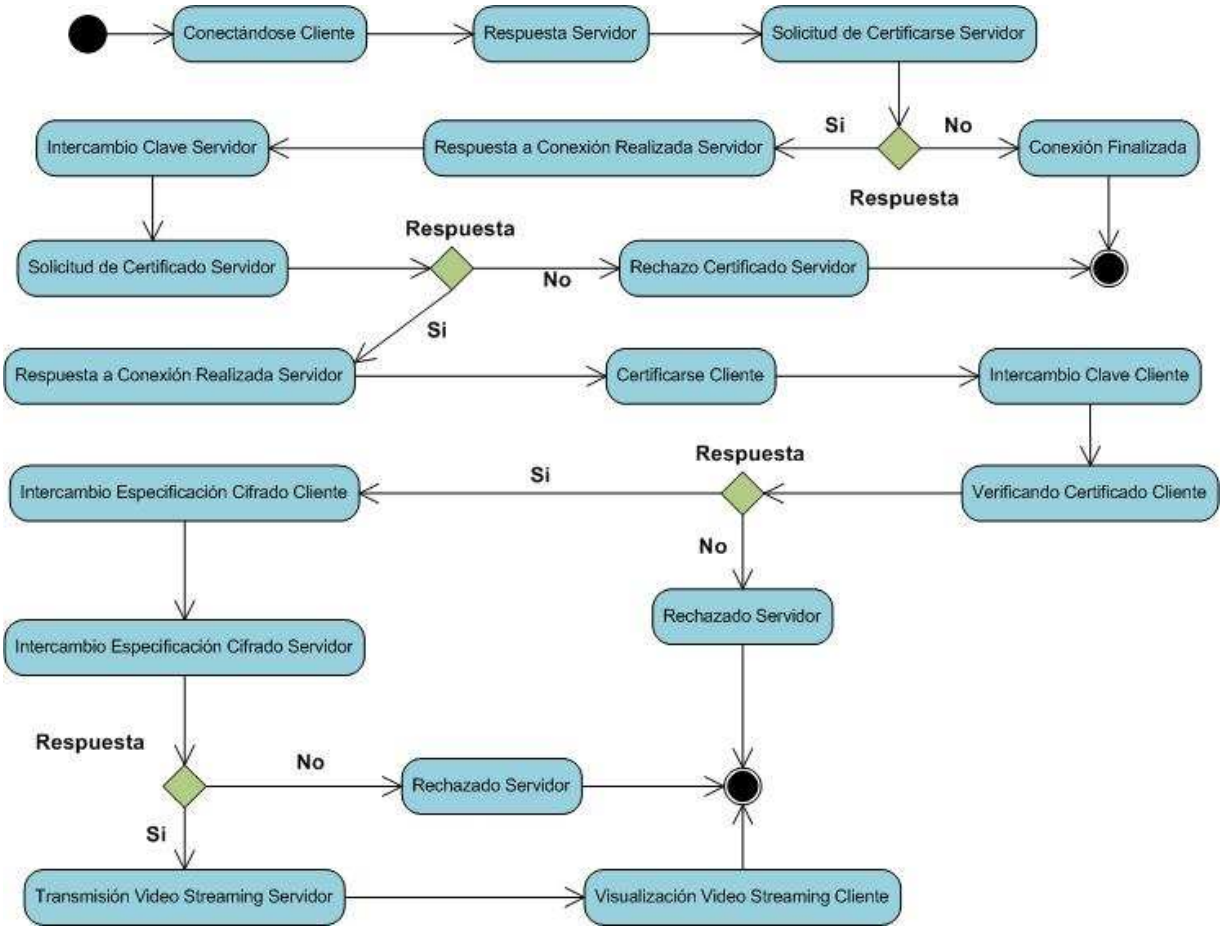

Figura 58 – Proceso Transmisión Segura.

5.5 Ventajas del Modelo Tele Vigilancia

El sistema de Tele Vigilancia Digital propuesto ofrece toda una serie de ventajas y funcionalidades avanzadas que no puede proporcionar un sistema de Tele Vigilancia Analógico. Entre las ventajas se incluye la accesibilidad remota, la alta calidad de imagen, la gestión de eventos y las capacidades de video inteligente, así como las posibilidades de una integración sencilla y una escalabilidad, flexibilidad y costo minimizado.

- **Accesibilidad Remota:** Se pueden configurar las cámaras de red y el servidor para acceder a ellas de forma remota, lo que permite a diferentes usuarios autorizados visualizar video en vivo y grabado en cualquier momento y desde prácticamente cualquier ubicación del mundo. Esto resulta ventajoso si los usuarios quisieran que otra empresa, como por ejemplo una empresa de seguridad, tuviera también acceso al video. En un sistema analógico tradicional, los usuarios necesitarían encontrarse en una ubicación de supervisión en el lugar para ver y gestionar el video, y el acceso al video desde fuera del lugar no sería posible sin un equipo como un codificador de video o un grabador de video digital (DVR) de red.
- **Alta calidad de imagen:** En una aplicación de Tele Vigilancia, es esencial una alta calidad de imagen para poder capturar con claridad un incidente en curso e identificar a las personas u objetos implicados. Con las tecnologías de barrido progresivo y megapíxel, una cámara de red puede producir una mejor calidad de imagen y una resolución más alta que una cámara analógica. Asimismo, la calidad de la imagen se puede mantener más fácilmente en un sistema de video digital en red que en uno de vigilancia analógica. Con los sistemas analógicos actuales que utilizan un DVR como medio de grabación, se realizan muchas conversiones analógicas a digitales, en primer lugar, se convierten en la cámara las señales analógicas a digitales y después otra vez a analógicas para su transporte, después, las señales analógicas se digitalizan para su grabación. Las imágenes capturadas se degradan con cada conversión entre los formatos analógico y digital, así como con la distancia de los cables. Cuanto más lejos tienen que viajar las señales de video, más débiles se vuelven. En un sistema de Tele Vigilancia Digital, las imágenes de una cámara de red se digitalizan una vez y se mantienen en formato digital sin conversiones innecesarias y sin degradación de las imágenes debido a la distancia que recorren por una red. Además, las imágenes digitales se pueden almacenar y recuperar más fácilmente que en los casos en los que se utilizan cintas de video analógicas.
- **Gestión de eventos y video inteligente:** A menudo existe demasiado contenido de video grabado y una falta de tiempo suficiente para analizarlo adecuadamente. Las cámaras de red avanzadas con inteligencia o análisis integrado pueden ocuparse de este problema al reducir la cantidad de grabaciones sin interés y permitir respuestas programadas. Este tipo de funcionalidad no está disponible en un sistema analógico. Las cámaras de red incluyen funciones integradas como la detección de movimiento por video, alarma de detección de audio, alarma antimanipulación activa, conexiones de entrada y salida (E/S) y funcionalidades de gestión de alarmas y eventos.

  Estas funciones permiten que las cámaras de red analicen de manera constante las entradas para detectar un evento y responder automáticamente a éste con acciones como la grabación de video y el envío de notificaciones de alarma.
- **Integración sencilla y preparada para el futuro:** Los dispositivos de video basados en red y en estándares abiertos se pueden integrar fácilmente con sistemas de información basados en un computador y Ethernet, sistemas de audio o de seguridad y otros dispositivos digitales, además del software de gestión de video y de la aplicación según sea requerido.

- **Escalabilidad y flexibilidad:** Un sistema Tele Vigilancia en red puede crecer respecto a las necesidades del usuario. Los sistemas basados en comunicación por Red ofrecen a muchas cámaras de red, así como a otros tipos de aplicaciones, una manera de compartir la misma red inalámbrica o con cable para la comunicación de datos, de este modo, se puede añadir al sistema cualquier dispositivo de video en red sin que ello suponga cambios significativos o costosos para la infraestructura de red. Esto no sucede con un sistema analógico. En un sistema de Tele Vigilancia analógico, se debe extender un cable coaxial directamente desde cada cámara a un punto de visualización o grabación. Asimismo, se deben usar cables de audio independientes si se requiere audio. Los sistema de Tele Vigilancia basados en red también se pueden implementar y utilizar en red desde prácticamente cualquier lugar, y el sistema puede ser tan abierto o cerrado como se necesite.
- **Baja Inversión:** Un sistema de Tele Vigilancia Digital basado en red tiene normalmente un costo total inferior al de un sistema analógico tradicional. Una infraestructura de red IP a menudo ya está implementada y se utiliza para otras aplicaciones dentro de una organización, por lo que una aplicación de video en red puede aprovechar la infraestructura existente. Las redes basadas en IP y las opciones inalámbricas constituyen además alternativas mucho menos caras, que el cableado coaxial y de fibra tradicionales utilizados por un sistema analógico. Por otro lado, las transmisiones de video digitales se pueden transmitir por todo el mundo mediante una gran variedad de infraestructuras inter operativas. Los costos de gestión y equipos también son menores ya que las aplicaciones y el almacenamiento se ejecutan en servidores basados en sistemas abiertos, de estándar, no en hardware propietario como un DVR en el caso de un sistema analógico. Además, la tecnología PoE (Alimentación a través de Ethernet), que no se puede aplicar a un sistema de video analógico, se puede utilizar en un sistema en red . PoE permite a los dispositivos en red recibir alimentación de un switch u otro dispositivo compatible con PoE a través del mismo cable Ethernet que transporta los datos. Ofrece un ahorro sustancial en los costos de instalación y puede aumentar la fiabilidad del sistema.

5.6 Ventajas Seguridad

A continuación se mostraran las ventajas de utilizar seguridad en esta investigación y en la propuesta de diseño.

- **Privacidad:** A través de la utilización de las distintas técnicas de autenticación, se han utilizado los certificados digitales para mantener la mejor privacidad entre la transmisión del servidor y el usuario que accede al contenido transmitido. Por esta razón, se pretende transmitir el contenido solo a aquellos usuarios que están autorizados a acceder a dicho contenido.

- **Confiabilidad:** En la transmisión del contenido multimedia a través de las redes de Internet, existe la posibilidad de que este contenido pueda ser interceptado y luego modificado, con ello provocando problemas en nuestro sistema. Frente a esto y para mantener el contenido desde origen a fin, sin alterar su esencia, es que la utilización de cifrado entre otras técnicas, permiten que este sea íntegro de inicio a fin.
- **Disponibilidad:** El sistema de tele vigilancia debe estar prácticamente 100% disponible, cuando un usuario desea visualizar o conectarse al sistema. Por ello que la utilización de los distintos mecanismos de seguridad proveen esta disponibilidad, apoyados de distintos mecanismos que se han utilizado en esta investigación, los cuales han sido nombrados a través de este documento.
- **Estabilidad:** El sistema de tele vigilancia permite una mayor estabilidad frente a un sistema que no posea o utilice mecanismos de seguridad. Como se menciono anteriormente la disponibilidad de un sistema de tele vigilancia debe estar cercando al 100%, por ello que sistemas sin los mecanismos adecuados de seguridad, sufrirían ataques o eventualidades que evitarían el normal funcionamiento del sistema, frente a esta disyuntiva, es que se han utilizado las técnicas, mecanismos y herramientas acordes al contexto de los sistemas de tele vigilancia, para mantener el rendimiento deseado y evitar ataques de cualquier índole.
- **Acceso Remoto:** Es posible accesar en forma remota al sistema de televigilancia, como a sus distintos servidores, con el fin de revisar su funcionamiento, disponibilidad, y auditar su rendimiento constantemente, además de revisar la seguridad y rendimiento del sistema de televigilancia.
- **Transparente:** A nivel de seguridad, la utilización de los mecanismos de seguridad en esta investigación son transparentes para su uso, a nivel de usuario, administrador y de aplicaciones.
- **Acceso Controlador:** Provee los servicios y técnicas de autenticación para el manejo y conexiones entre el servidor y el usuario. Permite gestionar cada una de las conexiones permitidas, además de rechazar o aceptar a cada usuario que cumpla los requisitos de seguridad necesarios.

6 Prototipo

La implementación de este diseño, se ha llevado a cabo a través de la utilización de distintas herramientas y aspectos técnicos, con el fin de mejorar la calidad de servicio en la transmisión de video.

A continuación se explicará el trabajo realizado, de manera detallada, aludiendo tanto a los aspectos utilizados a nivel de software, hardware y consideraciones técnicas relevantes para la investigación. Se presenta la arquitectura implementada en el prototipo.

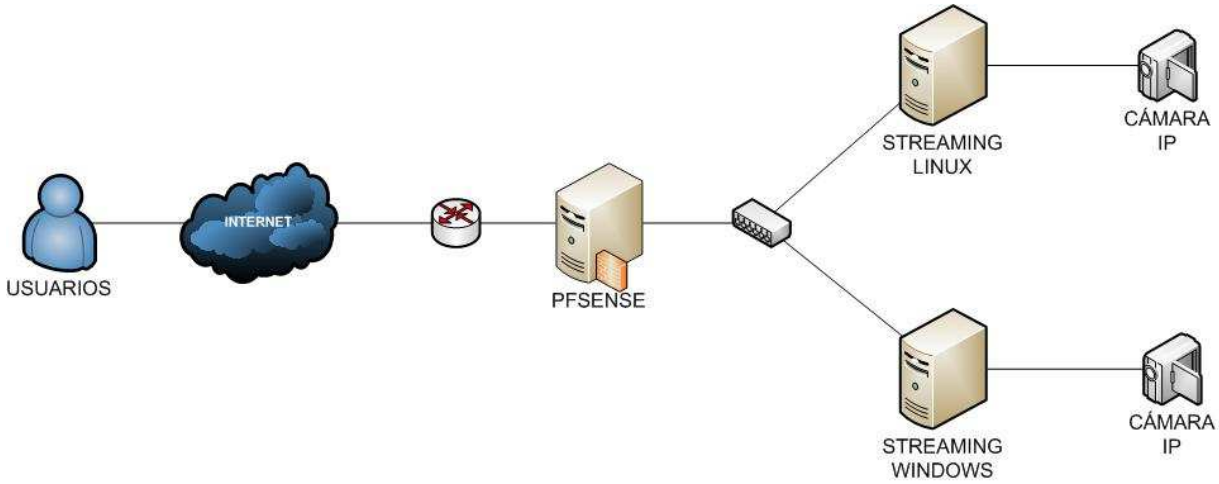

Figura 59 – Esquema de Implementación.

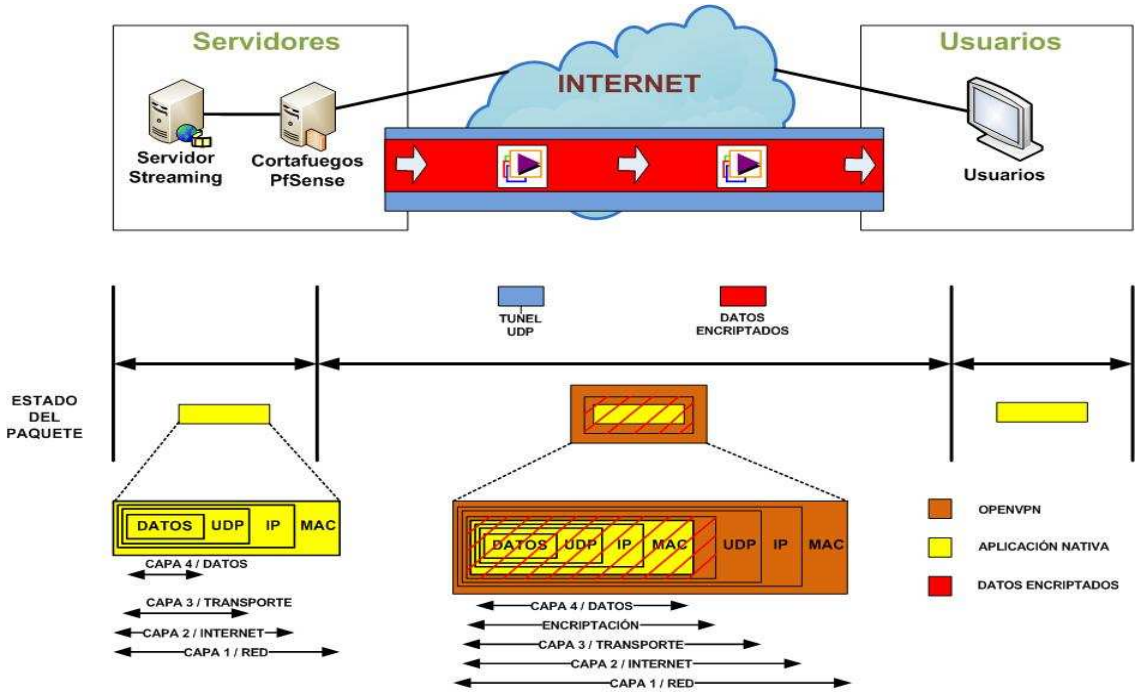

Figura 60 – Funcionamiento Implementación.

En las siguientes secciones se describirán cada uno de los aspectos que aluden a esta arquitectura, así también, indicar cada proceso y las herramientas asociada a cada uno de ellos.

6.1 Video

Para el desarrollo del diseño, la utilización de los dispositivos especificados en la propuesta hubiese sido lo mas acorde, sin embargo, para los efectos de desarrollo e implementación del diseño, es que se ha utilizado una especificación distinta a lo que se plantea. A continuación, se describe el dispositivo de Tele Vigilancia utilizado en esta investigación.

6.1.1 Dispositivo Tele Vigilancia

Para situarnos en la propuesta del proceso de transmisión de video seguro, se toma la siguiente Figura como referencia, la cual indica en que parte del desarrollo e implementación se encuentra la investigación.

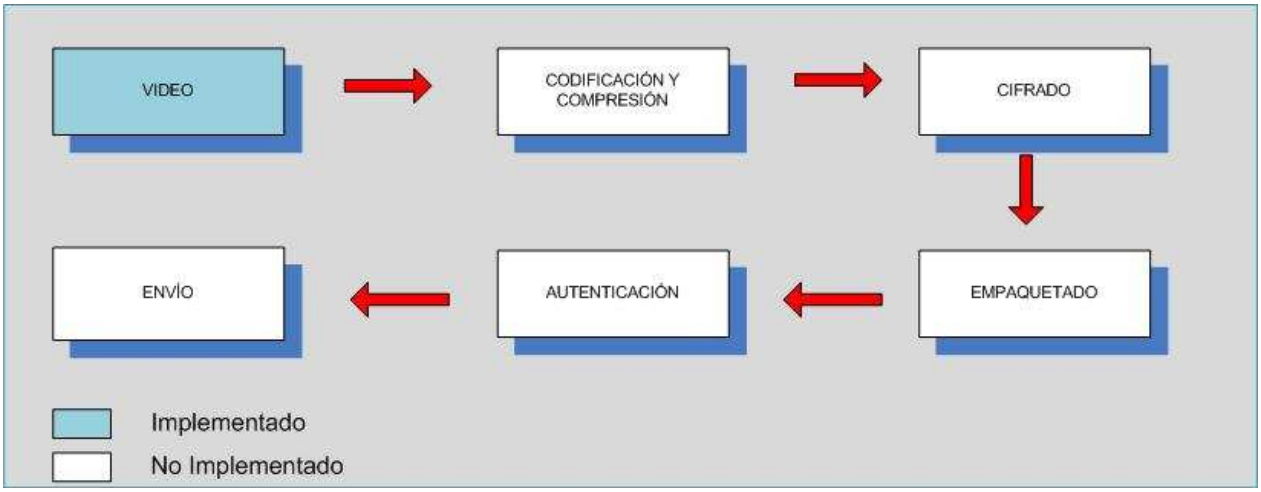

Figura 61 – Implementación Video.

El desarrollo de este proceso básicamente está en relación, a la utilización de dispositivos emisión de video, es decir, de cámaras de red o IP, las que gracias a sus innumerables ventajas y aportes al desarrollo de aplicaciones en transmisión de video a través de Internet, dan la oportunidad y la facilidad de poder complementar y aplicar esta investigación.

A continuación, se dan algunas características del dispositivo, cámara de vigilancia IP DCS-2102 de D-Link, utilizada en este prototipo.

6.1.1.1 Descripción General

La cámara de vigilancia IP DCS-2102 de D-Link proporciona una solución de vigilancia versátil y única. A diferencia de una cámara estándar conectada a Internet, la cámara IP DCS-2102 es un sistema completo de seguridad y vigilancia, ya que incorpora una CPU interna y un servidor Web, que transmite imágenes de vídeo de alta calidad entregando la posibilidad de mantener ambientes totalmente vigilados, durante las 24 horas del día.

La cámara de vigilancia IP DCS-2102 permite acceder a las imágenes en cualquier momento y controlar todas las funciones operativas de la cámara en forma remota desde cualquier computador o computador portátil, ya sea desde la red local como a través de Internet utilizando de manera fácil rápida y sencilla un navegador Web.

La instalación de la cámara es simple y la interfaz de configuración es intuitiva y basada en WEB, esto permite la más rápida integración a su red cableada Ethernet/Fast Ethernet. La cámara DCS-2102 también incorpora funciones de detección de movimiento y control remoto haciendo de la cámara DCS-2102 una completa solución de seguridad.

Utilizando las funciones Snapshot y Recording, características diseñadas para capturar al instante cualquier momento desde una ubicación remota, permite guardar fotos y grabar vídeo y audio directamente desde un navegador Web, a un disco duro local sin necesidad de instalar ningún software. La cámara DCS-2102 le permite grabar directamente a un dispositivo de almacenamiento que se encuentre dentro de su red de área local, sin el uso de una PC dedicada para almacenar los videos grabados.

Esta solución avanzada de monitoreo remoto de D-Link incorpora puertos conectores I/O (puerto de entrada y salida), para conectar dispositivos de movimiento o sensores de alertas como: balizas, portones o puertas de movimiento eléctrico. Además, incorpora audio bidireccional, lo que permite escuchar lo que pasa en el área de monitoreo a través del computador, o bien, emitir un sonido a través de un micrófono lo que se reproduce a través del puerto de salida de audio que trae la DCS-2102. También incorpora la facilidad de grabar directamente a través de una tarjeta de memoria SD que se inserta en el costado de la cámara para reproducirlo posteriormente en cualquier dispositivo multimedia que soporte dicho formato.

Tabla 15 – Descripción Técnica Cámara Ip.

Ítem	Característica Técnica
Sensor de Imagen	• CMOS • Barrido progresivo de 1/3” • 1.3 megapíxel
Objetivo	• De 2.7 mm / F de 1.0 • Iris fijo o DC • Auto foco
Día/ Noche	• Configurable
Sensibilidad Lumínica (Lux)	• De 4 a 10000 • color
Compresión de Video	• H.264
Resolución Máxima de video (Pixeles)	• 640 x 480
Imágenes por Segundo	30 (640 x 480)
Pan/Tilt/Zoom	• Posiciones predefinidas
Entradas / Salidas	1 o varias
Seguridad	• Contraseña multinivel • Filtro de direcciones ip • Cifrado HTTPS
Red	• IPv4 • IPv6 • Q&S
POOE	• Disponible clase 1 a 3 • C/S calentador
otros	• IEEE inalámbrica 802.11 b/g • Uso interior exterior • Certificación IP66 • Auto slip • Visibilidad Nocturna

6.2 Codificación, Compresión y Tecnología Streaming

Otro aspecto relevante de esta investigación, es la utilización de la tecnología Streaming. Por ello que en la siguiente Figura, se muestra la etapa lograda de esta investigación.

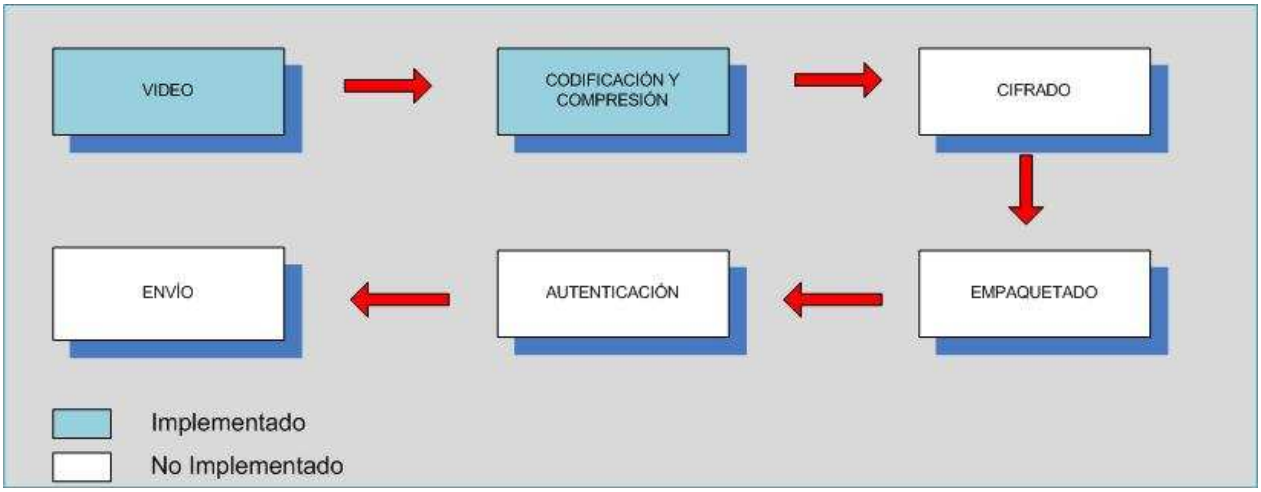

Figura 62 – Aplicación de Codificación y Compresión de video.

¿Por qué la Tecnología Streaming?. Esta es una pregunta que tal vez aparece, frente a la posibilidad y autonomía de utilización de las cámaras IP, de forma automatizada e independiente. La tecnología cada vez va evolucionando, pero los aspectos de calidad de servicio, frente a bajos ancho de banda, dan a conocer una problemática evidente, privando a muchos usuarios, el acceso a contenidos multimedia de mejor calidad.

La autonomía y versatilidad de las cámaras IP, proporcionan muchas ventajas y utilidades, tanto en proyectos de envergadura grande, mediano y pequeño. Sin embargo, la principal desventaja y problemática que poseen estos dispositivos, esta relacionado al acceso en forma concurrente del dispositivo, es decir, si muchos usuarios se conectan para visualizar video, en forma simultánea, con distintos anchos de banda, provocaría que el dispositivo "Cámara IP", tenga una sobrecarga de solicitud, lo que conlleva a que el dispositivo no responda de la manera como se esperaría, por ende, se pierde calidad de servicio y fluidez en la reproducción y visualización de video.

Con la tecnología streaming, podremos satisfacer dicha necesidad, apoyada de una arquitectura cliente-servidor, que optimiza la sobrecarga de solicitud de peticiones. En la siguiente figura, se muestra la arquitectura cliente- servidor propuesta.

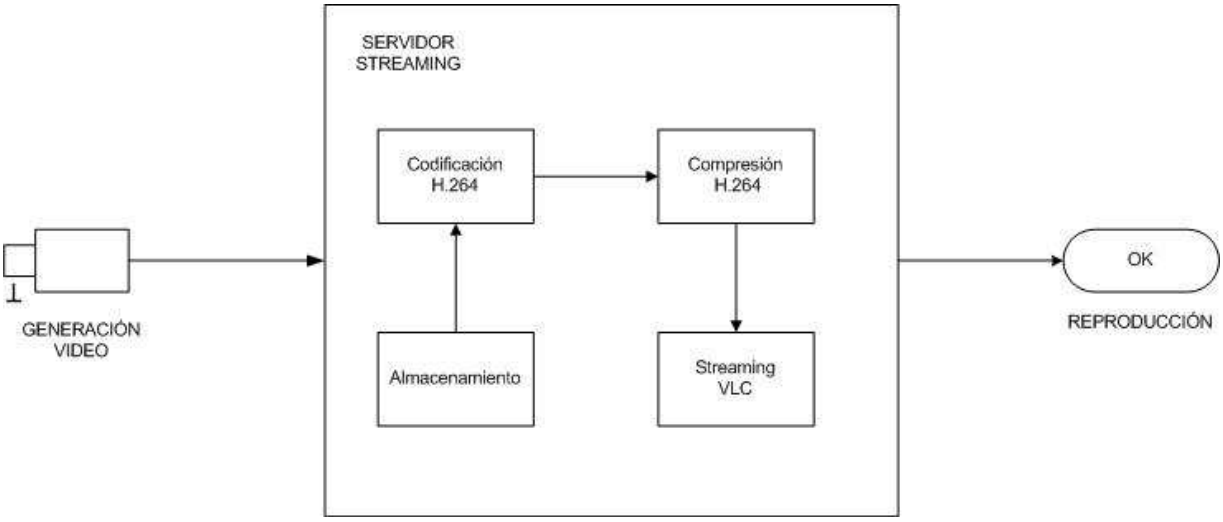

Figura 63 – Proceso Arquitectura de Cliente - Servidor.

A continuación se hace referencia, a software y hardware utilizado en la arquitectura streaming.

6.2.1 Software

Para la implementación de la tecnología streaming, es necesario utilizar aplicaciones, las cuales proveerán los servicios de reproducción de video con calidad de servicio a través de Internet, frente a distintos ancho de banda.

La utilización de estas aplicaciones de código libre, darán la oportunidad de poder implementar nuevas ideas y aspectos, relacionados a los mecanismos de seguridad que aborda esta investigación. A continuación, se alude a las aplicaciones y características de los sistemas utilizados.

6.2.1.1 VideoLan

VideoLan es un proyecto compuesto por un equipo de voluntarios, que desarrollan software libre multimedia, liberado bajo GNU. VideoLan es una solución la cual utiliza su reproductor multimedia VLC, el cual puede ser utilizado como servidor y como cliente para escuchar y recibir flujos de red. VLC es capaz de escuchar todo los formatos que soporta.

La siguiente figura describe la arquitectura streaming de VideoLan.

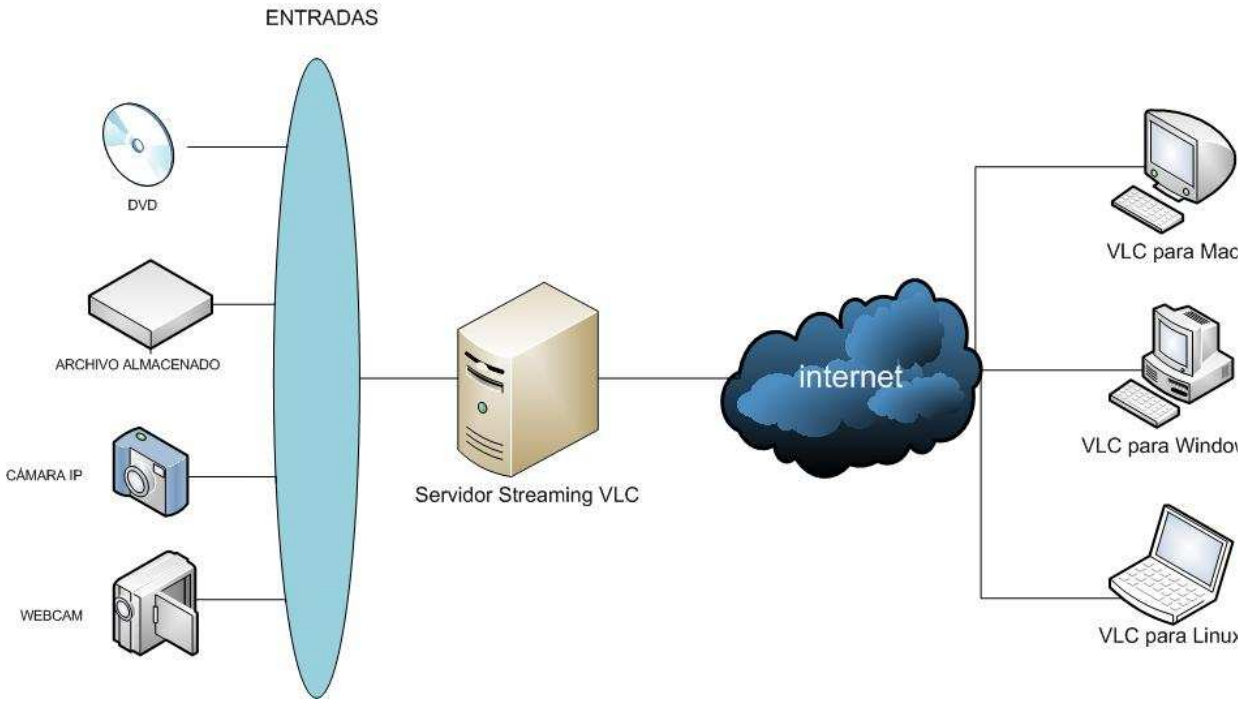

Figura 64 –Arquitectura de Cliente – Servidor VideoLan.

6.2.1.1.1 Características Utilizadas

Las configuraciones utilizadas para el prototipo son las descritas en las tablas siguientes.

Tabla 16 – Aspectos Técnicos Soportados - Protocolos.

Protocolos de salida	Windows	Linux
RTP/UDP	OK	OK
RTSP	OK	OK

Tabla 17 – Aspectos Técnicos Soportados – Formatos de Entradas.

Formatos de Video Entrada	Windows	Linux
UDP/RTP Unicast/Multicast	OK	OK

Tabla 18 – Aspectos Técnicos Soportados – Formatos de Video Salida.

Formatos de Video Salida	Windows	Linux
H.264/MPEG-4 AVC	OK	OK

6.2.1.1.2 Características Técnicas

Las siguientes tablas muestran algunas características Técnicas soportadas.

Tabla 19 – Aspectos Técnicos Soportados - Protocolos.

Protocolos de salida	**Windows**	**Linux**
RTP/UDP	OK	OK
RTSP	OK	OK
RTP/DCCP	X	OK
Raw UDP	OK	OK
RTP Multidifusión	OK	OK
HTTP	OK	OK
MMSH	OK	OK
Transcodificación	OK	OK

Tabla 20 – Aspectos Técnicos Soportados – Formatos de Entradas.

Formatos de Video Entrada	**Windows**	**Linux**
UDP/RTP Unicast/Multicast	OK	OK
HTTP/FTP	OK	OK
MMS	OK	OK
TCP/RTP Unicast	OK	OK
DCCP/RTP Unicast	X	X
Archivo	OK	OK

DVD/CD Video	OK	OK
MPEG encoder	OK	OK
Video adquirido	OK(Direct Show)	OK (Isight)
MPEG	OK	OK
AVI	OK	OK
ASF/WMV/WMA	OK	OK
MP4/MOV/3GP	OK	OK
OGG/OGM	OK	OK
MKV	OK	OK
REAL	OK	OK
WAV	OK	OK
FLAC	OK	OK
FLV	OK	OK

Tabla 21 – Aspectos Técnicos Soportados – Formatos de Video Salida.

Formatos de Video Salida	Windows	Linux
MPEG-1/2	OK	OK
DIVX	OK	OK
MPEG-4	OK	OK
H.263/ H.263I	OK	OK
H.264/MPEG-4 AVC	OK	OK
THEORA	OK	OK
MJPEG	OK	OK
WMV ½	OK	OK
WMV 3/WMV -9 /VC-1	OK	OK
Sorenson 1/3 (Quicktime)	OK	OK

Indeo Video V3	OK	OK
REAL VIDEO ½ Y 3/4	OK	OK

6.2.1.2 WebcamXP

Es una poderosa herramienta de monitoreo de cámaras de red y Webcams. Permite la grabación y posee un software streaming para uso privado y profesional. Ofrece características únicas e inigualables, con facilidad de uso que permite manejar múltiples fuentes de video en un mismo computador. Es una herramienta ideal para garantizar una supervisión de manera remota desde Internet.

Algunas características de este software se describen en la siguiente tabla.

Tabla 22 – Aspectos Técnicos WebcamXP.

Ítem	Descripción
Dispositivos Soportados	• Cámaras USB • Tarjeta capturadora de TV • Cámaras IP • Archivos de Video (AVI/WMV/MP4/MOV/MPEG4/H.264) • Streams Windows Media
Modo de Transmisión	• Imágenes JPEG • Clientes Flash • JavaScript (MPEG O JPEG) • Video streaming Flas • Dispotivos Móviles
Características Adicionales	• Control de pan/til/zoom de manera local y remota • Soporta FTP/FTPS y HTTP/HTTPS post • Detección de Movimiento. • Gestión de usuario • Grabación Permanente • Soporta audio de cámaras

6.3 Cifrado

Uno de los motivos más relevantes de esta investigación se relaciona, con la utilización de mecanismos de seguridad aplicados a la transmisión de video streaming, por ello que en la siguiente figura, se alude al proceso en el actual el prototipo se sitúa.

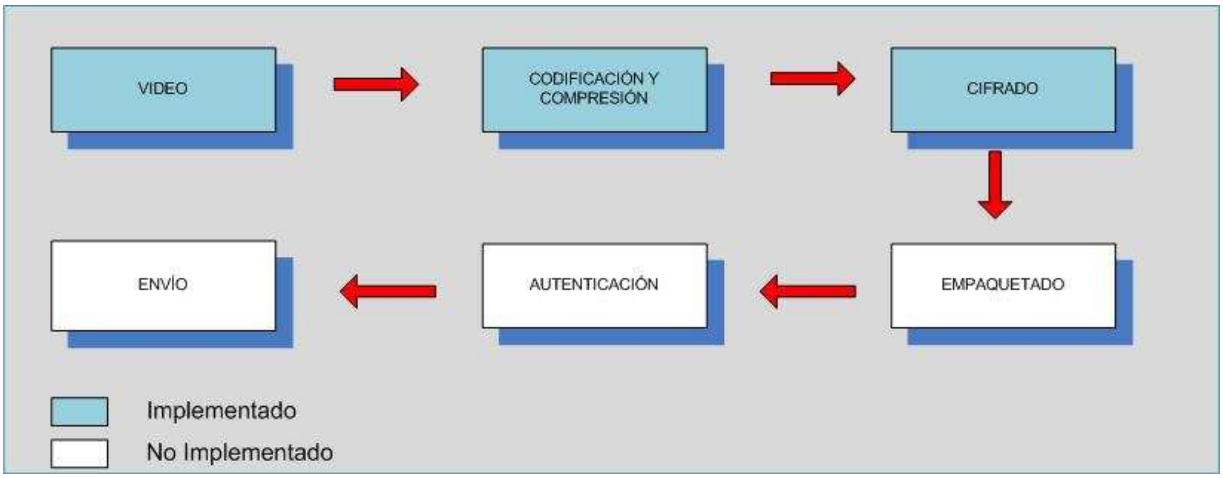

Figura 65 – Aplicación de Cifrado.

Como se mencionó anteriormente, para el cifrado del contenido multimedia transmitido a través de Internet, se ha utilizado, el algoritmo simétrico AES de 256 bit, con ello logrando integridad y robustez en la transmisión de contenido streaming. Además en el proceso de autenticación, se utilizan otros tipos de cifrado, cifrado asimétrico que será abordado en la sección correspondiente.

6.4 Empaquetado

En este proceso, se han utilizado algunos protocolos que están en la dirección de proveer una buena calidad de servicio, con el fin de obtener una fluidez de transmisión, menor retardo de la transmisión y mejor calidad de imagen.

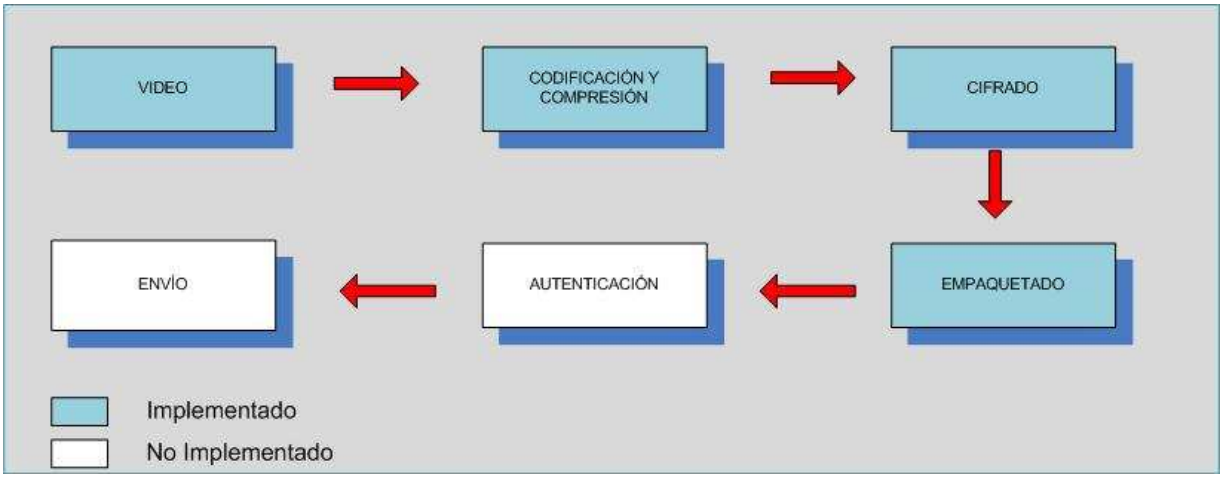

Figura 66 – Empaquetado.

En la siguiente imagen, se muestran los protocolos utilizados en la implementación del diseño de esta propuesta.

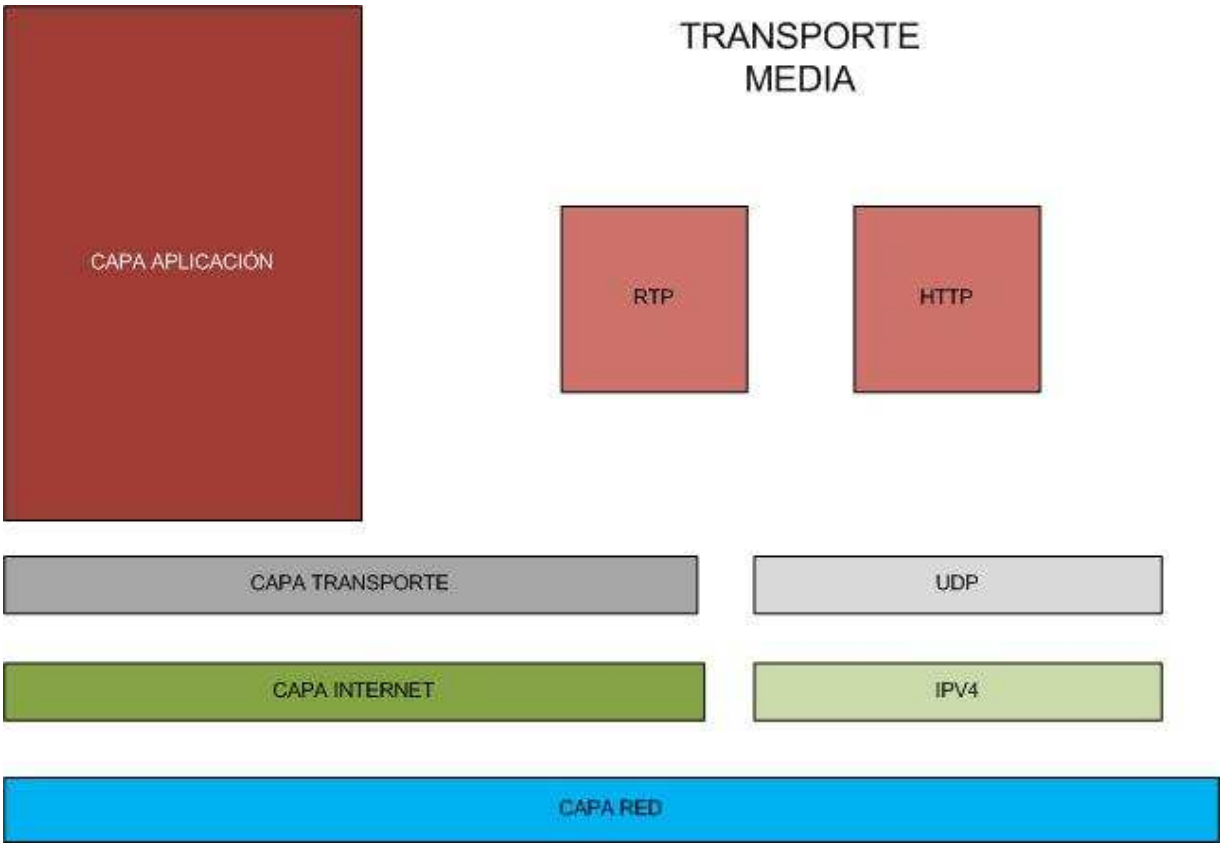

Figura 67 – Aplicación de Empaquetado.

Se ha utilizado en la capa de Internet Ipv4, con el fin de estandarizar y utilizar este protocolo que actualmente es el más usado en las aplicaciones multimedia. En la capa de transporte para prevalecer una transmisión fluida y con el menor tiempo de retardo, es que se hace indispensable el uso del protocolo UDP. Para finalizar en la capa de aplicación de han utilizado dos protocolos con el fin de realizar prueba y poder evidenciar comparaciones, que demuestran que RTP tiene mejores prestaciones que http.

6.5 Autenticación

Para toda implementación de mecanismos o técnicas de seguridad es necesario tener en cuenta la triada de la seguridad, la que considera la autenticación, confidencialidad y disponibilidad de los recursos, en este caso los multimedia, además de no repudio, que conforman 4 aspectos relevantes y los cuales fueron implementados a través del prototipo.

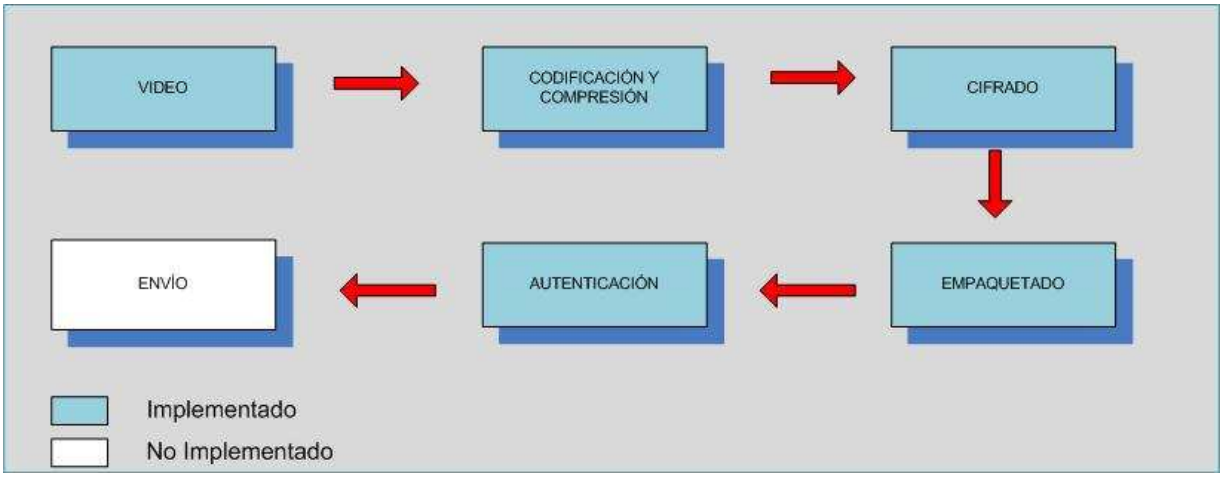

Figura 68 – Aplicación de Autenticación.

En esta parte del proceso propuesto, es necesario que el usuario del prototipo de alguna manera se pueda identificar como quien dice ser, por ello que se ha utilizado cifrado asimétrico, a través del uso de certificados digitales, a través de una red privada virtual o VPN, utilizando un algoritmo de cifrado RSA de 2048 bits y con un algoritmo simétrico para el transporte AES de 256 bits, a través de TLS.

Además, se ha incluido la verificación de clave por medio del certificado, con el fin de aumentar los niveles de seguridad, además de personalizar a cada uno de los usuarios y así poder manejar los tiempos o caducar los permisos y certificados que han sido entregados.

6.6 Envío

A este nivel, el paquete de datos tiene contenido multimedia con códec h.264, luego esta cifrado con algoritmo AES 256 bits, después se ha generado una comunicación segura a través de una VPN a través, de TLS, por medio de certificados digitales con claves cifradas con RSA de 2048 bits.

Es en este momento, donde el paquete de datos, puede ser trasferido, cuya secuencia como se ha mostrado en el proceso propuesto, comienza con la generación de video por parte de las Cámaras IP, luego este video es llevado a los servidores Streaming para poder manejar la concurrencia de usuario, como así también mantener y mejorar la calidad de imagen y de transmisión.

En seguida, los paquetes son cifrados, luego empaquetados a través de los protocolo UDP y RTP, para poder ser transmitidos. Luego se realiza la autenticación de los usuarios a través de los certificados digitales y la clave privada, cuya finalidad es crear un canal seguro a través de una VPN, una vez verificados estos parámetros, con una autenticación exitosa, se prosigue a enviar los paquetes de datos en forma permanente, de acuerdo a las solicitudes de los clientes.

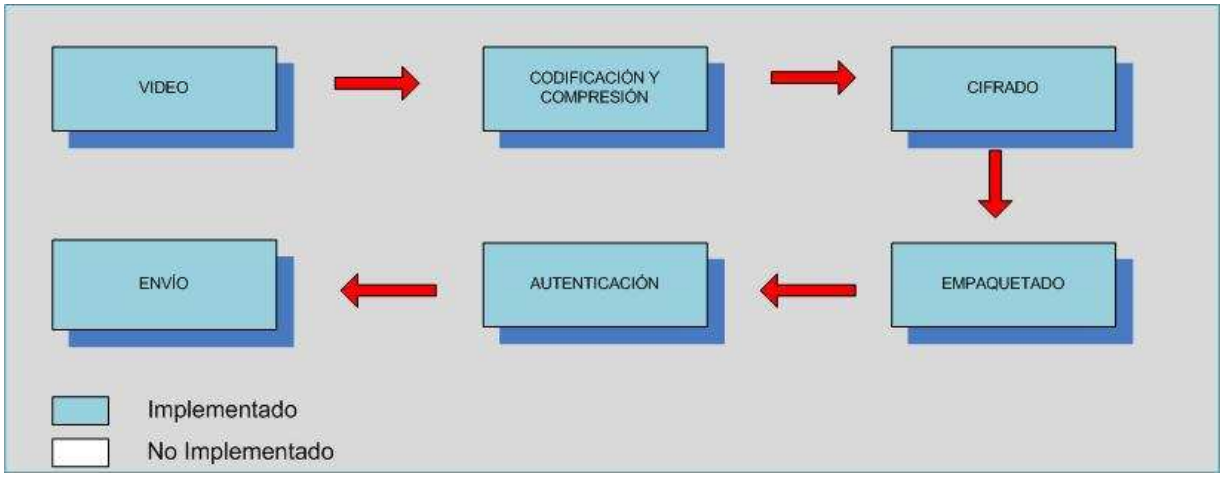

Figura 69 – Aplicación de Envío.

6.7 Herramientas Utilizadas

6.7.1 Openvpn

Openvpn es una solución utilizada en esta propuesta, la cual permite la conectividad a través de SSL/TLS para la VPN. Permite y da la posibilidad de conectarse punto a punto, aplicable y utilizada en esta propuesta. Además de utilizar y dar soporte de seguridad, da la posibilidad de tener una amplia configuración la cual se ha utilizado para obtener balanceo de cargas.

Agregando, se ha implementado esta solución, ya que a través de PFsense, se han podido realizar conexiones de capa 2 o 3, utilizando cifrado asimétrico con SSL/TLS, con el fin de asegurar la identidad de los usuarios a conectar. Se han generado certificados digitales, los cuales a través de Openvpn fueron creados, tomando en cuenta que la entidad certificadora sea nuestra propuesta.

Sin embargo, la posibilidad de usar otro tipo de VPN, como Ipsec que dan mayor soporte y seguridad, se opacan ya que Openvpn provee también seguridad, estabilidad y simplicidad frente a la posibilidad antes mencionada. Asimismo, se adecua fácilmente en Pfsense y es capaz de manejar control de tráfico y calidad de servicio.

Respecto a SSL/TLS este se compone de cuatro protocolos. Estos protocolos funcionan de manera idéntica en SSL y en TLS pero incorporan algunos detalles en TLS para su mejor funcionamiento. A continuación se definen estos cuatro protocolos utilizados, sin entrar en mucho detalle:

- **Record Protocol:** encapsula los protocolos de nivel más alto y construye un canal de comunicaciones seguro. Se podría decir que es un protocolo de transporte.
- **Handshake Protocol:** se encarga de gestionar la negociación de los algoritmos de cifrado y la autenticación entre cliente y servidor. Define las claves de sesión utilizadas para cifrar. Se podría decir que es un protocolo de autenticación.
- **Change Cipher Spec Protocol:** es un mensaje de un byte para notificar cambios en la estrategia de cifrado.
- **Alert Protocol:** señaliza alertas y errores en la sesión establecida.
-

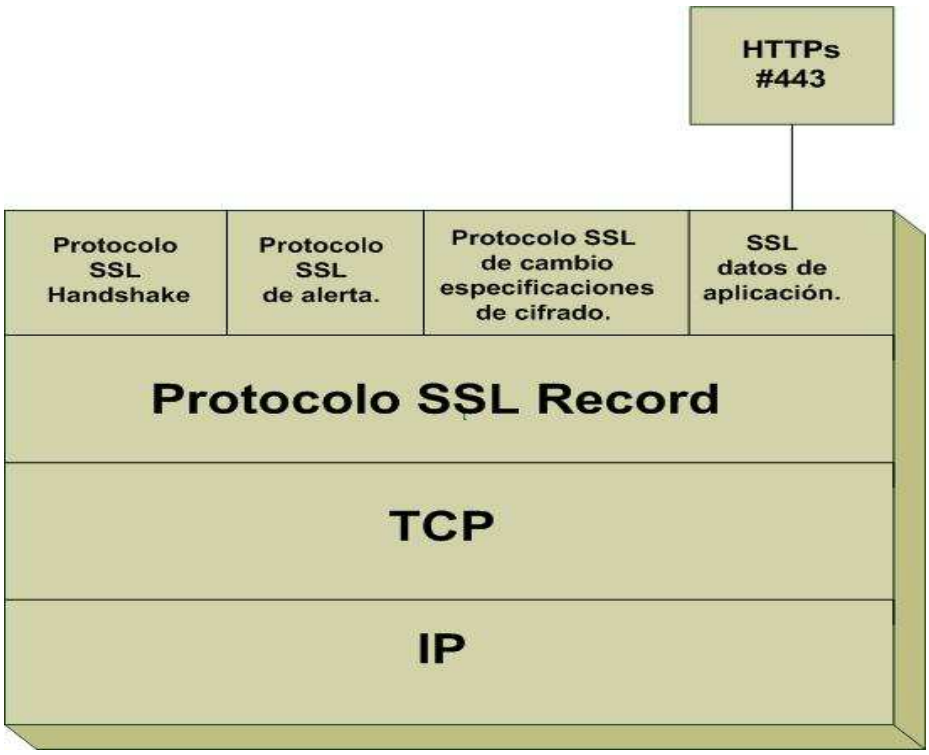

Figura 70 –TLS en modelo OSI.

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución siendo una de las más populares la biblioteca OpenSSL. SSL es capaz de trabajar con la mayoría de protocolos que trabajan sobre TCP de tal manera que el IANA les tiene asignado un número de puerto por defecto, por ejemplo el protocolo HTTP sobre SSL ha sido denominado HTTPS y tiene como puerto el 443.

SSL se ha implementado como un esquema de clave pública para el intercambio de claves de sesión. En primer lugar cliente y servidor intercambian una clave de longitud suficiente mediante un algoritmo de cifrado asimétrico como RSA utilizando certificados. Mediante esa clave se establece un canal seguro, utilizando para ello un algoritmo simétrico AES. Los mensajes a ser transmitidos, se fragmentan en bloques, se comprimen y se les aplica un algoritmo Hash para obtener un resumen (MAC del mensaje) para asegurar la integridad.

En SSL/TLS una sesión es una asociación entre un cliente y un servidor. Las sesiones se crean mediante el protocolo Handshake y coordina los estados del cliente y del servidor. El estado de una sesión incluye la siguiente información:

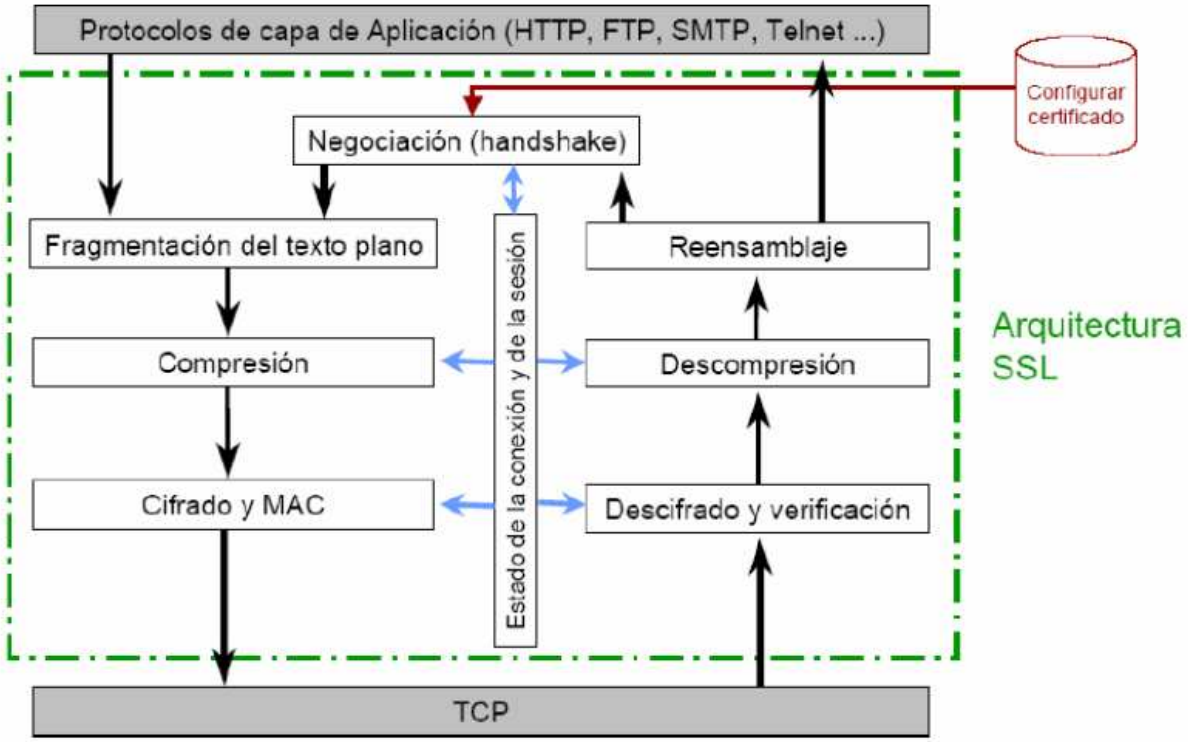

Figura 71 – Arquitectura SSL.

- **Identificador de Sesión:** consiste en una secuencia arbitraria de bytes elegida por el servidor para identificar una sesión activa.
- **Certificado de la Entidad Par:** el certificado del otro extremo de la comunicación (puede ser nulo).

- **Método de Compresión:** indica el algoritmo usado para comprimir los datos antes de cifrarlos.
- **Especificación de Cifrado:** especifica el algoritmo de cifrado de datos (AES) y el algoritmo MAC (SHA-1). También define atributos como el tamaño del Hash.
- **Clave Maestra:** una clave secreta de 48 bytes intercambiado entre cliente y servidor.

En SSL/TLS una conexión es transitoria y está asociada solamente a una sesión, mientras que una sesión puede tener múltiples conexiones. En otras palabras, las sesiones se usan para evitar la costosa negociación de los parámetros de cada conexión. El estado de una conexión incluye la siguiente información:

- **Valores Aleatorios del Servidor y del Cliente:** es una secuencia de bytes elegido por el servidor y el cliente para cada conexión.
- **Clave Secreta MAC de Escritura del Servidor:** es el secreto utilizado en operaciones MAC sobre los datos del servidor.
- **Clave Secreta MAC de Escritura del Cliente:** es el secreto utilizado en operaciones MAC sobre los datos del cliente.
- **Clave de Escritura del Servidor**: es la clave secreta para el cifrado de datos por el servidor y descifrado de datos por el cliente.
- **Clave de Escritura del Cliente**: es la clave secreta para el cifrado de datos por el cliente y descifrado de datos por el servidor.
- **Vector de Inicialización (IV) del Cliente y Servidor:** vectores de inicialización utilizados para bloques de cifrado en estado CBC.
- **Número de Secuencia:** cada estado de conexión contiene un número de secuencia que se mantiene independientemente para los estados de lectura y escritura. El número de secuencia debe ser reseteado a cero cada vez que un estado de conexión pasa a estado activo.

Los cuatro protocolos de los que se compone SSL/TLS y utilizados en la implementación son: Protocolo Record, Protocolo Handshak, Protocolo Cambio Especificación de Cifrado y Protocolo Alerta.

EL SSL/TLS Protocolo Record es el protocolo de transporte que proporciona a cada conexión:

- **Confidencialidad:** utilizando una clave compartida generada durante el protocolo Handshake para el cifrado convencional de los datos.
- **Integridad del Mensaje:** el protocolo de Handshake también genera una clave secreta común que se usa para formar el MAC o código de autenticación del mensaje.

En el funcionamiento del SSL Protocolo Record intervienen mecanismos criptográficos, para los cuales son necesarios ciertos parámetros como la clave secreta para el cifrado. Estos parámetros se negocian durante el establecimiento del protocolo Handshake, que además permite la autenticación de cliente y servidor.

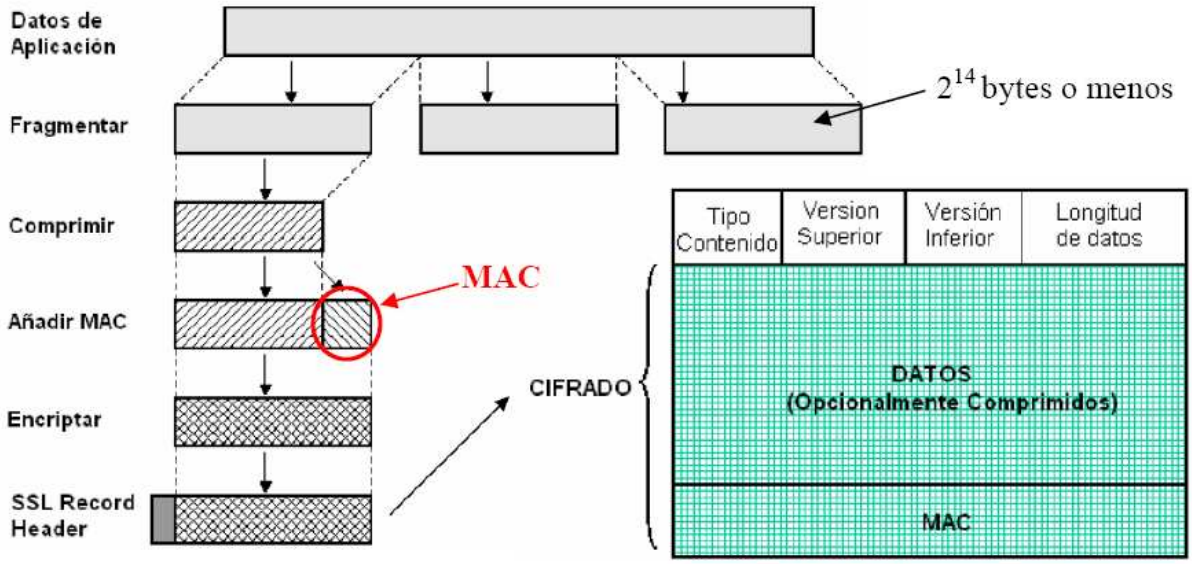

Figura 72 – Cifrado y Formato de Datos de Aplicación con Protocolo Record.

El protocolo más importante que forma SSL/TLS es el Handshake Protocol. Mediante este protocolo se generan los parámetros criptográficos que van a definir el estado de una sesión (una sesión SSL/TLS siempre empieza con el Handshake). Este protocolo permite la autenticación entre el cliente y el servidor y la negociación de los algoritmos de cifrado y las claves y subclaves. Por ejemplo, uno de los parámetros a los que deben llegar a acuerdo el cliente y el servidor es la versión de SSL/TLS y método de compresión.

El protocolo Handshake opera sobre el Record Protocol de SSL/TLS y se establece antes de enviar los datos de aplicación. También cabe destacar que tiene dos modos de negociación de sesión: el "Full Handshake", para la primera conexión, y el "Abbreviated Handshake", para conexiones posteriores. Este protocolo consta de cuatro fases en los que se negocian los parámetros de una sesión:

- **Fase 1:** se establecen las capacidades de seguridad (versión de protocolo, identificador de sesión, suite de cifrado, método de compresión y números aleatorios iniciales).
- **Fase 2:** en esta fase el servidor puede enviar un certificado, intercambio de clave y solicitud de certificado.
- **Fase 3:** el cliente envía su certificado, en caso de habérselo solicitado, el intercambio de clave y puede que envíe verificación de certificado.
- **Fase 4:** se produce el intercambio de suite de cifrado y finalización del protocolo Handshake. En esta fase se completa el establecimiento de la conexión segura.

En la fase 1 del protocolo Handshake el cliente envía al servidor la información necesaria para poder establecer una comunicación segura con SSL/TLS. El servidor decidirá si soporta esos parámetros que el cliente le ha enviado y se lo comunica al cliente. Por ejemplo, el cliente le comunicará la suite de cifrado y el servidor le contestará con la suite de cifrado que va a utilizar junto con otros parámetros.

El mensaje "Client_Conectándose" es el primer mensaje que se envía en la fase 1 del protocolo Handshake. Este mensaje contiene los siguientes parámetros a negociar entre cliente y servidor:

- **Versión:** número de la versión más alta de SSL/TLS que el cliente soporta.
- **Valor Aleatorio:** número aleatorio inicial del cliente.
- **Identificador de Sesión:** si el valor del identificador de sesión es diferente de cero, se tendrá que crear una nueva conexión dentro de esa sesión actualizándolos parámetros de la conexión existente, si el valor es cero indica una nueva conexión en una nueva sesión por lo que se actualizarán los valores tanto de la sesión como de la conexión.

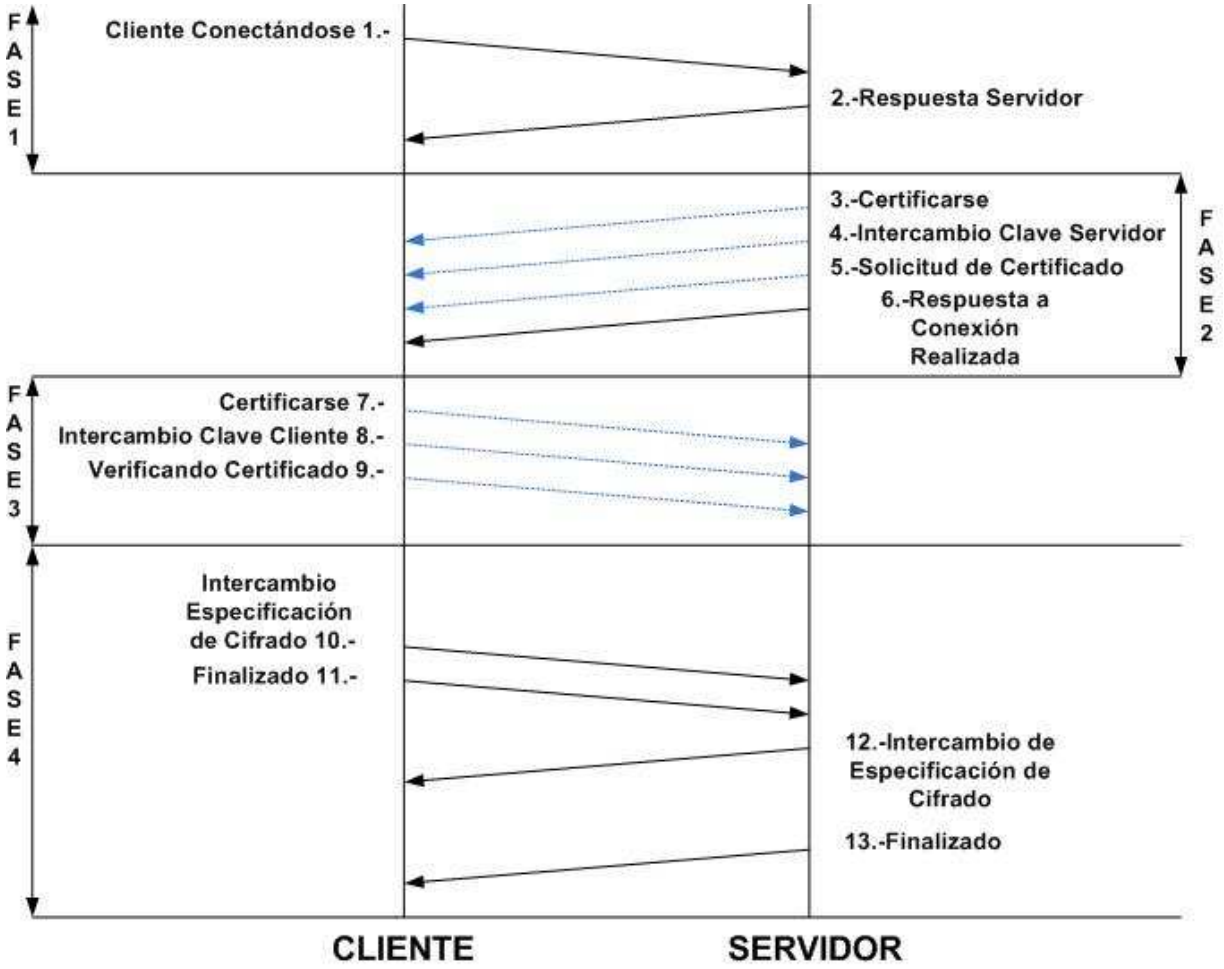

Figura 73 – Fases y Mensajes del Protocolo Handshake de SSL/TLSs.

- **Suite de Cifrado:** contiene una lista de suites de cifrado soportados por el cliente. En esta suite de cifrado deberán aparecer el algoritmo de intercambio de claves, el algoritmo de cifrado, el tipo de cifrado, el tamaño del Hash, parámetros para calcular claves, tamaño de vector de inicialización.
- **Método de Compresión:** el método o métodos que soporta el cliente para comprimir los datos de aplicación.

El mensaje "Servidor Respuesta" es enviado por el servidor tras haber recibido el mensaje "Cliente Conectándose" por parte del cliente. En este mensaje el servidor selecciona los parámetros que soporta el cliente:

- **Versión:** el servidor es el que elige la versión de SSL/TLS más alta propuesta por el cliente y que, además, soporta el servidor.
- **Valor aleatorio:** número aleatorio inicial del servidor.
- **Identificador de Sesión:** si el identificador de sesión del cliente, recibido por el servidor, es igual a cero, el identificador de sesión del servidor contendrá un valor distinto de cero, indicando que se ha creado una nueva sesión. Por otro lado, si el identificador de sesión del cliente es diferente de cero, el servidor comprobará en su caché si guarda información sobre esa conexión, y si es así y se puede crear una nueva conexión responde con el mismo identificador de sesión que el del cliente.
- **Suite de Cifrado:** escoge de entre una lista de suites de cifrado soportados por el cliente. En esta suite de cifrado deberán aparecer el algoritmo de intercambio de claves, el algoritmo de cifrado, el tipo de cifrado, el tamaño del Hash, parámetros para calcular claves, tamaño de vector de inicialización.
- **Método de Compresión:** el servidor escoge el método que soporta el cliente_para comprimir los datos de aplicación.

En la fase 2 del protocolo Handshake se produce, en pocas palabras, la autenticación del servidor e intercambio de claves entre cliente y servidor. Los mensajes enviados en esta fase son "Certificarse", "Intercambio Clave Servidor", "Solicitud de Certificado" y "Respuesta a Conexión Realizada", siendo este último el único mensaje que el servidor está obligado a enviar al cliente.

El primer mensaje de la fase 2 es el mensaje "Certificarse", que contiene el certificado (firmado por la CA) del servidor y que permite autenticarse al cliente. Este certificado contiene, además, la clave pública del servidor que será utilizada para intercambiar las claves de sesión.

El segundo mensaje de la fase 2 es el mensaje "Intercambio Clave Servidor". Este mensaje contiene la clave pública del servidor para el intercambio de claves. Este mensaje no es necesario si el servidor ha enviado su certificado con los parámetros públicos RSA para el intercambio de claves.

El mensaje “Solicitud de Certificado” es el tercer mensaje de la fase 2 y tiene la función de pedir al cliente que se autentique, para ello le pide al cliente un determinado tipo de certificado y una autoridades de certificación (CA).

En el mensaje “Respuesta a Conexión Realizada” no se envía ningún parámetro, ya que pone fin a los mensajes de la fase 2 asociados al servidor. Con la información enviada en esta fase el cliente autentica al servidor. Utilizando RSA para intercambio de claves, el servidor envía una clave pública para que el cliente cifre con ella la información necesaria para generar una clave secreta común y la devuelva al servidor.

De este modo, el servidor la descifrará con la clave privada y podrá generar la misma clave común. Por otra parte, en caso de que el servidor no transmita su certificado al cliente, le debe enviar una clave pública mediante el mensaje “Intercambio Clave Servidor” utilizando para ello el algoritmo Diffie-Hellman.

La fase 3 del protocolo Handshake solo se lleva a cabo en el caso en que haya que autenticar al cliente (pues el servidor envió el mensaje “Solicitud de Certificado”). En tal caso, el cliente debe responder con su certificado, si lo tiene, o con un mensaje de alerta indicando que no lo tiene (alerta “No Certificado”). Los posibles mensajes que puede enviar el cliente en esta fase del protocolo Handshake son: “Certificado”, “Intercambio Clave Cliente” y “Verificar Certificado”.

El primer mensaje enviado por el cliente en la fase 3 es el mensaje “Certificarse”, en el que incluye el certificado del cliente para autenticarse al servidor.

El segundo mensaje de la fase 3 es el mensaje “Intercambio Clave Cliente”, en el que el cliente envía al servidor una clave secreta o número aleatorio generado, también denominada clave pre-master, de 48 bytes, cifrada con la clave pública del servidor. El servidor obtendrá dicha clave pre-master descifrando con su clave privada. El cliente y el servidor utilizarán la clave pre-master para calcular la clave maestra, las claves de sesión y las claves MAC.

El tercer mensaje de la fase 3 es el mensaje “Verificar Certificado”, en el que se verifica que el cliente posee la clave privada en concordancia con el certificado del cliente. Este mensaje se envía junto al anterior y consta de una firma Hash que abarca los mensajes anteriores. El cifrado se realiza con la clave privada del cliente.

La fase 4 del protocolo Handshake es la última fase de este protocolo, y sin entrar mucho en detalle, el cliente envía un mensaje al servidor diciendo que los siguientes mensajes serán cifrados con la clave de sesión o clave maestra. Además envía un mensaje cifrado comunicando al servidor que la parte del cliente del protocolo Handshake ha finalizado.

Por otro lado, el servidor envía un mensaje al cliente diciendo que los mensajes serán cifrados con la clave de sesión o clave maestra. Por último, al igual que ha hecho el cliente, envía un mensaje cifrado diciendo que su parte del protocolo Handshake ha finalizado.

Esta fase consta de dos mensajes que son iguales tanto para el cliente como para el servidor. El primer mensaje es el "Intercambio Especificación de Cifrado" que sirve para dar como concluido el intercambio, pasando del estado pendiente al estado operativo. El segundo y ultimo mensaje es el "Finalizado" que sirve para finalizar el protocolo Handshake y para comenzar a transmitir los datos de aplicación protegidos con las claves y algoritmos negociados.

Por otra parte, OpenVPN permite encapsular el tráfico en paquetes que utilicen el protocolo de transporte UDP. Además otra característica muy interesante en las versiones más recientes de OpenVPN es la posibilidad de utilizar un único puerto en el servidor para todas las conexiones VPN o de aguantar más de una conexión TCP.

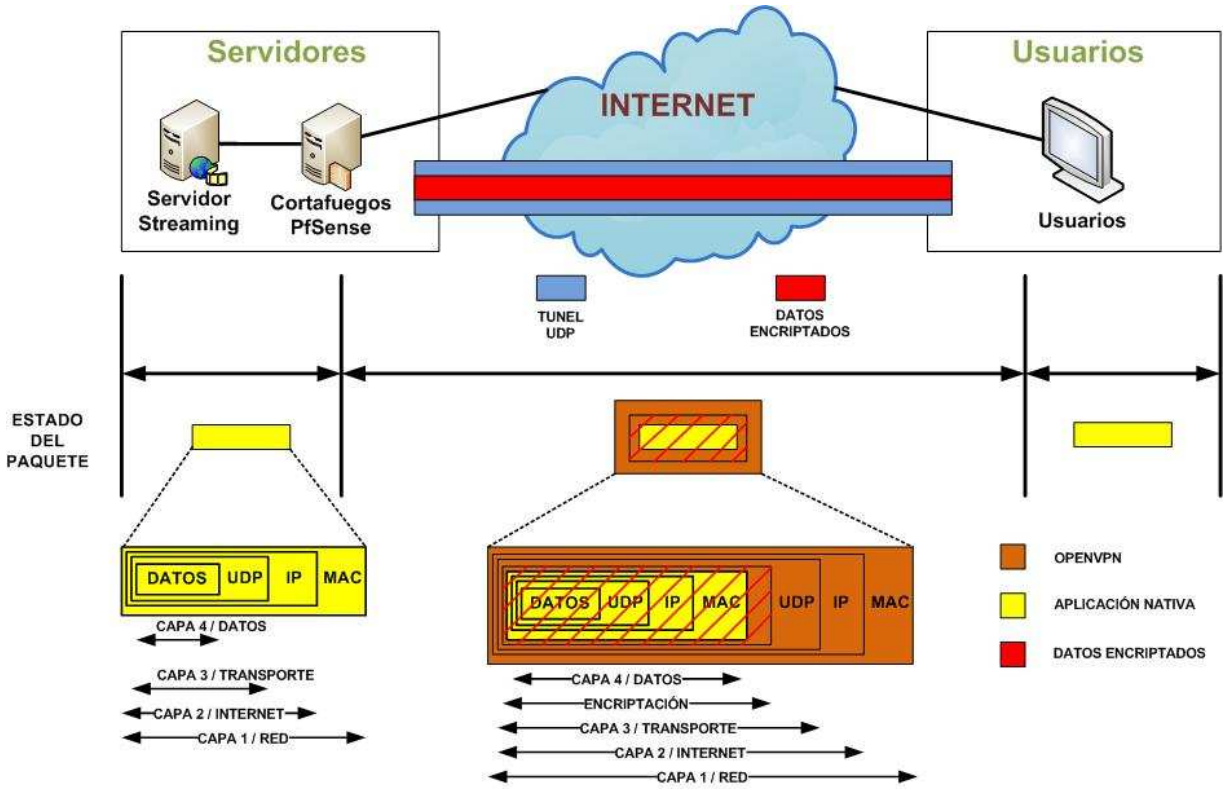

Figura 74 – Formato del Paquete Encapsulado por OPENVPN.

De entre todas las aplicaciones y características que OpenVPN ofrece se pueden citar las siguientes utilizadas en este proyecto:

- Posibilidad de implementar dos modos básicos, "bridge" o "tunnel", en la capa 2 o capa 3 respectivamente, con lo que se logarn túneles capaces de enviar información en otros protocolos no IP como IPX o broadcast (Netbios).

6.7.1.1 OpenVPN y Paquetes Necesarios

La herramienta OpenVPN debe ser instalada tanto en las máquinas que hagan de servidor como en las que hagan de clientes. No existe una versión para clientes y otra para servidores, desde que OpenVPN se instala en el PC, proporciona tanto las funciones del cliente como las del servidor con sus respectivos comandos y directivas.

OpenVPN corre casi completamente en el espacio de usuario no exigiendo ninguna modificación ni componente en el kernel del sistema operativo que no sean los controladores virtuales "TUN/TAP" disponibles para muchas plataformas tales como Windows, Linux, MAC OS X y variantes de BSD.

6.7.1.1.1 Los controladores virtuales TUN/TAP y VTUN

El modelo que, básicamente, utiliza OpenVPN para implementar una VPN se basada en utilizar el espacio de usuario y enlazar una interfaz de red virtual punto a punto llamada "tun" con otra interfaz de red virtual punto a punto ("tun") remota.

Un adaptador de red virtual "tun" a su misma vez se podría ver como un enlace punto a punto entre la tarjeta de red del PC y el sistema operativo. La interfaz "tun" en lugar de entregar los bits al medio físico los entrega al espacio de usuario del sistema operativo y éste abre, lee y/o escribe datos de paquete IP en la interfaz "tun" como si de un fichero se tratase.

Cuando una interfaz virtual TUN/TAP recibe el nombre "tun" significa que está trabajando en modo túnel (o tunnel) punto a punto, enlazando con otra interfaz virtual del mismo tipo. En la mayoría de los casos, y en este proyecto se implementarán túneles con el modo túnel, utilizando interfaces virtuales "tun".

Otra ventaja de utilizar el concepto de dispositivo de red virtual TUN/TAP es que se desplaza la complejidad de la VPN al espacio de usuario, separando lógicamente los componentes de red de los componentes de cifrado y seguridad, obteniendo, de esta manera, un código que pueda ser exportado a diferentes plataformas, y obteniendo también una interfaz intuitiva al usuario final.

6.7.1.1.2 Compresión con LZO

LZO es una librería multiplataforma de compresión de datos sin perdidas, escrito en ANSI C. LZO ofrece bastante velocidad en la compresión de datos y mayor velocidad en la descompresión de los datos, que es donde más destaca por su gran velocidad. Además no requiere memoria para la descompresión de los datos.

LZO implementa varios algoritmos de compresión y descompresión de datos con algunas de las siguientes características:

- La descompresión es simple y muy rápida.
- No requiere memoria para la descompresión.
- La compresión de los datos también es bastante rápida.

- Requiere de algún tipo de buffer de 64 kB de memoria para la compresión.Existen niveles de compresión de los datos mas bajos en el que, únicamente, se necesitan 8 kB de memoria.
- No necesita ningún tipo de buffer o memoria para la descompresión además de los buffers fuente y destino.
- Permite al usuario realizar un ajuste entre calidad de compresión y velocidad de compresión sin que la velocidad de compresión se vea afectada.
- Proporciona niveles de compresión para la realización de una pre-compresión de los datos con el que se logra un ratio de compresión totalmente competitivo.
- El algoritmo es sin perdidas.
- El algoritmo es thread-safe.
- LZO soporta superposición en las compresiones.

LZO utiliza un algoritmo de compresión en bloque, de manera que comprime y descomprime bloques de datos. Cuando LZO trata datos que no pueden comprimirse más, expande los datos de entrada, de cómo máximo 16 bytes, por datos de entrada de 1024 bytes.

Otro aspecto importante es la rapidez y depuración de esta librería. Cuando hay muchos ficheros de objetos, en su mayoría independientes unos de otros, las dimensiones de un ejecutable que esté relacionado con la biblioteca LZO suele ser bastante baja (de unos pocos kB), debido a que el enlazador solo añade los módulos que se necesitan utilizar realmente, consiguiendo así ejecutables más ligeros y una mayor rapidez.

6.7.1.1.3 Protocolo

A continuación se describe, sin entrar en mayor detalle el protocolo utilizado por OpenVPN y el formato de los paquetes de OpenVPN. Dicho protocolo se encuentra definido en el fichero de cabecera ssl.h. OpenVPN encapsula en un mismo datagrama UDP los canales de control y datos. Es decir, utiliza el mismo puerto para ambos canales, por lo que un datagrama UDP puede contener un mensaje de control y de datos a la vez. Además, un paquete de OpenVPN puede contener información IP o una trama Ethernet pudiendo operar a nivel IP o a nivel de enlace.

Utilizando UDP como protocolo encapsulador, se obtiene una encapsulación del paquete original como la que se muestra en la siguiente figura:

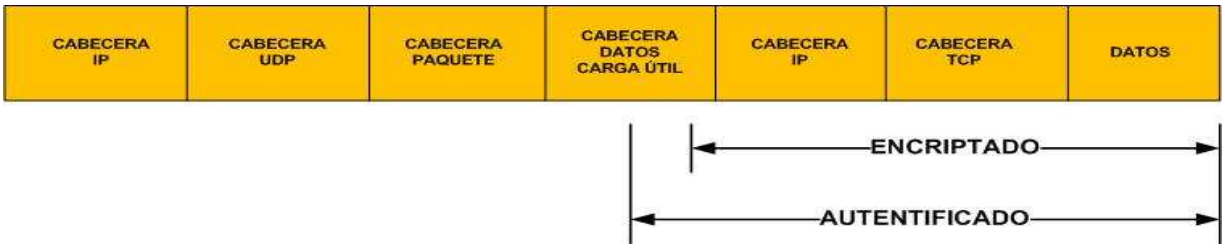

Figura 75 – Encapsulación del Canal de Datos por OpenVpn.

OpenVPN divide la cabecera del payload en dos partes: la cabecera del paquete, que identifica el tipo de paquete y el material o parámetros para las claves, y la cabecera del paquete de datos, que contiene parámetros de autentificación, vector de inicialización y campos de número de secuencia del paquete de datos. El formato de un paquete en OpenVPN es el siguiente:

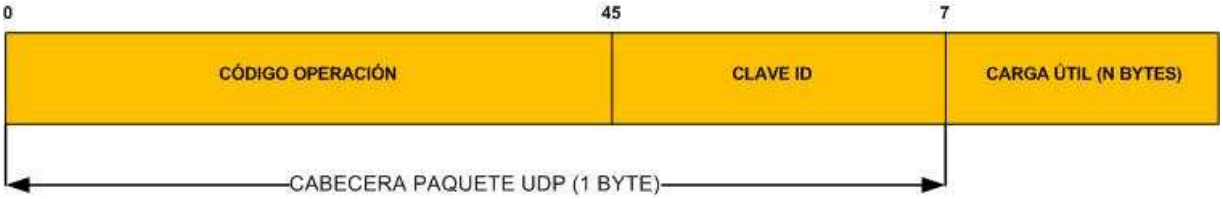

Figura 76 – Formato de un Paquete OpenVpn utilizando UDP.

- Código de Operación/ Clave Id (8 bits): al utilizar TLS:
  - Tipo de mensaje del paquete (5 bits): define el tipo de mensaje que contiene el paquete.
  - Clave ID (Identificador de clave, 3 bits): se refiere al identificador de clave de la sesión actual TLS. OpenVPN renegocia sin problemas las sesiones TLS utilizando un nuevo identificador de clave para la nueva sesión. En este caso, se permite el solapamiento entre la sesión TLS vieja y la sesión TLS nueva, proporcionando una transición estable para que el túnel pueda trabajar sin problemas.
  - Payload (carga de datos, n bytes): este campo puede ser un mensaje P_CONTROL, P_ACK o P_DATA.

6.7.1.1.4 UDP y TCP

OpenVPN permite, desde la versión 1.5, la posibilidad de utilizar los protocolos TCP o UDP como protocolos de transporte para establecer la comunicación con el host remoto. Para poder manejar esta característica OpenVPN proporciona la directiva donde se puede tener los valores udp, tcp-client o tcp-server. El protocolo por defecto utilizado es udp, por tanto, OpenVPN utilizará el protocolo udp cuando la directiva sea utilizada.

OpenVPN ha sido diseñado originalmente para operar de manera óptima utilizando como protocolo de transporte UDP, pero TCP puede utilizarse en situaciones donde UDP no puede ser usado. En comparación con UDP, TCP es menos eficiente y menos robusto cuando es utilizado sobre redes que usan alguna capa fiable y con posibles congestiones. Existen algunos casos, sin embargo, donde se usa TCP puede tener ventajas de seguridad y robustez frente a la utilización de UDP, como en el caso de crear túneles no IP o de utilizar aplicaciones sobre protocolos que no tienen ningún nivel de fiabilidad. Otro aspecto a favor de la aplicación de UDP frente a TCP es que el uso de UDP frente a TCP proporciona mejor protección frente a ataques de denegación de servicio (DoS) y frente al escaneo de puertos.

Muchas aplicaciones se pueden aplicar sobre OpenVPN, como en este caso la transmisión de video streaming, se ha utilizado el protocolo UDP frente al protocolo TCP por diversas razones. Para empezar, en la mayoría de los casos, los sistemas streaming aplican el protocolo RTP (Real-time Transport Protocol) que es transportado usando el protocolo UDP y es el que se ha utilizado para el transporte de video. Como ya se ha comentado TCP proporciona una conexión fiable, pero este aspecto, en los sistemas streaming no es bueno. Si se usa TCP en streaming, cuando un paquete es rechazado, el emisor vuelve a retransmitir el paquete ante la petición del receptor o receptores. Pero en este caso al reensamblar los paquetes de video retransmitidos en un stream de video podrían resultar demasiado tarde para obtener una reproducción fiable del video original. Por el contrario, UDP da por bueno paquetes enviados fuera de orden y no existe verificación (ACK) de si el paquete llega.

6.7.2 Pfsense

Es una suite completa, basada en FreeBsd, la cual entrega distintas herramientas propias de un cortafuego, como Nat, VPN, control de balanceo, entre otras. Se ha utilizado para el prototipo, con el fin de manejar 3 aspectos fundamentales: seguridad en el servidor streaming, VPN y control de tráfico.

Con los aspectos antes mencionados, es que Pfsense juega un papel fundamental, gracias a sus prestaciones e integridad con Openvpn.

La ventaja implementar PfSense son las siguientes:

- **Protege de intrusiones:** Evita el acceso al servidor streaming de aquellas entidades no autorizadas, con ello limita el acceso y solicita autenticación para aquellos que desean y tengan permisos para acceder a dicho contenido.
- **Protección de la Información Privada:** Permite definir los distintos niveles de acceso ala información de manera que en una organización, cada grupo de usuarios definido tendrá acceso sólo a los servicios e información que son estrictamente necesarios.
- **Optimización de Acceso:** Identifica aquellos elementos críticos y optimiza la comunicación entre usuario o cliente y servidor, con ello reconfigurar los parámetros de seguridad cada vez que sea necesario.
- **Gestión de Tráfico:** Permite el acceso y salida de contenido multimedia desde el servidor streming a Internet y viceversa. Maneja la comunicación y prioriza el contenido y paquetes de datos para optimizar la calidad de servicios del servidor streaming por efecto de peticiones simultáneas. Otorga la posibilidad de manejar los anchos de banda de entrada y salida a la red local y es capaz de encapsular y etiquetar cada paquete de datos con un identificador e índice de prioridad para un mayor rendimiento y transmisión de contenido multimedia.

- **VPN:** Maneja y controla la red privada virtual, utilizando Openvpn para realizar dicha labor. Es posible configurar, gestionar e implementar Openvpn en el servidor PfSense, con esto un manejo simple y efectivo de la configuración de los parámetros de la VPN. Es capaz de controlar y optimizar las peticiones de conexiones seguras y distribuye de mejor maneja las conexiones realizas en el servidor. Es capaz de otorgar otros aspectos de seguridad en caso necesario y prevalece una comunicación segura fiable y optimizada, ya que provee la utilización de protocolos que permiten una mejor calidad de servicio.
- **Manejo Red Interna:** Permite configurar y gestionar la red interna de los servidor, con ello el manejo de parámetros DNS, IPs, Host, entre otras. Otorga de manera mas fácil la configuración de dichos parámetros, además de su auditoría y constantes optimización y cambios de acuerdo a las necesidades de seguridad necesarias.

6.7.3 Sistemas Operativos

Los sistemas utilizados para la implementación de esta investigación se mencionan en la siguiente tabla.

Tabla 23 – Aspectos Técnicos Sistema Operativo.

Sistema	**Versión**
Windows	XP Profesional, SP2. Windows Server 2009.
Linux	Debian, Lenny 5.0.4
FreeBsd	PfSense 1.2.3

6.7.4 Hardware

El hardware utilizado para los efectos de implementación y pruebas se describe a continuación.

Tabla 24 – Aspectos Técnicos Hardware Cliente.

Ítem: Placa Madre	**Descripción**
Tipo de Procesador	Equipo Multiprocesador ACPI, Mobile DualCore Intel Core 2 Duo T5600, 1833 MHz (11 x 167)
Chipset	Intel Crestline-PM PM965
Memoria del Sistema	2048 MB (DDR2-667 DDR2 SDRAM)
Tipo de BIOS	Phoenix (11/19/08)
Memoria Cache	2 MB

Ítem: Almacenamiento	Descripción
Controlador IDE	Intel(R) ICH8M 3 port Serial ATA Storage Controller - 2828
Storage Controller	SCSI/RAID Host Controller
Disco duro	WDC WD2500BEVS-75UST0 (232 GB, IDE)

Ítem: Almacenamiento	Descripción
Tarjeta de Red	Marvell Yukon 88E8040 PCI-E Fast Ethernet Controller

Tabla 25 – Aspectos Técnicos Hardware Servidores.

Ítem: Placa Madre	**Descripción**
Tipo de Procesador	Equipo Multiprocesador, Pentium 3, 1200 Mhz.
Chipset	Intel
Memoria del Sistema	512 MB (DDR400 DDR SDRAM)
Memoria Cache	512 MB

Ítem: Almacenamiento	Descripción
Controlador IDE	Intel(R) ICH8M 3 port Serial ATA Storage Controller - 2828
Disco duro	WDC (40 GB, IDE)

Ítem: Almacenamiento	Descripción
Tarjeta de Red	Intel PCI-E Fast Ethernet Controller

Tabla 26 – Aspectos Técnicos Isp.

Ítem: Conexión Internet	Descripción
Conexión	2 MB
Velocidad de Subida	450 KB
Velocidad de Bajada	1200 KB

6.8 Calidad de servicio

Para manejar una buena calidad de servicio, anteriormente se han mencionado aspectos muy relevantes que apoyan y entregan una mejor transmisión de video a través de Internet. Es por ello que se alude a la utilización de protocolos de transmisión de video como RTP y UDP.

Como se mencionó en el ítem anterior, con Pfsense se ha manejado el balanceo de carga entrante y saliente, con ello apoyar una mejor calidad de servicio, a través de una fluidez y mayor envío de paquetes de datos de video.

7 Conclusión

Esta investigación nace ante la problemática existente en la transmisión de contenido en los sistemas de tele vigilancia, debido a la falta de seguridad que presentan las comunicaciones a través de las infraestructuras de red, como Internet. Por ello, que existe una amplia gama de posibilidades y herramientas, que pueden ser aplicadas al contexto de la tele vigilancia, y en respuesta, la investigación propone un modelo y herramientas que son aplicables y dan mejores posibilidades de obtener una comunicación más rápida, fluida y segura.

Como se ha mencionado a través de esta investigación, la tecnología utilizada para mantener y satisfacer los criterios de seguridad principales: confidencialidad, autenticidad, integridad y no repudio, es el uso e implementación de una VPN basada en protocolos SSL/TLS, implementada por ser una herramienta completa, flexible, simple, robusta, económica y escalable.

En la confección del marco teórico para esta investigación, fue necesario realizar un estudio acabado de las distintas tecnologías y tópicos, que enmarcan la aplicación de mecanismo de seguridad informática, en la transmisión de video streaming para los sistemas de Tele Vigilancia. Es por ello que a lo largo de este documento se ha hecho mención al marco teórico, cumpliendo con el primer objetivo de esta investigación.

Respecto a lo anterior, es posible aplicar mecanismos de seguridad en la transmisión de video a través de las redes como Internet, por ello, que se ha propuesto un modelo que satisface la necesidad de proteger los medios de transmisión, cuyo fin es su utilización en los sistemas de Tele Vigilancia actuales. Frente a esto, se cumple el segundo objetivo de esta investigación, a través del diseño propuesto en este documento.

Además, se dan evidencias del cumplimento de los procesos de desarrollo del prototipo, que da cuenta la utilización de mecanismos de seguridad aplicados a la transmisión multimedia. En consecuencia, el documento cita resultados obtenidos en esta etapa final, además de un análisis a cada uno de ellos.

Asimismo, en las etapas del desarrollo del proyecto, se han reforzado y refinado algunos términos y tópicos relevantes del modelo propuesto, cuyo fin es obtener nuevos conocimientos y habilidades en aspectos de seguridad informática, que fueron aplicados en esta propuesta.

En esta investigación se abordaron los aspectos mas actuales desde el punto de vista tecnológico, los cuales fueron aplicados al prototipo, sin embargo, no deja de lado la posibilidad de poder aplicar otras técnicas futuras o recientes que puedan reforzar y mejorar los resultados obtenidos por esta propuesta, ya sea a nivel de hardware, software, metodologías, mecanismos o técnicas, en las tres directrices de esta investigación, calidad de servicio, sistemas de tele vigilancia y ,mecanismo de seguridad.

No solo es necesario considerar las tecnología que aborda esta investigación, sino también aquellas que van en evolución y que afectan o benefician en forma directa a esta propuesta, como por ejemplo dispositivos móviles, anchos de banda, tecnología 3G, entre otras, y que pueden dar pie a nuevas ideas o desarrollos que puedan mejorar la seguridad y la transmisión de contenido a través de Internet.

Para finalizar, se ha demostrado a través del prototipo y sus resultados que es posible aplicar mecanismos de seguridad en la transmisión de video streaming, por ello que se han considerando los aspectos mas relevantes del modelo propuesto, sin dejar de lado aspectos técnicos, modelos, tecnologías y nuevas ideas que puedan aportar al mejor desarrollo de esta investigación en el tiempo.

Es de vital importancia, que los sistemas de tele vigilancia utilicen mecanismos de seguridad, ya que su expansión y utilización, otorgan la posibilidad de ataques de distinta índole, vulnerando el sistema propiamente tal. Además, se ha demostrado que la utilización de técnicas de seguridad aplicadas a la transmisión de video streaming, no generan mayores efectos a nivel de calidad de servicio, es decir, que al utilizar mecanismos de seguridad se ha demostrado que el rendimiento del sistema no ha sido afectado a gran escala, asimismo, su utilización genera diversas ventajas como robustez, seguridad, escalabilidad, entre otras, frente al pequeño impacto que afecta al rendimiento del sistema.

8 Referencias

[1] Instituto Nacional de Estadística, Encuesta de Seguridad Ciudadana, Ciudad Valparaíso, Encuesta relativa por sexo, rango edad y clasificación socioeconómica, Abril 2008.

[2] Sistemas Analógicos, 2007. http://www.mailxmail.com/curso-televigilancia-seguridad-electronica/sistemas-analogicos

[3] Sistemas Digital Basado en Computador, 2007. http://www.mailxmail.com/curso-televigilancia-seguridad-electronica/sistema-video-digital-basado-pc.

[4] Distintos tipos de Cámaras, 2007. http://www.mailxmail.com/curso-televigilancia-seguridad-electronica/distintos-tipos-camaras-tecnologias

[5] Cámaras de Televigilancia, 2009. http://es.ati247.com/products/products_cats.asp?clidcat=9

[6] Cámaras de Televigilancia, 2009. http://www.midisec.com/

[7] Elementos de Cámaras, 2009. http://www.axis.com/products/video/about_networkvideo/light_sensitivity.htm

[8] Request For Coment 791, Internet Protocol, 1981.

[9] Request For Coment 2460, Internet Protocol Version 6, 1998.

[10] Request For Coment 1180, Tutorial TCP/IP, 1991.

[11] RTP: A Transport Protocol for Real-Time Applications, http://www.ietf.org/rfc/rfc3550.txtS, 2003.

[12] Request For Coment 2326,introducción Real Time Streaming Protocol, 1998.

[13] Especificación RTMP, 2009. http://www.adobe.com/devnet/rtmp/

[14] Request For Coment 3711, Real Time Control Protocol, 2004.

[15] SRTP: The Secure Real time Transport Protocol, www.ietf.org/rfc/ rfc3711.txtS, 2004.

[16] Request For Coment 3261, SIP, 2002.

[17] VLAN Insecurity, 2003. http://www.spirit.com/Network/net0103.html

[18] Una Arquitectura de Control de Acceso a Redes de Área Local Inalámbricas 802.11, 2003. http://ditec.um.es/~ocanovas/papers/802.1X.pdf

[19] Request For Coment 2660, 1999.

[20] Request For Coment 2764, 2000.

[21] Request For Coment 2411, 1998.

[22] ¿Por qué Quicktime?, 2009. http://www.apple.com/es/quicktime/whyqt/

[23] Formatos de Archivo AVI, 2009. http://support.microsoft.com/kb/316992

[24] Diccionario Informático, Concepto Real Video, 2009. http://www.alegsa.com.ar/Dic/realvideo.php

[25] Windows Media Video, Microsoft, 2009. http://www.microsoft.com/windows/windowsmedia/forpros/codecs/video.aspx

[26] Especificación ASF, 2009. http://www.microsoft.com/windows/windowsmedia/forpros/format/asfspec.aspx

[27] Guía de Aprendizaje Flash Video, 2009. http://www.adobe.com/es/devnet/flash/articles/video_guide.html

[28] Request For Coment 3170, 2001.

[29] Joan Daemen and Vincent Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard Springer, 2002.

[30] Kent, S. and Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, http://www.ietf.org/rfc/rfc2401.txt , November 1998.

[31] Kent, S. and Atkinson, R., "IP Encapsulating Security Payload (ESP)", IETF RFC 2406, http://www.ietf.org/rfc/rfc2406.txt , November 1998

[32] Bozoki E., IP Security Protocols, Dr. Dobb's Journal, 1999, Pág. 42-55.

[33] Qiao, L. and Nahrstedt, K., Comparison of MPEG Encryption Algorithms, Computers and Graphics, Vol. 22, 1998, Pág. 437-448.

[34] Dierks, T. and Allen, The TLS Protocol, Version 1.0, IETF RFC 2246, http://www.ietf.org/rfc/rfc2246.txt, 1999.

[35] Meyer, J. and Gadegast, F., Security Mechanisms for Multimedia with Example MPEG-1 Video, Tech. Uni. de Berlin, 1995

[36] Lin, C-W., Zhou, J., Youn, J. and Sun, M-T., MPEG Video Streaming with VCR Functionality, IEEE Transactions on Circuits and Systems for Video Technology, 2001, Pág. 415-425.

[37] [19] Qiao, L., Nahrstedt, K. and Tam, M.-C., Is MPEG Encryption by using Random List instead of Zig-Zag order secure?, IEEE International.

[38] Qiao, L. and Nahrstedt, K., A New Algorithm for MPEG Video Encryption, 1st International Conference on Imaging Science, Systems and Technology (CISST97), 1997, Pág. 21-29.

[39] Shi, C. and Bhargava, B., Light-weight MPEG Video Encryption Algorithm , Multimedia98, 1998, Pág. 55-61.

[40] Shi, C. and Bhargava, B., An Efficient MPEG Video Encryption Algorithm, 17th IEEE Symposium on Reliable Distributed Systems, October 1998, Pág. 381-386.

[41] Shi, C. and Bhargava, B., A Fast MPEG Video Encryption Algorithm, ACM Multimedia '98, 1998, Pág. 81-88.

[42] Shi, C. and Bhargava, B., A Fast MPEG Video Encryption Algorithm", ACM Multimedia '98, 1998, pp. 81-88

[43] Zeng, W. and Lei, S., Efficient Frequency Domain Video Scrambling for Content Access Control, ACM Multimedia99, 1999, Pág. 285-294

[44] Zeng, W., Wen, J. and Severa, M., Fast Self-Synchronous Content Scrambling by Spatially Shuffling Codewords of Compressed Bitstreams, IEEE International Conference on Image Processing, 2002, Pág. 169-172

[45] Griwodz, C., Merkel, O., Dittmann, J. and Steinmetz, R., Protecting VoD the Easier Way, ACM Multimedia98, 1998, Pág. 21-28.

[46] Tosun, A. S. and Feng, W.-C., Efficient Multi-layer Coding and Encryption of MPEG Video Streams, IEEE International Computing Expo, 2000, Pág. 119-122

[47] Tosun, A. S. and Feng, W.-C., A Light-weight Mechanism for Securing Multi-Layer Video Streams, IEEE International Conference on Information Technology: Coding and Computing, 2001, Pág. 157-161

[48] Alattar, A. M. and Al-Regib, G. I., "Evaluation of Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-Streams, IEEE Symposium on Circuits and Systems, 1999, Pág. 340-343

[49] Alattar, A. M., Al-Regib, G. I. and Al-Semari, S. A., Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-Streams, International Conference on Image Processing, 1999, Pág. 256-260.

[50] Spanos, G. A. and Maples, T. B., Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications, IEEE 15th Annual International Conference on Computers and Communications, 1996, Pág. 72-78

[51] N. B. of Standards, Digital signature standard, National Bureau of Standards, Tech. Rep. FIPS Publication 186, 1994.

[52] D. Eastlake 3rd and P. Jones, “US Secure Hash Algorithm 1 (SHA1), RFC 3174, 2001.

[53] Axis, Ficha Técnica Cámaras de Red, http://www.axis.com/products/video/camera/index.htm, 2008.

[54] But, J., Implementing Encrypted Streaming Video in a Distributed Server Environment, Submitted to IEEE Multimedia, Abril 2004.

[55] But, J. and Egan, G., Designing a Scalable Video On Demand System, International Conference on Communications, Circuits and Systems (ICCCAS'02), Pág. 559-565.

[56] Reisslein, M., Hartanto, F. and Ross, K. W., "Interactive video streaming with proxy servers (extended version)", Tech. Rep., GMD FOKUS, Junio 1999.

[57] Wu, D., Hou, Y. T., Zhu, W., Zhang, Y-Q. and Peha, J. M., Streaming Video over the Internet: Approaches and Directions, IEEE Transactions on Circuits and Systems for Video Technology, vol. 11 no. 3, 2001, Pág 402-414

[58] Frimout, E. D., Biemond, J. and Lagendick, R. L., Extraction of a dedicated fast playback MPEG bit stream, Proceedings of the SPIE, vol. 2501, 1995, Pág 76-87

9 Anexos

9.1 Configuración

9.1.1 OpenVpn

9.1.1.1 Servidor Linux Debian

Para la configuración de un túnel de comunicación segura, es necesario configurar el servidor de enrutamiento. Por ello que se ha utilizado una distribución Linux Debian, con el fin de generar los CA y llaves correspondientes para ser utilizados en el servidor y clientes VPN.

OpenVpn para estos efectos, posee dos modos de funcionamiento: Enrutado y Puente, los cuales se conocen como Routing y modo Ethernet Bridging. Existen tanto ventajas como desventajas de cada uno de estos modos, sin embargo para esta investigación, se ha utilizado el modo Routing, el cual es uno de los modos más comunes para configurar VPNs.

A continuación se explican cada uno de los pasos y comandos a ejecutar para la configuración de una VPN con OpenVpn.

Se instala el paquete OpenVpn en el servidor Debian.

- **apt-get install openvpn.**

La configuración OpenVpn en modo routing, bajo una arquitectura cliente y servidor, con estructura de certificados digitales, comienza con establecer los KPI. El KPI consiste de un certificado (conocido también como llave pública) y llave privada separada para cliente y el servidor. Además, un certificado de autoridad certificadora CA y su respectiva llave privada usada para firmar cada certificado usado por los clientes y el servidor.

Para generar un CA y su llave privada, OpenVpn incluye un directorio de nombre "easy-rsa" dentro del cual se procedió a ejecutar los siguientes pasos. Ir a la siguiente ruta.

- **cd /usr/share/doc/openvpn/examples/easy-rsa/**

Una vez dentro del directorio "easy-rsa" se editan algunas de las líneas del archivo de nombre "vars", utilizando el siguiente comando.

- **vim vars**

El contenido que posee este archivo es amplio, pero se alude a continuación las líneas relevantes y modificadas en este proyecto.

… …

… …

export KEY_SIZE=2048

export KEY_COUNTRY=CL

export KEY_PROVINCE=VL

export KEY_CITY=Valparaíso

export KEY_ORG=”inf-pucv”

export KEY_EMAIL=”cadv1984@gmail.com”.

Como se puede observar, el contenido del archivo define variables las cuales deben ser cargadas para ser utilizadas posteriormente en la construcción del certificado, pudiendo tener valores según lo convenido y criterio del administrador de sistema, sin dejar ninguno de ellos en blanco. A continuación, se deben cargar las variables del archivo recién modificado, utilizando los siguientes comandos.

- **../vars**
- **./clean-all**

Para averiguar que esta todo en forma correcta, se debería poder constatar la existencia de un directorio con el nombre de la variable $KEY_DIR, por ello que es necesario ejecutar el siguiente comando.

- **echo $KEY_DIR**

En este punto, ya es posible comenzar con la creación del CA ejecutando el script “build-ca” y este script nos hará algunas preguntas de las cuales algunas ya tendrán los valores precargados del archivo de configuración “vars” previamente editado y pueden aceptarse como respuestas presionando ENTER, y otras opciones aún por rellenar con valores apropiados, como se muestra a continuación. Ejecutar el siguiente comando.

- **./build-ca**

Al ejecutar el comando anterior, el script mostrará la siguiente secuencia.

Generating a 2048 bit RSA private key

…….++++++

..++++++

writing new private key to ‘ca.key’

—–

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

—-

Country Name (2 letter code) [CL]:

State or Province Name (full name) [VL]:

Locality Name (eg, city) [Valparaíso]:

Organization Name (eg, company) [inf-pucv]:

Organizational Unit Name (eg, section) []:inf-pucv

Common Name (eg, your name or your server's hostname) []:

Email Address [cdiaz1984@gmail.com]:

Al momento de haber ingresado la información o ENTERs según corresponda, se debe verificar dentro del directorio "$KEY_DIR" la existencia de los archivos "ca.crt" (el CA) y "ca.key" (la llave privada del CA). Con la existencia de estos dos archivos se ha llegado a la instancia en que se ha creado correctamente el CA con su respectiva llave privada, la misma que debe ser mantenida en la más absoluta privacidad por razones de seguridad.

Luego es necesaria la generación del archivo de parámetros Diffie Hellman, el cual consiste en un protocolo que permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada). Se emplea generalmente como medio para acordar clase simétricas que serán empleadas para el cifrado de una sesión. Siendo no autenticado, sin embargo provee las bases para varios protocolos autenticados.

Por lo tanto es necesario generar un archivo que contenga los parámetros correspondientes del protocolo desde el mismo directorio de trabajo usado anteriormente para la generación de la CA. Por ello que es necesario ejecutar el script "build-dh", con el siguiente comando.

- **./build-dh**

Este comando genera el siguiente código mostrado en el terminal de comandos.

Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
…..+…….+…….+…….
……..+……+.
……..+……+…..+…….
…….+…….+……
……..+……..+…..+……..
…….+……
……..+…+…….+……+.
…..+……..+……..

…….+…….+……..
……..+…+…….
…….+…….+…..+.
……..+……..++*++*++*

Si todo ha funcionado correctamente, debería haberse creado el archivo "dh2048.pem", siendo 2048 el valor de tamaño de la clave, y este puede variar según se desee. Esta configuración se realiza en el archivo "var" anteriormente descrito.

Una vez terminado el proceso anterior, el paso siguiente es generar el certificado del servidor y su llave privada, para ello se ejecuta el script "build-key-server" pasándole como parámetro un nombre representativo para el servidor VPN como se puede observa en el siguiente comando que se debe ejecutar.

- **./build-key-server vpn-server**

En el comando anterior, "vpn-server" se refiere al nombre del servidor VPN, solo un nombre representativo. Lo que genera el comando anterior se aprecia en el siguiente texto.

Generating a 2048 bit RSA private key

……++++++

.++++++

writing new private key to 'vpn-server.key'

—

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

—

Country Name (2 letter code) [CL]:

State or Province Name (full name) [VL]:

Locality Name (eg, city) [Valparaíso]:

Organization Name (eg, company) [inf-pucv]:

Organizational Unit Name (eg, section) []:inf-pucv

Common Name (eg, your name or your server's hostname) []:vpn-server

Email Address [cadv1984@gmail.com]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Using configuration from /root/easy-rsa/openssl.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName RINTABLE:'CL'

stateOrProvinceName RINTABLE:'VL'

localityName RINTABLE:'Valparaíso'

organizationName RINTABLE:'inf-pucv'

organizationalUnitName RINTABLE:'inf-pucv'

commonName RINTABLE:'vpn-server'

emailAddress :IA5STRING:'cadv1984@gmail.com'

Certificate is to be certified until Aug 1822:09:07 2017 GMT (3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

En esta fase es indispensable que el valor del "Common Name" en la creación del certificado sea el mismo que el pasado como parámetro al script. Para verificar que el proceso está correcto, se debe verificar que se hayan creado un par de archivos de extensión ".crt" y ".key" dentro del directorio "$KEY_DIR" con el nombre especificado como parámetro al script, resultando en está ocasión "vpn-server.crt" y "vpn-server.key".

Hasta este punto ya se ha creado el CA, el certificado del servidor y el archivo de parámetros Diffie Hellman, por ello se considera que este proceso debe realizarse solo una única vez, por ello no hay que ejecutar nuevamente el script "clean-all" si antes no se ha hecho un respaldo del contenido del directorio "$KEY_DIR".

Para generar certificados para clientes en un futuro, hay que considerar que deben cargarse las variables de entorno desde el archivo "vars" usando el siguiente comando.

- **../vars**

Una vez generado el certificado y llave del servidor, es necesario crear los certificados de clientes y sus llaves privadas. Esta fase consta de dos pasos, el primero consiste en crear una solicitud de certificado y la segunda consiste en la firma de dicha solicitud para generar al fin el certificado del cliente. Para este proceso debe utilizarse el script "build-req" ó "build-req-pass". La diferencia de usar uno u otro consiste en que el segundo protegerá la llave privada con una contraseña para mayor seguridad en caso de robo del certificado y su llave. En esta investigación se ha utilizado "build-req-pass" por motivos de obtener una mayor seguridad. Para generar los certificados y llaves privadas se ejecuta el siguiente comando.

- **./build-req-pass cliente0**

En el comando "cliente0" va a representar el nombre del cliente para la conexión VPN. El comando ejecutado genera el siguiente código.

Generating a 2048 bit RSA private key

…….++++++

……++++++

writing new private key to 'cliente0.key'

Enter PEM pass phrase:

Verifying – Enter PEM pass phrase:

—

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

—

Country Name (2 letter code) [CL]:

State or Province Name (full name) [VL]:

Locality Name (eg, city) [Valparaíso]:

Organization Name (eg, company) [inf-pucv]:

Organizational Unit Name (eg, section) []:inf-pucv

Common Name (eg, your name or your server's hostname) []:cliente0

Email Address [cadv1984@gmail.com]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

En esta fase es importante recordar que también el valor del "Common Name" debe ser el mismo que se pasó como parámetro al script. Si todo ha funcionado en forma correcta, se debe haber creado un archivo extensión ".key" y otro de extensión ".csr" dentro del directorio "$KEY_DIR" con el nombre especificado para el cliente. El paso siguiente, es firmar la solicitud de certificado del cliente ejecutando el script "sign-req" pasándole como parámetro el nombre anterior dado al cliente correspondiente. Para este proceso es necesario ejecutar el siguiente comando.

- **./sign-req cliente0**

Este comando genera el siguiente código.

Using configuration from /root/easy-rsa/openssl.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName RINTABLE:'CL'

stateOrProvinceName RINTABLE:'VL'

localityName RINTABLE:'Valparaíso'

organizationName RINTABLE:'inf-pucv'

organizationalUnitName RINTABLE:'inf-pucv'

commonName RINTABLE:'cliente0′

emailAddress :IA5STRING:'cadv1984@gmail.com'

Certificate is to be certified until Aug 18 22:35:26 2017 GMT (3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

Una vez terminado de ejecutar el comando anterior, se ha obtenido un archive de extensión ".crt" con el nombre del cliente dentro del directorio "$KEY_DIR". Con este punto ya se finaliza el proceso de creación de certificados y llaves para los clientes y/o el servidor.

9.1.1.2 Servidor PfSense

PfSense es una distribución basada en FreeBSD, derivada de m0n0wall, de libre distribución. Su objetivo para este proyecto, es tener un servidor cortafuegos fácilmente configurable a través de una interfase Web instalable en cualquier computador.

El cortafuegos forma parte del kernel del sistema, en otras palabras, se trata del "Packet Filter (PF)" originario de OpenBSD. Este incluye funcionalidades como regular de caudal ALTQ, que permite asignar prioridades por tipo de tráfico, y es por este motivo su gran importancia en este proyecto.

9.1.1.2.1 Instalación

Para la instalación de PfSense, se utiliza un computador con dos tarjetas de red. Este cortafuegos, se utiliza como se mencionó anteriormente para capturar paquetes de tráfico y así proporcionar dos funcionalidades importantes para este proyecto, la de utilizar este servidor PfSense como servidor de VPN y además de filtrado y priorización de paquetes de datos multimedia. Para utilizar este servidor es necesario realizar su instalación y configuración correspondiente, por lo que a continuación se explica la instalación y luego la configuración a seguir.

El primer paso es instalar PfSense en el servidor o computador con dos o más tarjetas de red, en otras eventualidades se pueden utilizar otro tipo de dispositivos para realizar esta labor, sin embargo para esta investigación y como se mencionó anteriormente, se ha utilizado un computador normal con dos tarjetas de red. Por ello que la instalación comienza, con el menú que aparece en la siguiente imagen, el cual indica, las opciones a las cuales se puede acceder en la instalación.

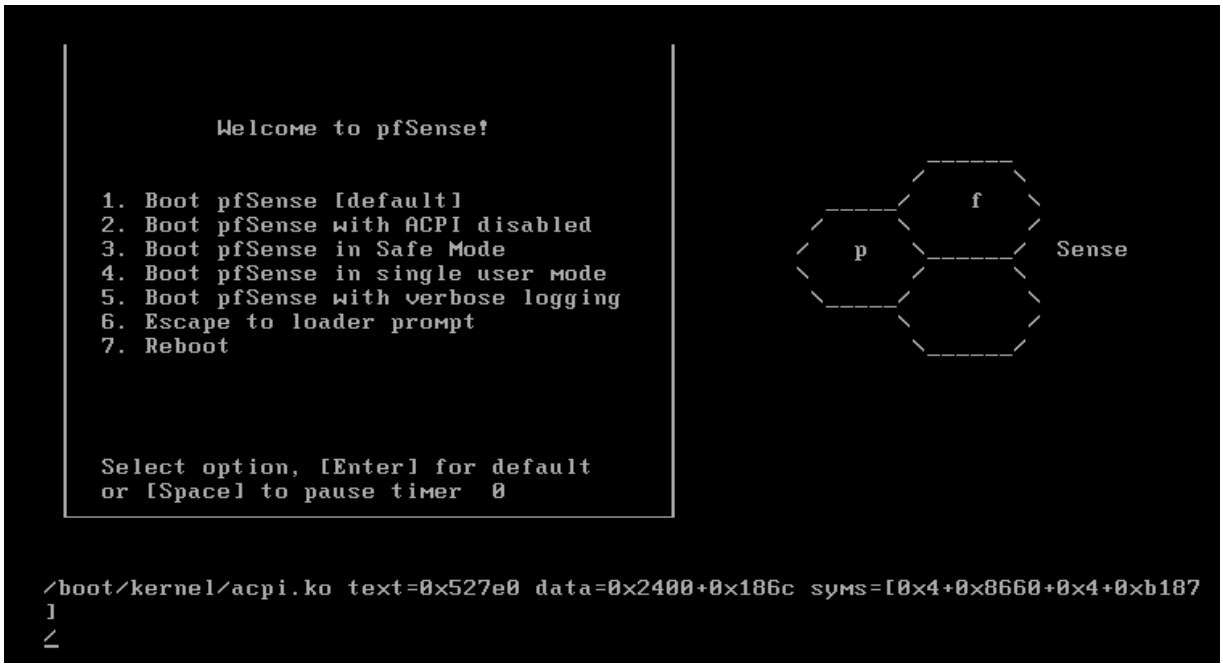

Figura 77 – Instalación Paso 1 PfSense.

De las opciones que aparecen en el menú, se selecciona la opción 1, la que despliega la siguiente vista. En esta, se debe ingresar alguna de las dos opciones que aparecen en el menú, una de ellas es entrar en modo de "Recuperación", opción "R", o en modo de "Lanzamiento del Instalador" que corresponde a la opción "I". Para esta ocasión, se ha ingresado con la opción "I".

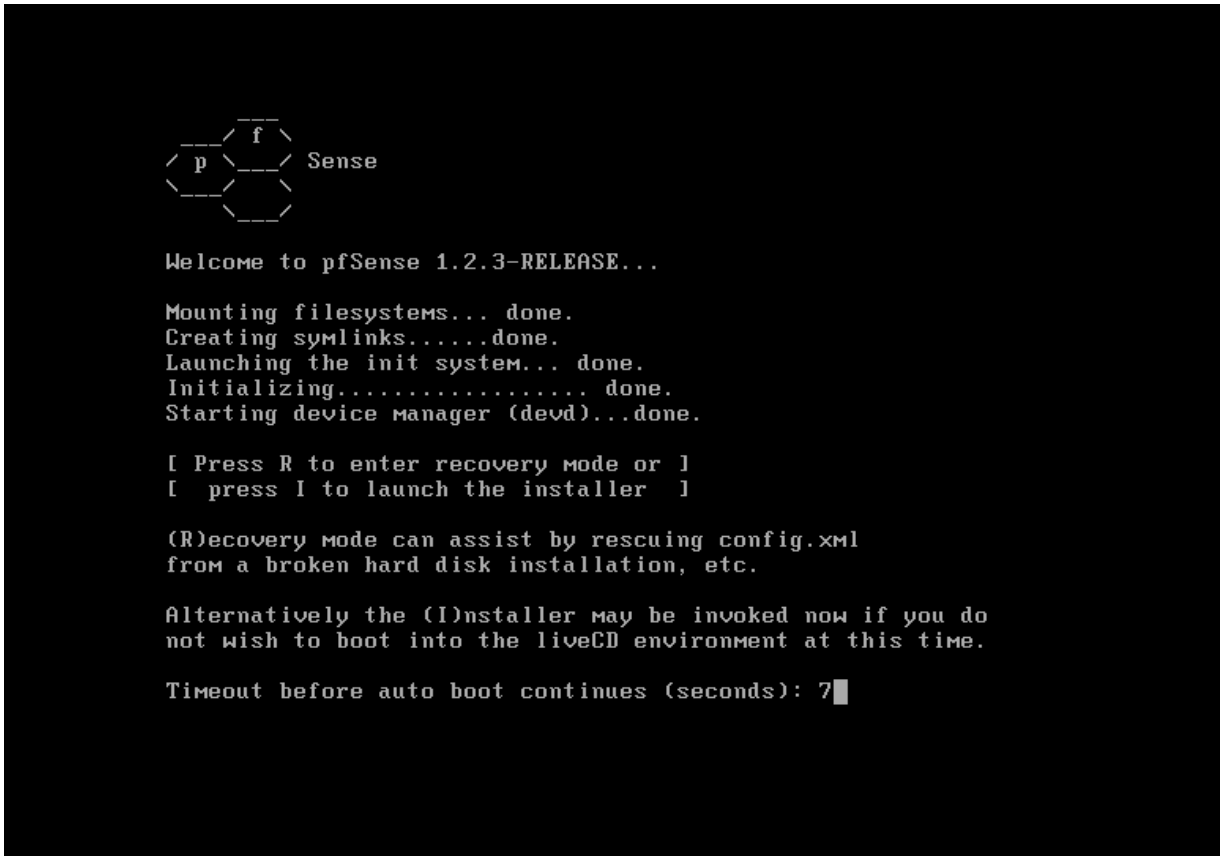

Figura 78 – Instalación Paso 2 PfSense.

Una vez seleccionada esta opción, comienza el proceso de instalación de PfSense, con ello la primera vista, en donde salen las opciones de la configuración. Se recomienda en todo el proceso de instalación utilizar la configuración por defecto o que el sistema selecciona, con el fin de evitar problemas o realizar configuraciones que provoquen el mal funcionamiento del sistema. A continuación se muestra la primera vista de configuración de la instalación.

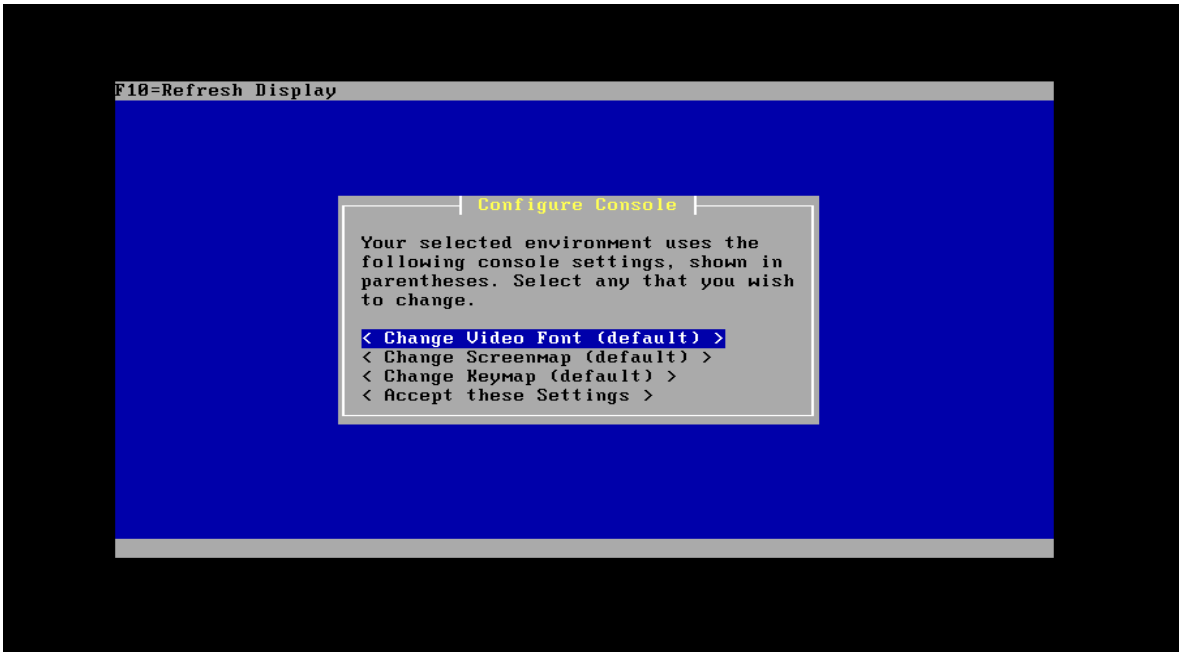

Figura 79 – Instalación Paso 3 PfSense.

En esta figura, se debe seleccionar la primera opción tal como se indica en la imagen. Luego es necesario configurar la fuente de la consola, seleccionado nuevamente la opción que nos indica el sistema.

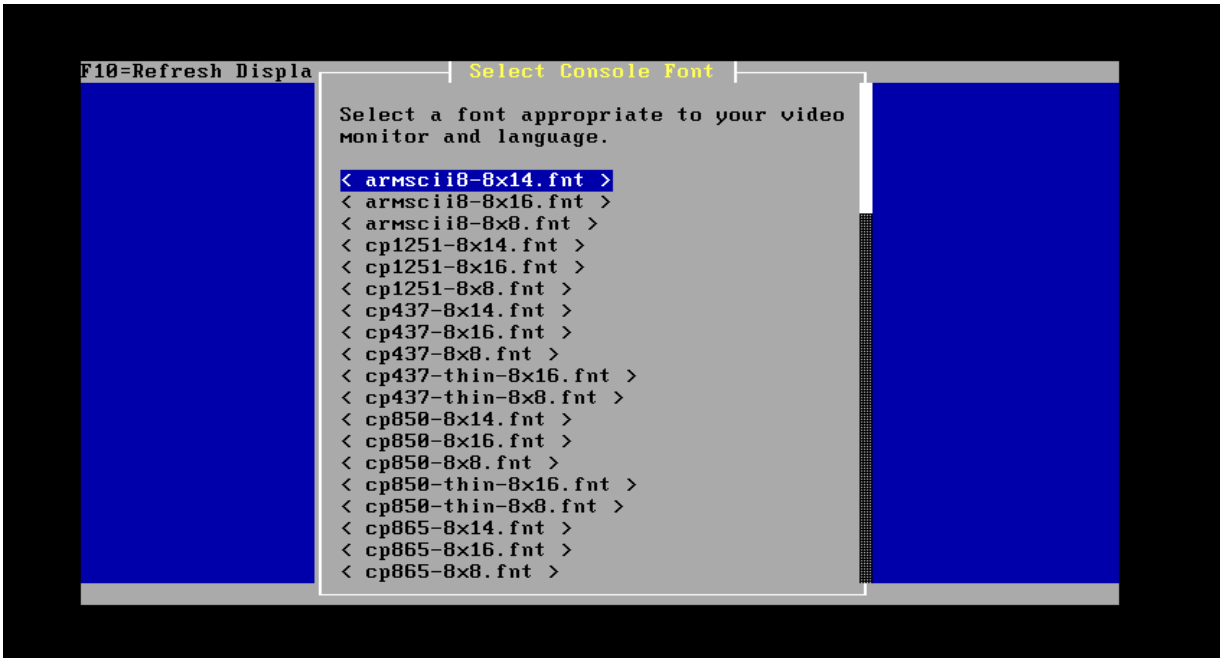

Figura 80 – Instalación Paso 4 PfSense.

Nuevamente nos aparece la imagen que indica la configuración de la consola, pero esta vez con un matiz, ya que ha asociado la configuración que se ha realizado en la imagen anterior.

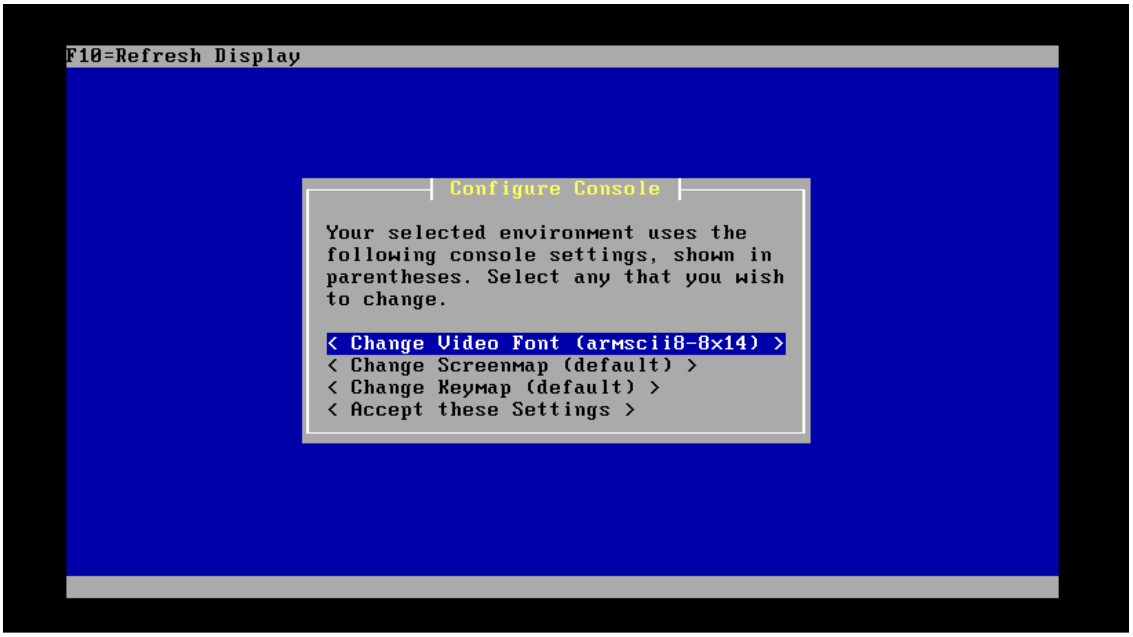

Figura 81 – Instalación Paso 5 PfSense.

Luego seleccionar "Custom Install," de la imagen, para acceder a la vista de selección de unidad de disco, ambas figuras se muestran a continuación.

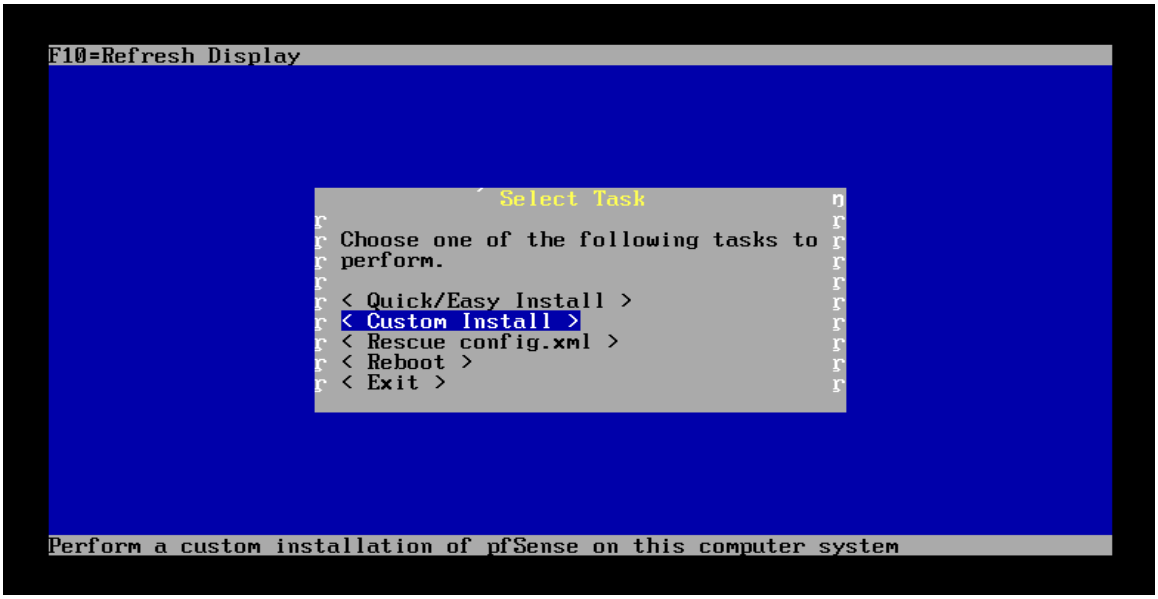

Figura 82 – Instalación Paso 6 PfSense.

Figura 83 – Instalación Paso 7 PfSense.

Después el sistema nos muestra la opción de seleccionar el formato del disco, optando por la opción que aparece en la figura.

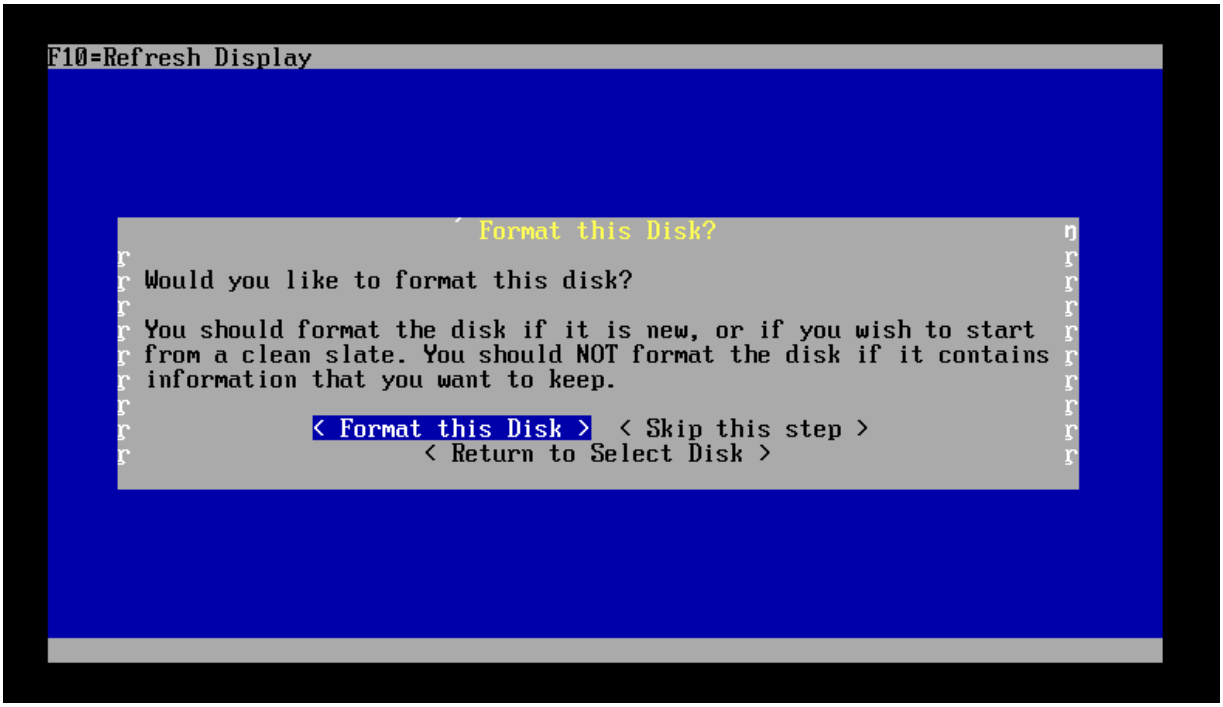

Figura 84 – Instalación Paso 8 PfSense.

Se selecciona la geometría del disco, el sistema propone la más correcta por lo que se selecciona la opción “Usar esta Geometría”, tal como aparece en la figura.

Figura 85 – Instalación Paso 9 PfSense.

Aparece un mensaje de advertencia, dando a conocer que la información de la partición seleccionado será eliminada.

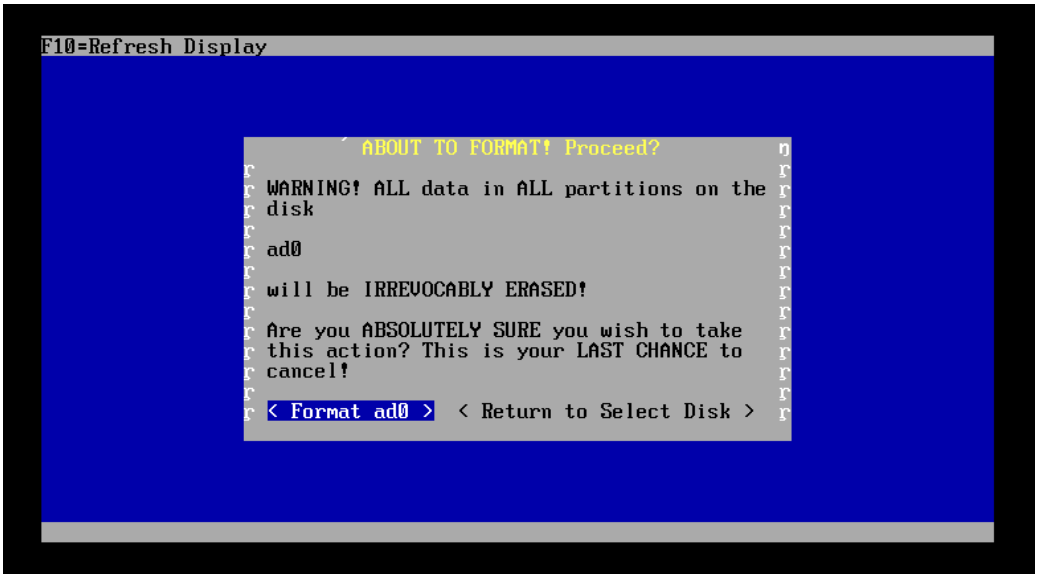

Figura 86 – Instalación Paso 10 PfSense.

El sistema indica si se requiere particionar el disco, en este caso aceptamos y seguimos y se visualiza la siguiente ventana.

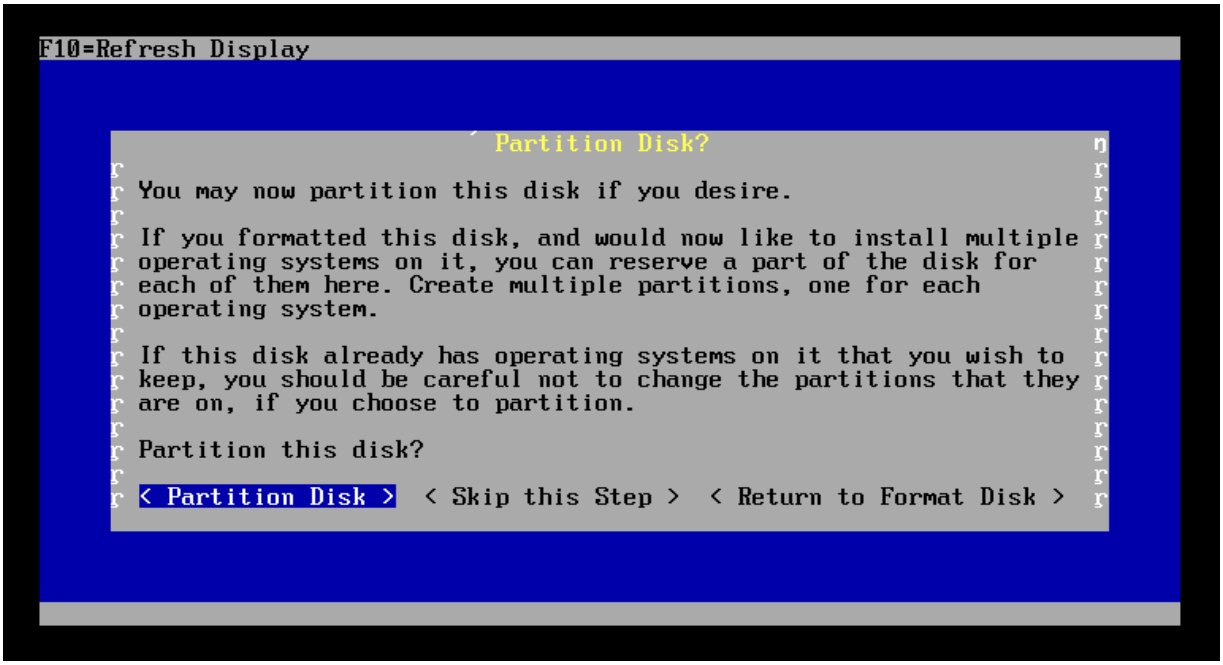

Figura 87 – Instalación Paso 11 PfSense.

Figura 88 – Instalación Paso 12 PfSense.

En esta ventana, se realizan las particiones o se selecciona la que el sistema propone, en este caso, se utiliza la partición del tipo FreeBSD. A continuación de seleccionar, la partición tipo FreeBSD y la siguiente etapa muestra un mensaje de confirmación si desea continuar de todas formas con el particionado, después se acepta tal como aparece en la imagen y finalmente muestra un mensaje de información del particionado.

Figura 89 – Instalación Paso 13 PfSense.

Figura 90 – Instalación Paso 14 PfSense.

Ahora se va a instalar el sector de inicio en el disco duro, se debe presionar “enter" en aceptar e instalar Bootblock.

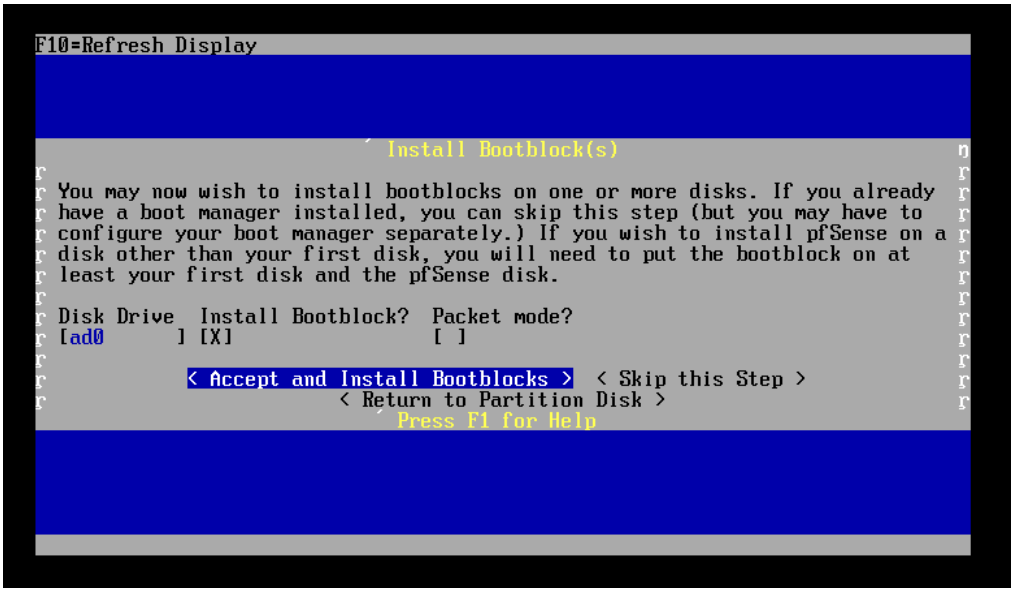

Figura 91 – Instalación Paso 15 PfSense.

El sistema consulta, en que partición se va a instalar.

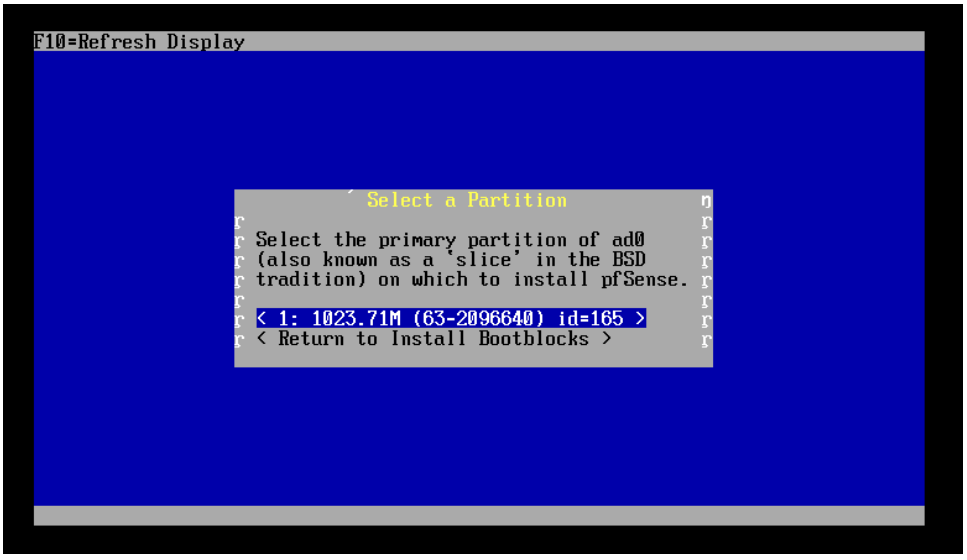

Figura 92 – Instalación Paso 16 PfSense.

El sistema muestra una ventana de seguridad, para consultar si se está seguro de realizar la acción.

Figura 93 – Instalación Paso 17 PfSense.

Figura 94 – Instalación Paso 18 PfSense.

El sistema muestra la subpartición del espacio reservado para PfSense, por ello muestra las siguientes opciones, las cuales se deben seleccionar tal como propone el sistema.

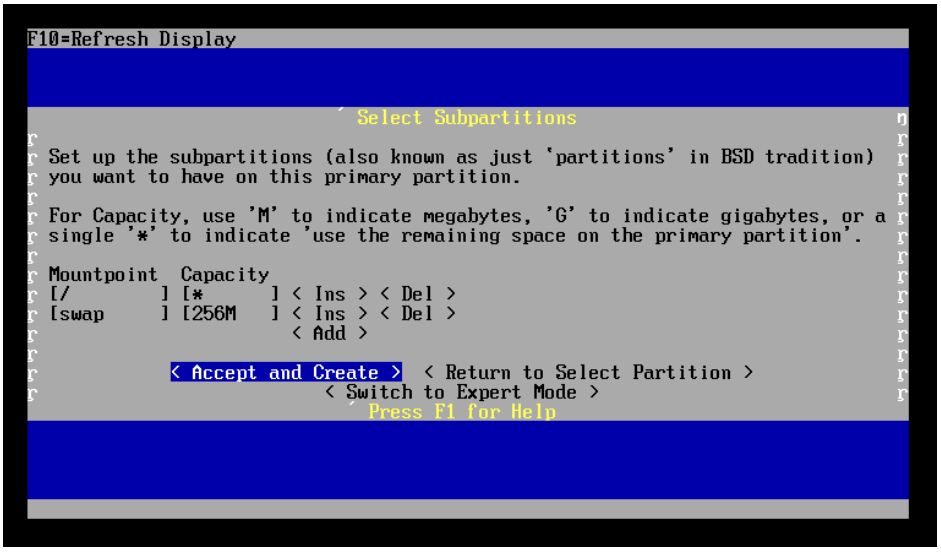

Figura 95 – Instalación Paso 19 PfSense.

Para finalizar la instalación se acepta la ventana anterior, y el sistema comienza a cargar la información al disco, con ello comienza la instalación propiamente tal, de acuerdo a las características antes mencionada que posee el equipo utilizado para esta instalación, esta demorará aproximadamente unos 2 a 4 minutos aproximadamente.

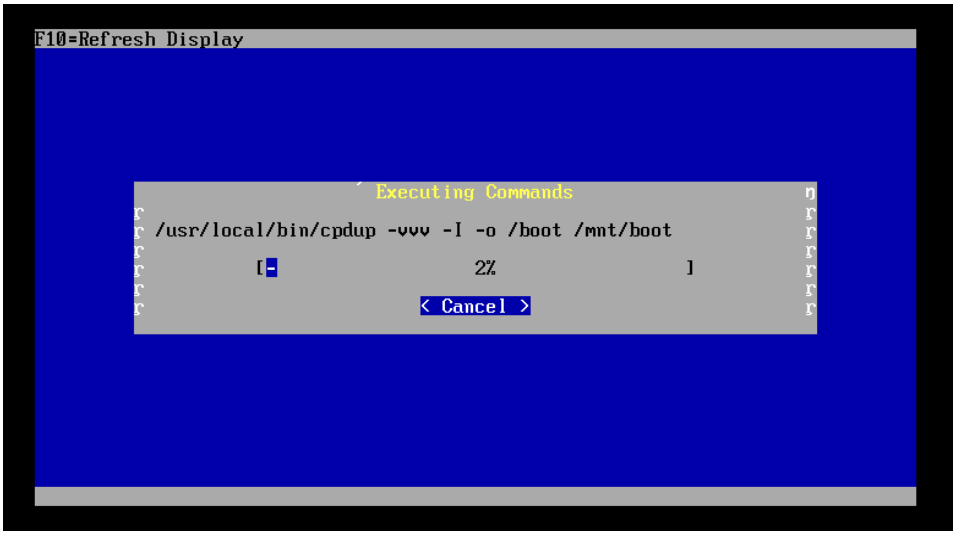

Figura 96 – Instalación Paso 20 PfSense.

Una de las últimas etapas es seleccionar el kernel a instalar, por ello tomar la opción que propone el sistema.

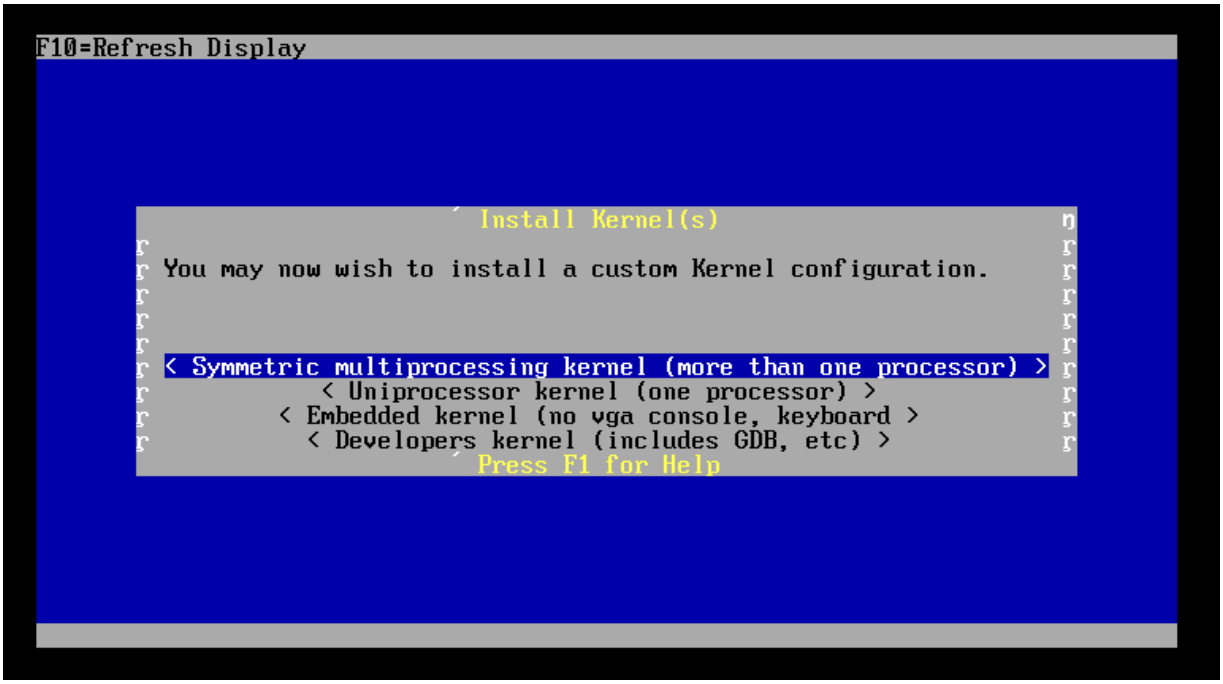

Figura 97 – Instalación Paso 21 PfSense.

Figura 98 – Instalación Paso 22 PfSense.

Finaliza este proceso con el reinicio del sistema, con este paso cumplido el sistema PfSense ha sido instalado exitosamente.

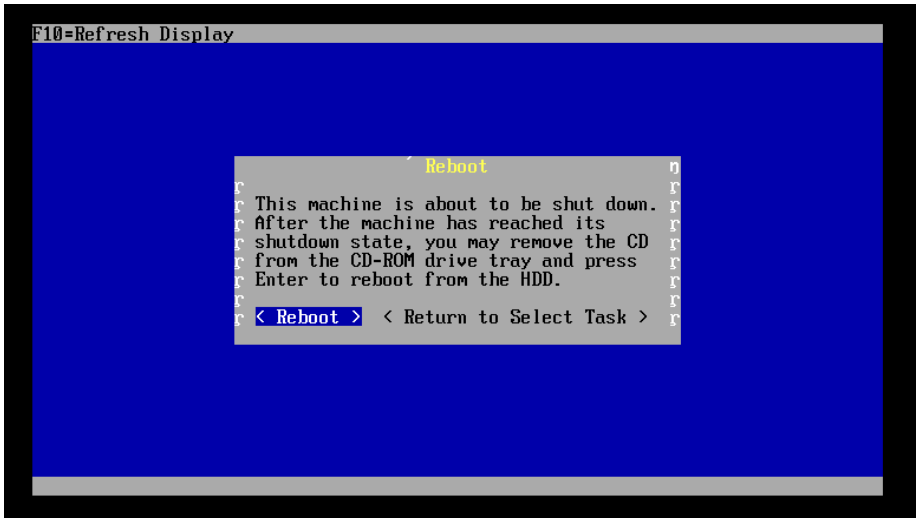

Figura 99 – Instalación Paso 23 PfSense.

9.1.1.2.2 Configuración

Una vez instalado PfSense es necesario, configurar este cortafuego tanto la entrada de tráfico o WAN, como también la red local LAN. Al reiniciar el sistema, PfSense muestra distintas opciones para su configuración, pero este proyecto solo alude a la configuración de LAN y WAN, por ello que el sistema nos muestra la siguiente secuencias de pasos a configurar.

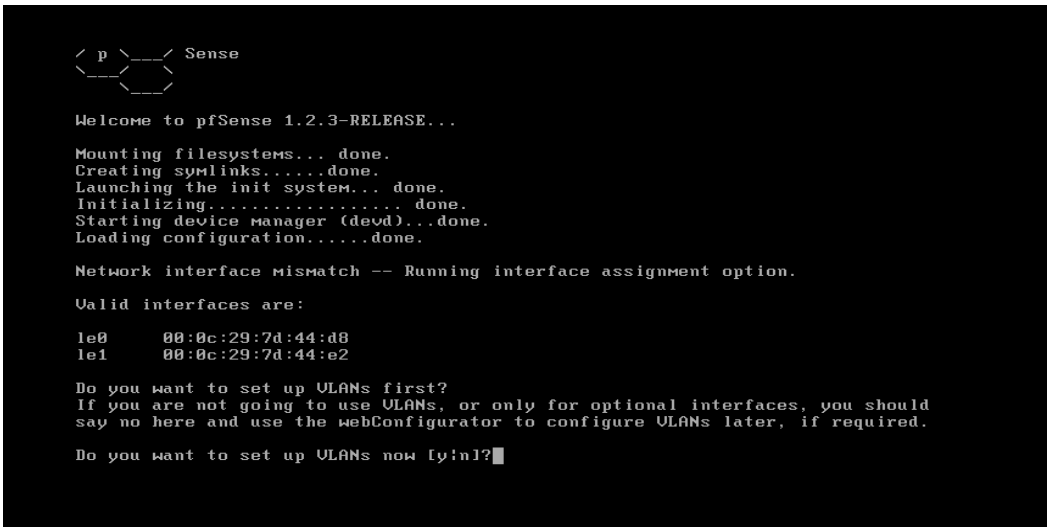

Figura 100 – Instalación Paso 24 PfSense.

Como se puede apreciar, el primer paso es configurar VLANs para el cortafuego, para este proyecto no aplica esta configuración, por lo que la respuesta a dicha pregunta en "n". Para la segunda configuración, es necesario indicar qué tarjeta de red está asignada para LAN, por ello hay que indicar el nombre de la tarjeta que corresponda. De la misma forma, se debe indicar la tarjeta asignada para WAN. Luego se finaliza la configuración, no ingresando ningún tipo de dato u opción.

El sistema una vez configurado, nos mostrará la confirmación correspondiente a la operación.

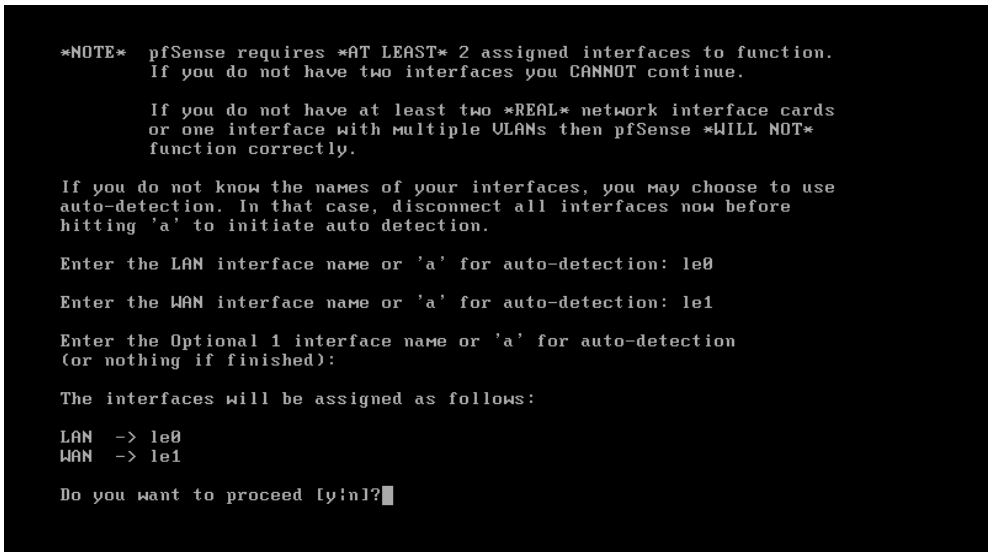

Figura 101 – Instalación Paso 25 PfSense.

Para pasar al paso siguiente de configuración, es necesario aceptar la operación tal como aparece en los procedimientos destacados. El siguiente paso, es configurar las IPs de LAN y WAN respectivamente.

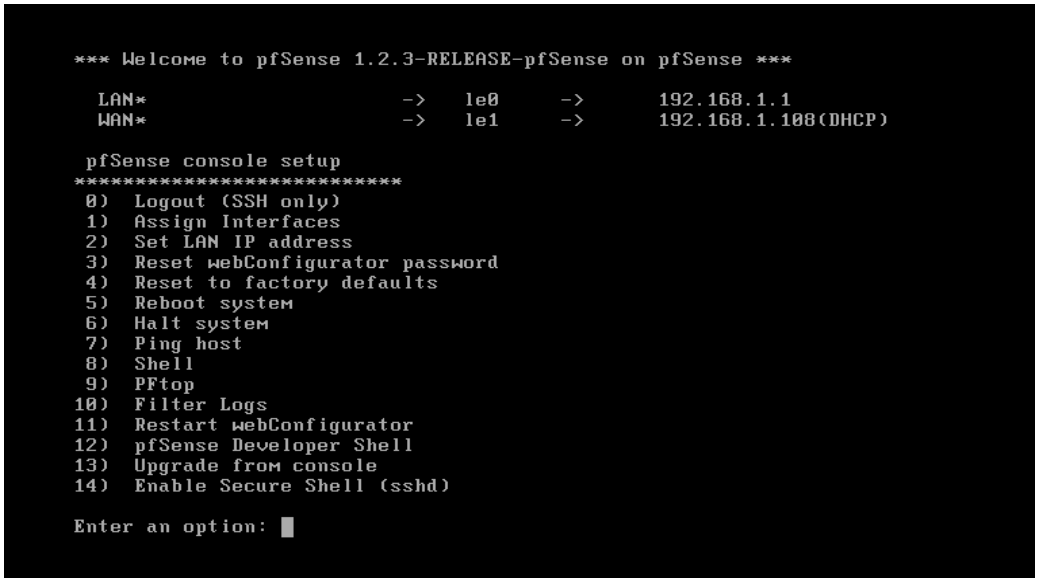

Figura 102 – Instalación Paso 26 PfSense.

El sistema por defecto carga su configuración, indica un menú de consola y presenta al final, la dirección IP de la LAN por defecto 192.168.1.1. Del menú de consola, se selecciona la opción dos, que indica "Set LAN IP Address", con ello se modifica la dirección IP utilizada para la LAN según corresponda o se necesite. En este proyecto se ha utilizado la IP por defecto, es decir 192.168.1.1, utilizando la máscara de subred 24, sin activar el servidor DHCP, tal como aparece en los siguientes códigos de consola.

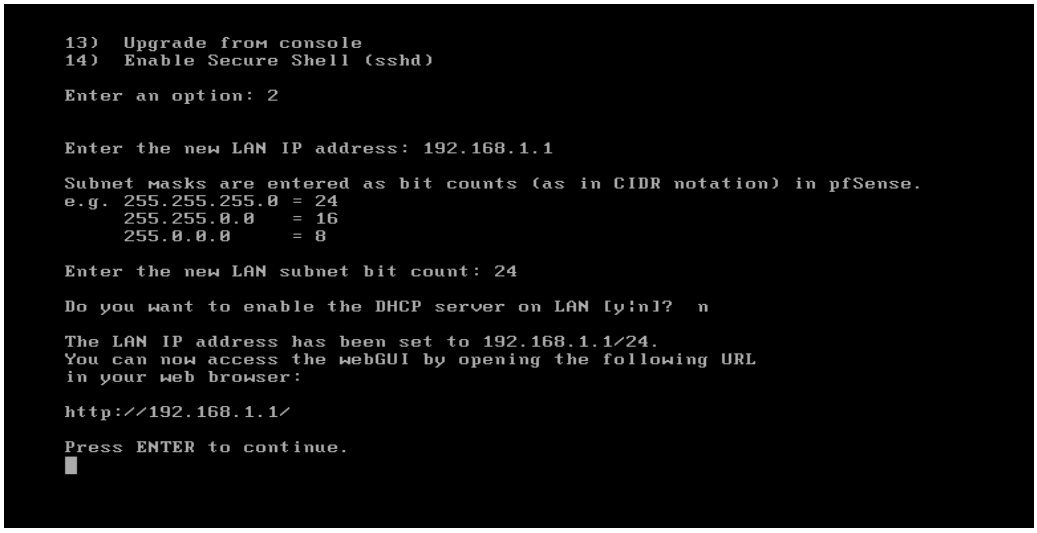

Figura 103 – Instalación Paso 27 PfSense.

Una vez culminada esta operación, se indica por pantalla la nueva dirección, y con ésta dirección se puede ingresar al configurador Web de PfSense, a través de un navegador, cuyo computador este conectado a la LAN del servidor PfSense.

Ya es posible ver el configurador Web a través de un navegador si todo ha sido correctamente configurado. La etapa siguiente es configurar el navegador Web de los ítems relevantes para la puesta en marcha del prototipo.

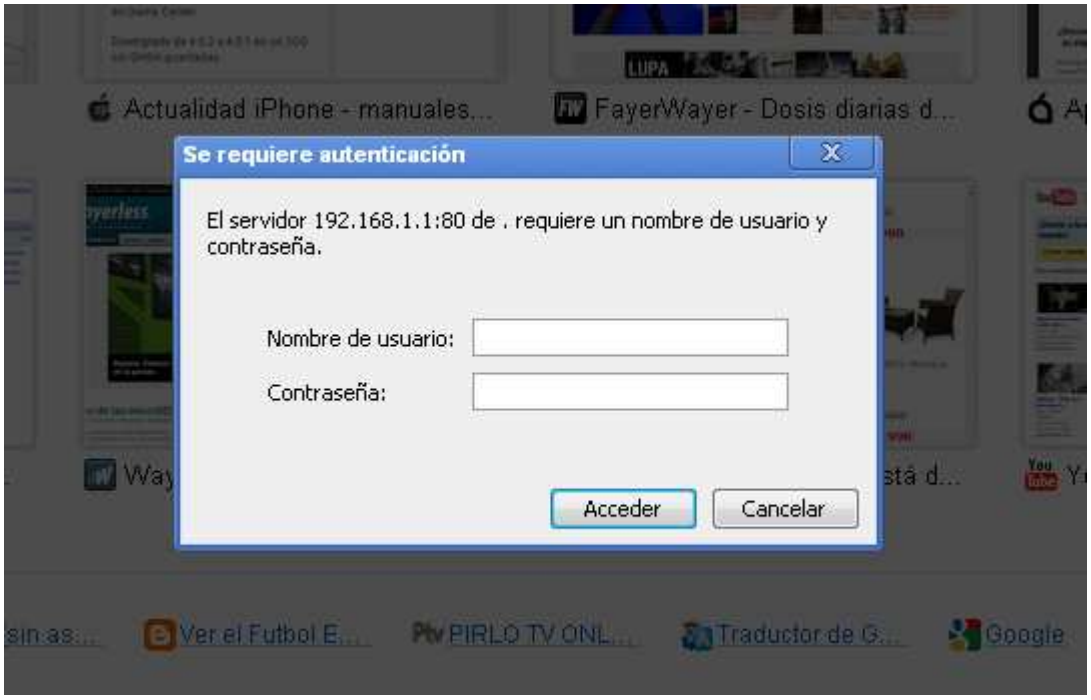

Figura 104 – Login PfSense.

Para ingresar al configurador Web, se accede a través de la dirección "192.168.1.1" y se utilizan los siguientes datos:

- Usuario: admin.
- Contraseña: pfsense.

Al ingresar por primera vez se ingresa a un asistente, pero se puede obviar al hacer clic en la imagen "PfSense", esto dependerá de lo que se desea realizar, pero en esta ocasión se ha optado por realizar la configuración manual.

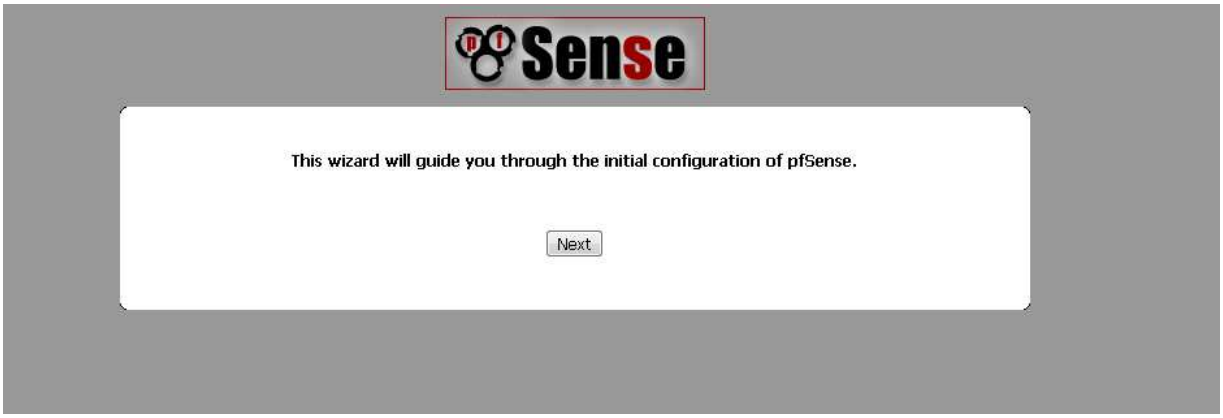

Figura 105 – Configuración PfSense.

Respecto a las configuraciones generales y avanzadas de PfSense, no se hicieron modificaciones, se utilizaron las configuraciones por defecto del cortafuego. En relación a la configuración del servidor DNS y DHCP, se configuraron en el servidor streaming, por pruebas preliminares del prototipo, por ende que estas configuraciones no se explican en esta investigación. La siguiente figura muestra la vista principal de PfSense.

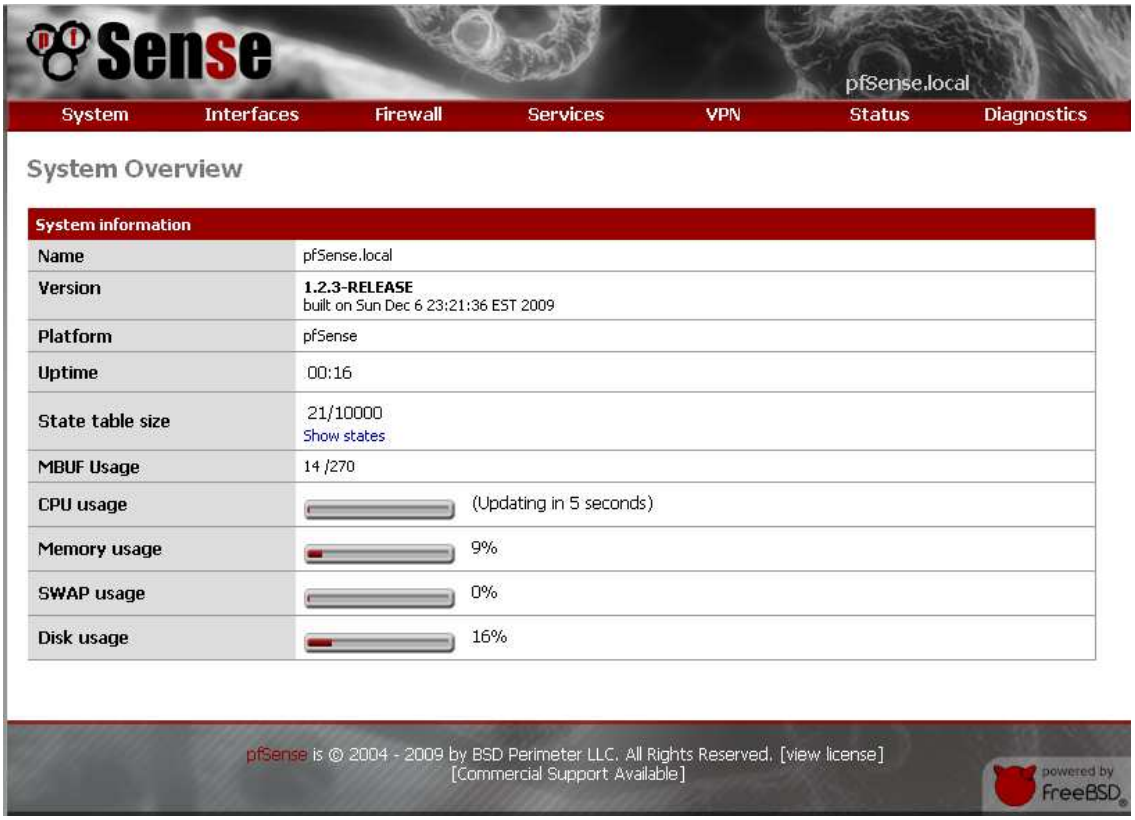

Figura 106 – Vista Principal PfSense.

Para efectos de realizar otras configuraciones generales, se accede a “System” y luego “General Setup”, donde se realizan las configuraciones básicas del cortafuegos, y que se aprecia en la siguiente figura.

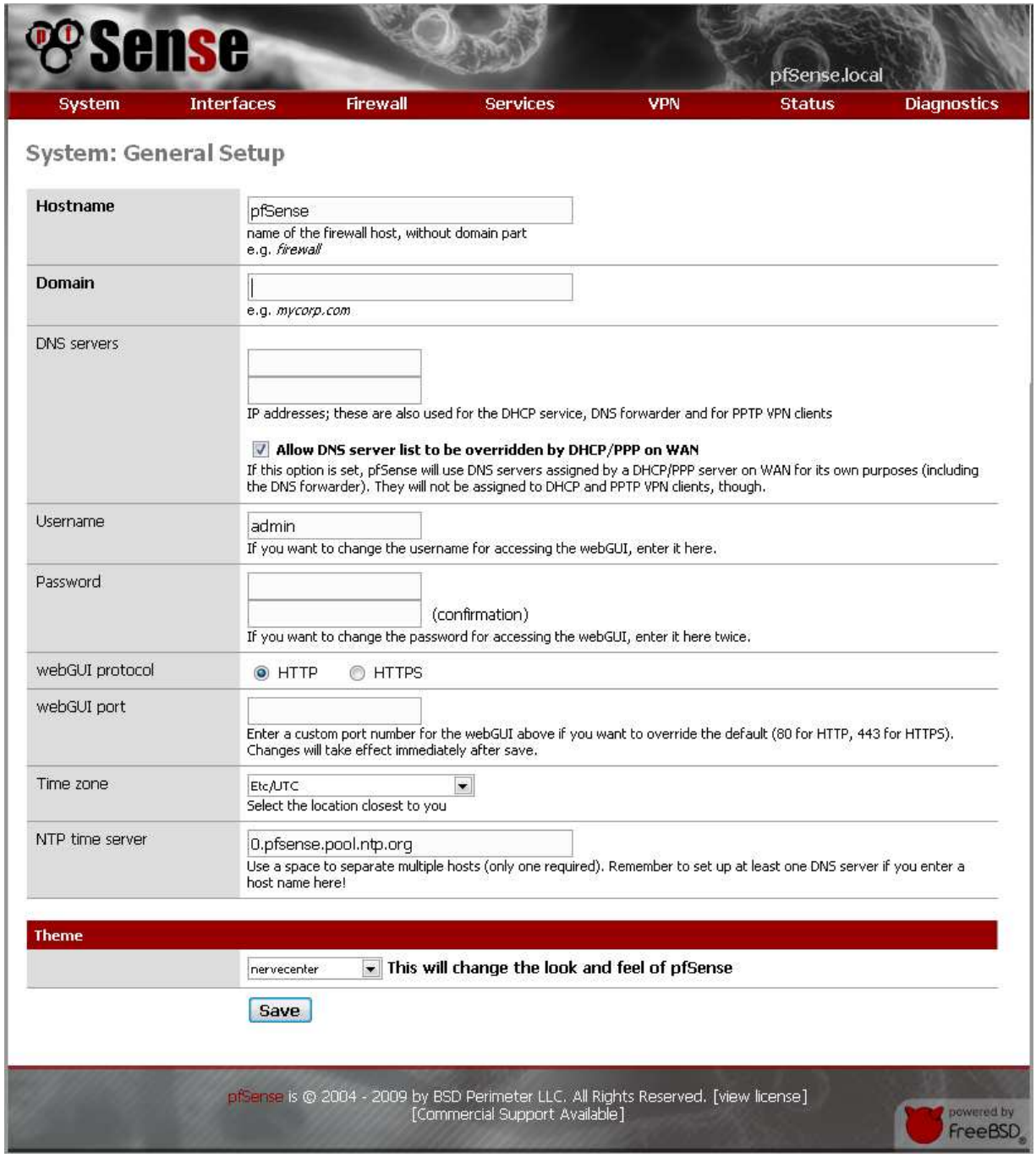

Figura 107 – Configuración Personal PfSense.

Si se desea acceso a la consola por SSH y/o realizar servicios de HTTPS, hay que realizar ajustes en “System” y luego “Advanced Functions”. Para este prototipo no se han realizado estas configuraciones, pero si es interesante mostrar la vista con el fin de tener algún acercamiento a su configuración.

A continuación se muestran la asignación de la interfaz tanto de LAN como WAN.

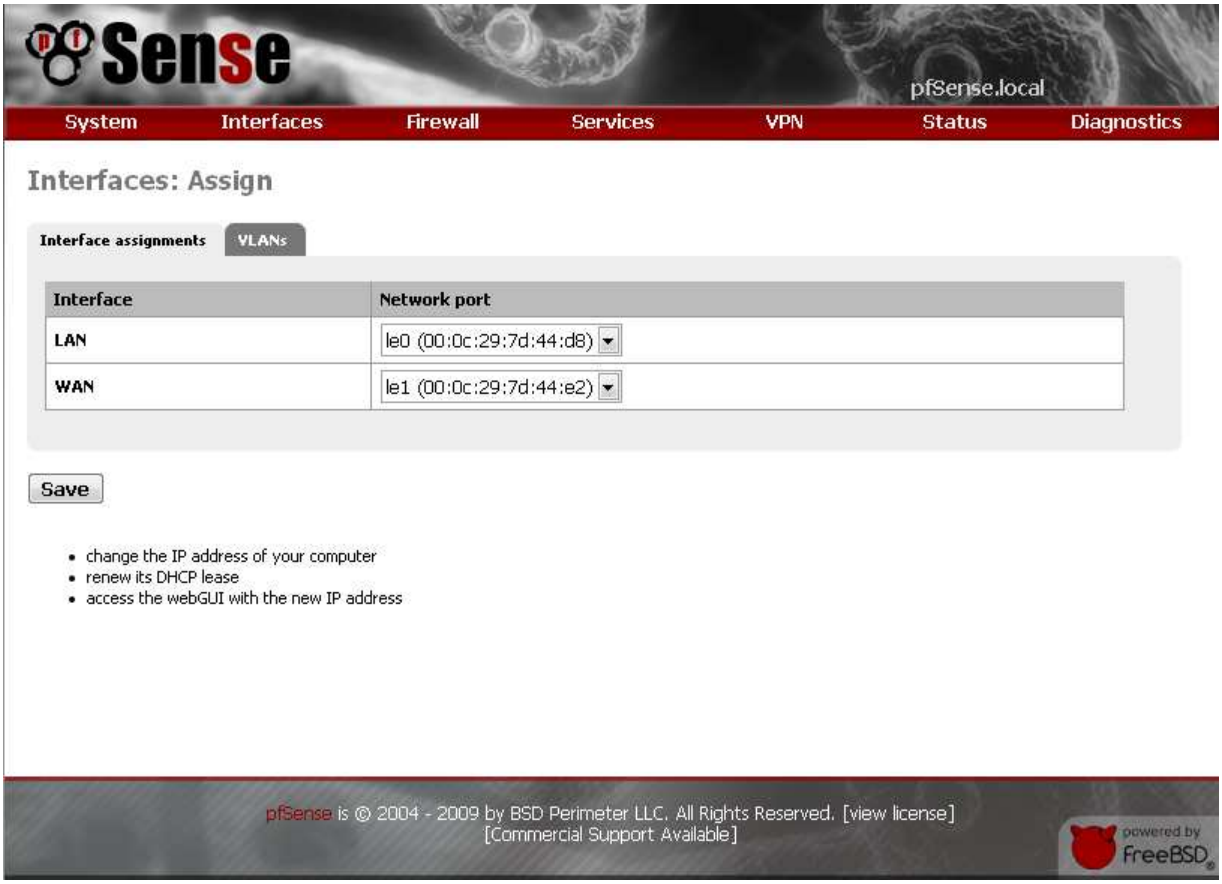

Figura 108 – Configuración Intefaces PfSense.

Para realizar una nueva configuración de LAN vía Web, es necesario acceder al menú principal, en “Interfaces” y luego “LAN”, donde se muestra la siguiente configuración.

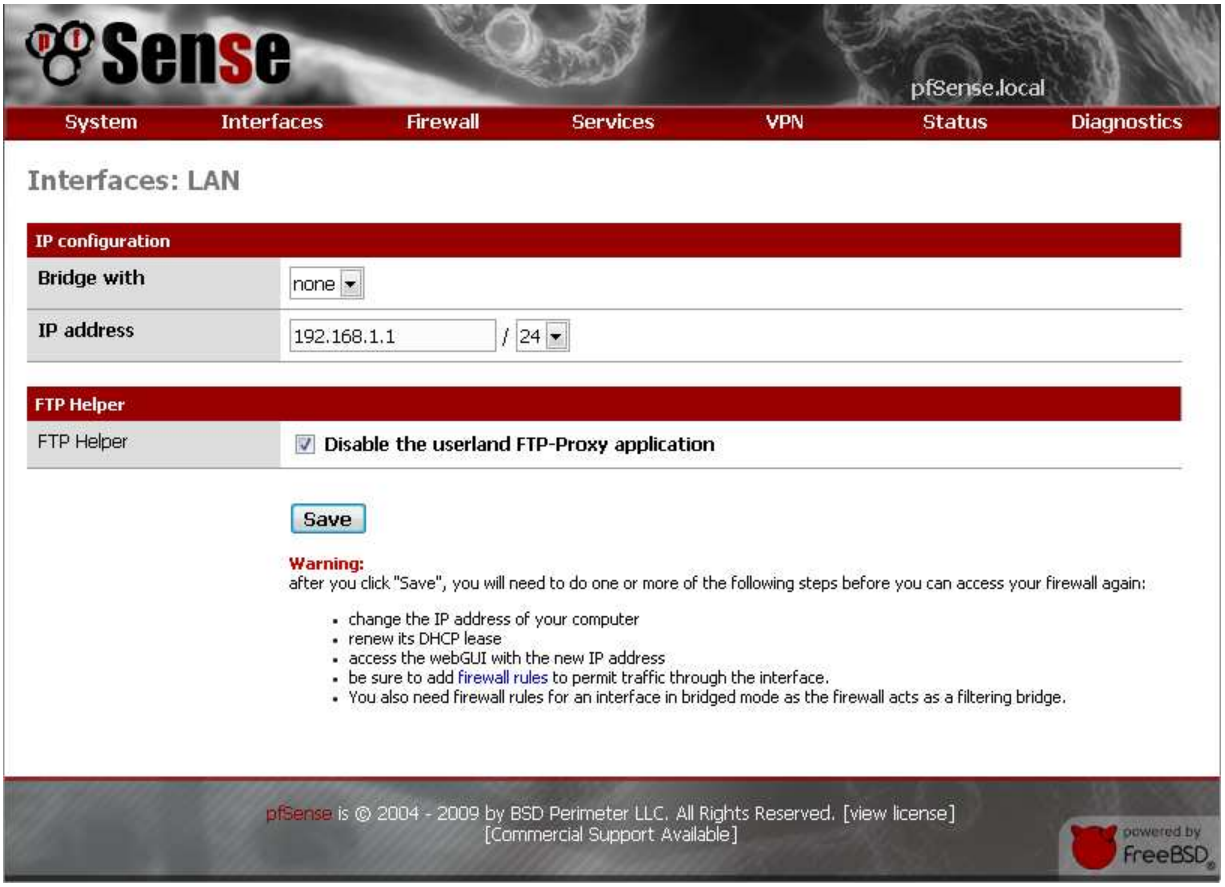

Figura 109 – Configuración Intefaces LAN PfSense.

Para realizar una nueva configuración de WAN vía Web, es necesario acceder al menú principal, en “Interfaces” y luego “WAN”, donde se muestra la siguiente configuración.

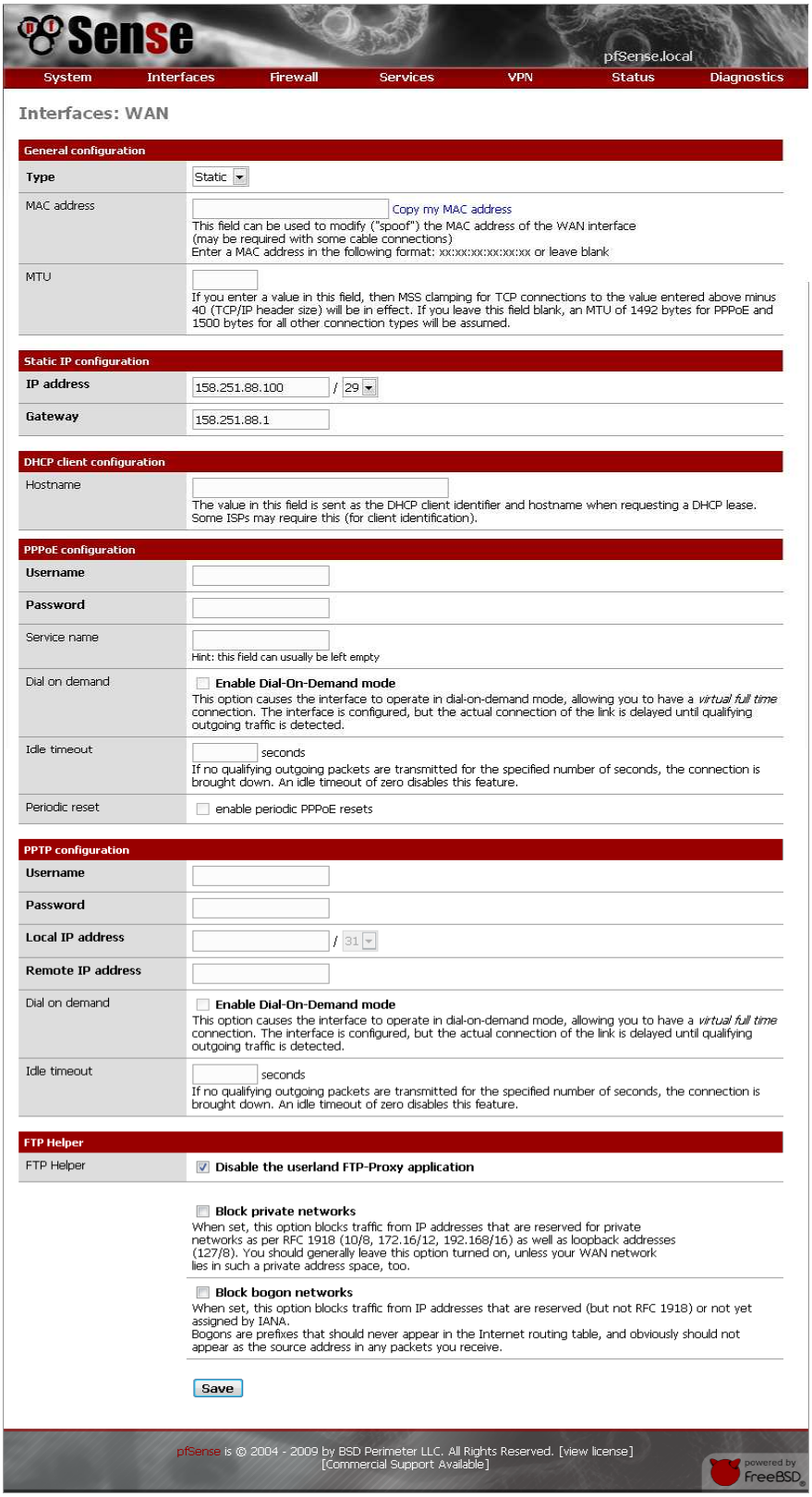

Figura 110 – Configuración Intefaces WAN PfSense.

En esta etapa, se aconseja ir a “Diagnostics”, luego “Backup/Restore”, después “Remote” y guardar la configuración. Se genera un archivo XML a guardar. Además el nombre de este archivo queda serializado con la fecha y hora, por lo que en caso de problemas puede ser muy útil recuperar la última configuración buena y conocida. Este archivo XML contiene información delicada, por lo que debe almacenar en un lugar seguro.

Para la configuración NAT del cortafuego, se habilitaron tanto para las conexiones entrantes como salientes las reglas que aparecen en la siguiente figura.

Para el acceso a los servicios internos desde el exterior es necesario configurar el “Port Forward”, lo que se conoce con el nombre de “abrir puertos”.

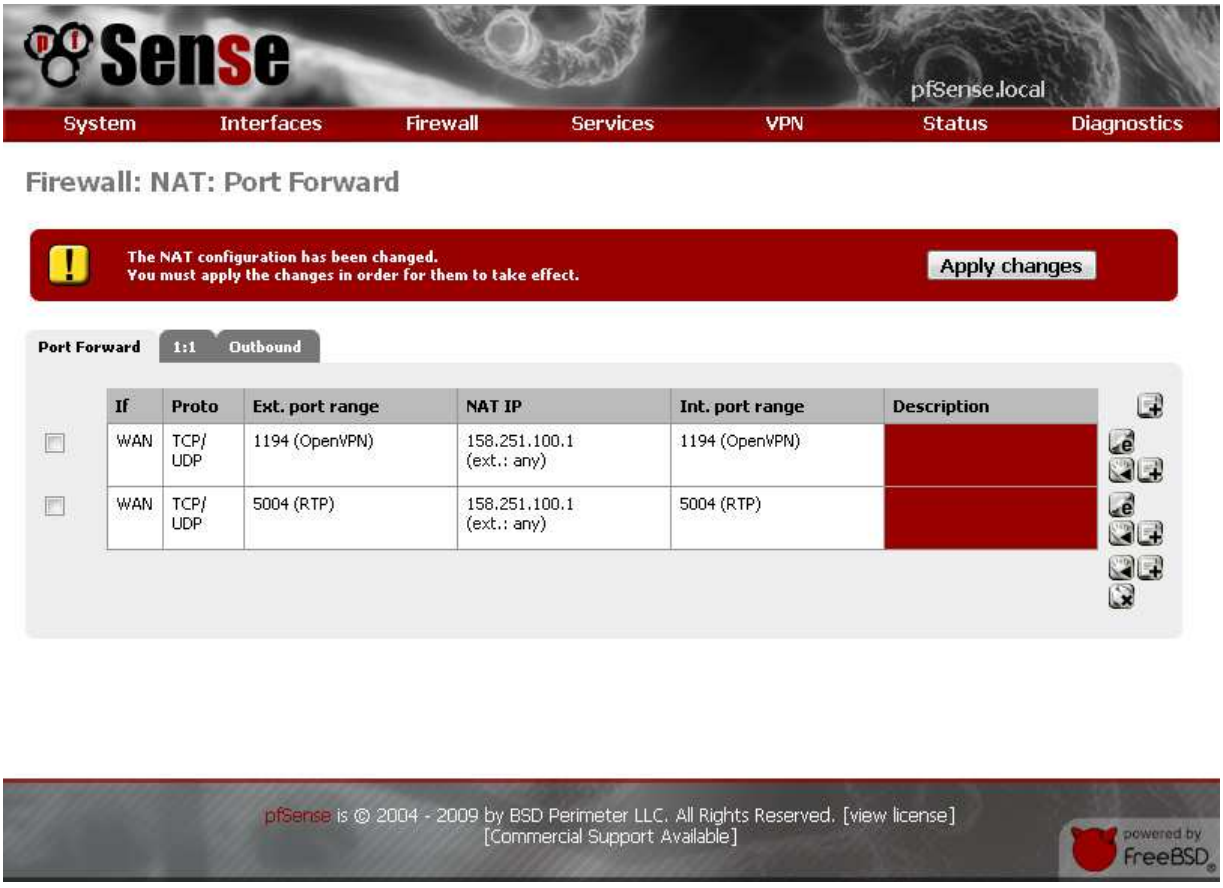

Figura 111 – Configuración Intefaces NAT PfSense.

Para el acceso desde dentro de la red hacia el exterior, es necesario configurar el “Outbound” del cortafuego tal como se aprecia en la figura.

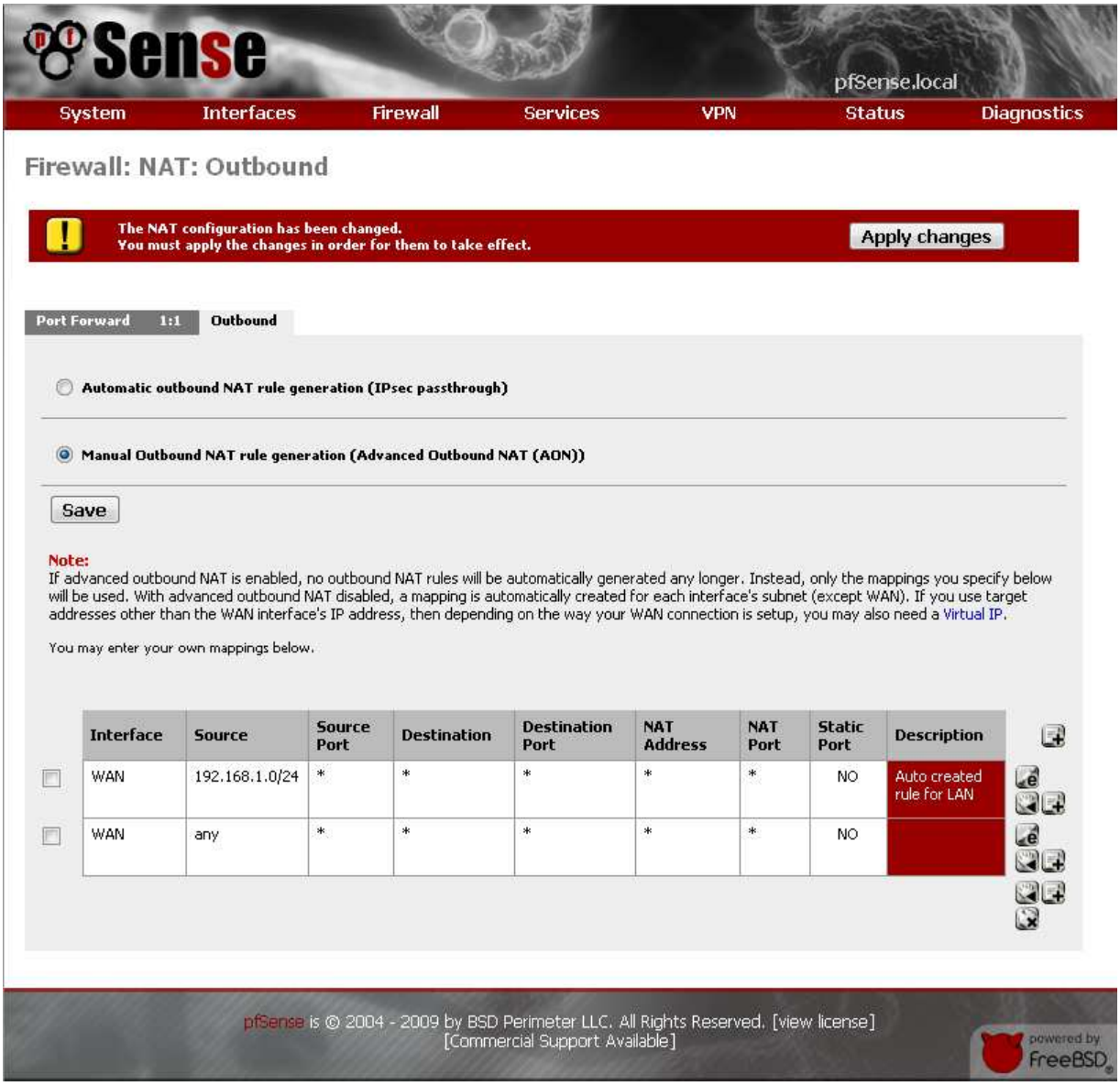

Figura 112 – Configuración NAT Outbound PfSense.

Para las reglas del cortafuego, es necesario comprender de que estas se ejecutan según en el orden en que están puestas, y si no se cumple alguna de ellas el paquete de datos es bloqueado. Las acciones que se pueden realizar son tres, rechazar, pasar y bloquear. Las reglas configuradas para WAN y LAN, se aprecian en la siguiente figura.

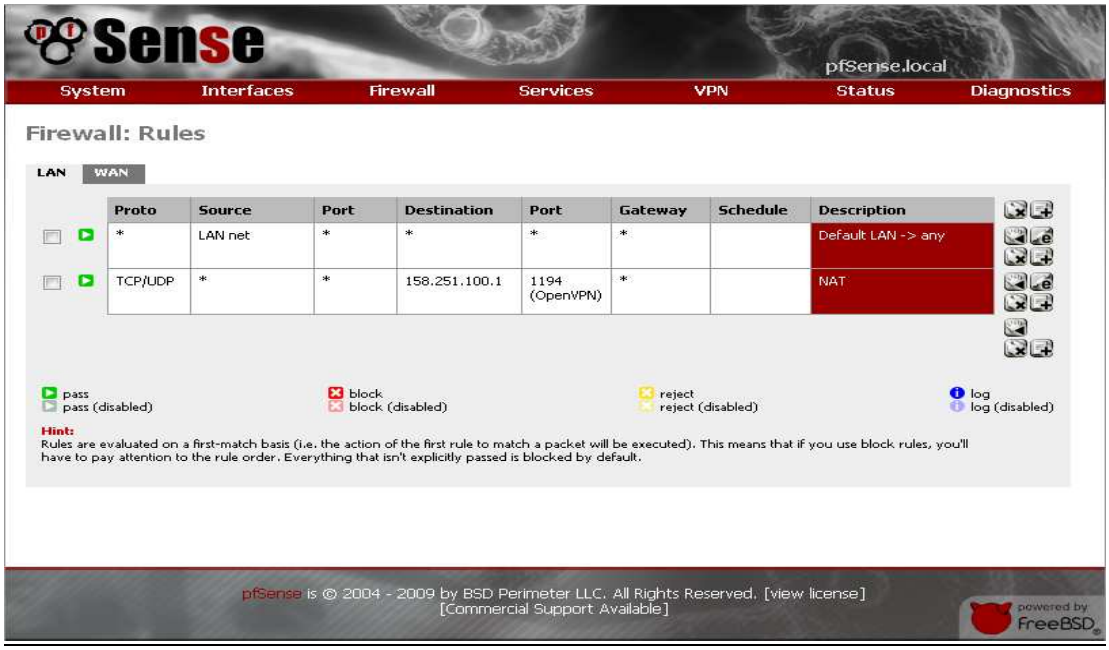

Figura 113 – Configuración Rules LAN PfSense.

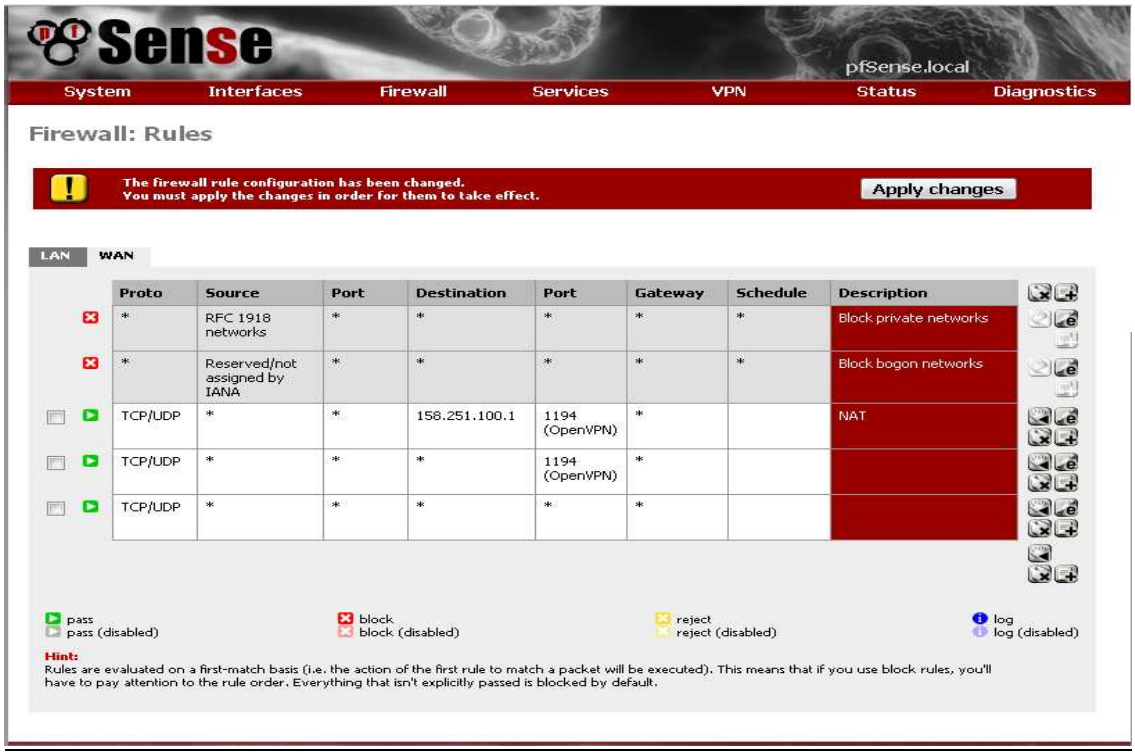

Figura 114 – Configuración Rules WAN PfSense.

Para configurar el regulador de caudal, aspecto muy importante en esta investigación para aumentar, priorizar y acelerar el proceso de envío de datos a través de Internet, es necesario tener en cuenta que consiste en un conjunto de herramientas de calidad de servicio, que permiten generar colas de tráfico, asignando anchos de banda y prioridad,

PfSense otorga un asistente para la configuración de "Traffic Shaper", la primera vez que se ejecuta muestra la siguiente imagen. Se accede del menú principal, desde "Firewall" y luego en el enlace "Traffic Shaper".

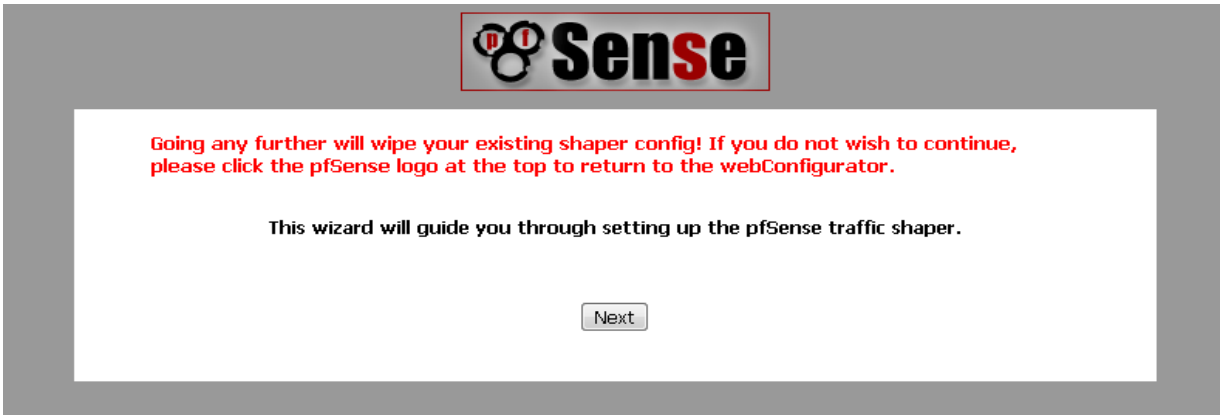

Figura 115 – Configuración Traffic Shaper PfSense.

Hay que tener en cuenta de que al volver a entrar al asistente resetea la configuración que se tenía anteriormente. En el proceso de configuración si se hace clic en la imagen de PfSense, se cancela la acción de "Traffic Shaper".

Para configurar lo que interesa para esta investigación, es necesario accionar el botón "next" hasta que aparezca la siguiente ventana.

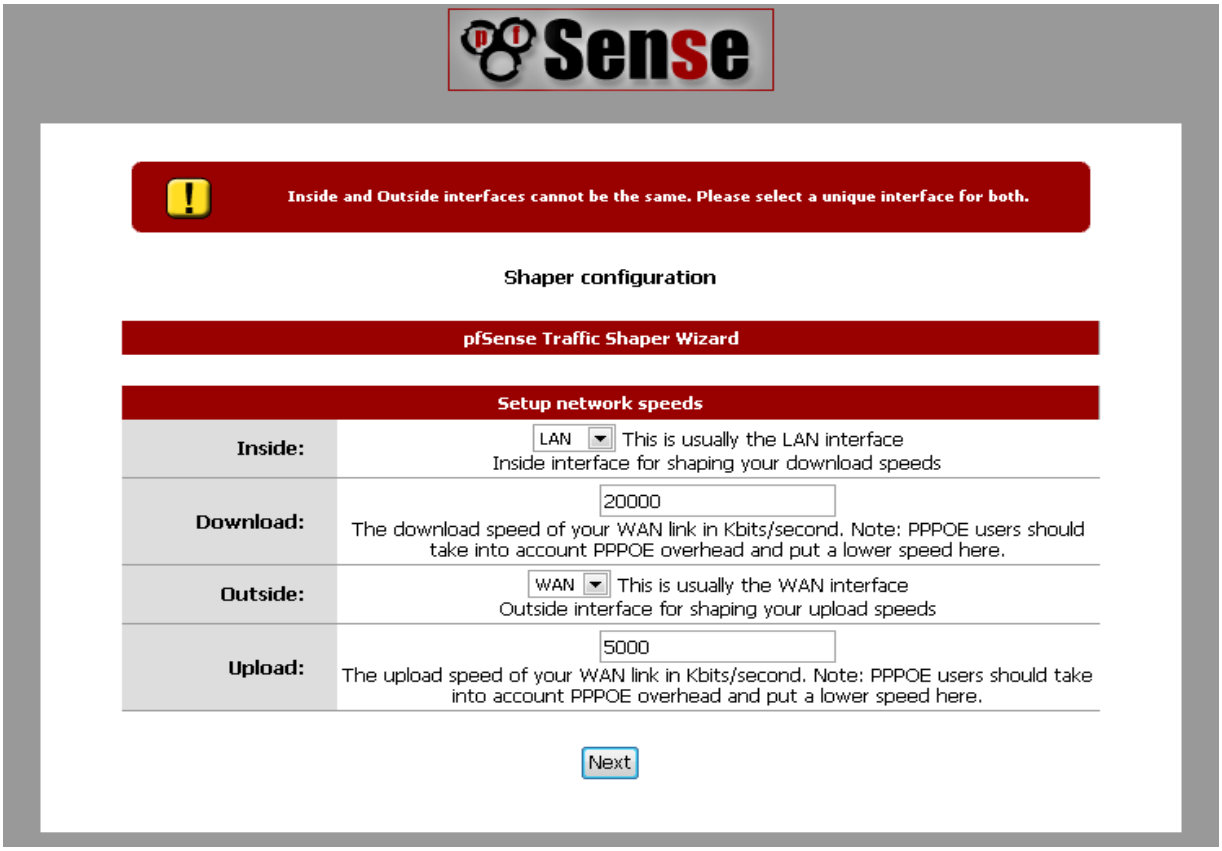

Figura 116– Configuración Traffic Shaper 1 PfSense.

Como se aprecia en la figura, se activan los tipos de tráfico aplicables a la investigación. Luego accionamos “next” y se llega la pantalla final del asistente. Haciendo clic en “Finish” se activa la nueva configuración del tráfico mostrando la siguiente ventana.

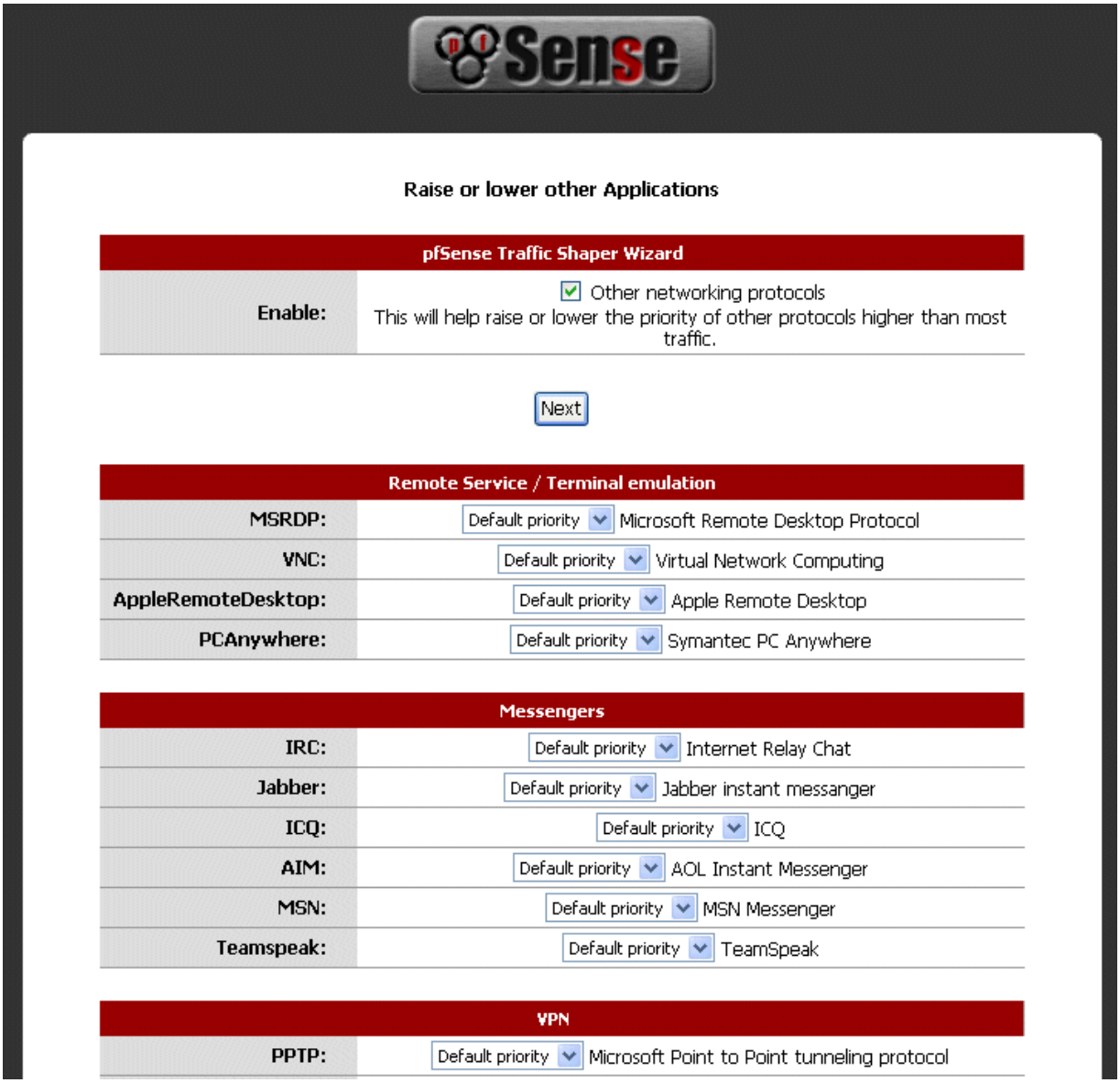

Figura 117 – Configuración Traffic Shaper 2 PfSense.

Una vez finalizada la configuración, se cargan las reglas y se puede accesar al estado de las colas creadas, tal como se aprecia en la figura.

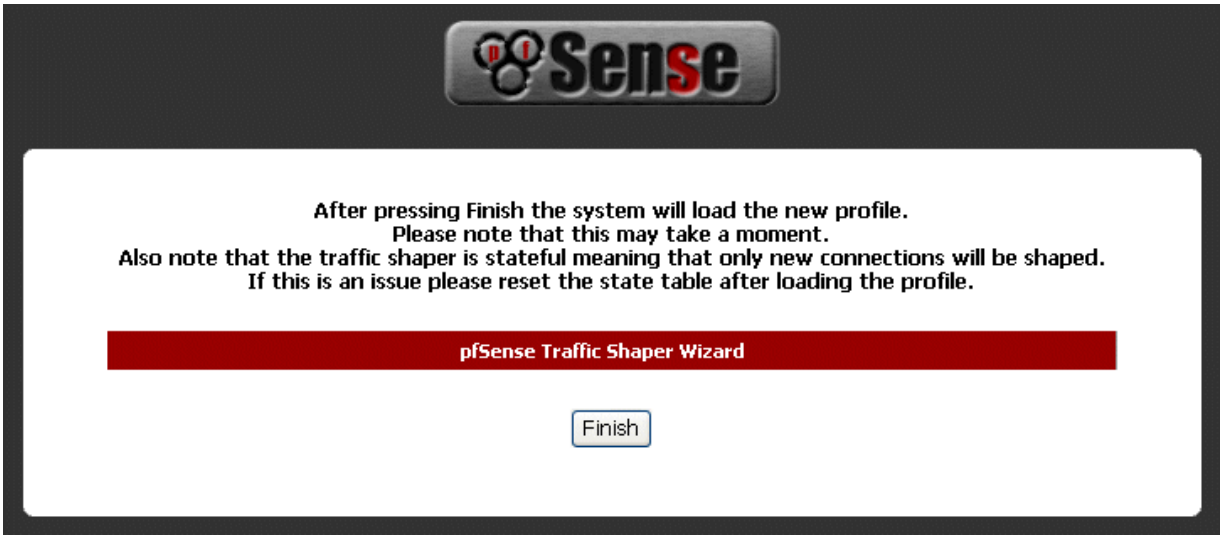

Figura 118– Configuración Traffic Shaper 3 PfSense.

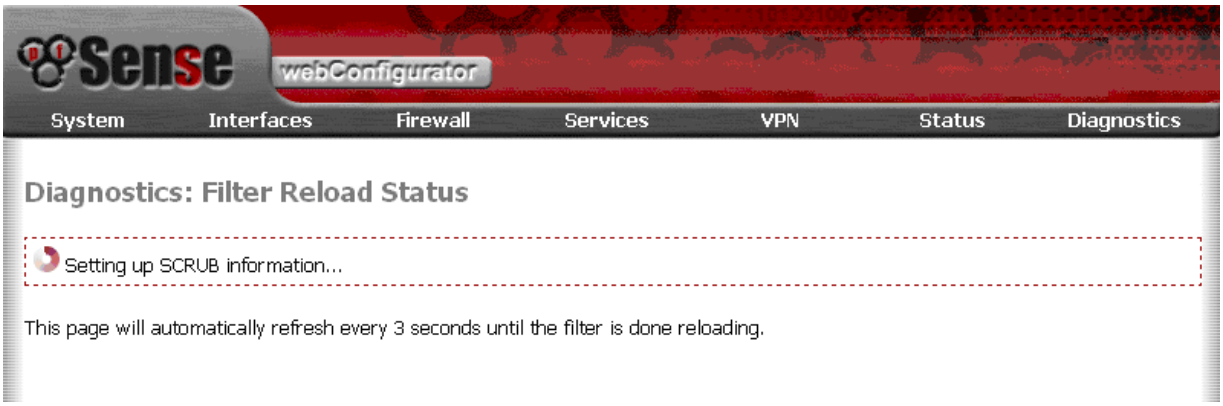

Figura 119– Configuración Traffic Shaper 4 PfSense.

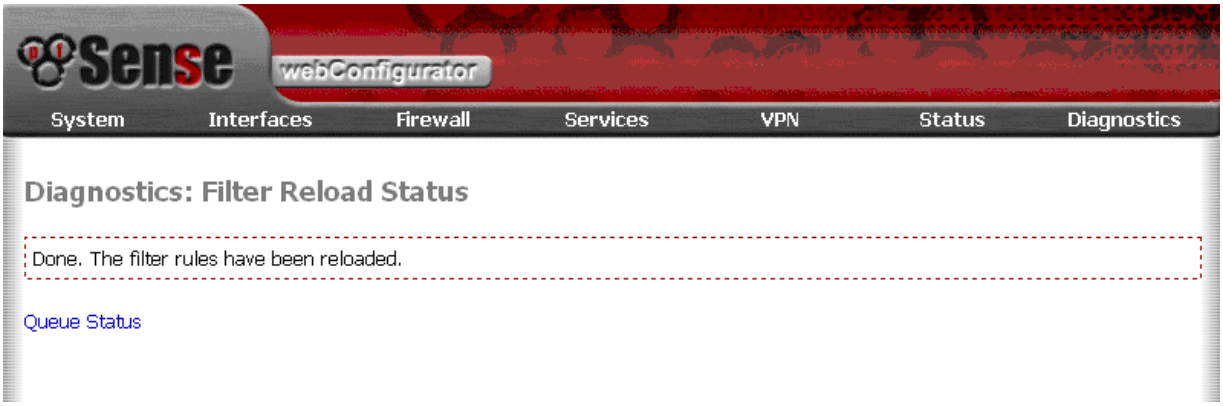

Figura 120– Configuración Traffic Shaper 5 PfSense.

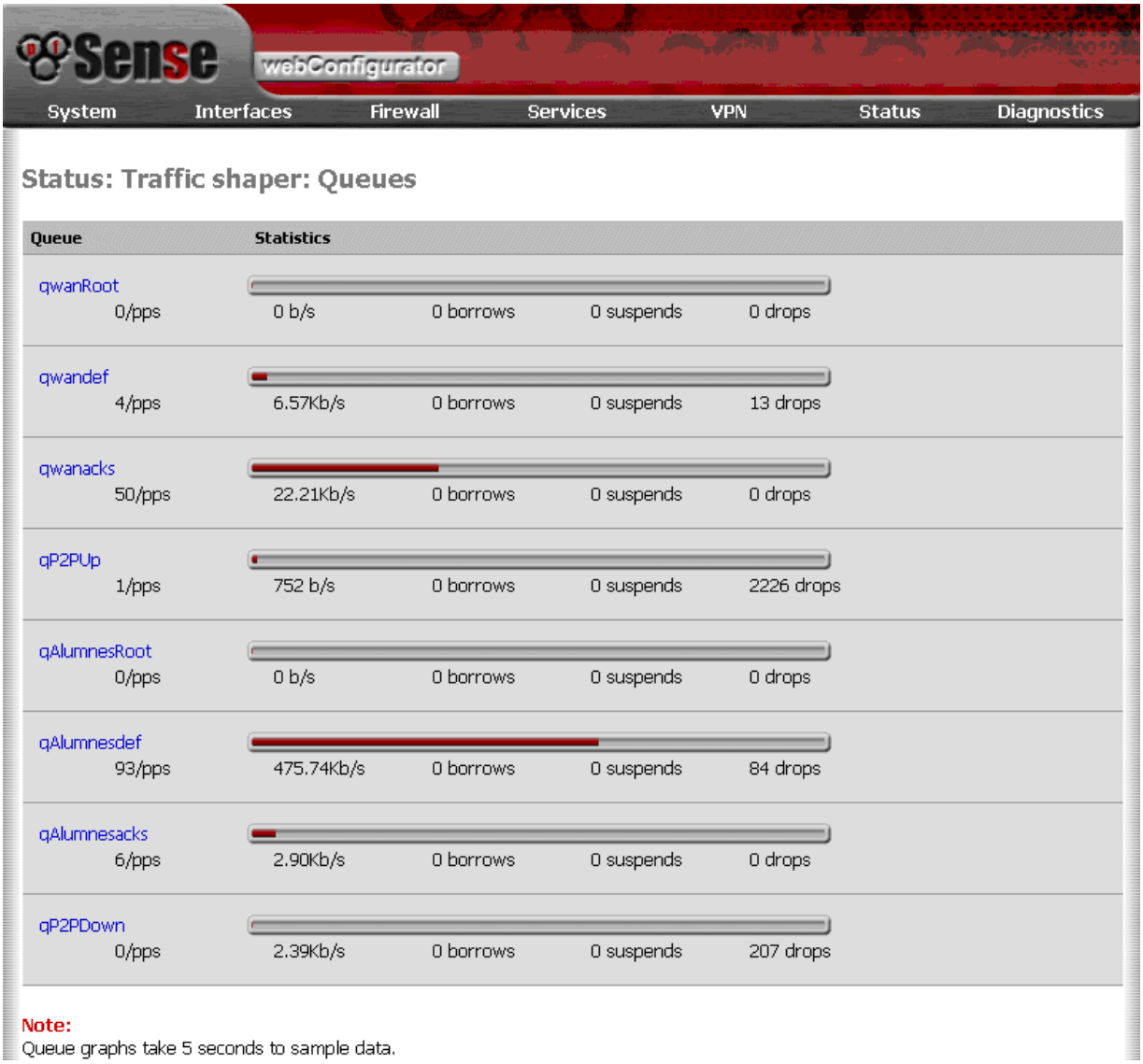

Figura 121– Status Traffic Shaper PfSense.

Para configurar OpenVpn en PfSense, es necesario ir a menú principal, luego "VPN", después "OpenVPN" y finalmente "Servers". Es necesario ingresar la información que aparece en la figura, la cual es obtenida en el proceso anterior que se realizó en el servidor Debian, explicado en capítulos anteriores. Por ello que tanto los certificados como las claves utilizadas en la VPN, son obtenidos en las etapas anteriores.

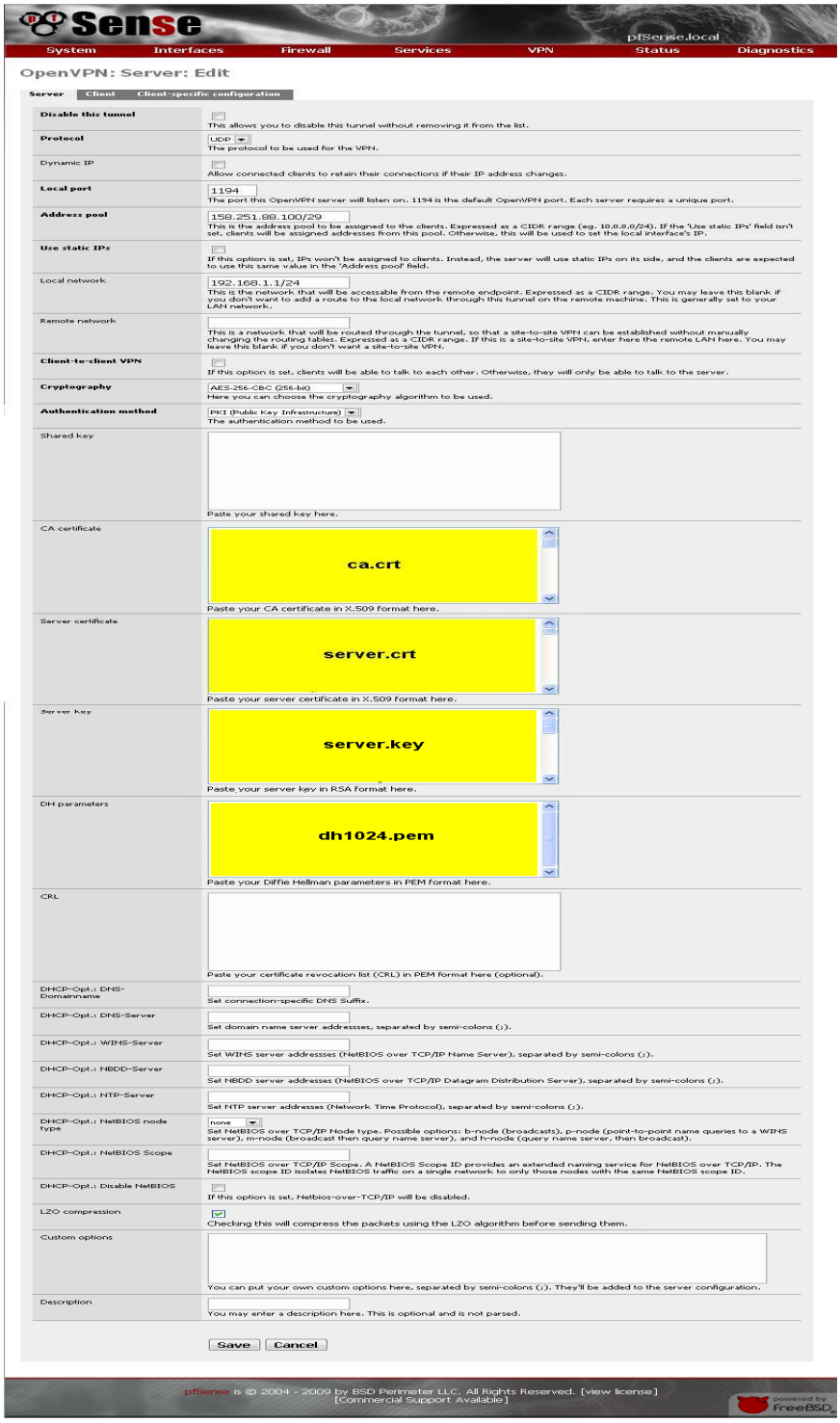

Figura 122 – Status Traffic Shaper PfSense.

Una vez que hayan sido configurados estos parámetros, es posible realizar un VPN, desde un cliente tal como se explica a continuación.

9.1.1.3 Cliente Windows

Para la utilización de OpenVpn en sistemas Windows, es necesario descargar el programa que se encuentra en la página oficial OpenVpn. El proceso de instalación es tan sencillo como seguir las instrucciones y seleccionar las opciones que nos presente el asistente de instalación.

El proceso de instalación comienza con la siguiente figura.

Figura 123 – Instalación OpenVpn.

Se pulsa en “Siguiente” y se presenta la ventana con la licencia Open Source, la cual se debe accionar el botón “I Agree” para seguir la instalación.

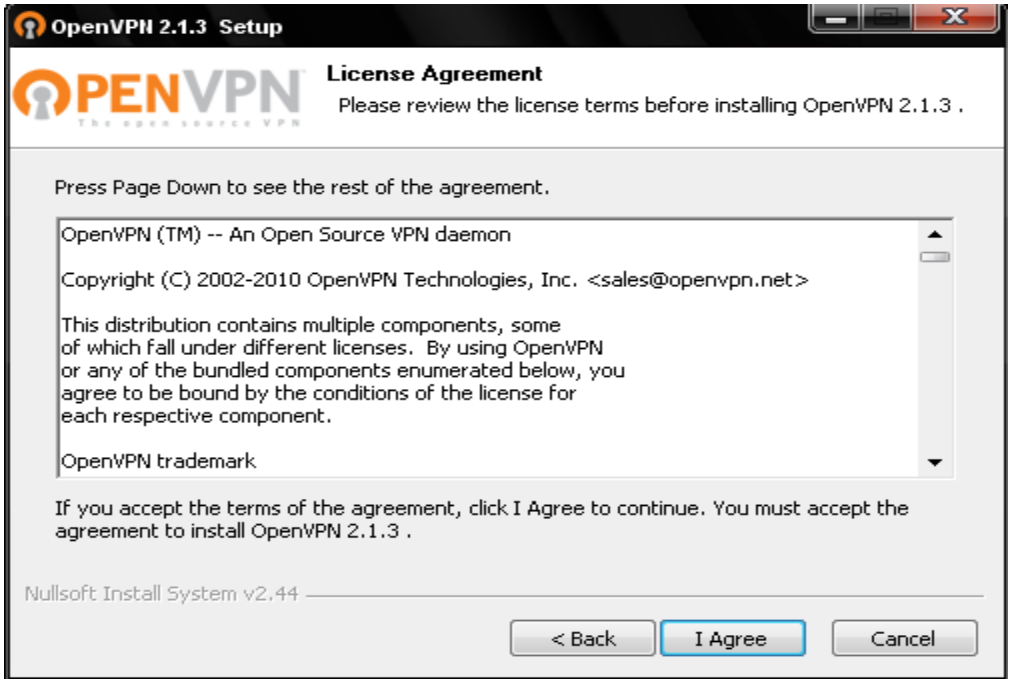

Figura 124 – Instalación Paso 1 OpenVpn.

Una vez accionada la ventana anterior, se seleccionan los componentes a instalar, por defecto se seleccionan todos, tal como se muestra en la siguiente figura.

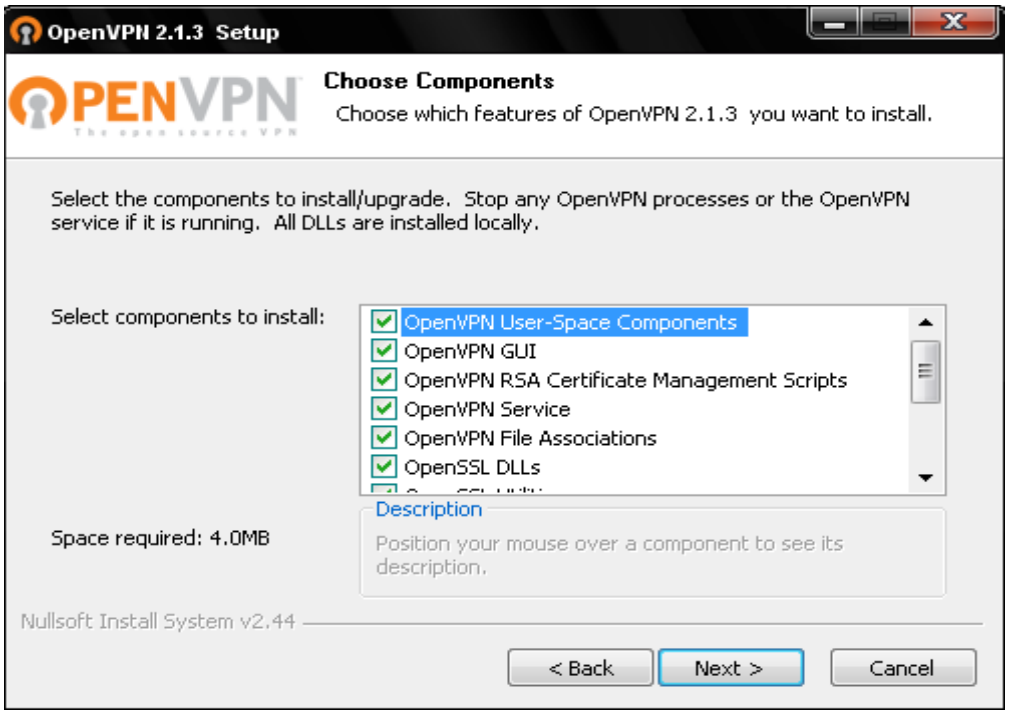

Figura 125 – Instalación Paso 2 OpenVpn.

El proceso siguiente, es seleccionar el directorio donde se instalará la aplicación, tal como aparece en la siguiente figura.

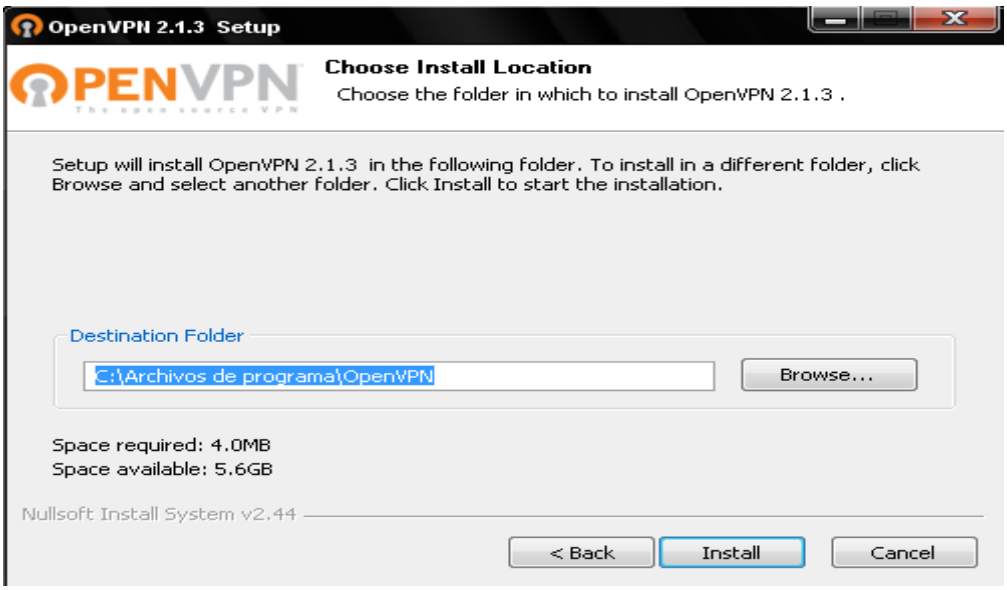

Figura 126 – Instalación Paso 3 OpenVpn.

Al accionar el botón “Install” comienza la instalación de la aplicación, tal como se muestra en la siguiente figura.

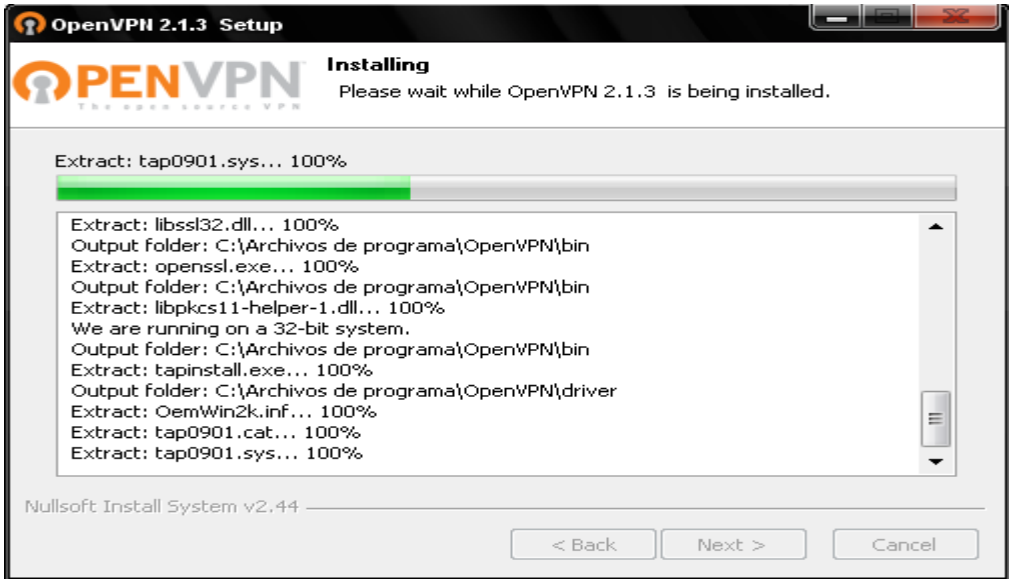

Figura 127 – Instalación Paso 4 OpenVpn.

A este punto, el proceso de instalación ha finalizado con la siguiente figura.

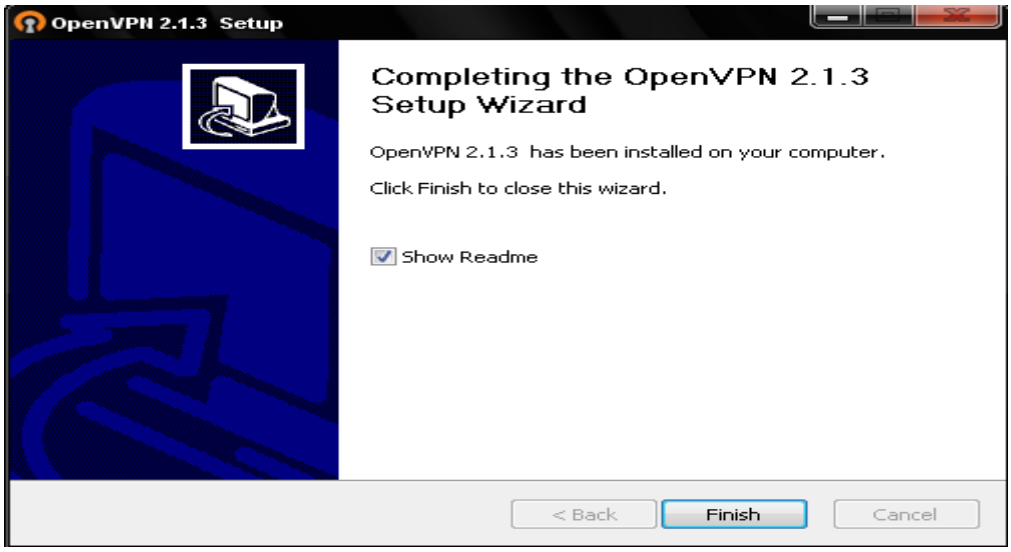

Figura 128 – Instalación Paso 5 OpenVpn.

Para comprobar que la VPN se ha instalado como un servicio, se debe realizar la siguiente secuencia: ir a Inicio – Panel de Control – Herramientas Administrativas – Servicios, y se puede comprobar que se ha instalado el servicio OpenVpn, aunque se encuentra detenido, como se puede observar en la siguiente figura.

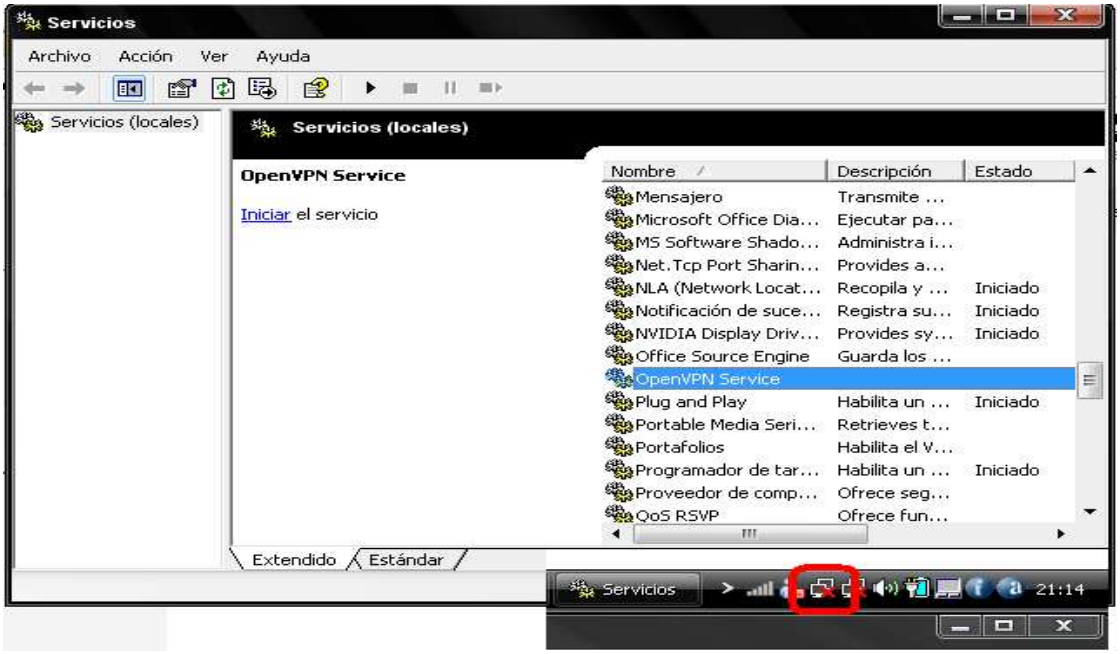

Figura 129 – Instalación Paso 6 OpenVpn.

También se puede observar que se tiene un ícono de una conexión de red que no está activada, dado que el túnel no se encuentra activado.

Una vez instalada la aplicación OpenVpn en un cliente Windows, es necesario dirigirse a la siguiente ruta.

- **C:\Archivos de programa\OpenVPN\config**

En este directorio se borra toda la información que se encuentre, luego se crea un archivo con el nombre "clienteX.ovpn", donde "X" representa al número de cliente y se ingresa la siguiente información al archivo.

```
############################################################
# Archivo de configuración de clientes OpenVPN             #
# ******   Por ningún motivo intente cambiar    ******** #
# ******    la configuración de este archvo     ******** #
# ******    a menos que sepa muy bien lo que    ******** #
# ******          está haciendo                 ******** #
# Por cualquier consulta, escribir a            #
# cadv1984@gmail.com                            #
#                                               #
# En linux este archivo debe tener sufijo .conf #
# En windows este archivo debe tener sufijo .ovpn #
############################################################


client                  # indica cliente puede ser también server para un
                        servidor linux
dev tun                 # indica tipo de red virtual, TAP capa 2, TUN capa 3 como
                        enrutador.
```

proto udp	**# protocolo udp para mayor seguridad y mejor qos**
tls-client	**# OpenVPN utiliza el puerto 1194 UDP por defecto.Cada túnel OpenVPN debe usar un número de puerto diferente lport o rport pueden usarse. para denotar diferentes puertos para local y remoto.**
remote 158.251.88.100 1194	**# Hostname o dirección IP del servidor OpenVPN también se especifica el puerto en el que el servidor OpenVPN escucha peticiones.**
resolv-retry infinite	**# Trata de resolver el hostname del servidor infinitamente Muy útil, cuando el cliente o servidor OpenVPN tienen i dirección IP dinamica.**
nobind	**# No hacer bind a un número de puerto local en especifico**
;user nobody	**# Los usuarios linux pueden descomentar las siguientes 2 líneas y obtener seguridad adicional (el proceso de openvpn se ejecutará en el usuario nobody)**
;group nogroup	**# Rebajar UID y GID a "nobody" después de la inicialización para más seguridad.**
persist-key	**# Descomente ésto para una detección mas fiable cuando el sistema pierde su conexión. Por ejemplo, conexiones telefónicas o portátiles que se desplazan a otros sitios.**
persist-tun	**# Descomente ésto para una detección mas fiable cuando el sistema pierde su conexión. Por ejemplo, conexiones telefónicas o portátiles que se desplazan a otros sitios.**

ca ca.crt	**# Fichero de la Autoridad de Certificación (CA)**
cert cliente16.crt	**# Nuestro certificado/clave pública**
key cliente16.key	**# Nuestra clave privada**
cipher AES-256-CBC	**# Cifrado criptográfico que usará OpenVPN.**
;dh dh2048.pem	**# Cifrado D-H.**
;duplicate-cn	**# Para usar la misma clave en varios clientes**
ns-cert-type server	**# Protección anti Man In The Middle Solo aceptar conexiónes de servidores OpenVPN que tienen el atributo extendido nsCertType=server. Esta es una protección importante para protegerse contra ataques potenciales de tipo mitm.**
ping 15	**# Enviar un ping UDP al extremo remoto una vez cada 15 segundos para mantener el estado la conexión en el firewall activa. Descomente esto si está usando un firewall con estado.**
ping-restart 45	**# Descomente ésto para una detección mas fiable cuando el sistema pierde su conexión. Por ejemplo, conexiones telefónicas o portátiles que se desplazan a otros sitios.**
ping-timer-rem	**# Descomente ésto para una detección mas fiable cuando el sistema pierde su conexión. Por ejemplo, conexiones telefónicas o portátiles que se desplazan a otros sitios.**
;comp-lzo	**# LZO es una librería de compresión de datos diseñada para comprimir y descomprimir en**

tiempo real. Esto significa que favorece la velocidad frente al ratio de compresión.

verb 3 **# Nivel de información.**

Una vez almacenada esta información, el siguiente paso es llevar "ca.crt", "cliente0.crt" y "cliente0.key" que fueron creados anteriormente en el servidor Linux Debian, al computador cliente y pegarlos en el directorio siguiente.

- **C:\Archivos de programa\OpenVPN\config**

Luego se carga "OpenVpn GUI" desde inicio – programas – openvpn – OpenVPN GUI, y aparece al costado del reloj el ícono correspondiente a OpenVpn, luego solo basta un clic derecho sobre el ícono y luego clic en "Connect". Finalmente, se realiza la conexión de la VPN al servidor sin problemas si todo esta correcto, por ello el siguiente paso es realizar la transmisión de video streaming.

Este archivo de configuración se puede reutilizar para todos los usuarios, con ello se debe configurar solo una vez, y luego se puede reutilizar cuantas veces sea necesario, solo hay que considerar en cambiar las siguientes líneas:

- **cert cliente16.crt:** Corresponde al certificado digital del "cliente16", donde "cliente16" corresponde al nombre del cliente que desea conectarse al servidor.
- **key cliente16.key:** Corresponde a la clave del "cliente16", donde "cliente 16" corresponde al nombre del cliente que desea conectarse al servidor.
- **remote 158.251.88.100 1194:** Corresponde a la ip del servidor al que se desea conectar el usuario.

9.1.2 VLC

Streaming es un término que se refiere a ver u oír un archivo directamente en una página Web (o servidor) sin necesidad de descargarlo antes al ordenador. En términos más complejos podría decirse que describe una estrategia sobre demanda para la distribución de contenido multimedia a través del Internet.

Este tipo de tecnología permite que se almacenen en un búfer lo que se va escuchando o viendo. El streaming hace posible escuchar música o ver videos sin necesidad de ser descargados previamente.

Con VLC se puede hacer streaming de muchas formas pero en esta investigación se ha utilizado la transmisión a través de http, por motivos de simpleza y facilidad.

VLC media player es un reproductor multimedia del proyecto VideoLAN, es un software libre distribuido bajo la licencia GPL. Soporta muchos códecs de audio y video, así como diferentes tipos de archivos, además de DVD, VCD y varios protocolos streaming. También puede ser utilizado como servidor en unicast o multicast, en IPv4 o IPv6, en una red de banda ancha. Utiliza la biblioteca códec libavcodec del proyecto FFmpeg para manejar los muchos formatos que soporta, y emplea la biblioteca de descifrado DVD libdvdcss para poder reproducir los DVD cifrados. Además VLC tiene soporte para Video4Linux. Es multiplataforma contando con versiones para GNU/Linux, Microsoft Windows, Mac OS X, BeOS, BSD, Pocket PC, Solaris.

Figura 130 – Instalación VLC.

9.1.2.1 Instalación VLC

Para la instalación de VLC es necesario considerar dos aspectos importantes, uno es el servidor y otros es el cliente. Por ello que en ambos lugares es necesario instalar VLC.

Para la instalación de VLC en el servidor streaming es necesario realizar los siguientes pasos:

Abrir una consola y poner:

- **sudo aptitude install vlc mozilla-plugin-vlc**

Para ejecutarlo ir a "Aplicaciones – Sonido y video – VLC media player" o escribir directamente a una consola:

vlc

Es necesario saber la Ip del Servidor para poder acceder al contenido multimedia transmitido, por ende que es necesario configurar el servidor streaming. Además es importante tener en cuenta otras consideraciones importantes que serán explicadas a continuación.

9.1.2.1.1 Servidor Streaming

En la configuración del servidor streaming, se configura VLC de la siguiente manera. Se abre la aplicación VLC, hay que dirigirse a "Medio", luego "Emisión" y finalmente la pestaña "Aparato de Captura", tal como se aprecian en las figuras.

Figura 131 – Configuración Paso 1 VLC.

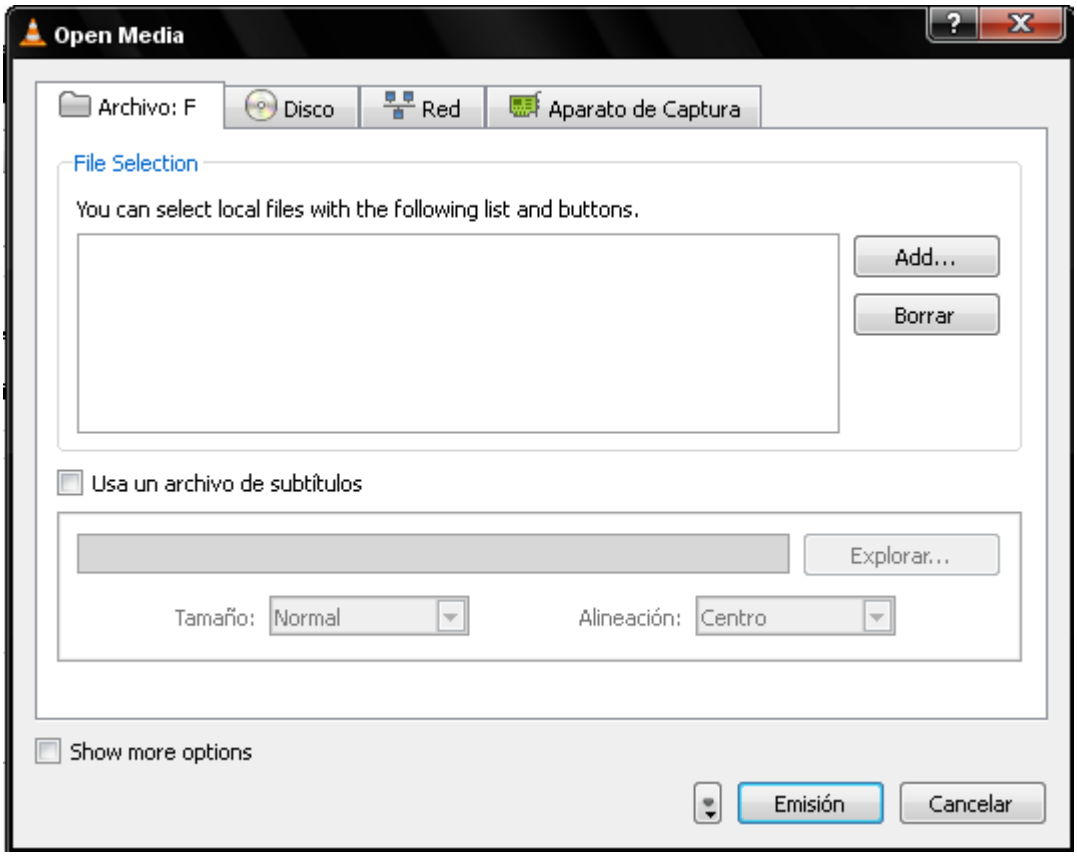

Figura 132 – Configuración Paso 2 VLC.

En la figura se aprecian varias cosas importantes y relevantes a configurar. La primera de ellas se encuentra en la parte superior, “Protocolo de Red” la que indica el “Protocolo” que se utilizará para la transmisión de video streaming, la “Dirección” que indica la Ip que se utiliza para acceder al servidor streaming, y finalmente el “Puerto” el que será utilizada para acceder a la transmisión.

Dependiendo de la versión de VLC, en algunos casos en vez de la pestaña “Aparato de Captura”, puede decir “Archivo”, entre otras. También se puede acceder directamente al dispositivo entrando en el enlace correspondiente como indica la figura.

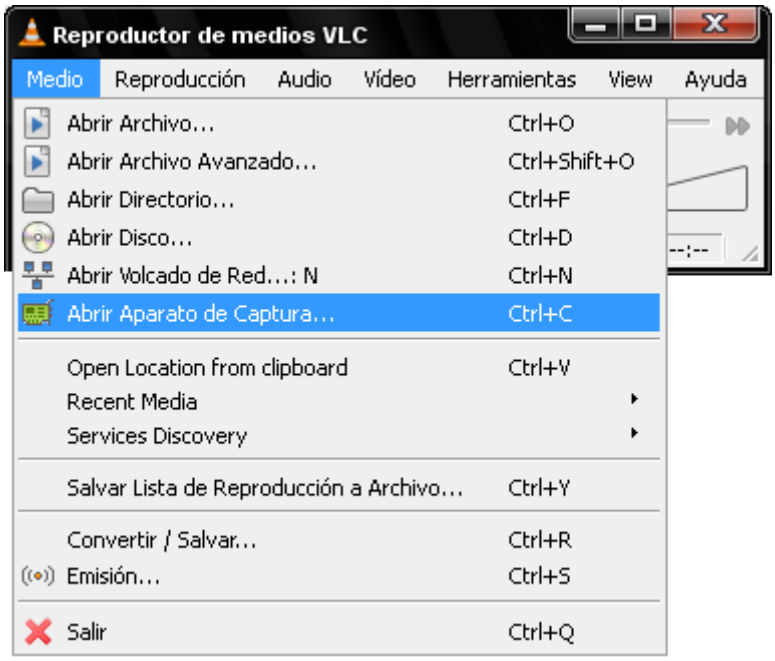

Figura 133 – Configuración Paso 3 VLC.

Luego en la siguiente figura, se observa la opción de selección del dispositivo, es en este botón donde se ingresa la cámara Ip a utilizar, por ello se acciona el botón “Configurar” y se accede a la siguiente figura.

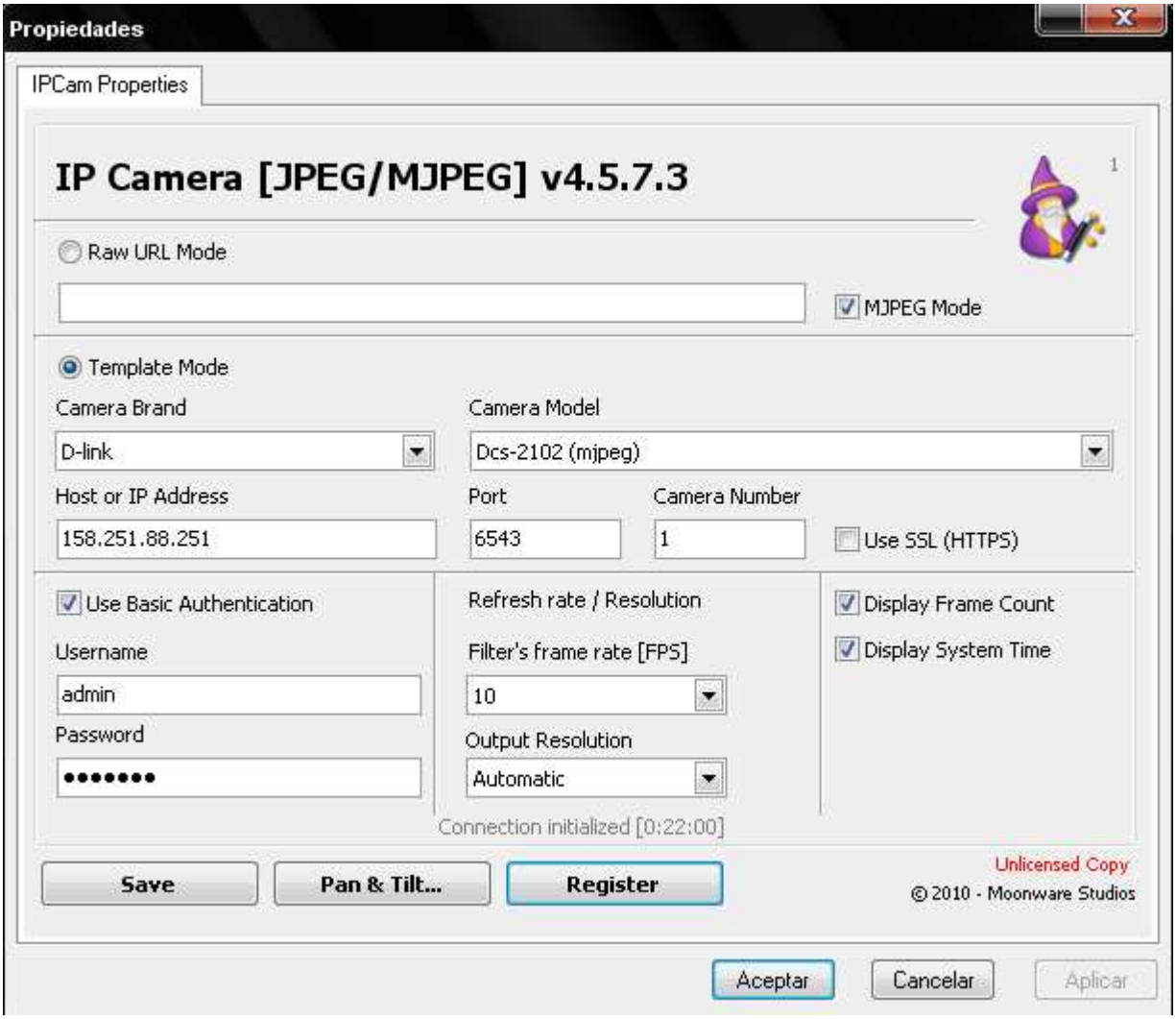

Figura 134 – Configuración Paso 4 VLC.

Como se puede apreciar, se ingresan las propiedades de la cámara Ip a utilizar, en este caso, se muestra la configuración utilizada en este proyecto, cuyas características de definen a continuación.

La cámara utilizada, tal como se mencionó en el inciso anterior, es una D-Link modelo Dsc-2102, cuya configuración que posee dentro de la universidad está asociadas a la siguiente información.

- Ip Cámara: 158.251.88.251
- Puerto: 6543
- User: Admin
- Pass: jmxe4lx
- FPS: 10.

- Resolución: Automática.

Es posible utilizar otro tipo de dispositivos a emitir, como cámaras de video, Webcams, archivos, entre otros, y eso dependerá de lo que se desea realizar.

Una vez configurada la cámara Ip, se acepta la configuración y se selecciona en la ventana el tipo de transmisión a realizar por parte de la cámara, la que corresponde a "Ip Camera [RTSP]", tal como aparece en la siguiente figura.

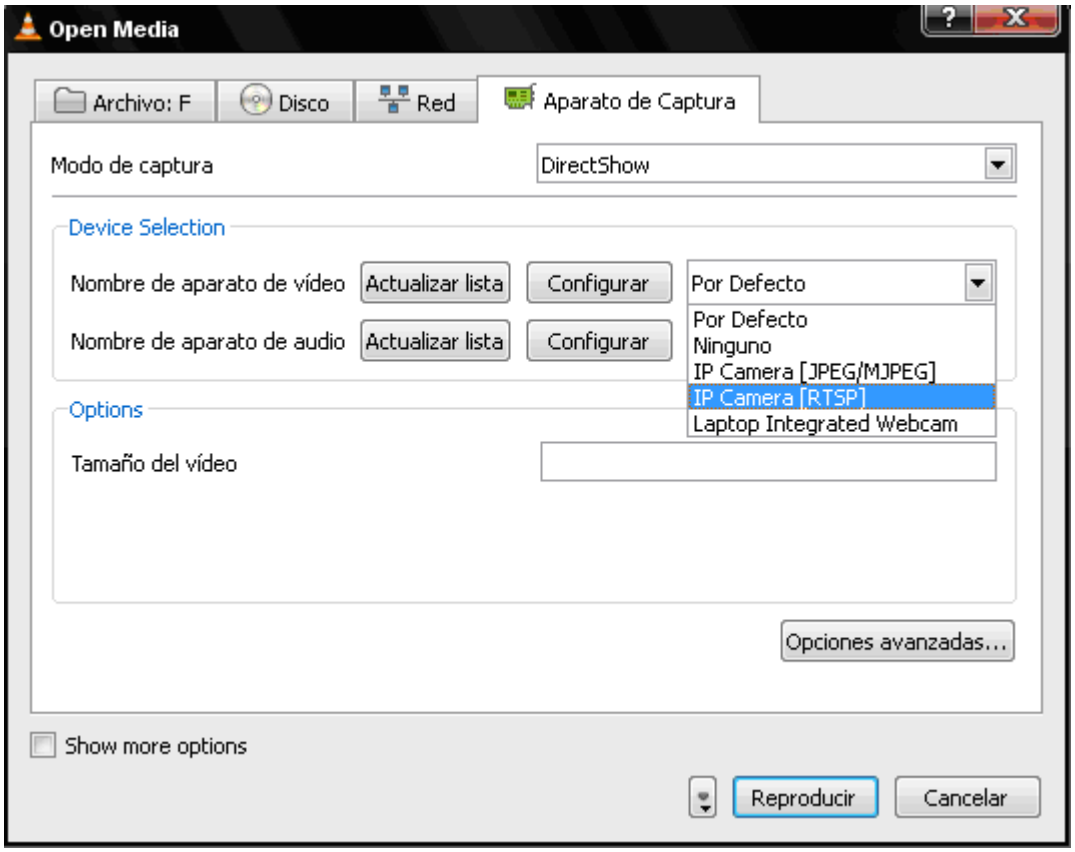

Figura 135 – Configuración Paso 5 VLC.

Luego se observa en la parte inferior el botón "Reproducir", el cual en la parte izquierda aparece un menú desplegable, y se selecciona la opción "Emitir", tal como aparece en la figura.

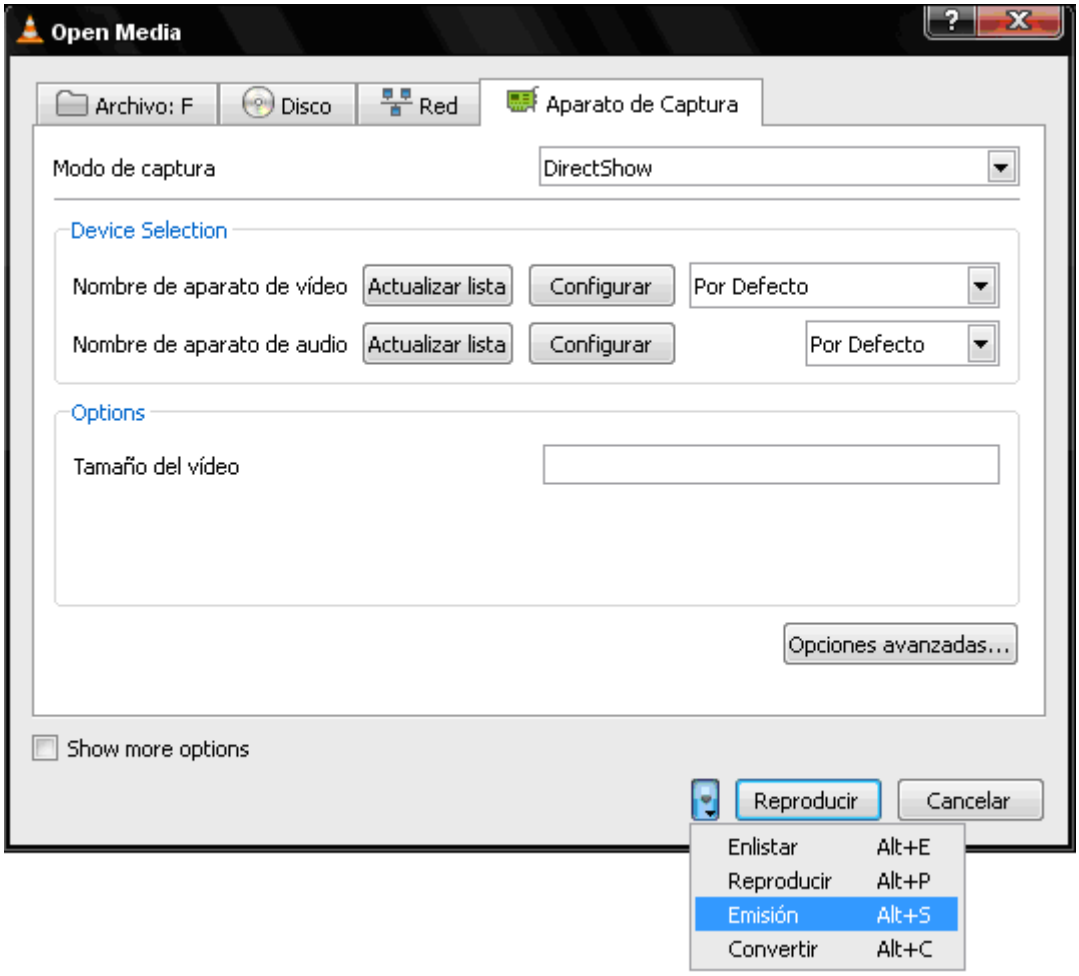

Figura 136 – Configuración Paso 6 VLC.

En la ventana, se verán varias opciones, la primera de ellas “Source”, la que indica la ruta donde se encuentra el fichero de video. Luego, se acciona el Botón siguiente para seguir con la configuración.

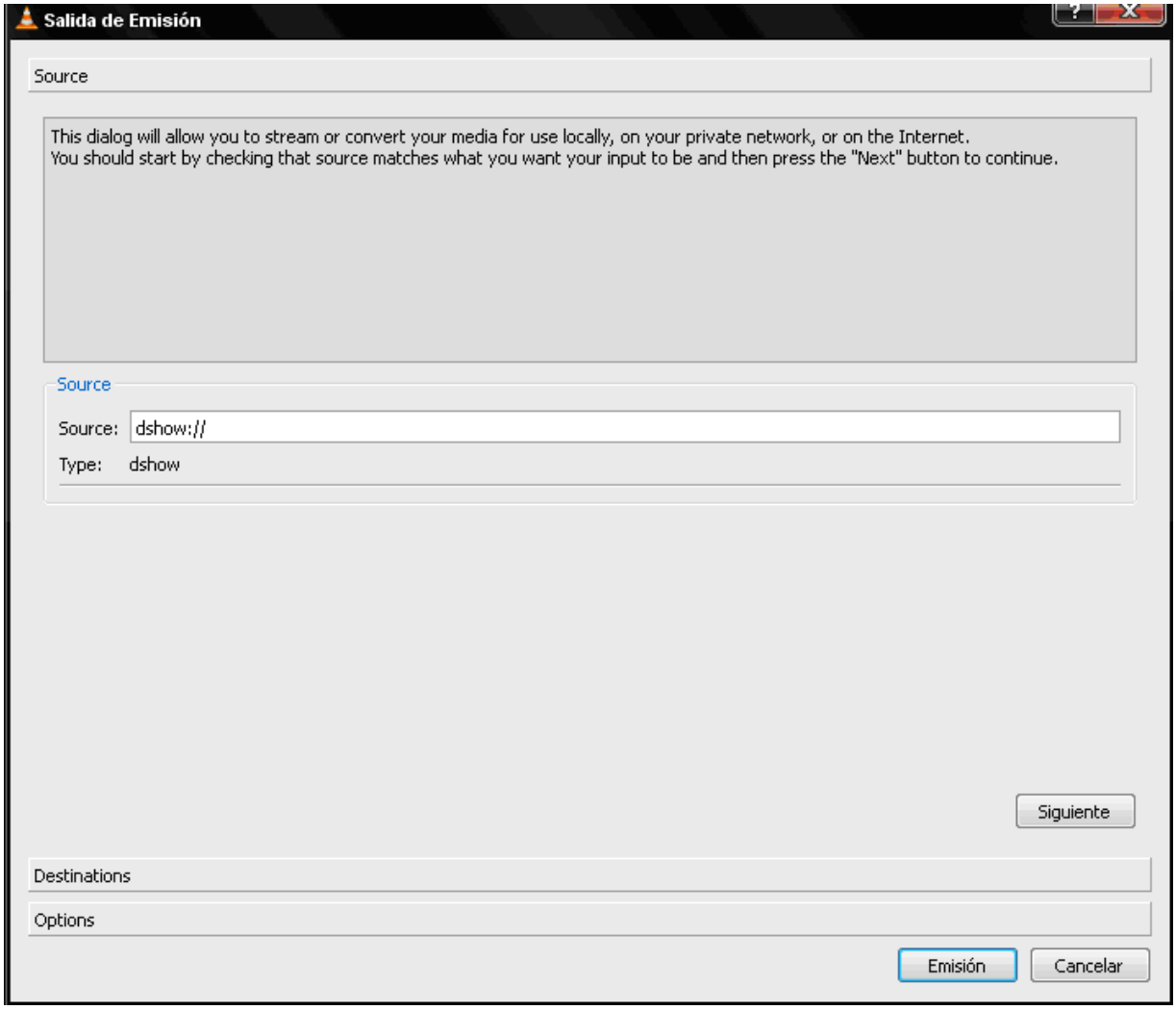

Figura 137 – Configuración Paso 7 VLC.

En la siguiente opción “Destino”, como se aprecia en la figura es posible configurar el destino que se utilizará para la transmisión, además indicar la visualización del video en forma local, como las opciones de transcodificación para la transmisión de video, tal como aparece en la figura.

En un comienzo, seleccionar “Display Locally” es de suma importancia para verificar el funcionamiento local, y luego remoto del contenido, ya que en un comienzo existe la posibilidad de configuraciones erróneas o problemas en la conexión.

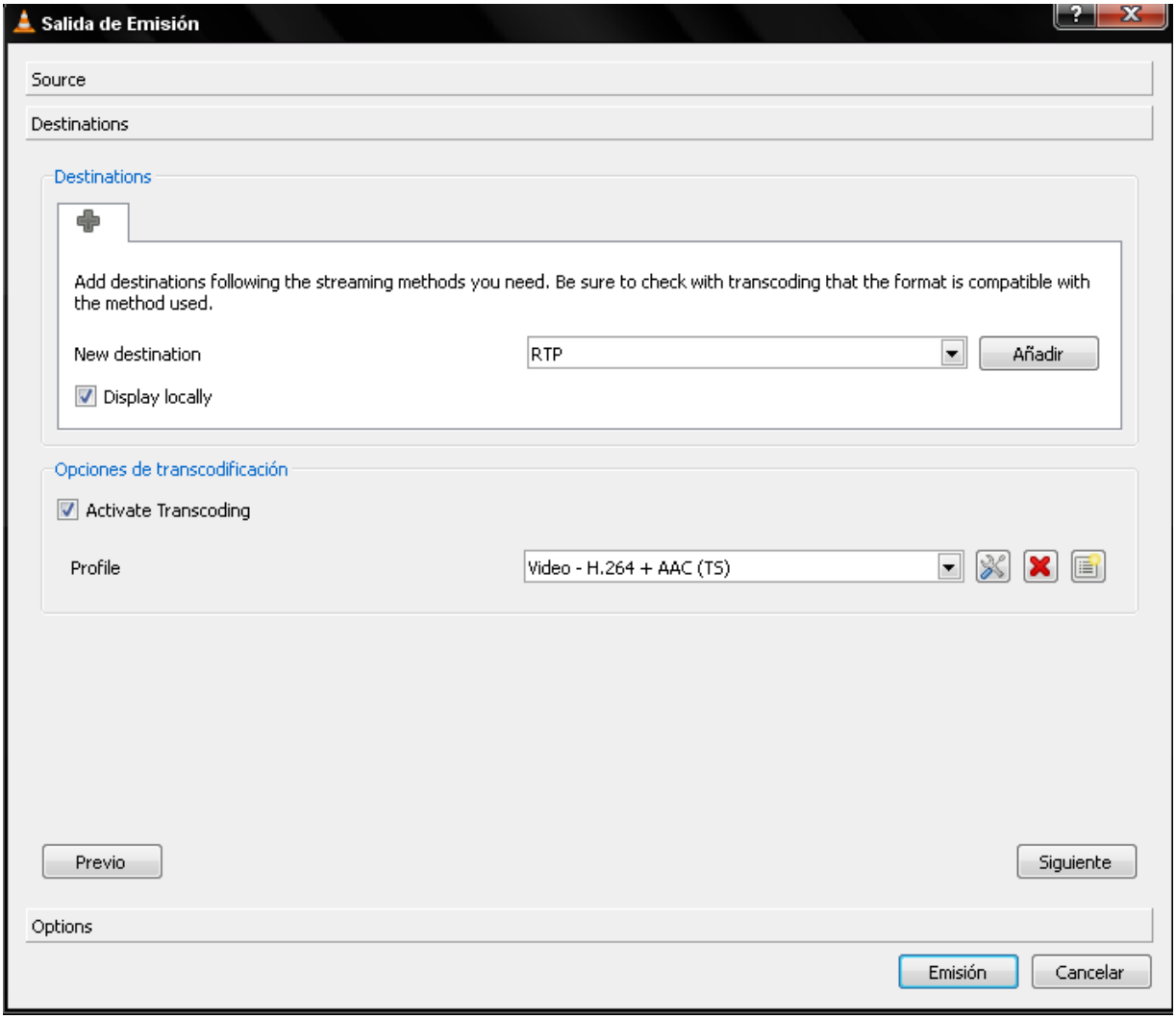

Figura 138 – Configuración Paso 8 VLC.

Luego al seleccionar el destino y accionar "añadir", se despliega la siguiente figura, en la que es posible configurar la dirección Ip y Puerto para la transmisión del video streaming. Por ello que se ha utilizado la Ip del servidor streaming, y la configuración restante se deja por defecto.

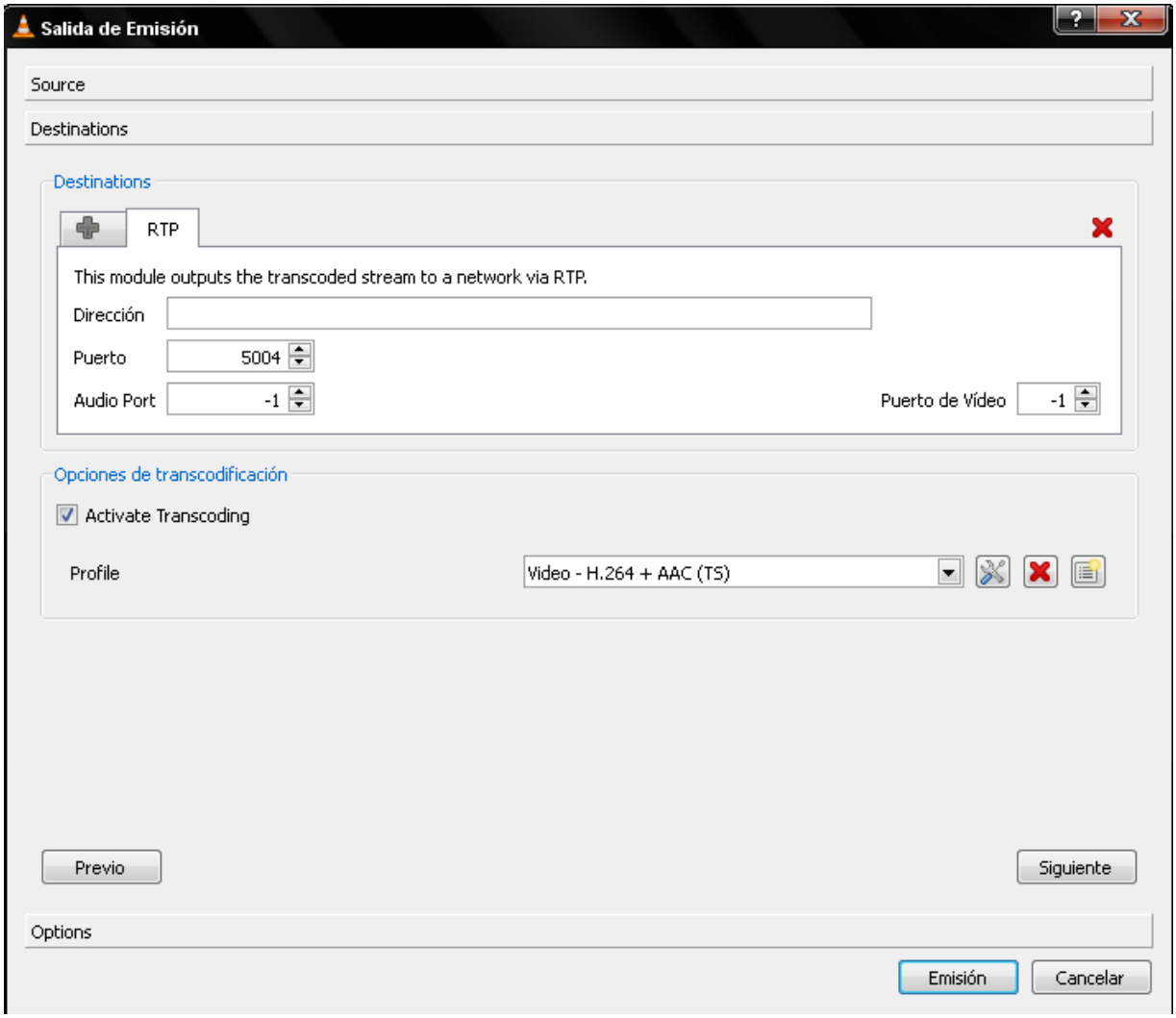

Figura 139 – Configuración Paso 9 VLC.

Respecto a las "Opciones de Transcodificación", es posible realizar configuraciones, que puedan mejorar la calidad o transmisión del contenido multimedia, por ende a continuación se muestra la configuración utilizada en este proyecto.

El encapsulamiento utilizado para una mejor transmisión y visualización del contenido multimedia, se ha utilizado MPEG-TS, el cual proporciona una mejor calidad de video y compresión para el envío de paquetes streaming.

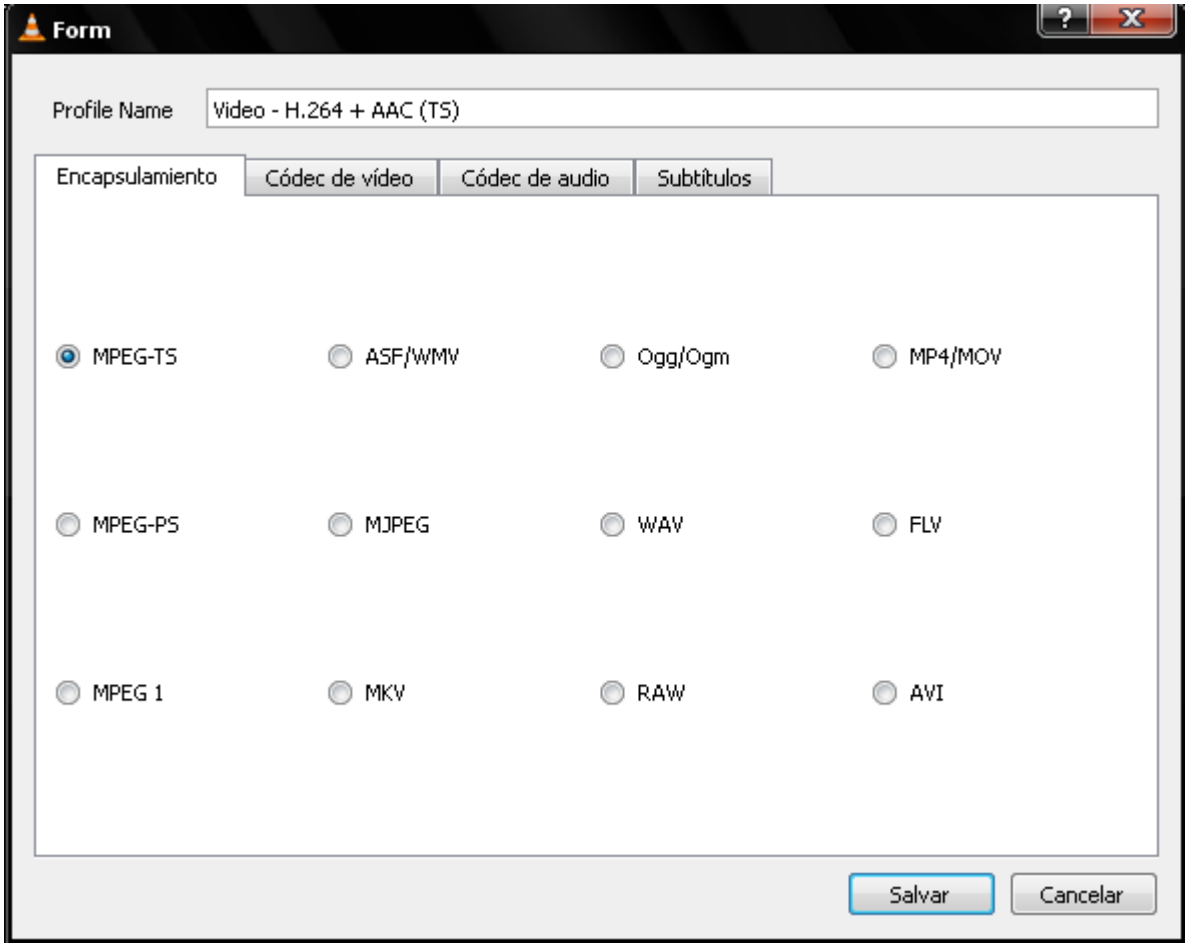

Figura 140 – Configuración Paso 10 VLC.

Respecto a los códecs se ha mantenido la configuración original tal como se aprecia en la siguiente figura.

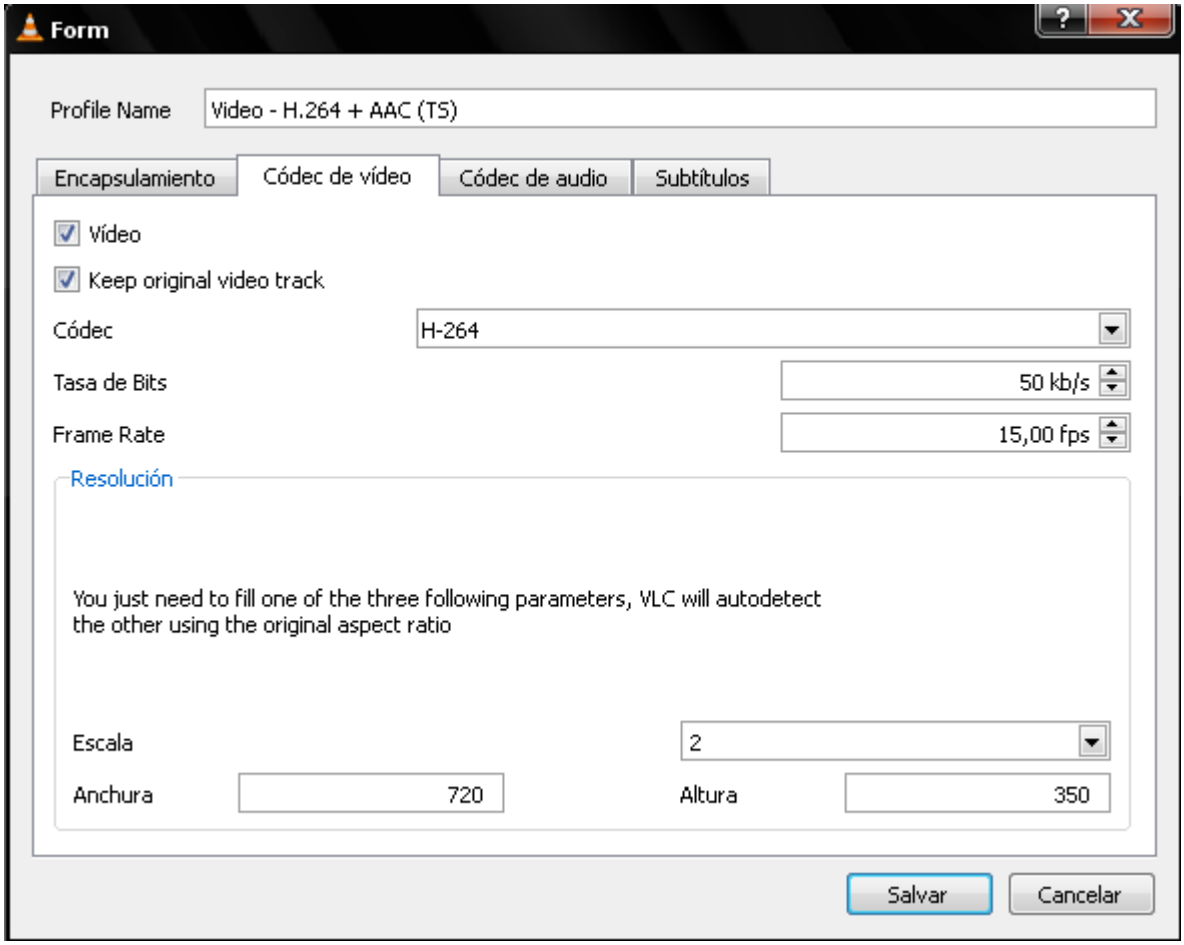

Figura 141 – Configuración Paso 11 VLC.

Respecto a Audio y Subtitulo, no hay configuración respectiva, ya que en este proyecto no se han utilizado ninguno de estos tópicos.

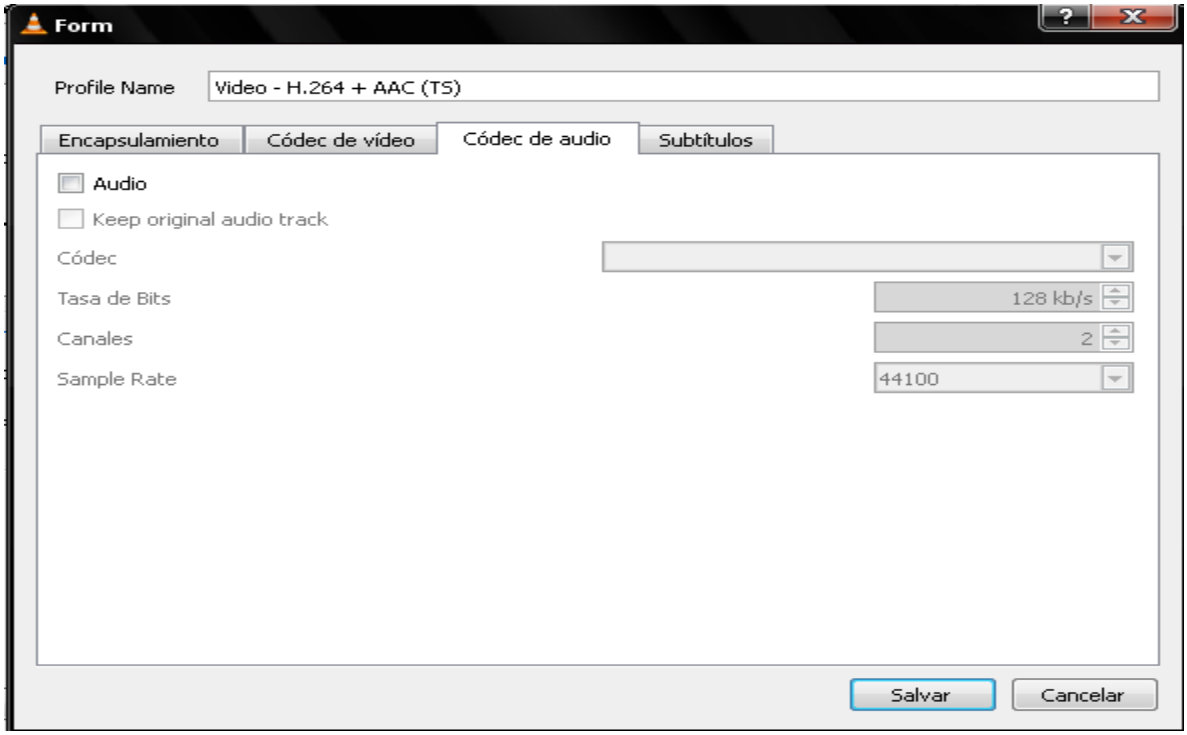

Figura 142 – Configuración Paso 12 VLC.

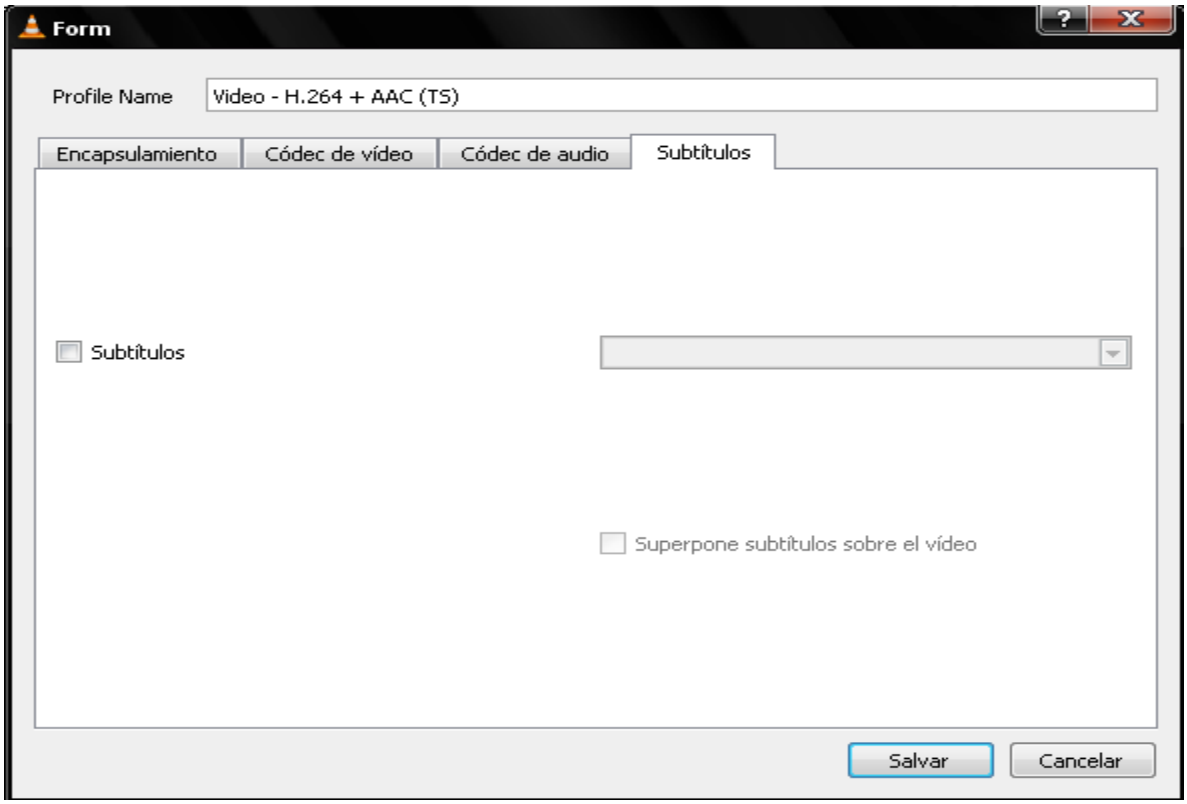

Figura 143 – Configuración Paso 13 VLC.

Finalmente, en la siguiente figura se seleccionan la casilla “Mantener Abierta Salida de Emisión”, lo demás no es aplicable o relevante para este proyecto, así que queda tal cual se aprecia en la figura. Luego se acciona el botón “Emisión” y se estará emitiendo contenido multimedia.

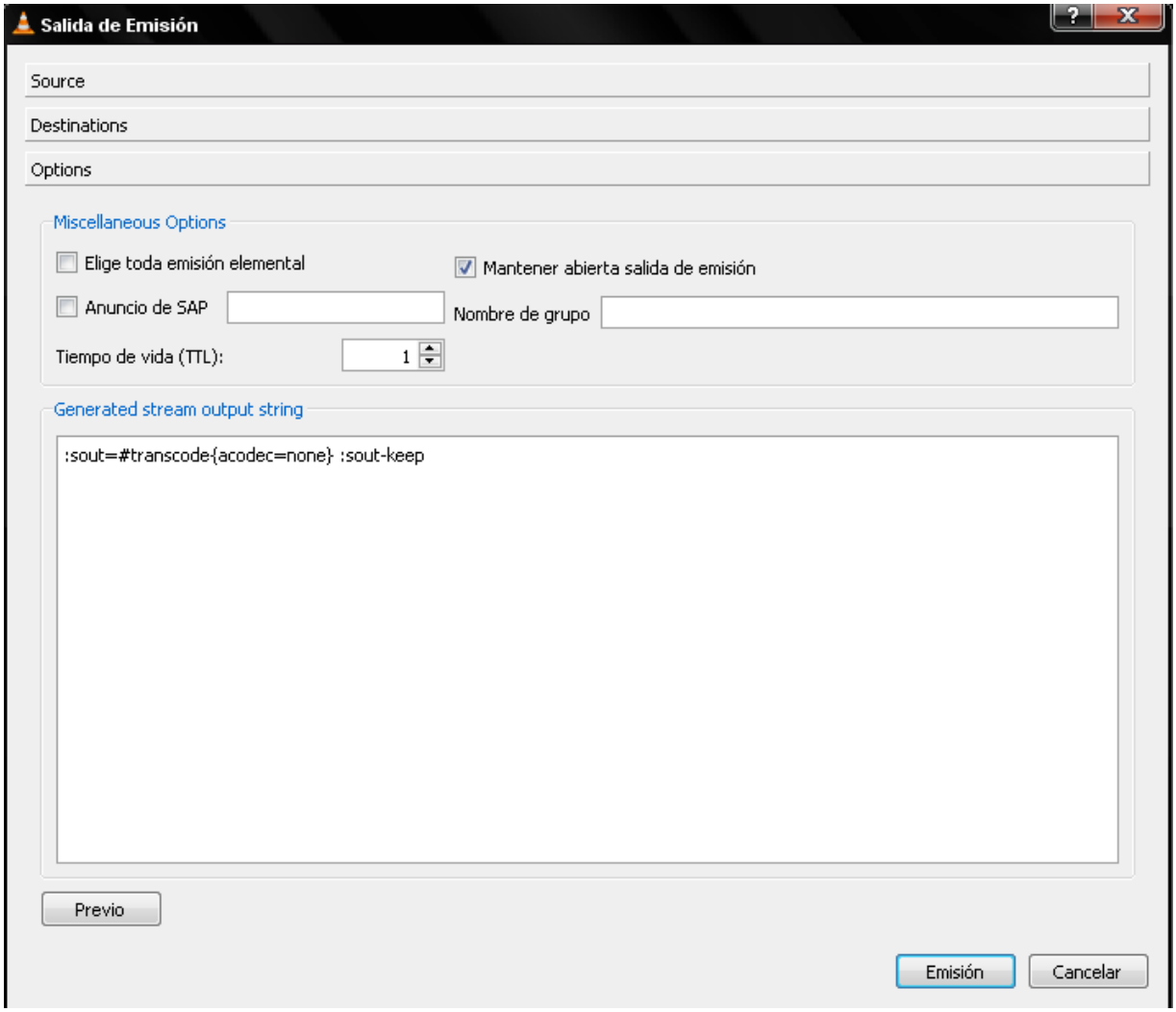

Figura 144 – Configuración Paso 14 VLC.

Finalmente, se visualiza en la siguiente forma.

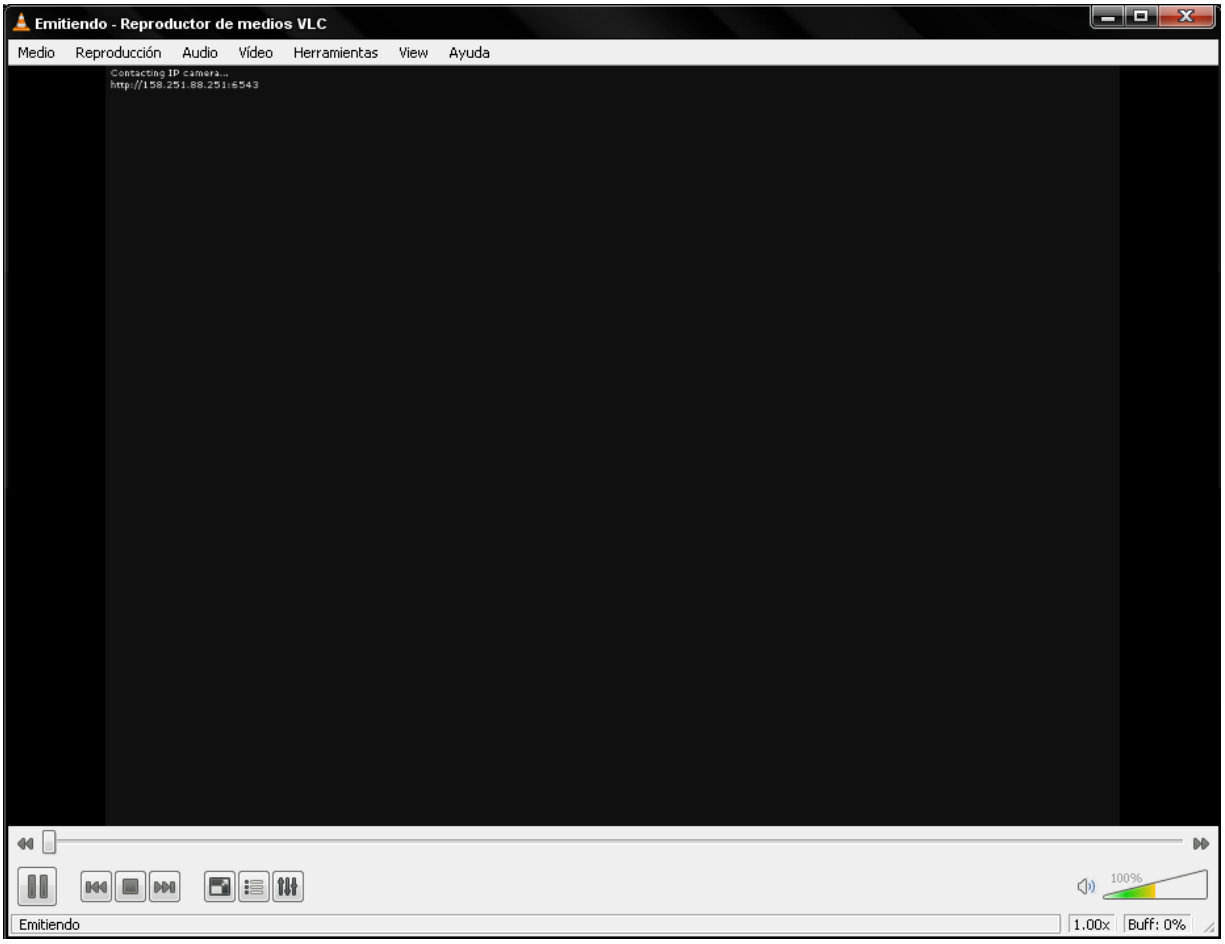

Figura 145 – Transmisión Servidor Streaming VLC.

9.1.2.1.2 Cliente Streaming

Como se mencionó anteriormente se ejecuta la aplicación VLC, luego ir al siguiente enlace tal como se aprecia en la figura.

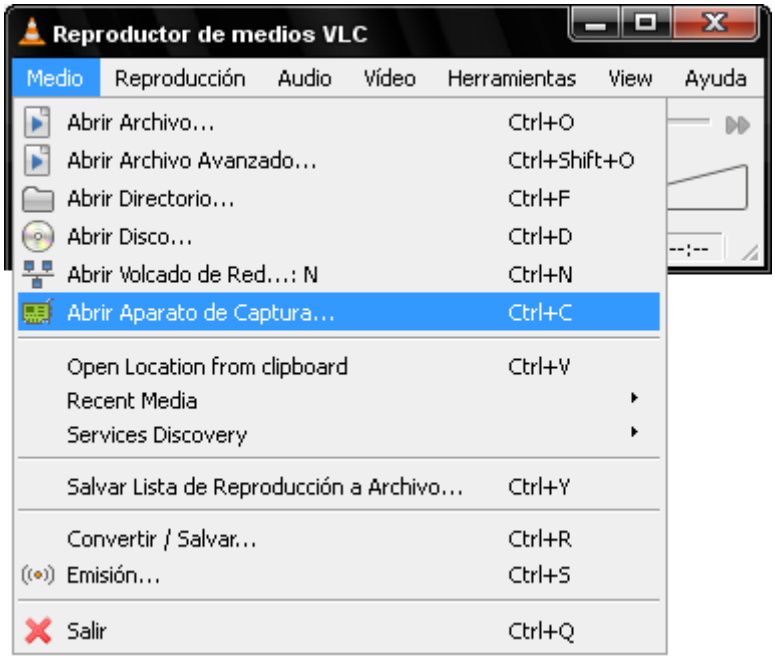

Figura 146 – Transmisión Streaming Cliente Paso 1 VLC.

Como se mencionó, es posible que en algunos casos dependiendo de la versión de VLC, es posible que "Medio" puede identificarse como "Archivo" u otra forma.

Luego se accede a la siguiente ventana, que de manera muy intuitiva y fácil , se debe indicar el protocolo, dirección y puerto configurado en el servidor, para poder comenzar a disfrutar y visualizar del contenido multimedia.

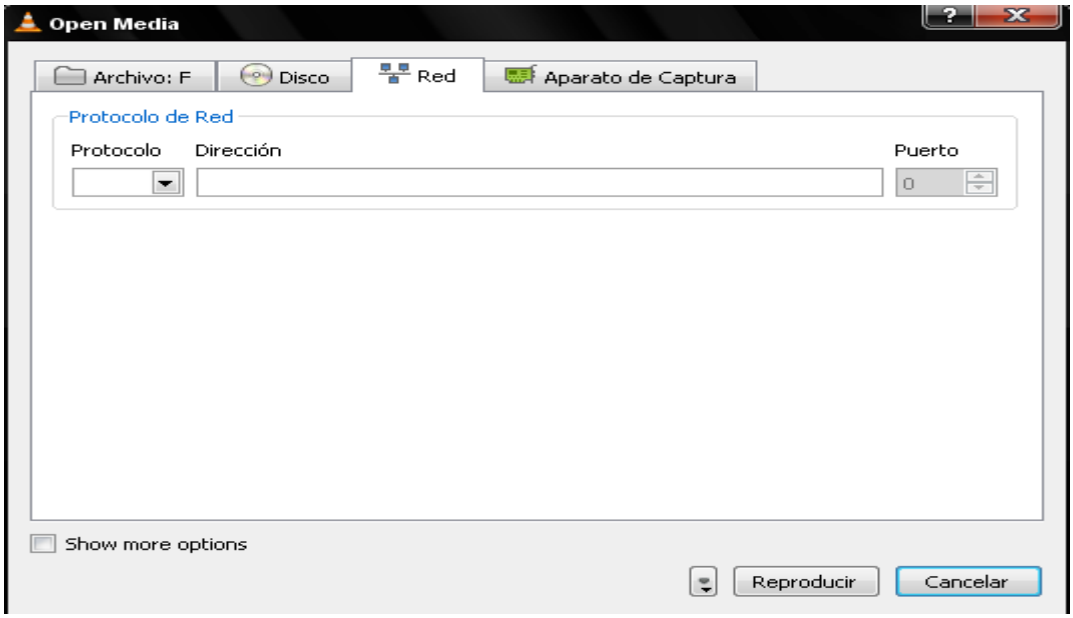

Figura 147 – Transmisión Streaming Cliente Paso 2 VLC.

En este caso:

- Ip: 192.168.1.199
- Puerto:5004
- Protocolo: Rtp.

Si existe dominio en la red, se podría acceder el nombre en vez de la dirección Ip, ya que la forma sería la misma, por ejemplo: ejemplodominio.dominio.cl:5004. Luego, se teclea enter, y es posible visualizar el contenido multimedia.

Es posible generar la transmisión de video, a través de la consola de comandos, pero como no se ha utilizado esta forma, no se abordará su configuración. Finalmente se visualiza la transmisión tal como aparece en la imagen.

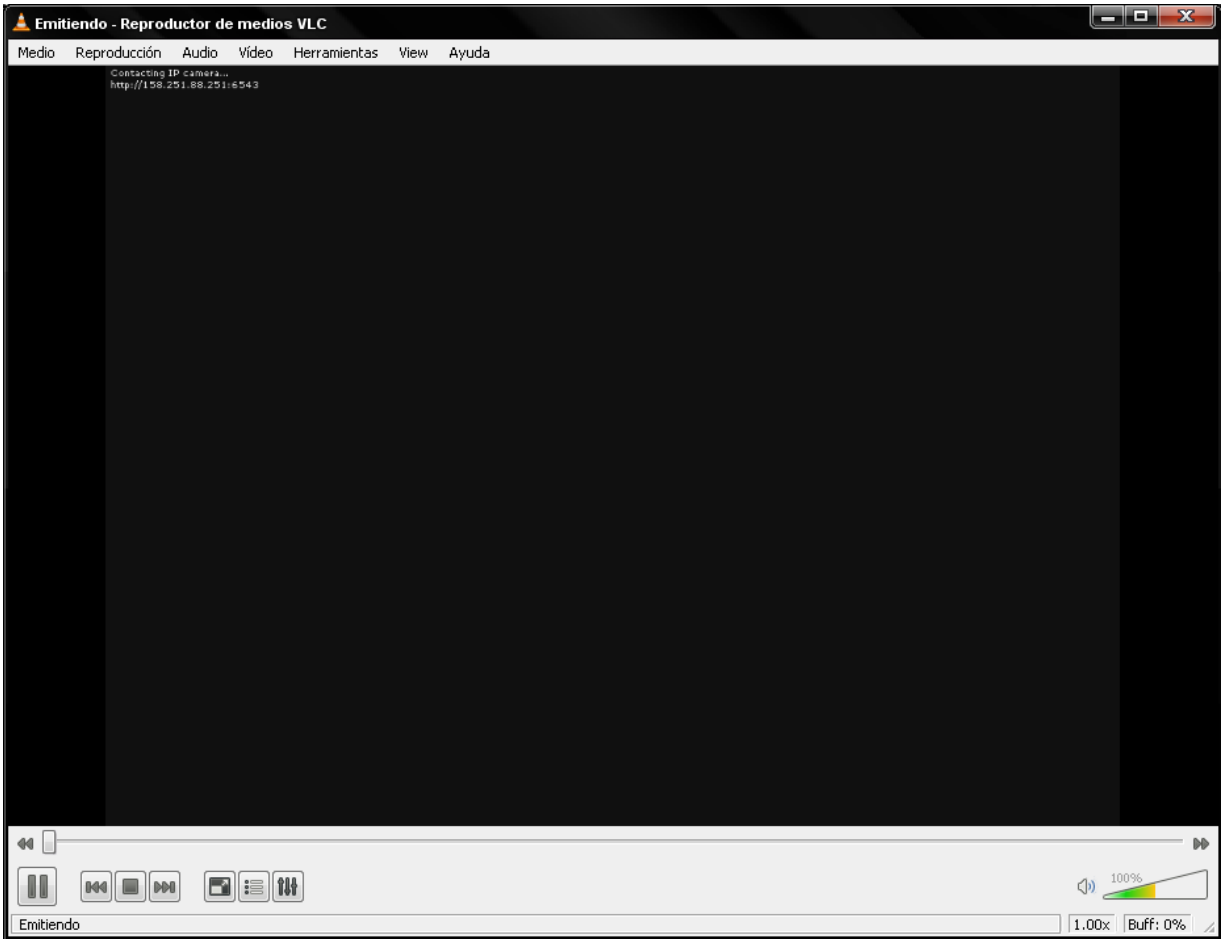

Figura 148 – Transmisión Streaming Cliente Paso 3 VLC.

9.2 Análisis de Resultados

9.2.1 Ambiente de Prueba

Para los efectos del prototipo, se han utilizado los equipos del laboratorio de informática de la Escuela de Ingeniería Informática, los cuales han sido utilizados dentro de las redes de la universidad, con ello la complejidad y la seguridad que pueda existir frente a la implementación de los dispositivos utilizados, es un aspecto a considerar.

Además algunas pruebas han sido realizadas dentro de la universidad, como otras fuera de estas, con el fin de dilucidar las respuestas tanto de los mecanismos de seguridad, como así también la calidad de servicio entregada por el servidor hacia fuera de la universidad.

9.2.2 Pruebas Preliminares

Los resultados que se muestran a continuación están en relación al rendimiento que pueda tener la transmisión de video streaming, antes de la aplicación de los mecanismos de cifrado, como después de su aplicación.

El siguiente gráfico muestra el rendimiento de video streaming antes de aplicar mecanismos de seguridad, a través de una red privada virtual (VPN) implementada.

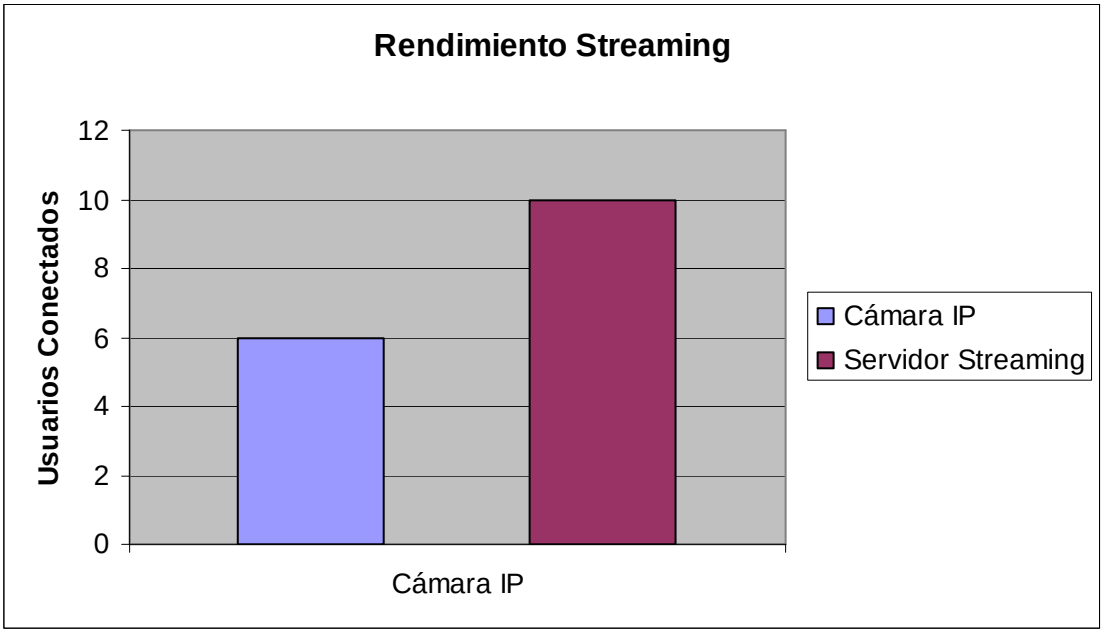

Figura 149 – Gráfico Rendimiento Streaming con VPN.

Este gráfico, evidencia el rendimiento del video streaming, visualizado en forma remota por cualquier usuario en particular. El gráfico representa, el rendimiento de una cámara IP, en contraposición de un servidor streaming. Primero, la representación de la cámara IP, da a conocer que de 10 conexiones realizadas hacia la cámara IP, o en otras palabras, que si 10 personas se conectan simultáneamente a la cámara ip evidenciarán, desde el sexto en adelante, un retardo o pérdida de calidad de servicio o de la visualización de video streaming.

Desde otra perspectiva, el servidor streaming, evidencia un mejor rendimiento debido a muchos factores, como lo es su mayor nivel de procesamiento de datos en comparación con una cámara IP, entre otros. Por ello que de 10 conexiones o usuarios conectados a la visualización del contenido multimedia, las 10 conexiones o usuarios, obtuvieron una buena calidad de servicio, es decir, visualizaron el video sin retardo o perdida de calidad de imagen.

El siguiente gráfico muestra el rendimiento de video streaming antes de aplicar mecanismos de seguridad, en una red de área local (LAN).

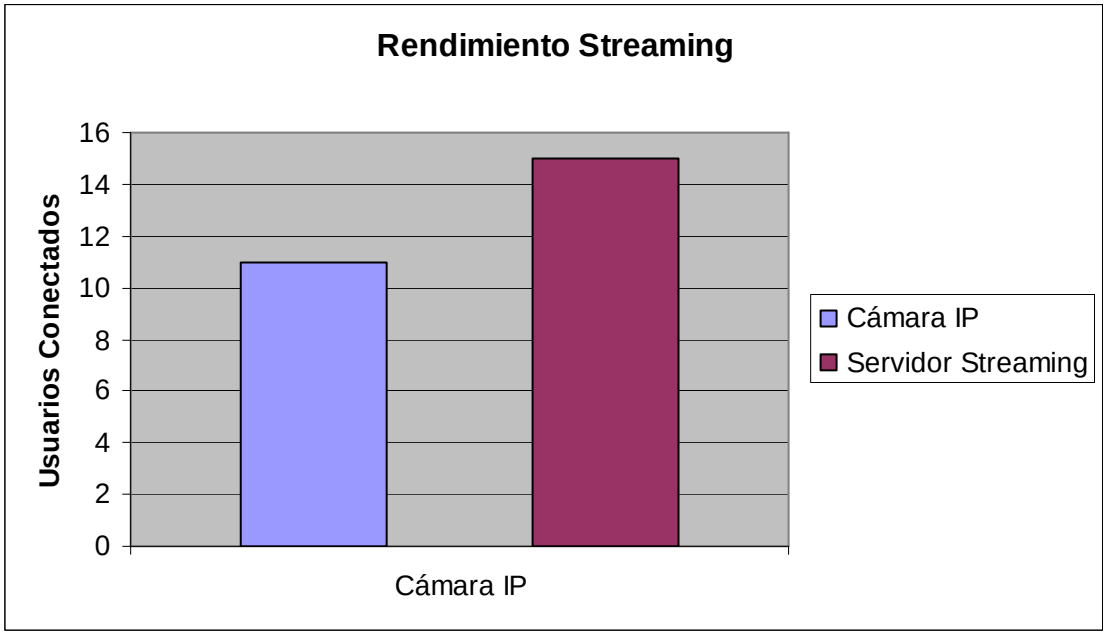

Figura 150 – Gráfico Rendimiento Streaming sin VPN.

Este gráfico, evidencia el rendimiento del video streaming, visualizado en forma local por cualquier usuario en particular. El gráfico representa, el rendimiento de una cámara IP, en contraposición de un servidor streaming. Primero, la representación de la cámara IP, da a conocer que de 15 conexiones realizadas hacia la cámara ip, o en otras palabras, que si 15 personas se conectan simultáneamente a la cámara IP evidenciarán, desde la conexión número 11 en adelante, un retardo o pérdida de calidad de servicio o de la visualización de video streaming.

Desde otra perspectiva, el servidor streaming, evidencia un mejor rendimiento debido a muchos factores, como lo es su mayor nivel de procesamiento de datos en comparación con una cámara IP, entre otros. Por ello que de 15 conexiones o usuarios conectados a la visualización del contenido multimedia, las 15 conexiones o usuarios, obtuvieron una buena calidad de servicio, es decir, visualizaron el video sin retardo o perdida de calidad de imagen.

Es evidente que no solo el rendimiento del servidor o las cámaras IP darán los resultados antes expuestos, factores como ancho de banda, enrutadores y velocidad de transmisión de datos, serán aspectos importantes y decidores en esta investigación.

A continuación se muestra una serie de pruebas realizadas a través de la utilización de herramientas de medición de tráfico con el fin de demostrar a nivel de transmisión de datos, el comportamiento y los tiempos de respuesta del prototipo.

9.2.3 Prueba de Ejecución Servidores Streaming Windows y Linux

Los siguientes gráficos muestran el comportamiento del tráfico, tanto desde el punto de vista de1 cliente, como desde el servidor de streaming. Por ello que el ambiente de pruebas se ha realizado en el prototipo, el cual está situado en la Escuela de Ingeniería Informática, por medio del acceso de 1 a 5 clientes en forma concurrente.

Estas pruebas consideran 4 aspectos fundamentales en el tráfico y envío de datos a través del prototipo, las cuales son: Tiempo de transmisión entre un dato enviado y otro, rango de pixeles por tick, tipo de unidad y escala.

A continuación se muestran 5 pruebas realizadas al prototipo con sus respectivos resultados representados por gráficos.

Tabla 27– Prueba con 1 Usuario.

Ítem	Descripción
N° Usuarios	1
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Paquete
Rango	100

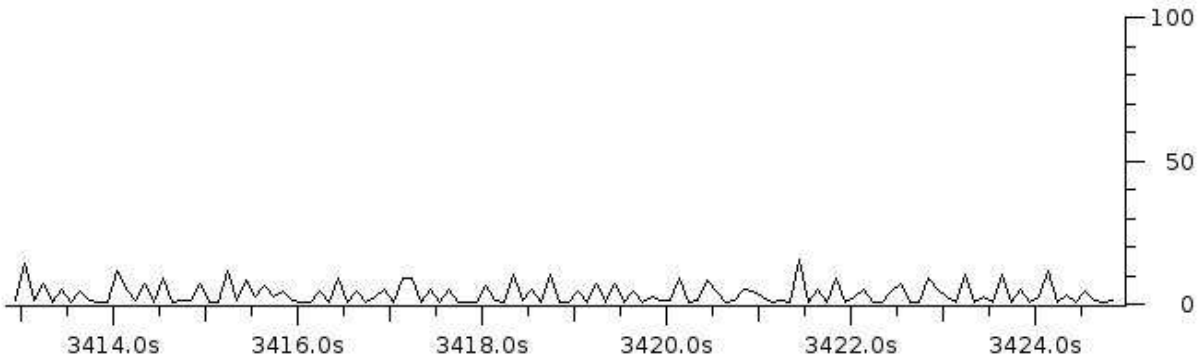

Figura 151 – Gráfico Rendimiento Streaming Servidor 1 Usuario.

Tabla 28– Prueba con 1 Usuario.

Ítem	Descripción
N° Usuarios	1
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bytes
Rango	200000

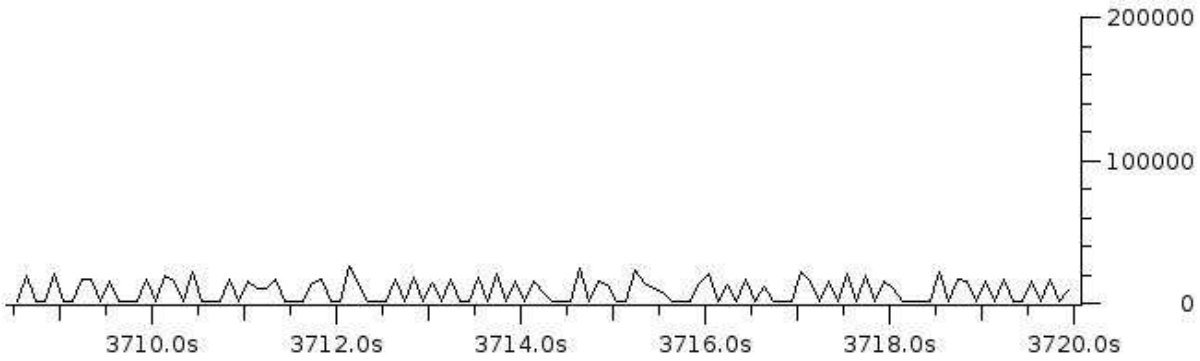

Figura 152 –Gráfico Rendimiento Streaming Servidor 1 Usuario.

Tabla 29– Prueba con 2 Usuario.

Ítem	Descripción
N° Usuarios	2
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Paquete
Rango	100

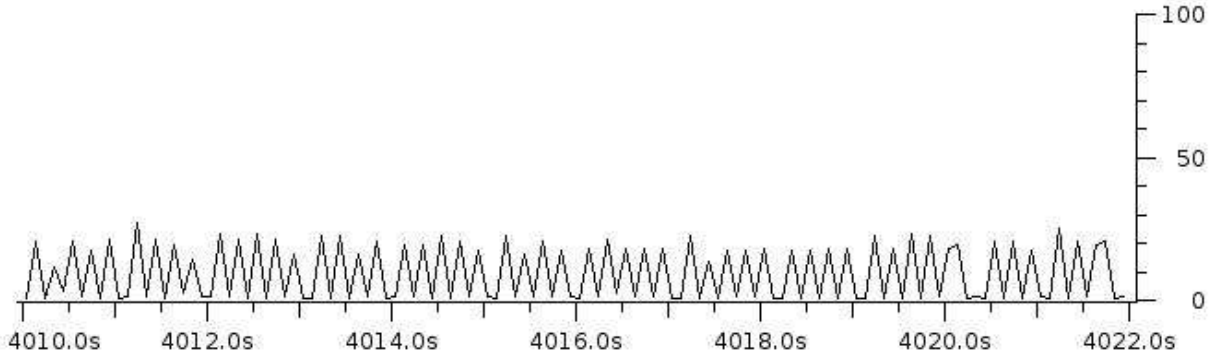

Figura 153 –Gráfico Rendimiento Streaming Servidor con 2 Usuarios.

Tabla 30– Prueba con 2 Usuarios.

Ítem	Descripción
N° Usuarios	2
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bytes
Rango	200000

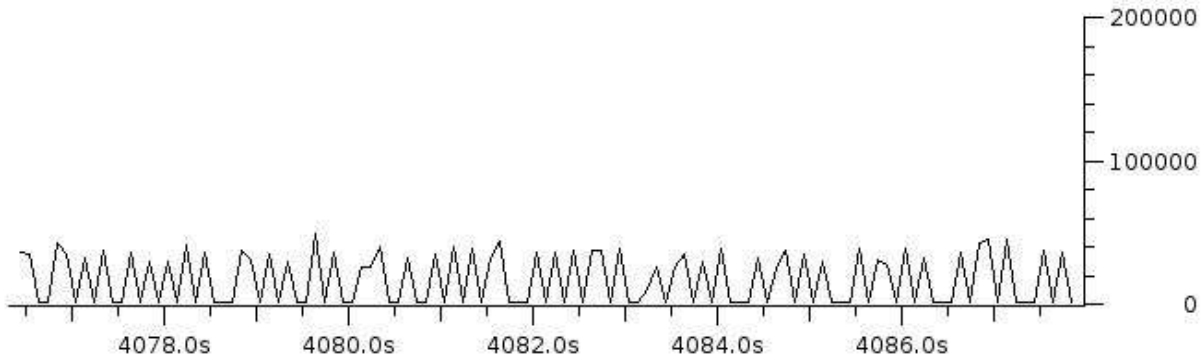

Figura 154 –Gráfico Rendimiento Streaming Servidor con 2 Usuarios.

Tabla 31– Prueba con 3 Usuario.

Ítem	Descripción
N° Usuarios	3
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Paquete
Rango	100

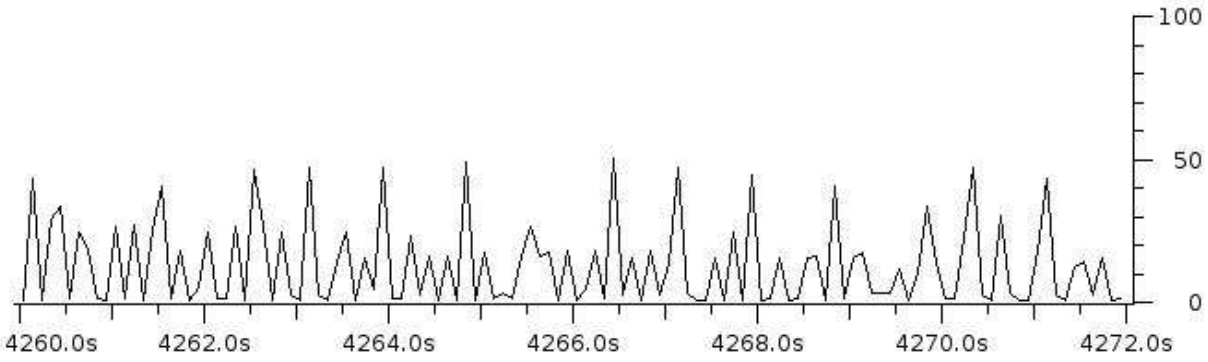

Figura 155 –Gráfico Rendimiento Streaming Servidor con 3 Usuarios.

Tabla 32– Prueba con 3 Usuarios.

Ítem	Descripción
N° Usuarios	3
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bytes
Rango	200000

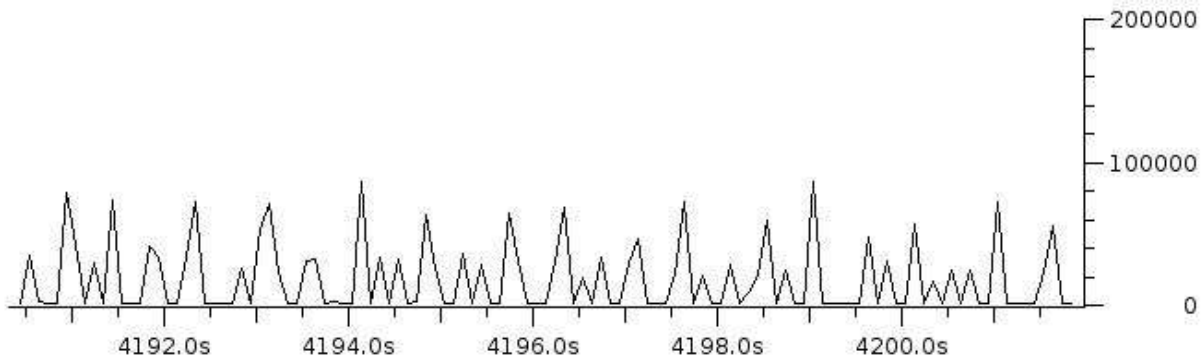

Figura 156–Gráfico Rendimiento Streaming Servidor con 3 Usuarios.

Tabla 33– Prueba con 4 Usuario.

Ítem	Descripción
N° Usuarios	4
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Paquete
Rango	100

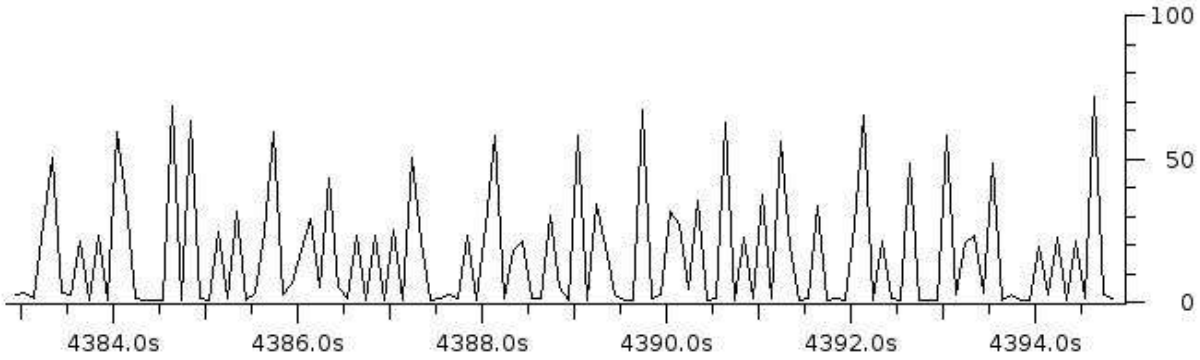

Figura 157–Gráfico Rendimiento Streaming Servidor con 4 Usuarios.

Tabla 34– Prueba con 4 Usuarios.

Ítem	Descripción
N° Usuarios	4
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bytes
Rango	200000

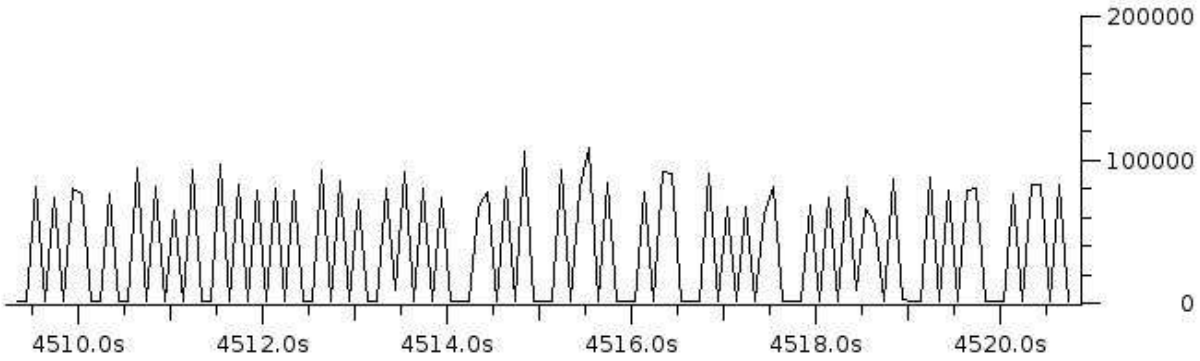

Figura 158–Gráfico Rendimiento Streaming Servidor con 4 Usuarios.

Tabla 35– Prueba con 5 Usuario.

Ítem	Descripción
N° Usuarios	5
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Paquete
Rango	100

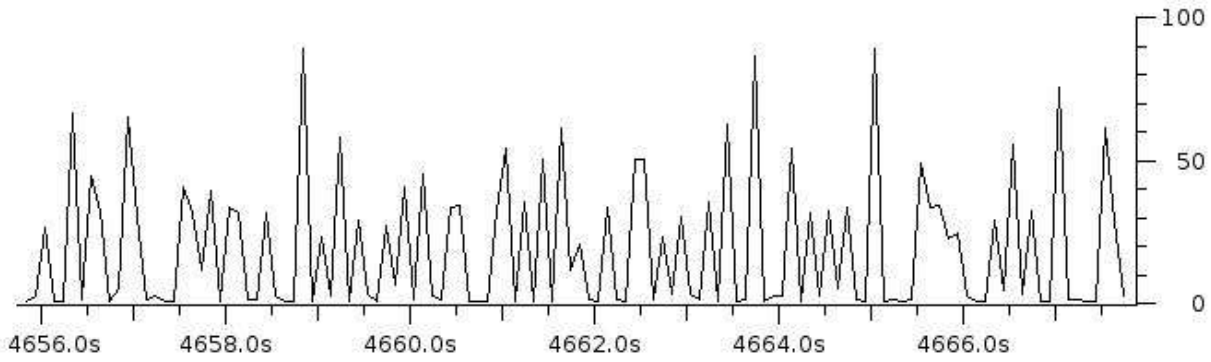

Figura 159–Gráfico Rendimiento Streaming Servidor con 5 Usuarios.

Tabla 36– Prueba con 5 Usuarios.

Ítem	Descripción
N° Usuarios	5
Intervalo de Tiempo	0.1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bytes
Rango	200000

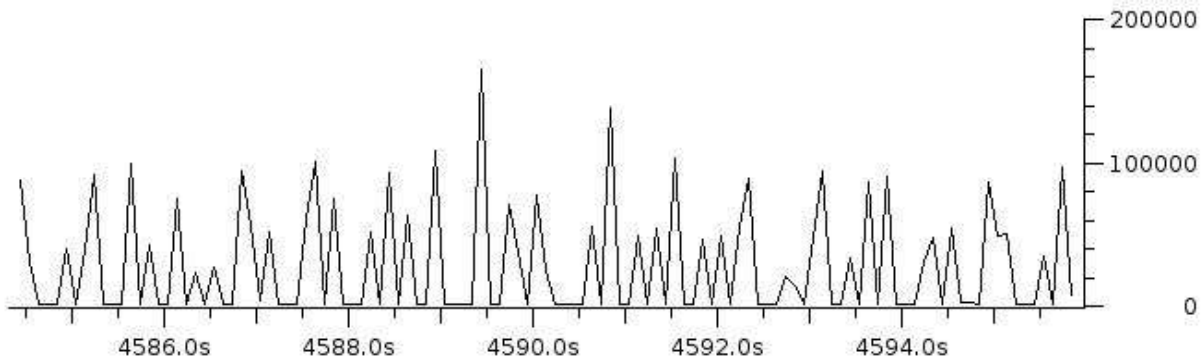

Figura 160–Gráfico Rendimiento Streaming Servidor con 5 Usuarios.

Como se puede apreciar en los gráficos a medida que los usuarios se van conectando, al servidor streaming para poder visualizar el contenido multimedia, el servidor va subiendo su tasa de datos enviados en forma mesurada y no en forma explosiva, ya que a través de los aspectos de calidad de servicio utilizados antes mencionados, el servidor maneja tanto la carga de entrada como de salida.

Se ha medido dos tipos de flujo a diferentes escalas cada uno, un flujo medido en bytes y el otro en número de paquetes que han sido enviados, con ello se evidencia que tráfico en pos de las solicitudes de visualización de video streaming.

Además, es más que claro que cada vez que se sume un usuario más a la visualización de streaming, es que aumentan tanto los paquetes transmitidos como el número de bytes enviados.

Tabla 37– Prueba con 15 Usuarios.

Ítem	Descripción
N° Usuarios	15
Intervalo de Tiempo	1 segundo
Pixeles por Tick	5
Tipo de transmisión	Paquete
Rango	2000

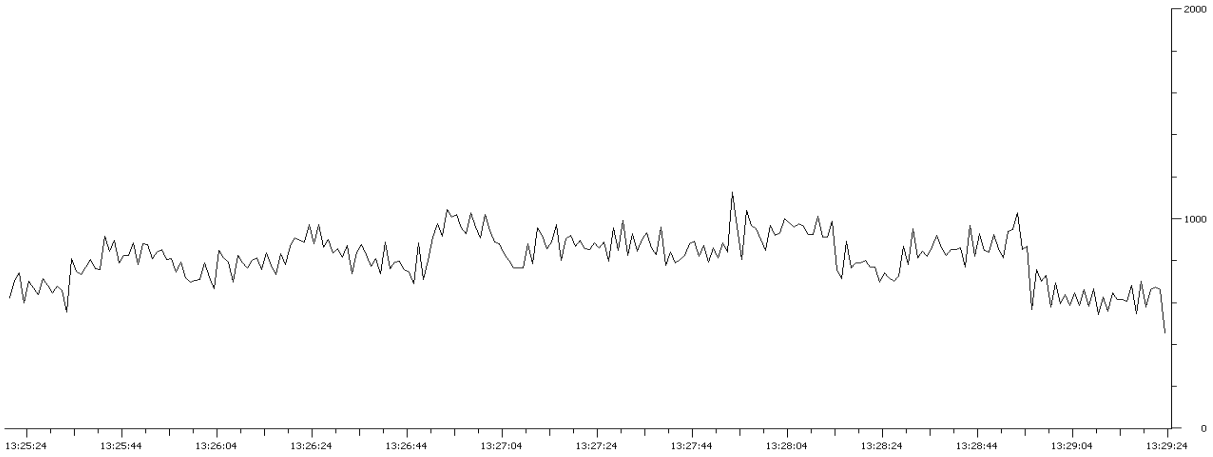

Figura 161–Gráfico Rendimiento Streaming Servidor Linux con 15 Usuarios.

Tabla 38 – Prueba con 15 Usuarios.

Ítem	Descripción
N° Usuarios	15
Intervalo de Tiempo	1 segundo
Pixeles por Tick	5
Tipo de transmisión	Byte
Rango	2000000

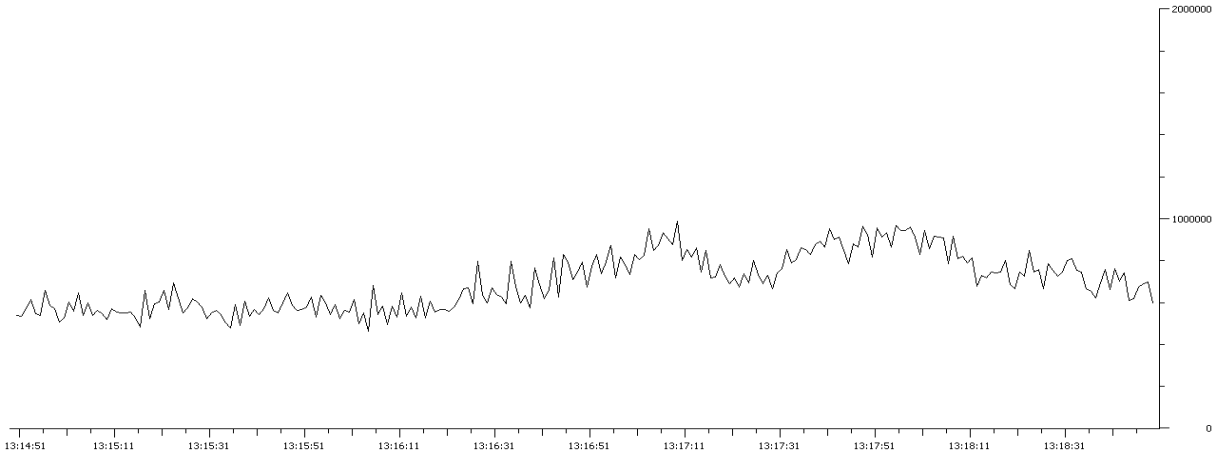

Figura 162 – Gráfico Rendimiento Streaming Servidor Linux con 15 Usuarios.

Tabla 39 – Prueba con 15 Usuarios.

Ítem	Descripción
N° Usuarios	15
Intervalo de Tiempo	1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bits
Rango	10000000

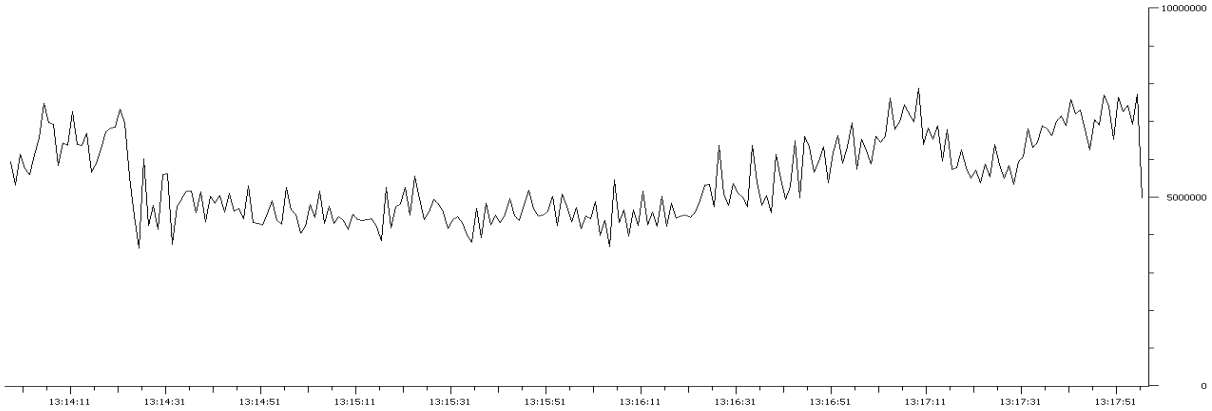

Figura 163 – Gráfico Rendimiento Streaming Servidor Linux con 15 Usuarios.

Tabla 40 – Prueba con 15 Usuarios.

Ítem	Descripción
N° Usuarios	15
Intervalo de Tiempo	1 segundo
Pixeles por Tick	5
Tipo de transmisión	Paquetes
Rango	2000

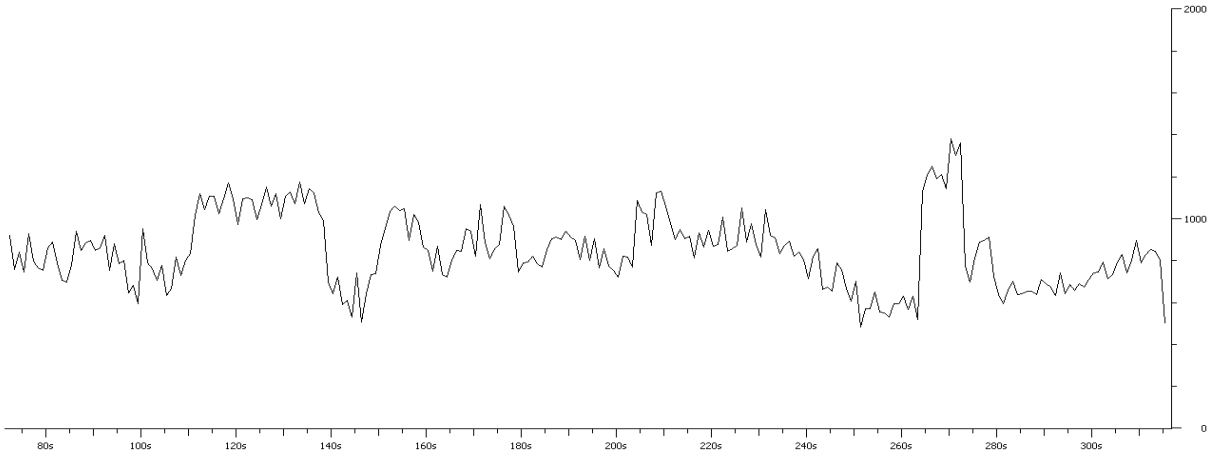

Figura 164–Gráfico Rendimiento Streaming Servidor Windows con 15 Usuarios.

Tabla 41– Prueba con 15 Usuarios.

Ítem	Descripción
N° Usuarios	15
Intervalo de Tiempo	1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bytes
Rango	2000000

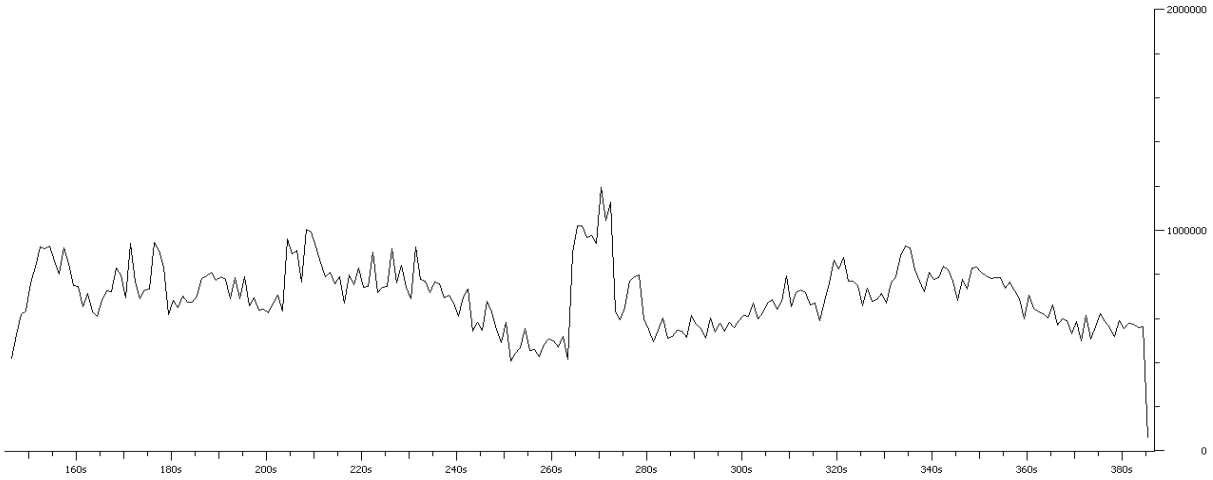

Figura 165–Gráfico Rendimiento Streaming Servidor Windows con 15 Usuarios.

Tabla 42 – Prueba con 15 Usuarios.

Ítem	Descripción
N° Usuarios	15
Intervalo de Tiempo	1 segundo
Pixeles por Tick	5
Tipo de transmisión	Bits
Rango	10000000

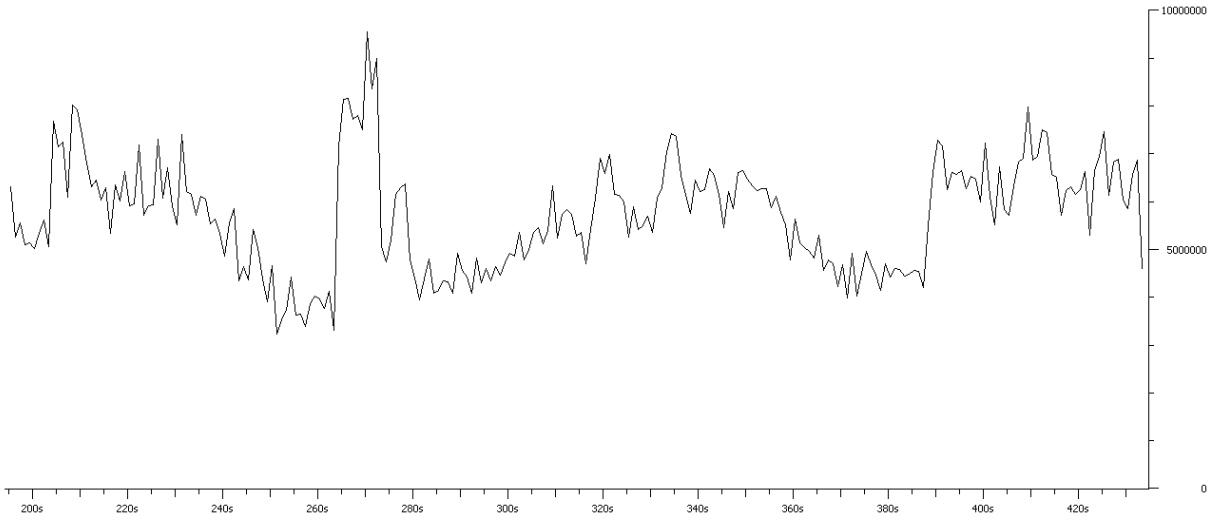

Figura 166 –Gráfico Rendimiento Streaming Servidor Windows con 15 Usuarios.

Es posible apreciar en las figuras antes presentadas, que la comparación entre los 2 tipos de servidores, tanto Windows como Linux, demuestran que la estabilidad y rendimiento de un servidor Linux, es relativamente mejor y estable respecto a la utilización de servidores Windows. Se evidencia una estabilidad y fluidez, que al transmitir video streaming desde los sistemas de tele vigilancia, el usuario es capaz de visualizar una fluidez del contenido visualizado. Los gráficos muestran una comparativa entre ambos SO, considerando tres criterios de medición: Bytes, Bits y Paquetes de datos, cuyos resultados se evidencian en la figuras antes visualizadas.

9.2.4 Pruebas Servidor PfSense

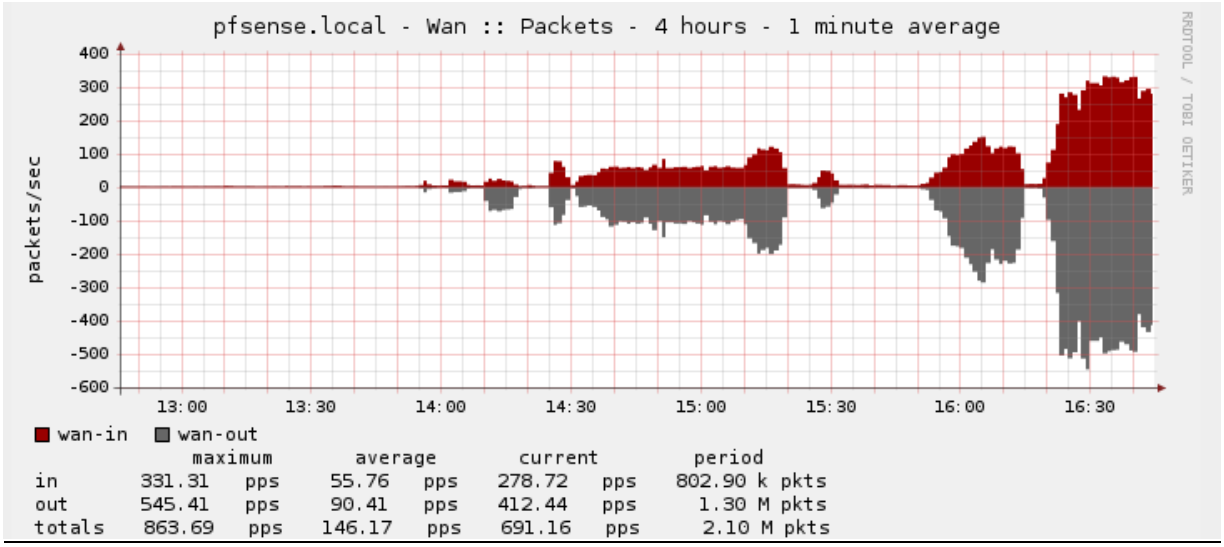

Figura 167 – Gráfico Rendimiento Paquetes Streaming Servidor Linux con 15 Usuarios.

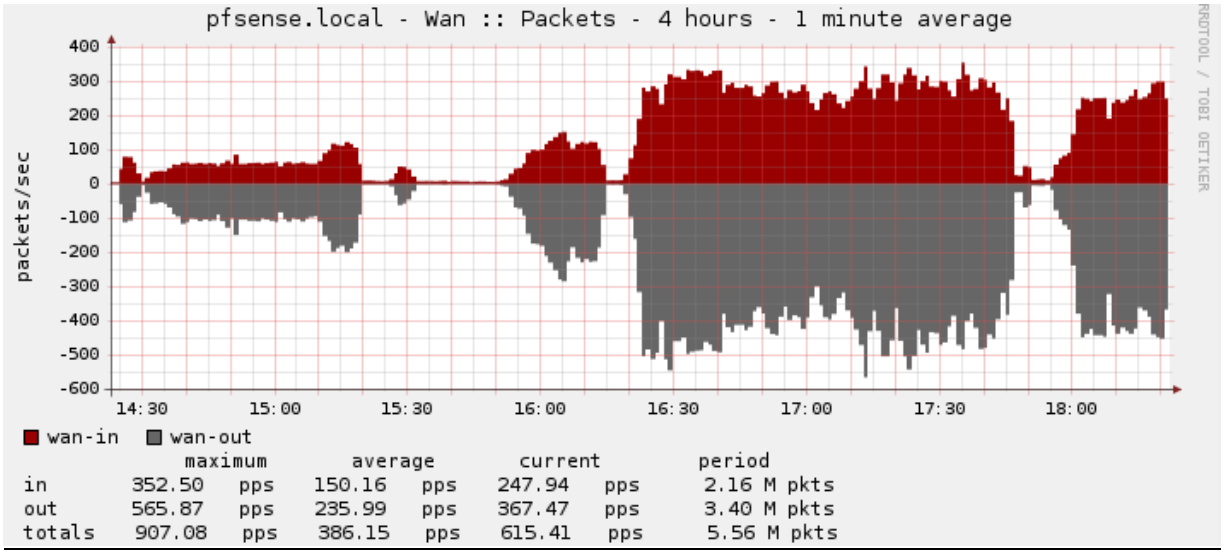

Figura 168–Gráfico Rendimiento Paquetes Streaming Servidor Windows con 15 Usuarios.

Como se aprecian en las dos figuras anteriores, existe una comparativa entre los dos sistema operativos, y una vez más comprueban que la utilización de un servidor streaming Linux es más óptimo en la transmisión de paquetes que un servidor Windows.

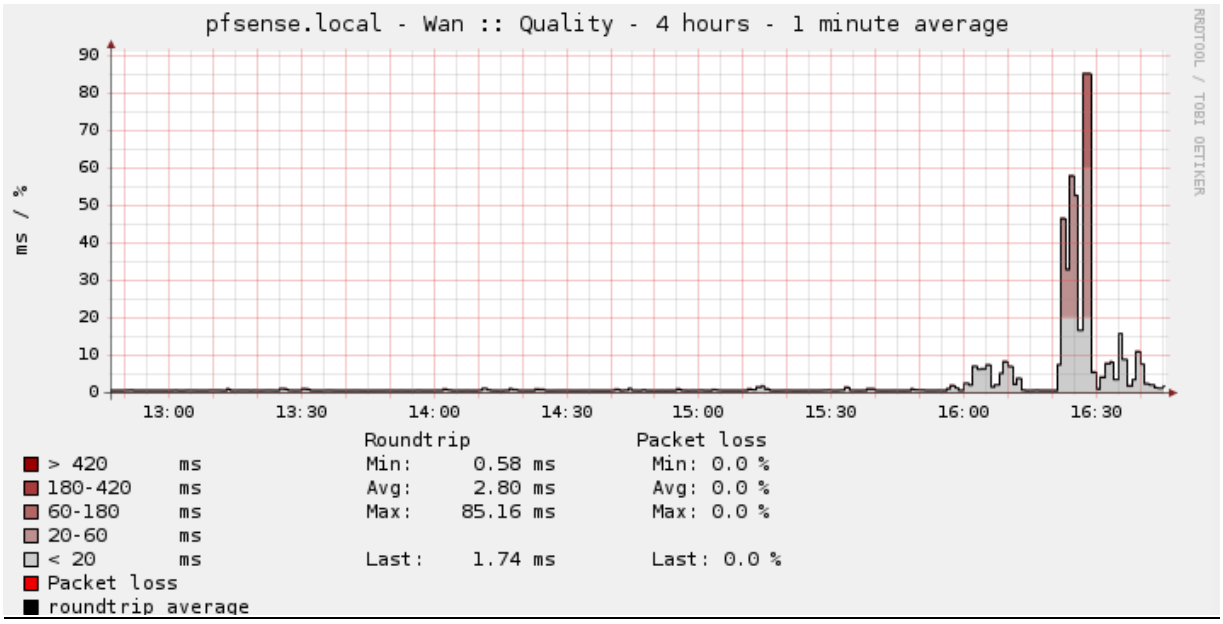

Figura 169–Gráfico Rendimiento Calidad Streaming Servidor Windows con 15 Usuarios.

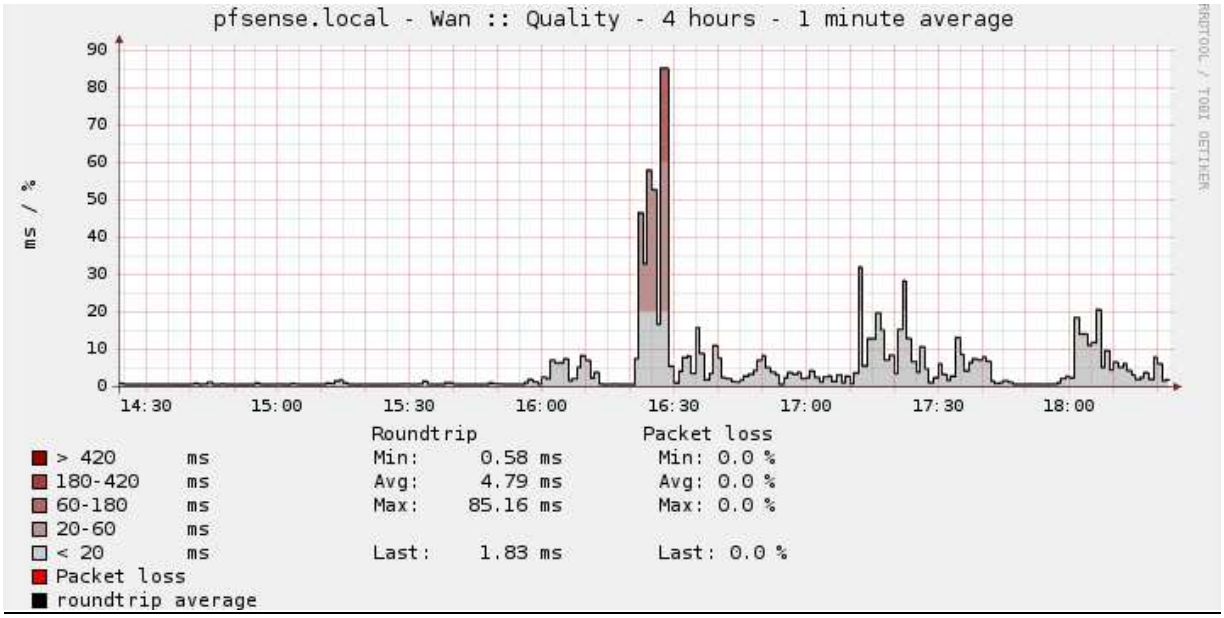

Figura 170–Gráfico Rendimiento Calidad Streaming Servidor Linux con 15 Usuarios.

Nuevamente las dos figuras anteriores evidencian el comportamiento de ambos servidores, en la transmisión del video streaming, proveniente de las cámaras de tele vigilancia, explicitando la diferencia entre ambos servicios, y corroborando que Windows es menos eficiente desde el punto de vista de calidad frente a Linux.

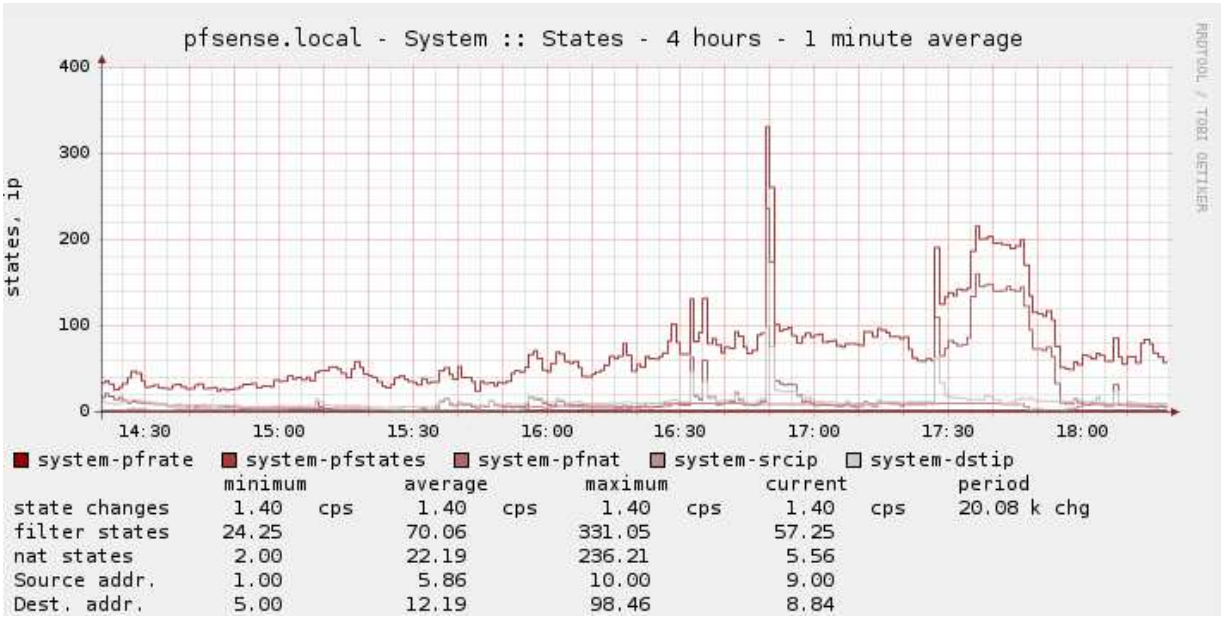

Figura 171–Gráfico Rendimiento Sistema Servidor PfSense con 15 Usuarios.

La imagen anterior muestra el rendimiento del servidor PfSense a nivel de sistema, una vez que se realiza cada una de las conexiones hacia el servidor PfSense, tanto para realizar la VPN, como luego realizar la transmisión streaming.

Es lógico que a medida que el servidor va obteniendo más peticiones, este aumente su nivel de procesamiento de sistema, por ende una mayor utilización de los recursos, y tal vez a gran escala una perdida de funcionamiento.

A mayor número de usuarios conectados y luego transmitiendo video, el servidor aumenta su utilización de procesamiento, luego baja este rendimiento hasta una estabilización que el servidor provee, para así mantener una buena disponibilidad y estabilidad de los servicios. Estas pruebas se realizaron en ambos sistemas operativos, transmitiendo video streaming desde la cámara de tele vigilancia.

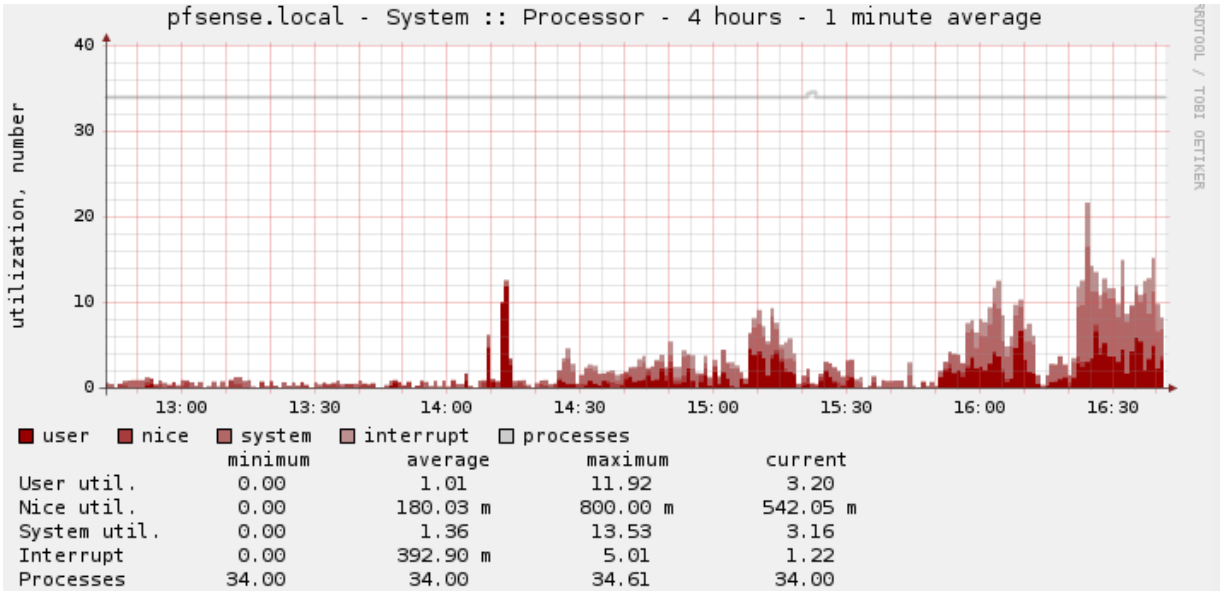

Figura 172–Gráfico Rendimiento Procesos Servidor PfSense con 15 Usuarios.

La figura muestra el procesamiento del servidor PfSense, dando como resultado un funcionamiento estable y fiable, pudiendo realizar las distintas conexiones VPN y luego transmitir el contenido de las cámaras de tele vigilancia. Se mantiene un nivel de procesamiento estable, subiendo cada vez que se realiza una nueva conexión pero luego estabilizándose y previendo una conexión estable y segura.

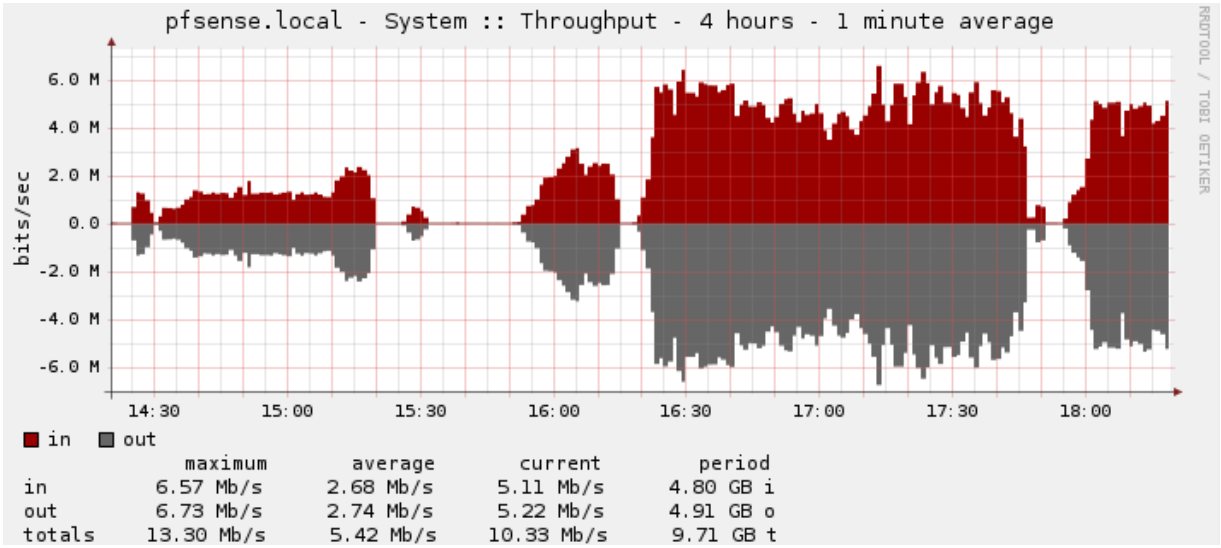

Figura 173–Gráfico Rendimiento Salida Servidor Pfsense con 15 Usuarios.

Como se puede apreciar en la figura, de 14:30 a 16:00 horas aproximadamente, se realizaron pruebas con servidor Linux, transmitiendo el contenido streaming y realizando la conexión VPN correspondiente, por ello que el rendimiento de salida una vez más con un servidor Windows es mas alto que un servidor Linux, ya que las pruebas que se realizaron en Windows, corresponden entre las 16:30 y 15:30 aproximadamente, con ello manteniendo la tesis, de que Linux tiene un mejor manejo como servidor streaming que Windows en esta investigación.

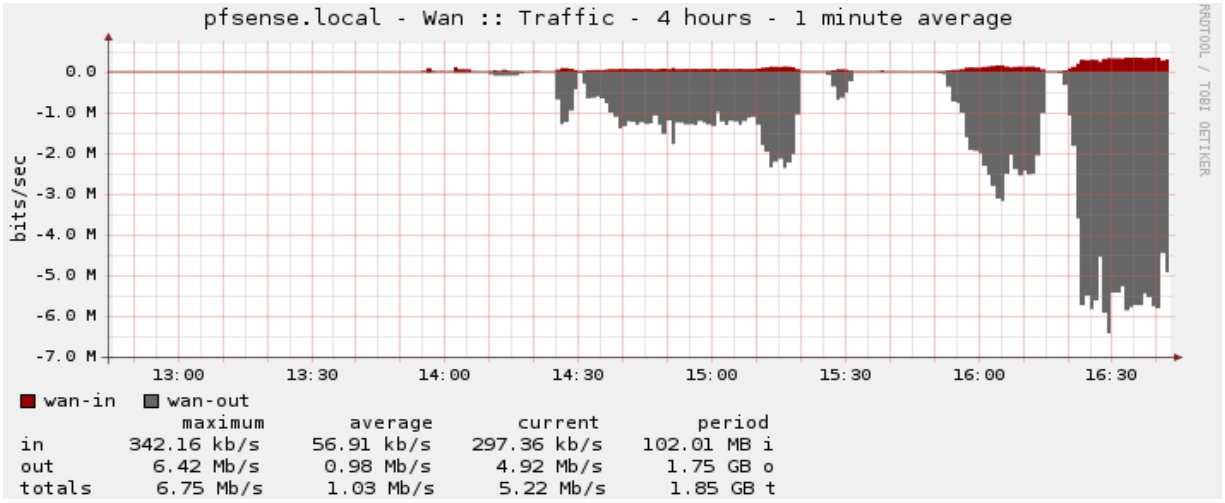

Figura 174–Gráfico Rendimiento Tráfico Streaming Servidor Linux con 15 Usuarios.

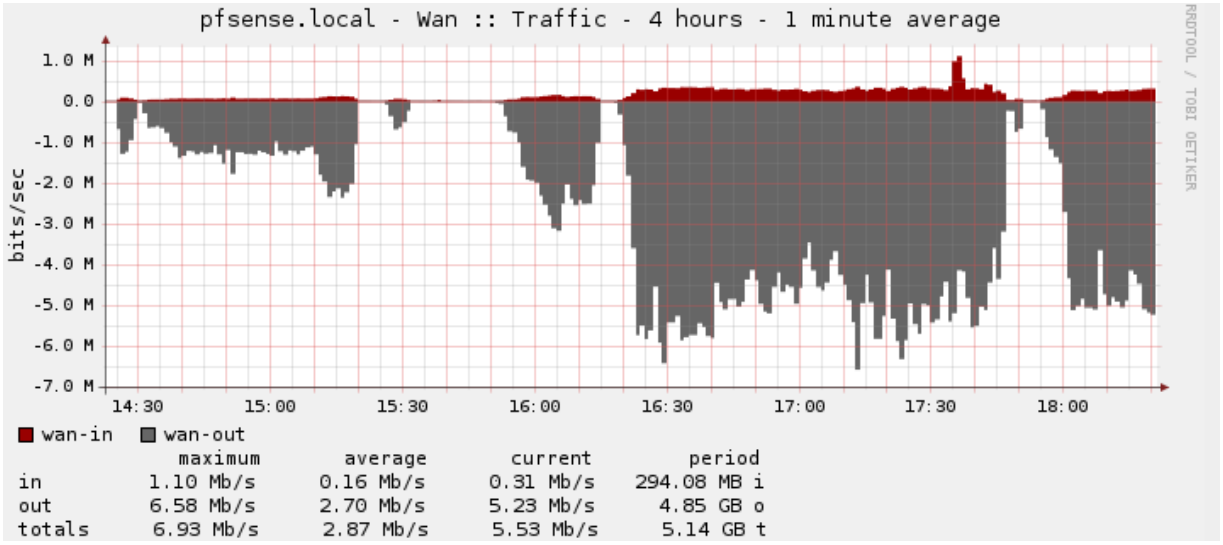

Figura 175–Gráfico Rendimiento Tráfico Streaming Servidor Windos con 15 Usuarios.

Para finalizar, las pruebas efectuadas tanto al servidor PfSense como a los servidores streaming, se aprecia en la figura el rendimiento del tráfico VPN en la red. Para el servidor Linux se hicieron pruebas entre las 14:30 y 15:30 horas. Para el servidor Windows, se realizaron entre las 16:30 y 15:30 aproximadamente, con ello demostrando que el tráfico de un servidor streaming Windows es mayor que Linux.

Para concluir las pruebas efectuadas en estas investigación, evidencian tal como dice la literatura y guías prácticas, que un servicio Windows tiene menos fiabilidad, estabilidad y rendimiento que un servidor Linux.

Además, demostrando que la utilización de VPN y luego transmisión de video streaming en este prototipo, se concluye que es válido el modelo, demostrando que es factible utilizar e implementar mecanismos de seguridad en un sistema de tele vigilancia.

9.2.5 Pruebas Sin Cifrado Servidor PfSense

Se realizaron pruebas de transmisión de video streaming, por ello que a continuación se muestra el efecto en el servidor pfsense, al proveer una comunicación sin ningún mecanismo de seguridad.

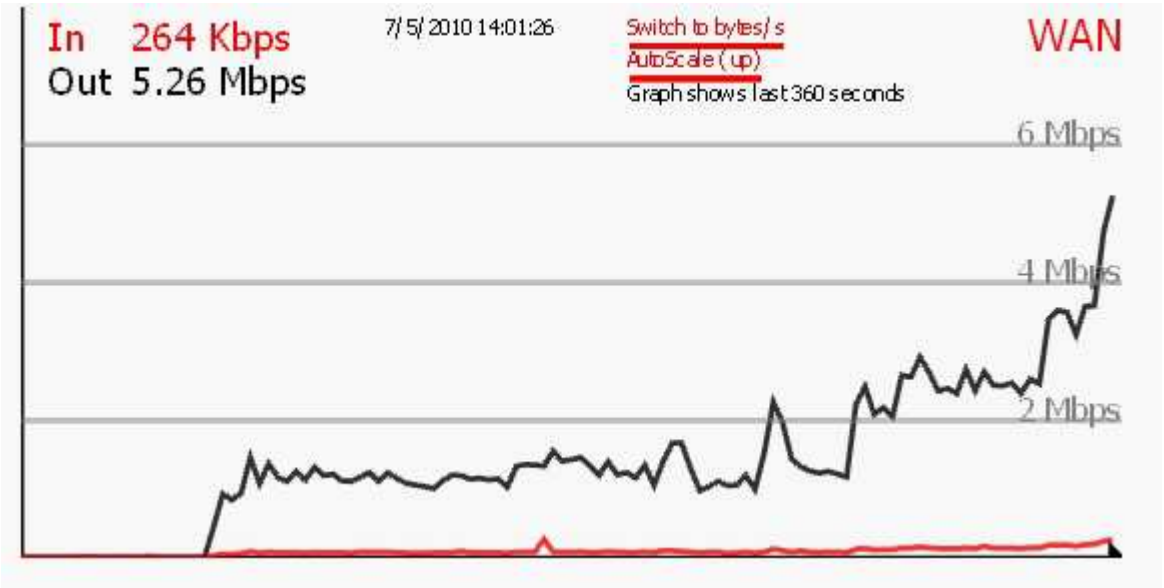

Figura 176–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Sin Cifrado 2 Usuarios.

Estos gráficos muestran la carga en el servidor PfSense, donde muestra la evolución y el rendimiento que va obteniendo el servidor cada vez que se van realizando conexiones y peticiones de streaming. Estas pruebas se realizaron con 2 y 3 usuarios respectivamente.

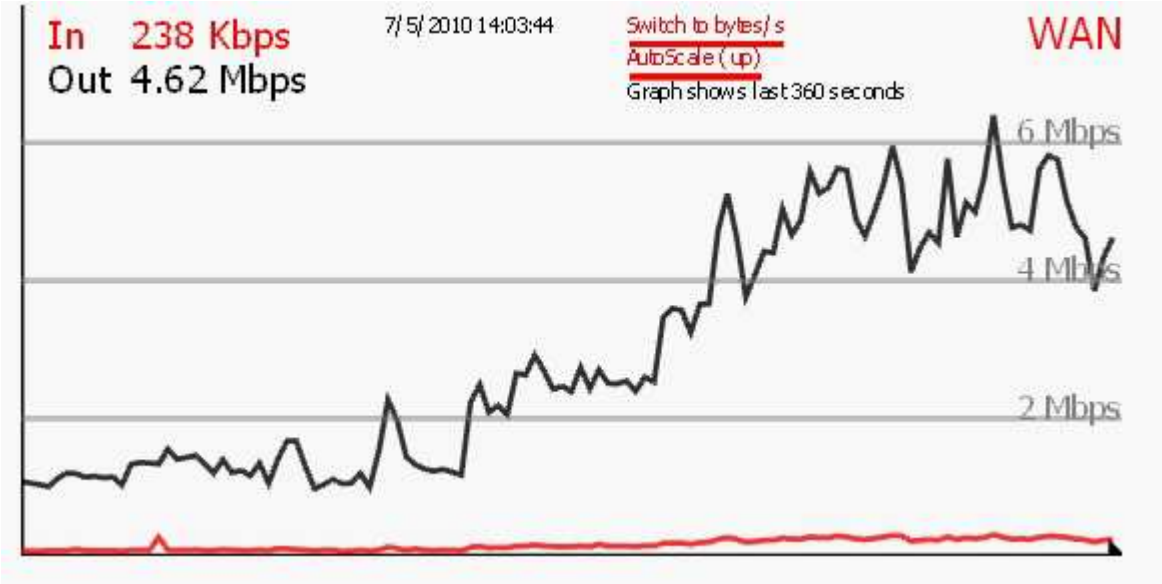

Figura 177–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Sin Cifrado 3 Usuarios.

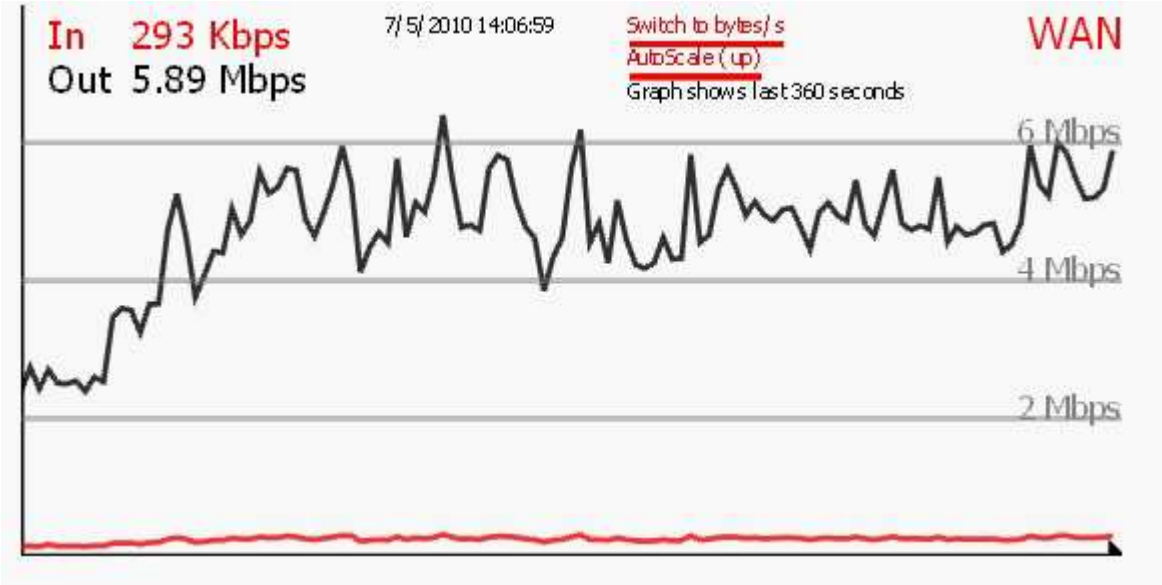

Figura 178–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Sin Cifrado 4 Usuarios.

Estos gráficos muestran la carga en el servidor PfSense, donde muestra la evolución y el rendimiento que va obteniendo el servidor cada vez que se van realizando conexiones y peticiones de streaming. Estas pruebas se realizaron con 4 y 5 usuarios respectivamente.

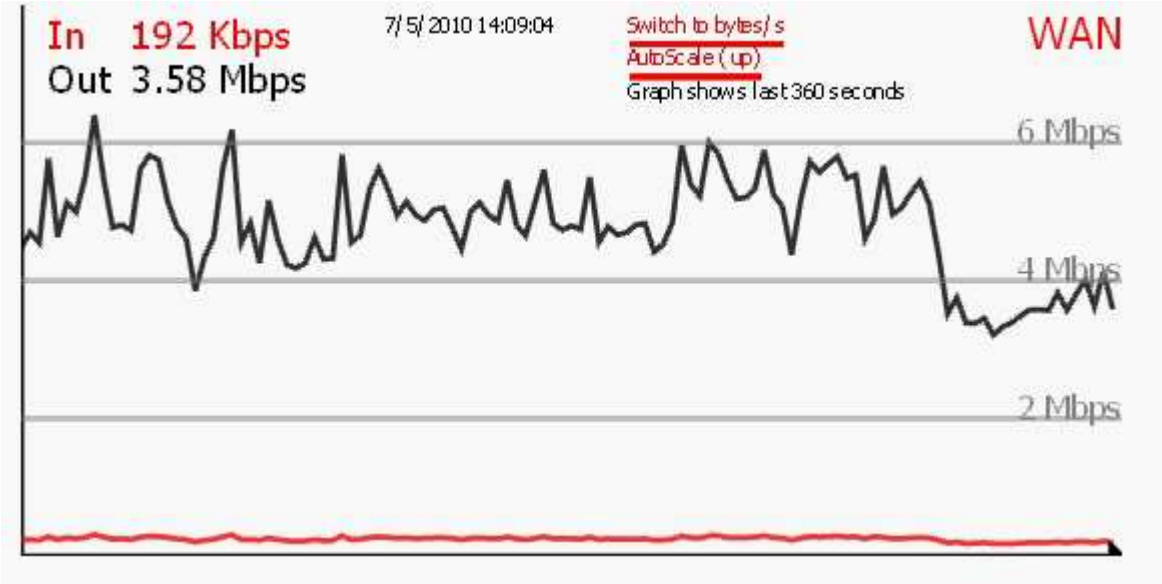

Figura 179–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Sin Cifrado 5 Usuarios.

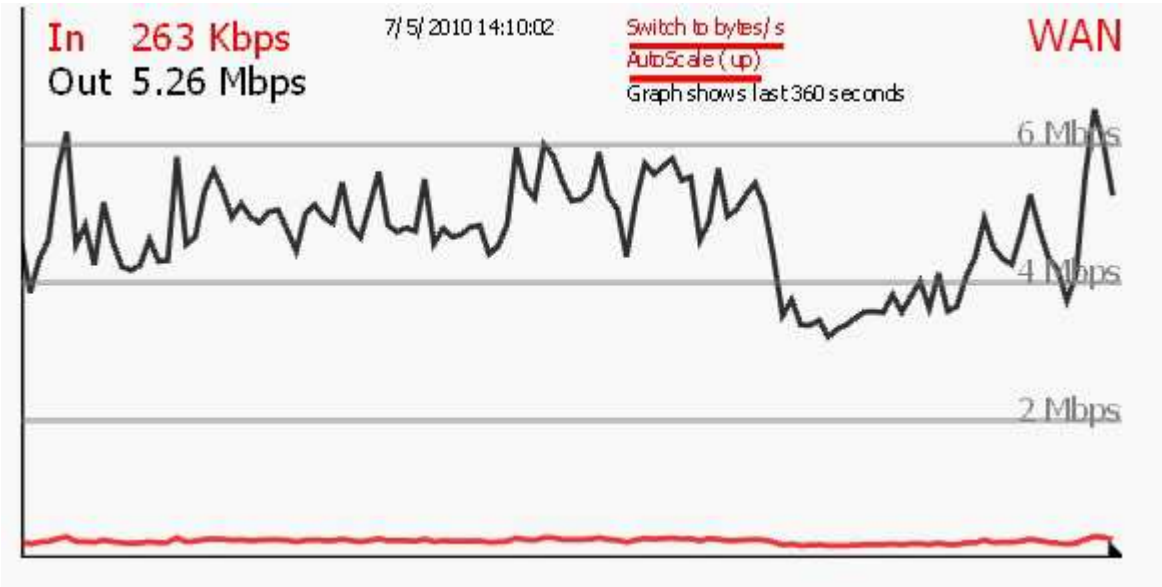

Figura 180–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Sin Cifrado 15 Usuarios.

Estos gráficos muestran la carga en el servidor PfSense, donde muestra la evolución y el rendimiento que va obteniendo el servidor cada vez que se van realizando conexiones y peticiones de streaming. Estas pruebas se realizaron con 15 usuarios respectivamente.

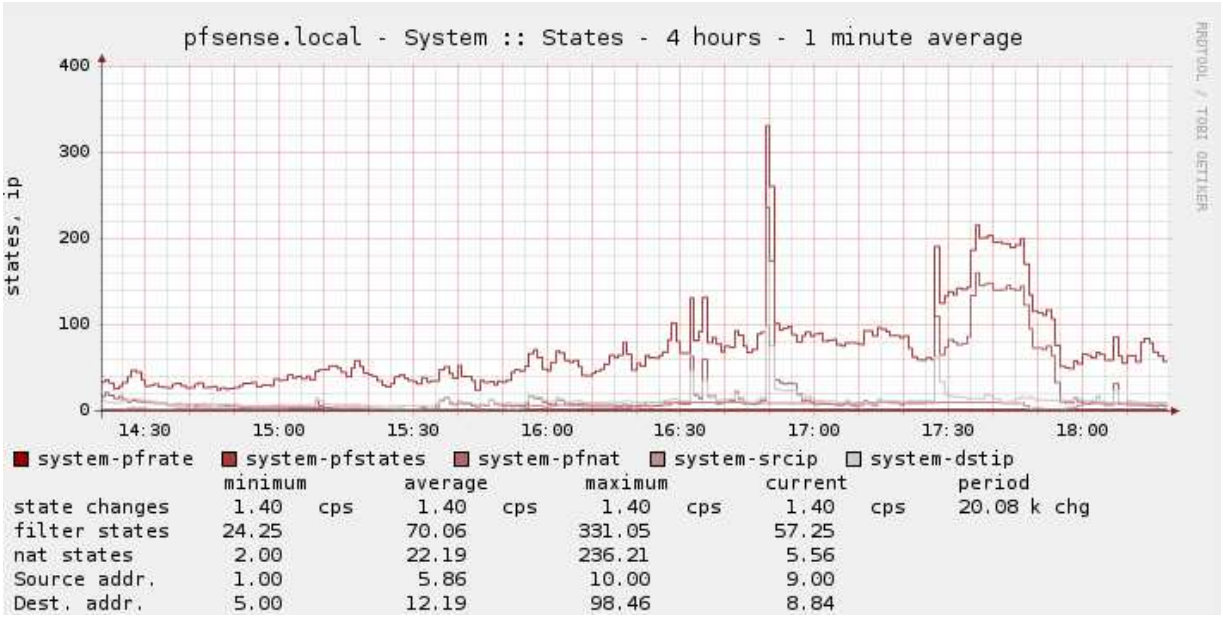

Figura 181– Gráfico Rendimiento Sistema Servidor PfSense Sin Cifrado 15 Usuarios.

Es posible apreciar en los gráficos, que la carga de datos sin cifrado en el servidor PfSense, va aumentando paulatinamente por cada petición o solicitud de video streaming. Esta carga afecta en forma mínima el rendimiento del servidor, en el manejo de paquetes de entrada y salida del servidor. Además es posible apreciar que el aumento en el manejo de ancho de banda es menor frente a la configuración de un servidor utilizando técnicas de seguridad.

Además la imagen anterior muestra el rendimiento del servidor PfSense a nivel de sistema, una vez que se realiza cada una de las conexiones hacia el servidor PfSense, sin aspectos de seguridad, para realizar la transmisión streaming.

Es lógico que a medida que el servidor va obteniendo más peticiones, este aumente su nivel de procesamiento de sistema, por ende una mayor utilización de los recursos, y tal vez a gran escala una perdida de funcionamiento.

A mayor número de usuarios conectados y luego transmitiendo video, el servidor aumenta su utilización de procesamiento, luego baja este rendimiento hasta una estabilización que el servidor provee, para así mantener una buena disponibilidad y estabilidad de los servicios. Estas pruebas se realizaron en ambos sistemas operativos, transmitiendo video streaming desde la cámara de tele vigilancia.

Es posible observar que entre los periodos 14 y 16 horas se muestra el rendimiento medio que provee el servidor PfSense sin cifrado, con ello demostrando la premisa de que al no utilizar medios de seguridad se obtiene un mejor rendimiento, sin embargo, este rendimiento es mínimamente menor al que se observar al utilizar mecanismos de seguridad, el que se encuentra entre las 16 y 18 horas.

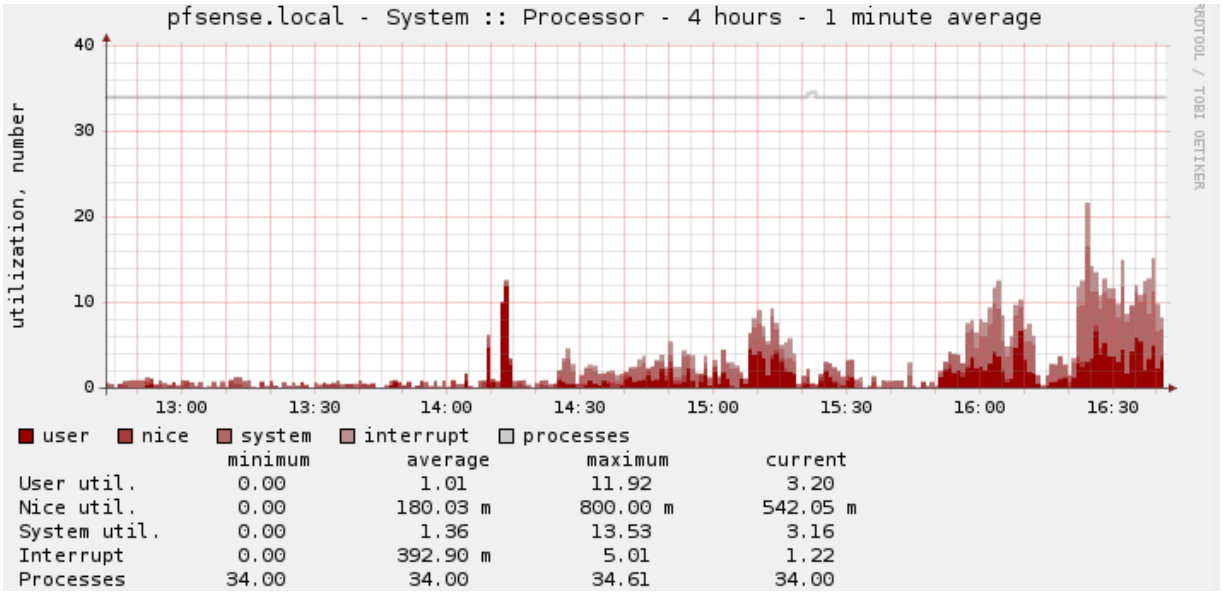

Figura 182– Gráfico Rendimiento Procesos Servidor PfSense Sin Cifrado 15 Usuarios.

La figura muestra el rendimiento del procesador del servidor PfSense, dando como resultado un funcionamiento estable y fiable. Se mantiene un nivel de procesamiento estable, subiendo cada vez que se realiza una nueva conexión, pero luego estabilizándose y previendo una conexión estable y segura. Es posible apreciar que en el rango entre las 14 y 15:30, se aprecia un uso menor en el rendimiento de procesamiento del servidor, con ello una menor carga y uso de recursos.

9.2.6 Pruebas Con Cifrado Servidor PfSense

Se realizaron pruebas de transmisión de video streaming, por ello que a continuación se muestra el efecto en el servidor pfsense, al proveer una comunicación con mecanismos de seguridad.

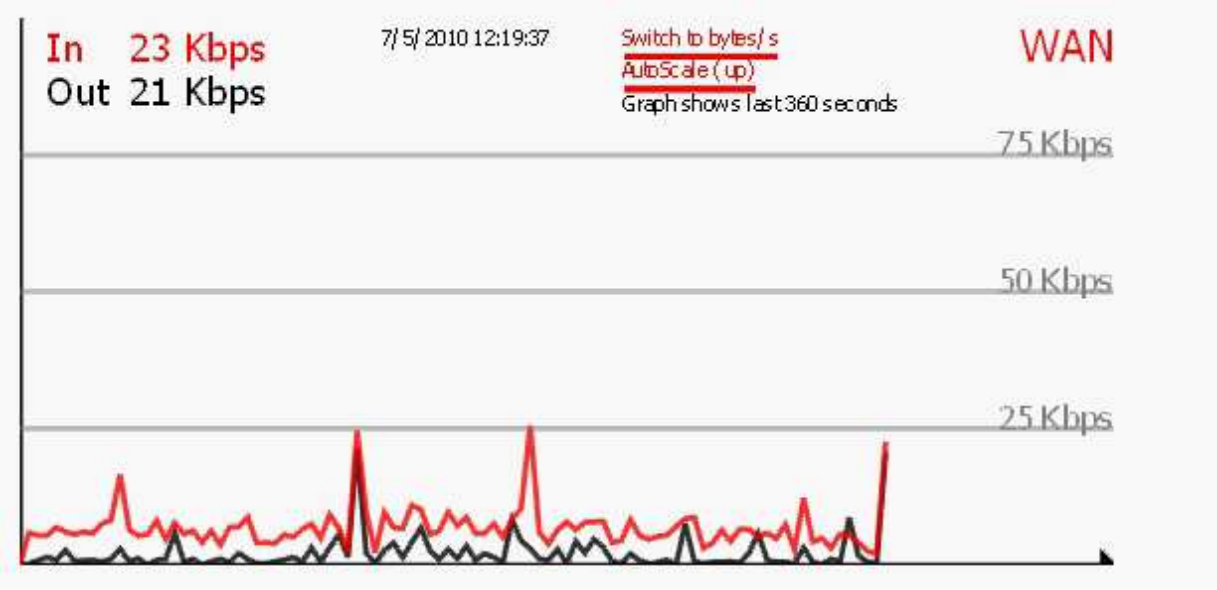

Figura 183–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Con Cifrado 2 Usuarios.

Estos gráficos muestran la carga en el servidor PfSense, donde muestra la evolución y el rendimiento que va obteniendo el servidor cada vez que se van realizando conexiones y peticiones de streaming. Estas pruebas se realizaron con 2 y 3 usuarios respectivamente.

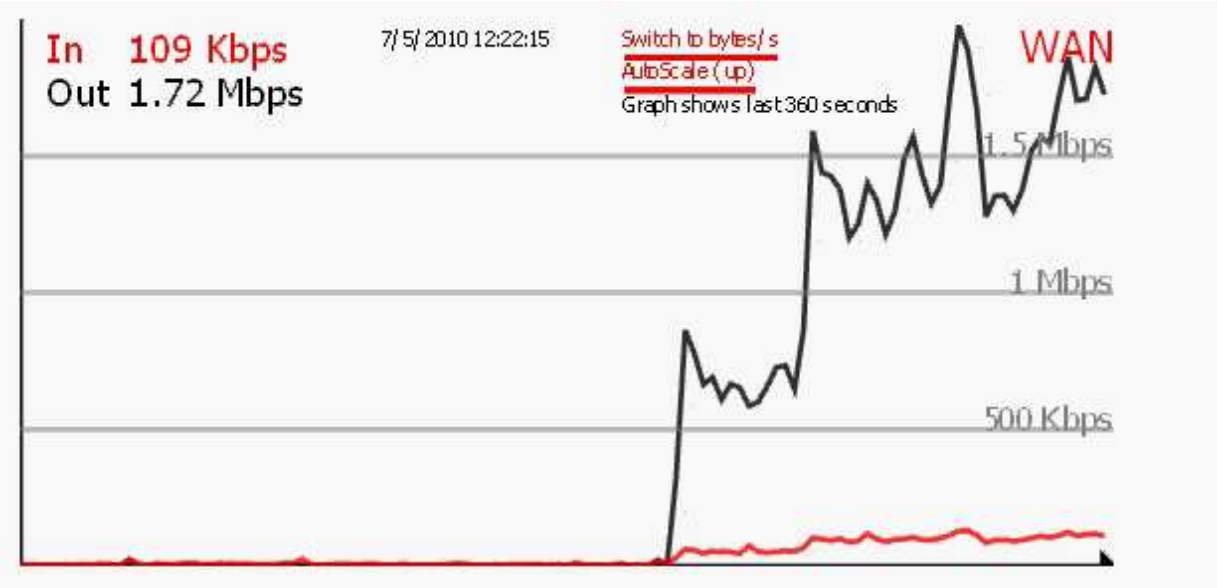

Figura 184–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Con Cifrado 3 Usuarios.

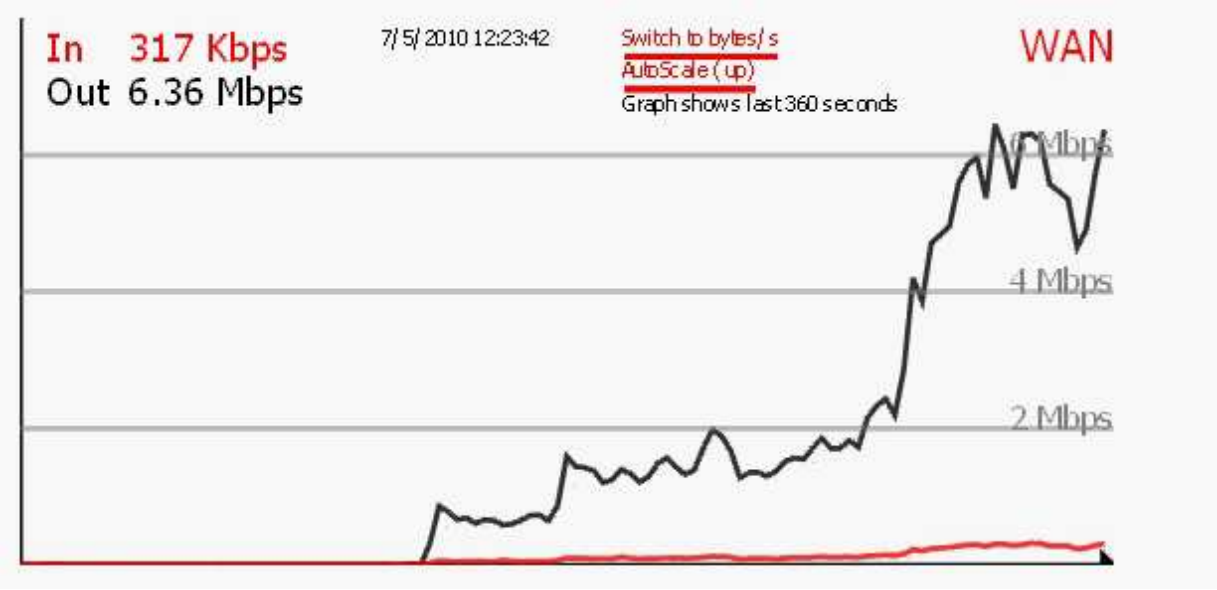

Figura 185–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Con Cifrado 4 Usuarios.

Estos gráficos muestran la carga en el servidor PfSense, donde muestra la evolución y el rendimiento que va obteniendo el servidor cada vez que se van realizando conexiones y peticiones de streaming. Estas pruebas se realizaron con 4 y 5 usuarios respectivamente.

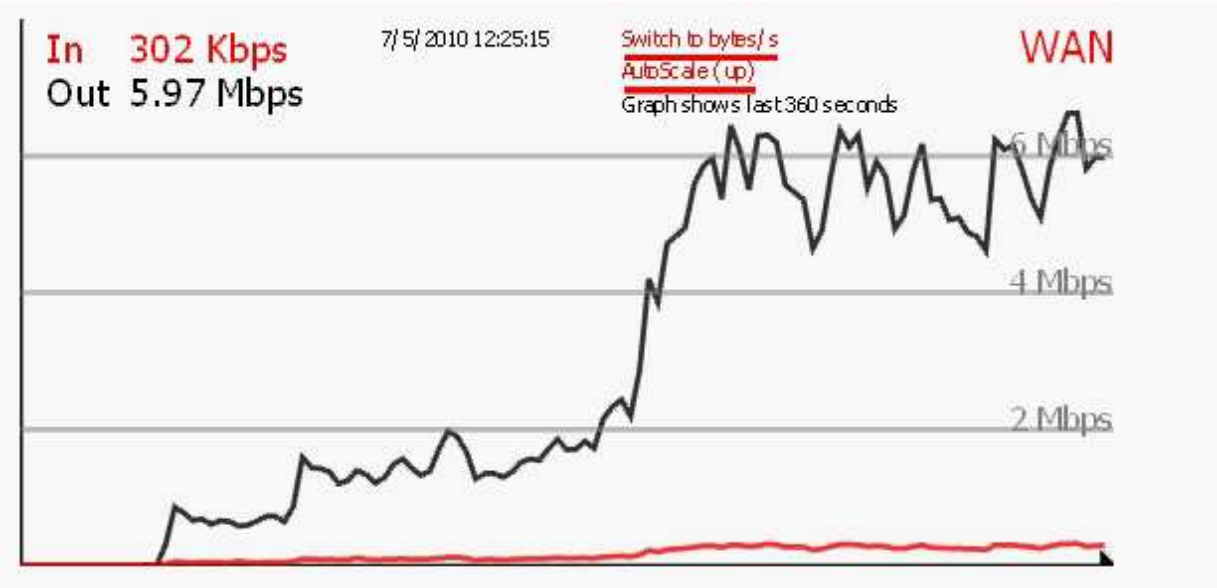

Figura 186–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Con Cifrado 5 Usuarios.

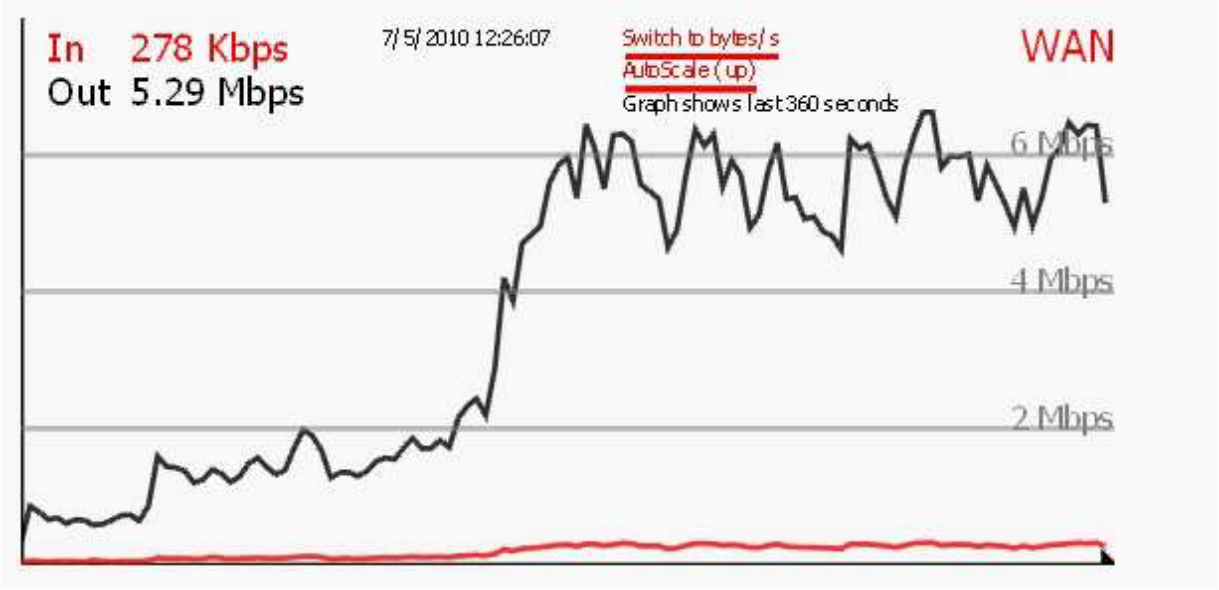

Figura 187–Gráfico Rendimiento Tráfico Streaming Servidor PfSense Con Cifrado 15 Usuarios.

Estos gráficos muestran la carga en el servidor PfSense, donde muestra la evolución y el rendimiento que va obteniendo el servidor cada vez que se van realizando conexiones y peticiones de streaming. Estas pruebas se realizaron con 15 usuarios respectivamente.

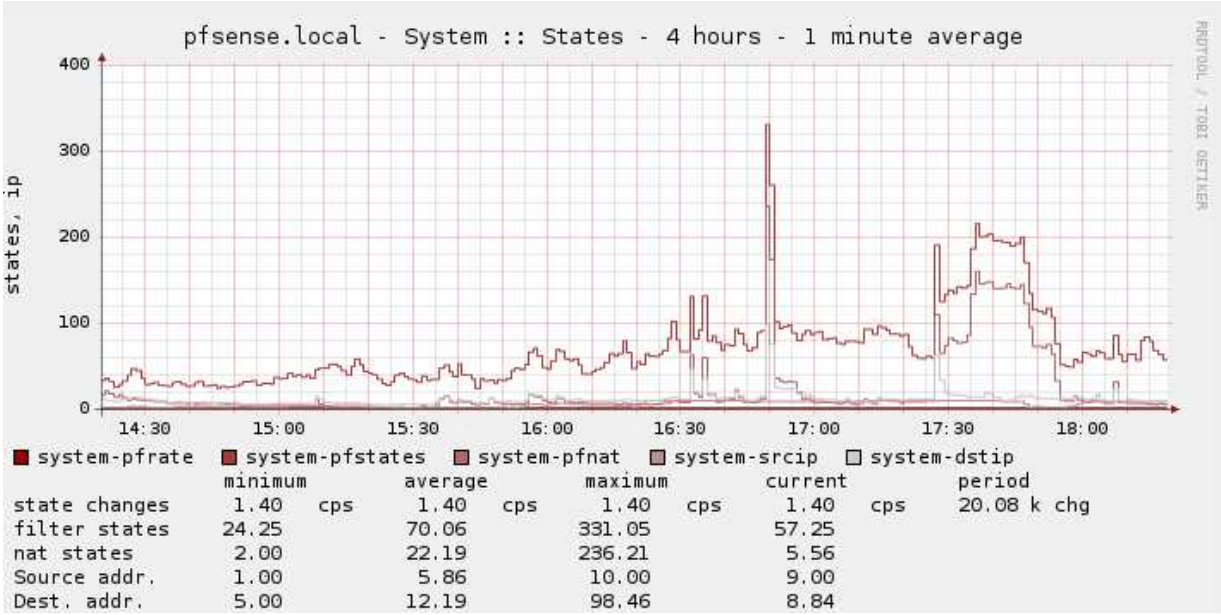

Figura 188– Gráfico Rendimiento Sistema Servidor PfSense Con Cifrado 15 Usuarios.

Es posible apreciar en los gráficos, que la carga de datos con cifrado en el servidor PfSense, va aumentando periódicamente por cada petición o solicitud de video streaming. Esta carga afecta de forma media al rendimiento del servidor, en el manejo de paquetes de entrada y salida del servidor. Además es posible apreciar que el aumento en el manejo de ancho de banda es medio, frente a la configuración de un servidor sin técnicas de seguridad.

Además la imagen anterior muestra el rendimiento del servidor PfSense a nivel de sistema, una vez que se realiza cada una de las conexiones hacia el servidor PfSense, con aspectos de seguridad, para realizar la transmisión streaming.

Es lógico que a medida que el servidor va obteniendo más peticiones, este aumente su nivel de procesamiento de sistema, por ende una mayor utilización de los recursos, y tal vez a gran escala una perdida de funcionamiento.

A mayor número de usuarios conectados y luego transmitiendo video, el servidor aumenta su utilización de procesamiento, luego baja este rendimiento hasta una estabilización que el servidor provee, para así mantener una buena disponibilidad y estabilidad de los servicios. Estas pruebas se realizaron en ambos sistemas operativos, transmitiendo video streaming desde la cámara de tele vigilancia.

Es posible observar que entre los periodos 16 y 18 horas se muestra el rendimiento medio que provee el servidor PfSense con cifrado, con ello demostrando la premisa de que al utilizar medios de seguridad se obtiene una mayor carga, sin embargo, este carga es mínimamente mayor.

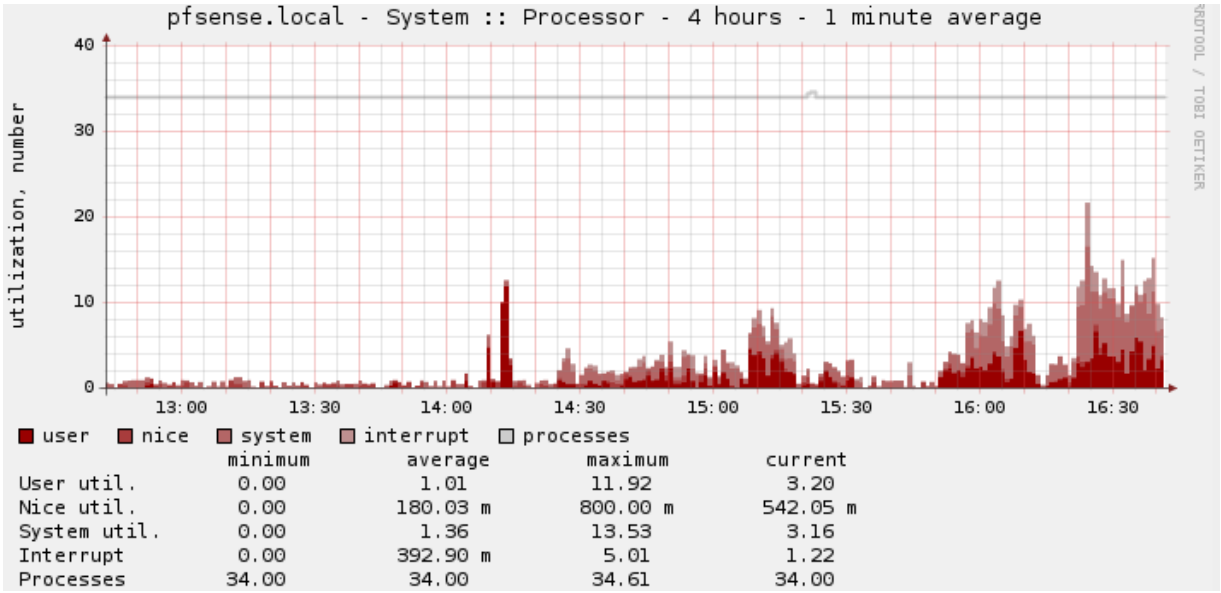

Figura 189– Gráfico Rendimiento Procesos Servidor PfSense Con Cifrado 15 Usuarios.

La figura muestra el rendimiento del procesador del servidor PfSense, dando como resultado un funcionamiento estable y fiable. Se mantiene un nivel de procesamiento estable, subiendo cada vez que se realiza una nueva conexión, pero luego estabilizándose y previendo una conexión estable y segura. Es posible apreciar que en el rango entre las 15:30 y 16:30, se aprecia un uso mayor en la carga de procesamiento del servidor, con ello una menor rendimiento y mayor uso de recursos, sin embargo, es posible apreciar que el aumento no es tan amplio como teóricamente se piensa, con ello logrando estabilizar y optimizar el uso de recursos en el sistema de tele vigilancia.