ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ANÁLISIS DE LAS ARQUITECTURAS DE CONEXIÓN DE REDES PRIVADAS VIRTUALES VPNs PARA LA TRANSMISIÓN DE VIDEOCONFERENCIA

AUTOR: JAVIER ELICIO SOLANO YANEZ

TUTOR: ING. GLORIA ARCOS., MSC.

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN INTERCONECTIVIDAD DE REDES

RIOBAMBA - ECUADOR

Agosto, 2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado "ANÁLISIS DE LAS ARQUITECTURAS DE CONEXIÓN DE REDES PRIVADAS VIRTUALES VPNs PARA LA TRANSMISIÓN DE VIDEOCONFERENCIA", de responsabilidad del Sr. Javier Elicio Solano Yánez, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Oswaldo Martínez. Ms.C **PRESIDENTE**	FIRMA
Ing. Gloria Arcos MsC. **DIRECTOR**	FIRMA
Ing. Diego Ávila MsC. **MIEMBRO**	FIRMA
Ing. Alberto Arellano MsC. **MIEMBRO**	FIRMA

Riobamba, Agosto del 2016.

DERECHOS INTELECTUALES

Yo, Javier Elicio Solano Yánez, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____
Javier Elicio Solano Yánez
0603146671

DECLARACIÓN DE AUTENTICIDAD

Yo, Javier Elicio Solano Yánez, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, 17 de Agosto del 2016.

_____
Javier Elicio Solano Yánez
0603146671

DEDICATORIA

Este trabajo de Investigación dedicado a Mí Esposa Verónica Morales a Mí Hija Arianita Juliette, por su amor, paciencia, ánimos que día a día dedican en las diferentes etapas de mi vida tanto profesional como personal.

A mis Padres, Hermanas, por estar siempre presente, con sus palabras de aliento, que no me permitían decaer para que siempre sea perseverante y que cumpla con mis ideales.

A mis tres ángeles que están en el cielo, abuelito, abuelita, hermana que si de manera física no lo están estoy seguro que siempre lo están de manera espiritual.

AGRADECIMIENTO

En primer lugar quiero agradecer a Dios por iluminarme, por darme fuerzas para superar obstáculos, dificultades y permitirme la consecución de este trabajo de investigación.

A mis maestros por compartir valiosas experiencias, conocimientos que me han permitido crecer de manera intelectual, personal.

Es oportuno mi agradecimiento al Ing. Diego Ávila quien con sus conocimientos, experiencia, su tiempo para la revisión, correcciones ha permitido la culminación de este proyecto de investigación.

Varias son las personas que han formado parte de mi vida profesional a las que me gustaría agradecerles por su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos, sin importar en donde estén quiero darles las gracias, por todo lo que me han brindado y por todas sus bendiciones.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

LISTA DE ANÉXOS

RESUMEN

La investigación tuvo como objetivo analizar las arquitecturas de conexión Red Privada Virtual (VPNs) en la transmisión de videoconferencia lo que permitirá determinar cuál es la mejor arquitectura que se debe implementar. Se planteó la hipótesis de investigación; "IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar el rendimiento en la transmisión de videoconferencia". Se utilizó el método de análisis de la varianza ANOVA de un factor con la prueba Post hoc, HSD Tukey, en la comparación de las arquitecturas con nivel de significancia menores a (0.05). Los indicadores utilizados fueron latencia, jitter, ancho de banda, porcentaje de datagramas recibidos, de un total de treinta muestras de cada uno de los servidores con software libre OpenVPN SSL, OpenSSH SSH, OPENSwan IPSec, con GNS3 de cisco para SSL, SSH, IPSec, la videoconferencia se realizó con el software Linphone. De acuerdo al análisis realizado con ANOVA se determinó que el protocolo de mejor rendimiento en las VPNs con software libre es OpenSSH, que corresponden a (0.034) latencia, (0.00) jitter, (0.00) datagramas recibidos. Tres de cuatro indicadores tienen menor nivel de significancia, lo cual permite rechazar la hipótesis planteada de estudio. Para dispositivos Cisco con datos obtenidos del simulador GNS3, el adecuado es IPSec, de acuerdo a la prueba de ANOVA, que corresponde (0.03) latencia, (0.00) jitter, (0.00) ancho de banda, lo cual permite afirmar la hipótesis de estudio planteada. El software libre permite crear VPN a costo bajo por lo que este software es implementado en un computador sin muchos requerimientos de CPU sobre Linux preferentemente sobre Centos. Se recomienda el uso de software libre por el costo de los equipos.

Palabras claves: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <TECNOLOGÍA DE COMUNICACIONES>, <INTERCONECTIVIDAD DE REDES>, <RED PRIVADA VIRTUAL> <SOFTWARE OPENVPN SSL> < SOFTWARE OPENSSH SSH> < SOFTWARE OPENSWAN IPSec> <SIMULADOR DE REDES >

SUMMARY

This research aimed to analyze the connection architecture Virtual Private Network (VPNs) in video conferencing transmission which will allow determining which one is the best to be implemented. This was the hypothesis: "IPSec is the best protocol which should be implanted in architecture VPN in order to better performance of video conferencing transmission". It was used the analysis of variance ANOVA of a factor through the test Post hoc, HDS Tukey, in comparison of architecture with lower significant level (0.05). Indicators used were latency, jitter, bandwidth, percentage of datagrams received from thirty samples of servers with open source such as: OpenVPN SSL, OpenSSH, OpenSwan IPSec, with GNS3 with cisco for SSL, SSH, IPSec, videoconferencing was conducted through Linphone software. Based on the analysis carried out by the means of ANOVA it was determined the protocol with the best performance in VPN was the open source OpenSSH which has (0.034) latency, (0.00) jitter, (0.00) datagrams received. Three up to four indicators have lower significant level which refused the hypothesis proposed in this study. IPSec is the appropriate for Cisco devices with data gotten from GNS3 simulator according to ANOVA test which has (0.03) latency, (0.00) jitter, (0.00) bandwidth which confirms the hypothesis proposed in this study. Open source allows creating VPN al low cost, so this software is implement in a computer without many requirements of CPU about Linux including Centos. It is recommended the use of open source because of the cost of equipment.

Key words: <TECHNOLOGY AND ENGINEERING SCIENCES>, < TECHNOLOGY OF COMMUNICATIONS>, <INTERCONNECTIVITY OF NETWORKS>, <VIRTUAL PRIVATE NETWORK> <SOFTWARE OPENVPN SSL> < SOFTWARE OPENSSH SSH> < SOFTWARE OPENSWAN IPSEC> <SIMULATOR NETWORKS >

INTRODUCCIÓN

El presente trabajo de investigación propone el "Análisis de las diferentes arquitecturas de conexión de VPNs (Redes Privadas Virtuales) para la transmisión de videoconferencia", para lo cual se procederá al estudio de las arquitecturas o protocolos; SSL, SSH, IPSec, de estas arquitecturas se medirá el rendimiento de la red en función de la latencia, jitter, ancho de banda, porcentaje de datagramas recibidos, en escenarios propuestos con el uso de software libre y con el simulador de gráficos de red GNS3 para equipos cisco.

Para la conexión de las arquitecturas VPNs con software libre se seleccionaron los siguientes programas: OpenVPN para SSL, OpenSSH para SSH, OPENSwan para IPSec, con el simulador de redes GNS3 se utilizarán, el router cisco 2960 para IPSec y SSH, el router cisco 3725 para SSL con el cliente sslclient-win, cada arquitectura es implementada en diferentes ambientes de pruebas, la videoconferencia se realiza con el software libre Linphone, este software puede ser instalado en Centos y Windows.

A través de la captura del tráfico se analizará el rendimiento de las arquitecturas de conexión VPN en los diferentes ambientes de simulación propuestos, se determinará cuál es la más adecuada en la realización de videoconferencia.

El Capítulo I, corresponde a la problemática de la investigación, el planteamiento del problema, formulación del problema, sistematización del problema, al igual que se hace referencia a la justificación, a los objetivos y la hipótesis.

El Capítulo II, corresponde a la revisión de literatura, en la cual se destacan contenidos relacionados con las diferentes arquitecturas de conexión VPN, SSL, SSH, IPSec, las características de cada una de las arquitecturas, consideraciones para la implementación de los escenarios propuestos en la simulación.

El Capítulo III, considera los métodos de investigación utilizados; método científico, utilizado para la observación recopilación de muestras de cada uno de los escenarios planteados. Comparativo, para comparar cada uno de los indicadores de rendimiento de red e identificar el de mayor rendimiento. Experimental, estadístico mediante el análisis de la varianza ANOVA con la prueba Post hoc, HSD de Tukey el cual permitirá identificar el protocolo que cumple con la hipótesis planteada.

El Capítulo IV, contempla el análisis, la interpretación de resultados de las muestras tomadas, las pruebas de rendimiento realizadas en cada uno de los escenarios con software libre y con el simulador de redes GNS3, estas serán comparadas mediante ANOVA, lo que permitirá determinar la arquitectura VPN de mejor rendimiento en la realización de la videoconferencia.

En este capítulo se afirmará o negará la hipótesis planteada, que es sí: "IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar el rendimiento en la transmisión de videoconferencia".

CAPITULO I

1. PROBLEMATIZACIÓN

1.1. Planteamiento del problema

Una red es la conjunción de dispositivos, que interconectan los equipos informáticos de una organización. Las empresas, organizaciones, instituciones buscan la posibilidad de comunicarse a nivel local o regional las cuales necesitan; comunicaciones rápidas, seguras y confiables sin importar el sitio de ubicación de sus oficinas, instalaciones o empleados. Realizar conexiones remotas a la red corporativa es una necesidad para las empresas. Uno de los sistemas más extendidos para comunicarse de forma remota segura con una red es a través de conexiones VPN.

Una VPN es una red privada virtual, que utiliza una red pública compartida usualmente Internet, para ofrecer a un cliente la facilidad y ventaja de realizar conexiones entre varios lugares o sitios remotos entre ellos, remplazando a conexiones dedicadas o líneas alquiladas por una VPN esta utiliza una "conexión virtual" a través de internet desde la red privada de la organización hasta el sitio o empleado remoto.

Una conexión VPN es también un punto crítico de entrada de todo tipo de seguridad, las VPNs crean túneles que pueden tener conexión directa a los servidores de la organización. Para lo cual son necesarias políticas de seguridad adecuadas para que la información no quede expuesta. Una red privada virtual se extiende mediante un proceso de encapsulación, en el caso de las VPNs con la encriptación de los paquetes de datos, la compartición, generación de claves, certificados.

La comunicación a través de redes VPN proporciona una solución escalable y segura que permite a las empresas ofrecer varios servicios entre ellos videoconferencia. Las redes virtuales privadas utilizan protocolos especiales de seguridad, los mismos que tienen métodos de cifrado, encubrimiento de la información, impidiendo obtener acceso a servicios de carácter privado, permitiendo el ingreso solo al personal autorizado. Para las VPNs se han desarrollado varias arquitecturas para resguardar la información en casi todas las capas de la pila del modelo

de interconexión de sistemas abiertos OSI (modelo de interconexión de sistemas abiertos ISO/IEC 7498-1) como se visualiza en la siguiente (Figura 1-1).

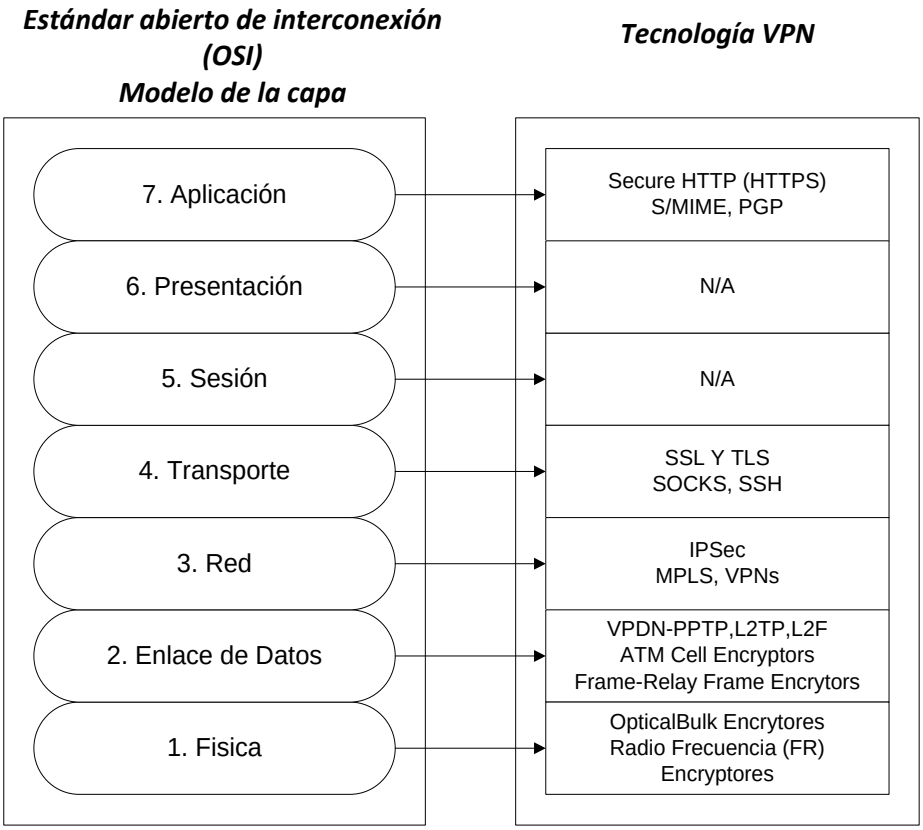


Figura 1-1: Modelo OSI y tecnologías VPN

Fuente: (Sosa Delgado & Velazques Sanches, 2000, pág. 28)

Tomado como referencia al modelo OSI presentado en la (Figura 1-1), se propone realizar es el análisis del rendimiento de la transmisión de videoconferencia en las siguientes arquitecturas:

- SSH (*Secure Socket Shell*), SSL (*Secure Sockets Layer*) de la capa 4.
- IPSec (*Internet Protocol Security*) de la capa 3.

1.2. Formulación del problema

¿Cuál de las arquitecturas SSL, SSH, IPSec implementada en una VPN tiene el mejor rendimiento en la transmisión de videoconferencia?

1.3. Sistematización del problema

- ¿Qué escenarios se van a desarrollar con arquitecturas VPNs, utilizando software libre y con el simulador de red GNS3 para equipos cisco?
- ¿Qué configuraciones se debe realizar con software libre y con GNS3 para crear una VPN en las diferentes arquitecturas propuestas?
- ¿Qué pruebas de rendimiento puedo realizar en una arquitectura VPN?
- ¿Qué arquitectura es la más adecuada para ser implementada en una VPN para establecer videoconferencia en función de su rendimiento?

1.4. Justificación

Varios son los posibles ataques a los que puede estar sujeta una red corporativa, empresa o un usuario en particular; se encuentran los virus, vándalos y troyanos; las acometidas de hackers como podrían ser ataques de reconocimiento, de acceso, de negación de servicios y de interceptación de datos, una empresa debe ser capaz de estar protegida frente a los ataques desde dentro de la misma, donde los empleados de forma inconsciente, negligente o vengativa pueden causar daños irreparables.

Una VPN (red privada virtual) es una red de información privada que hace uso de una infraestructura pública de telecomunicaciones, que conecta diferentes segmentos de red o usuarios a una conexión de red virtual, manteniendo la privacidad a través del uso de un protocolo de túnel o aislamiento simultáneamente con otras tecnologías que proveen seguridad. La función principal de una VPN, es de brindar conectividad a una red, a través de una red pública, precautelando la integridad de la información. Para la implementación de una VPN existen aspectos fundamentales que deben considerarse tales como: costo, desempeño, confianza, seguridad y rendimiento. De estas características, la seguridad, confidencialidad son las más primordiales, sin las debidas seguridades los aspectos fundamentales de una VPN no tienen mucha importancia puesto que queda a segundo plano que tan barata, rápida y confiable sea una red, sin las seguridades adecuadas los riesgos propenden la inestabilidad de la red en cada una de las VPNs para establecer conexiones crea túneles con diferentes tipos de autenticación así tenemos e llaves, certificados en su conexión.

La problemática radica en establecer la arquitectura VPN de mayor rendimiento al realizar videoconferencia, para lo cual cada arquitectura se comparara en función de la latencia, jitter,

ancho de banda, porcentaje de datagramas recibidos. Para lo cual se plantea los siguientes ambiente de pruebas.

En la (Figura 2-1) se plantean los diferentes ambientes de pruebas con el uso de software libre de cada una de las arquitecturas planteadas para esta investigación.

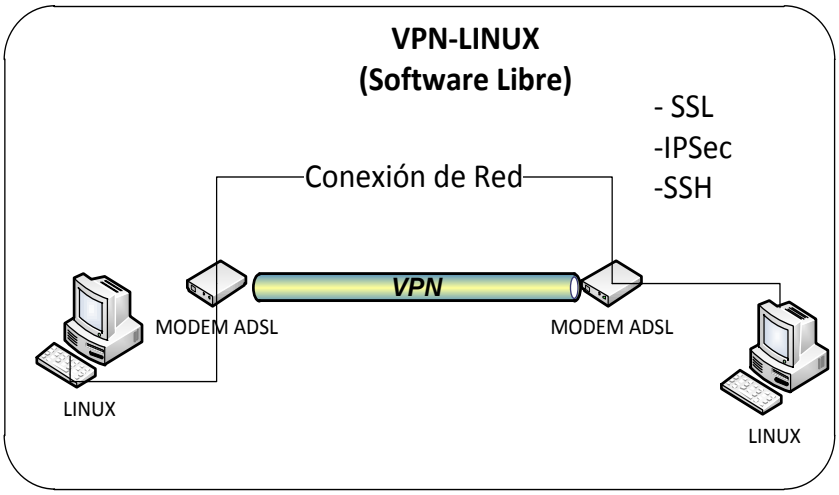


Figura 2-1: Ambiente de pruebas con software libre en Linux

Realizado por: Javier E. Solano Y. 2016

En la (Figura 3-1) se identifican los escenarios de pruebas con el simulador de redes GNS3 para equipos cisco.

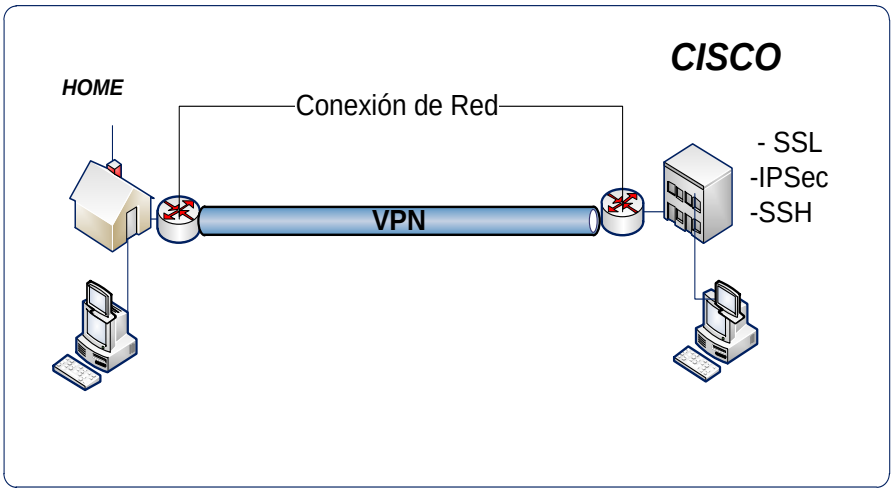


Figura 3-1: Ambiente de pruebas con GNS3 de Cisco

Realizado por: Javier E. Solano Y. 2016

1.5. Objetivos

1.5.1. *General*

Analizar las arquitecturas de conexión VPNs en la transmisión de videoconferencia lo que permitirá determinar cuál es la mejor arquitectura que se debe implementar.

1.5.2. *Específicos*

- Estudiar las siguientes arquitecturas para redes VPN, SSH, SSL, IPSec, en la transmisión de videoconferencia, implementada en escenarios con software libre y con el simulador de equipos cisco GNS3.
- Implementar escenarios de simulación que permita el estudio comparativo entre las arquitecturas VPN de software libre linux y GNS3 de cisco.
- Presentar el análisis de rendimiento latencia, jitter, ancho de banda, datagramas recibidos con la transmisión de videoconferencia en los escenarios propuestos con software libre OpenVPN SSL, OpenSSH SSH, OPENSwan IPSec) y con el simulador de redes Cisco GNS3 SSL, SSH, IPSec.

1.6. Hipótesis

"IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar el rendimiento en la transmisión de videoconferencia."

CAPITULO II

2. REVISIÓN DE LITERATURA

2.1. VPN (Red Privada Virtual)

Una VPN es una red de información privada que utiliza infraestructura pública de telecomunicaciones, permitiendo diferentes segmentos de red o usuarios a una red principal, manteniendo la privacidad a través del uso de un protocolo de túnel o aislamiento así como de otras tecnologías que proveen seguridad. La función principal de una VPN es la de brindar conectividad a una red, a través de una red pública, brindando la integridad de la información.

Para la implementación de una VPN, aseguran (Montes De los Santos, Corona Carrión, & Gonzáles Beltran, 2012, pág. 38), existen aspectos fundamentales que deben considerarse: "costo, desempeño, confianza y seguridad". De estas características, la seguridad es la más primordial, sin la existencia de esta característica las otras resultan ser improductivos; puesto que no importa qué tan barata, rápida, confiable sea una red, sin la seguridad adecuada los riesgos causaran la inestabilidad de la red dado que a los riesgos de seguridad hay aspectos del QoS (calidad de servicio) concernientes a el uso del internet, conexiones remotas.

Anteriormente las diferentes sucursales de una empresa podían tener, cada red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de mensajería electrónica e inclusive usar protocolos que difieran de los usados en otras sucursales. (Moreno Brito, 2008, pág. 130). Es decir, en cada lugar existía una configuración totalmente local que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma de manera remota.

A medida que la tecnología se ha incorporado a las empresas surge la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación este medio fueron las líneas dedicadas con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad. Además de la comunicación entre diferentes sucursales surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante RAS (accesos de servicios remotos), este tipo de

usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma. El gran inconveniente de las líneas dedicadas es su alto costo, ya que se suele cobrar un abono mensual más una tarifa se tienen en cuenta la duración de las llamadas y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas, y, además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos.

Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan. Las VPNs son una alternativa a la conexión de la WAN (conexión de redes extensas) mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones. (Ñacato Gualotuña , 2007, pág. 14).

2.2. ¿Por qué implementar VPNs?

Para poder efectuar conexiones remotas con alguna empresa, organización, se la puede realizar utilizando:

- **Línea Privada:** Uso de líneas de cobre o fibra óptica de un punto a otro, lo cual resultara costoso, si se quiere cubrir zonas extensas, mantenimiento, infraestructura, etc.
- **VPN:** En cuestión de costos resulta bajos de acuerdo al tipo de conexión que utilice y si es utiliza servicios telefónicos con conexión a internet resulta los valores económicos bajos. Con lo que hay la posibilidad que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

2.3. Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

a) **Identificación de usuario:** La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados, se debe proporcionar registros estadísticos que muestren quien acceso, que información es la que introdujo, actualizo, utilizo y cuando.

b) **Administración de direcciones:** La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

c) **Codificación de datos:** Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

d) **Administración de claves:** La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

e) **Soporte a protocolos múltiples:** La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen la IP (protocolo de internet), el IPX (intercambio de paquete de internet) entre otros.

2.4. Funcionamiento y características

Las VPNs permiten que las comunicaciones se realicen por un canal seguro. Para lo cual (Espinoza Velez, 2006, pág. 100) propone que debe cumplir con los siguientes requisitos:

- **Autenticación:** Estas técnicas son indispensables en las VPNs, las cuales aseguran que la información que se intercambia es con el usuario o dispositivo correcto. En la mayoría de los sistemas de autenticación usada en las VPNs se basan en un sistema de claves compartidas. La autenticación comienza al inicio de una sesión y luego de manera aleatoria durante el curso de la transmisión.
- **Integridad:** Las VPNs garantizan que los datos lleguen al receptor sean exactamente los que el emisor transmitió por el canal.
- **Tunneling:** Para el envío y recepción de información en una red privada a través de la red pública se establece túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autenticación, los cuales aseguraran la integridad de los datos transmitidos utilizando la red pública. Para lo cual será necesario tomar cuidado cuestiones de seguridad, a través de la encriptación, autenticación.

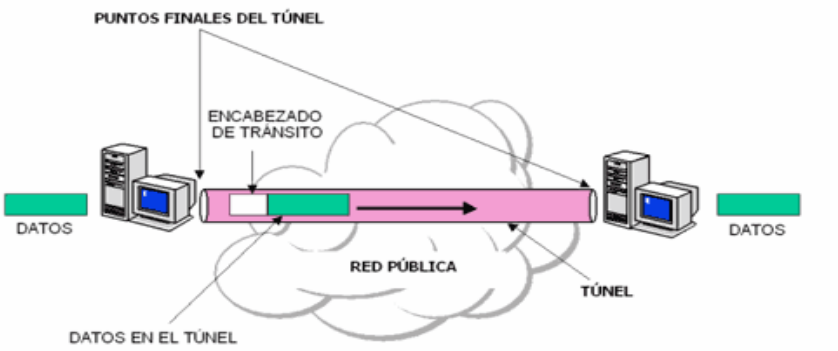


Figura 1-2: Túnel virtual de una VPN

Fuente: (Espinoza Velez, 2006), Estudio de los mecanismos de seguridad de las redes privadas virtuales

2.5. Encriptación de una VPN

Cada uno de los gateway envía su clave pública a todos los demás gateway pertenecientes al sistema. Con el uso de sistemas de encriptación simétricos, de clave pública y clave privada, la información se encripta matemáticamente de tal forma que es extremadamente complejo desencriptar la información sin poseer las claves. Existe un proceso de gestión de dichas claves (Key management) que se encarga de su distribución, se refresca cada cierto tiempo y revocarlas cuando sea necesario hacerlo. Se ha de conseguir un balance entre los intervalos de intercambio de las claves, la cantidad de información que se transfiere; un intervalo demasiado corto sobrecargaría los servidores de la VPN con la generación de claves mientras que uno excesivamente largo podría comprometer la clave y la información que esta protege. (Ruíz Gonzáles, 2002, pág. 2)

2.6. Algoritmos de encriptación

Una manera segura de la transmisión de datos o información en una VPN es implementar uno o más algoritmos de encriptación, en su configuración, como medio de comunicación se usa el internet o similares, datos que puede ser vulnerable por este medio al igual que puede ser fácilmente capturada por personas ajenas, pero con los medios de encriptación, a estos datos están cifrados y no puede ser entendible por personas ajenas. (Ortega, 2003, pág. 40)

2.6.1. *Principales algoritmos Simétricos - 3DES o TDES*

Fue emitido en 1999 como una versión mejorada de DES. Realiza tres veces el cifrado DES utilizando tres claves. La (Figura 2-2) muestra el diagrama que representa al algoritmo 3DES.

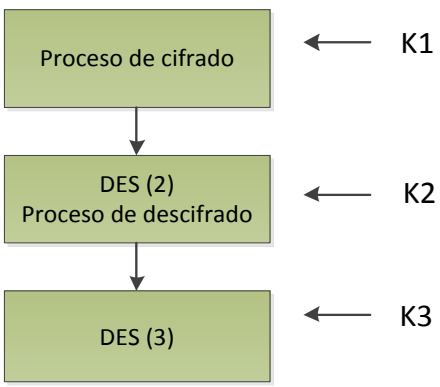


Figura 2-2: Cifrado triple DES

Fuente: (UNAM, 2012), Fundamentos de Criptografía

Cuando se descubrió que una clave de 56 bits (utilizada en el DES) no era suficiente para evitar un ataque de fuerza bruta, el 3DES fue elegido para agrandar la clave sin la necesidad de cambiar el algoritmo de cifrado.

Con tres claves distintas, 3DES tiene una longitud de clave efectiva de 168 bits aunque también se pueden usar dos claves haciendo *K1=K3* (ver Figura 2-2) con lo que se tiene una longitud de clave efectiva de 112 bits. Actualmente el 3DES sigue siendo utilizado pero cada vez más está siendo sustituido por el algoritmo AES que ha demostrado ser muy robusto y más rápido. (UNAM, 2012, http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/).

- **RSA** (Rivest-Shamir-Adleman), es el algoritmo de encriptación y autentificación más comúnmente usado, desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, y se incluye como parte de los navegadores de Netscape y Microsoft, así como sus aplicaciones. (Rivest, Shamir, & Adleman, 1983, pág. 100). El sistema de encriptación era propiedad de RSA Security hasta que en septiembre de 2000 caducó la patente que había sobre este algoritmo. Basado en la dificultad de la factorización en factores primos de números enteros bastante grandes y ampliamente utilizado en nuestros tiempos.

- El funcionamiento de este algoritmo se basa en multiplicar dos números primos extremadamente grandes, y a través de operaciones adicionales obtener un par de números que constituyen la clave pública y otro número que constituye la clave privada. Una vez que se han obtenido las claves, los números primos originales ya no son necesarios para nada, y se descartan. Se necesitan tanto las claves públicas como las privadas para encriptar y desencriptar, pero solamente el dueño de la clave privada lo necesitará. Usando el sistema RSA, la clave privada nunca necesitará ser enviada. La clave privada se usa para desencriptar el código que ha sido encriptado con la clave pública.

- Por tanto, para enviar un mensaje a alguien, hay que conocer su clave pública, pero no su clave privada. Al recibir el mensaje, se necesitará la clave privada para desencriptar. También se puede usar para autentificar un mensaje, firmando con la clave privada un certificado digital. Su longitud típica de llaves es 512 y 1024 bits. (Cevallos Rodriguez, 2006, pág. 30).

- **AES** (Advanced Encryption Standard), es un algoritmo de encriptación para proteger información delicada, aunque no clasificada, por las agencias gubernamentales de USA y como consecuencia puede transformarse en el estándar para las transacciones comerciales en el sector privado. La criptografía para las comunicaciones clasificadas, incluyendo los militares, es gestionada por algoritmos secretos. En enero de 1997, El NIST (Nacional

Institute of Standards and Technology) inició un proceso para encontrar un algoritmo más robusto que reemplazara a DES y en menor medida a triple DES (3DES). La especificación solicitaba un algoritmo simétrico usando encriptación por bloques de 128 bits de tamaño, que soportara como mínimo claves de 128, 192 y 256 bits. Debía ser royalty-free para su uso en todo el mundo, y ofrecer un nivel de seguridad suficiente para los próximos 20 ó 30 años. (De Luz, 2010, http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/).

- **DEA** (International Data Encryption Algorithm) es un algoritmo de encriptación desarrollado en el ETH de Zúrich (Suiza) por James Massey y Xuejia Lai. Usa criptografía de bloque con una clave de 128 bits, se considera como muy seguro. Está considerado como uno de los algoritmos más conocidos. Durante los años que lleva siendo usado, no ha sido publicado ningún método práctico para descifrarlo, a pesar de los numerosos intentos que han habido de encontrar uno. IDEA está patentada en USA y en la mayor parte de los países europeos, y la patente está en manos de Ascom-Tech AG. (Bermudez Fernández & Casanova Vasquez, 2011, págs. 23-24).

2.7. Arquitecturas de conexión VPN

Básicamente existen tres arquitecturas de conexión VPN:

2.7.1. *VPN de acceso remoto*

Esta es la arquitectura de conexión más utilizada actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos en oficinas comerciales, domicilios, hotel, aviones, etc., utilizando internet como vínculo de acceso. El cliente de acceso remoto llamado cliente VPN, se autentifica al servidor de acceso remoto identificado como el servidor VPN, y para una mutua autentificación, el servidor se autentifica ante el cliente. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura módems y líneas dedicadas 'dial-up'. (Pita, 2009, pág. 22).

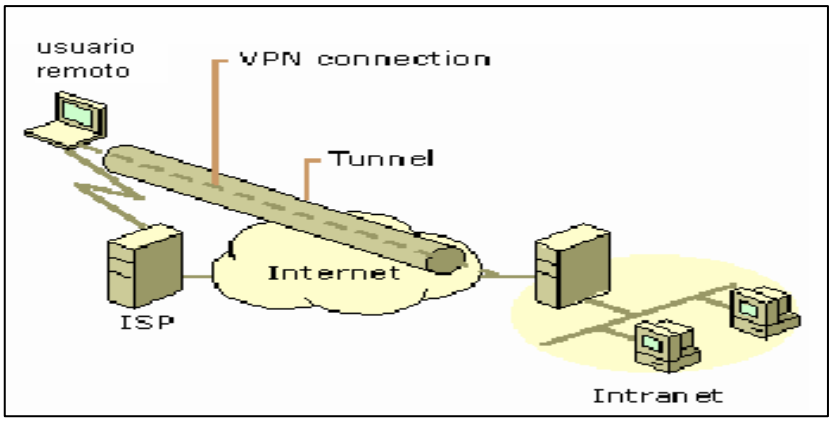


Figura 3-2: Usuario remoto VPN

Fuente: (Pita, 2009, pág. 22), Arquitectura de Red

2.7.2. *VPN punto a punto*

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN posee un vínculo permanente a internet acepta las conexiones vía internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a internet utilizando los servicios de su proveedor local de internet líneas dedicadas, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto, sobre todo en las comunicaciones internacionales. (INEM, 2012, pág. 2)

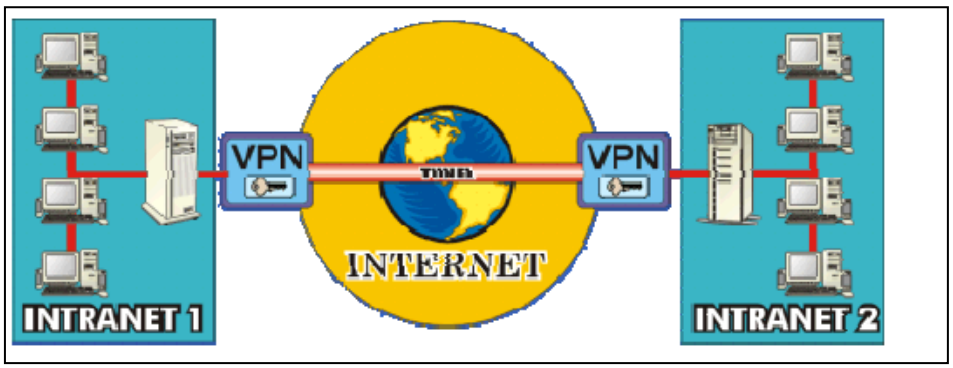


Figura 4-2: Conexión VPN punto a punto

Fuente: (INEM, 2012, pág. 2), Ficha de servicios de tecnologías de información

2.7.3. *VPN interna VLAN*

Esta conexión es la menos difundida pero una de las más poderosas para utilizar dentro de

la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar internet como medio de conexión, emplea la misma lan-local de la empresa. Esta conexión es muy útil para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas de área local (WiFi).

2.8. Conexiones VPN basadas en internet o en intranet

2.8.1. *VPN basadas en internet*

Si se opta por un conexión de VPN basada en internet, se tiene la ventaja que disminuyen los costos debido a que se puede ahorran los gastos de llamadas telefónicas de larga distancia y a números 1-800, y se aprovecha la gran disponibilidad de internet.

- **Acceso remoto a través de internet:** Cuando se trata de una acceso remoto a través de internet, los usuarios en vez de realizar una costosa llamada de larga distancia o a un número 1-800 para conectarse con un Network Access Service (NAS) de la compañía o externo, puede llamar a un ISP-Proveedor de servicio de internet local. Aprovechando esta conexión física con el ISP local, el cliente de acceso remoto inicia una conexión VPN a través del internet con el servidor VPN de la organización. Una vez creada la conexión VPN, el cliente de acceso remoto puede tener acceso a los recursos de la intranet privada. (Microsoft, 2005, pág. 3)

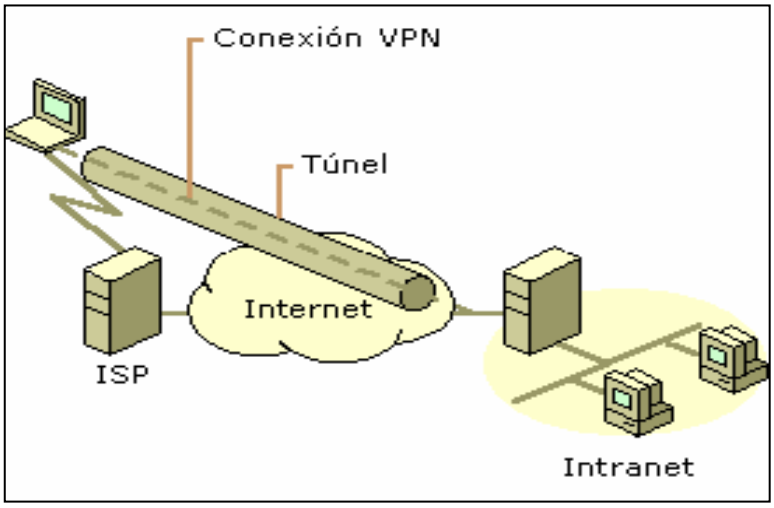


Figura 5-2: Acceso remoto a través de Internet

Fuente: (Microsoft, 2005, pág. 3), VPN basadas en Internet

- **Conexión de redes a través de internet:** Cuando se realiza una conexión de redes a través de internet, un enrutador reenvía paquetes a otro enrutador a través de una conexión VPN. Esto se conoce como una conexión VPN de enrutador a enrutador. (Microsoft, 2005, pág. 4)

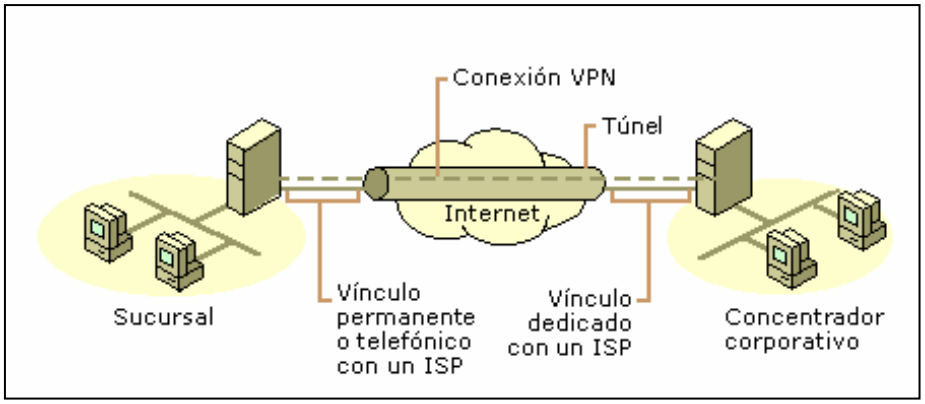


Figura 6-2: Conexión de redes a través de internet

Fuente: (Microsoft, 2005, pág. 4), VPN basadas en Internet

2.8.2. *VPN basadas en intranet*

Si se opta por una conexión de VPN basadas en intranet se tiene la ventaja que se aprovecha la conectividad IP en la intranet de una organización.

- **Acceso remoto a través de intranet:** En las intranets de algunas organizaciones o empresas, los datos de un departamento por ejemplo; el departamento financiero o de recursos humanos, son tan confidenciales que la red del departamento está físicamente desconectada de la intranet del resto de la organización. Aunque así se protegen los datos del departamento, se crea un problema de acceso a la información por parte de aquellos usuarios que no están físicamente conectados a la red independiente. (Arribas, 2006)

  Una VPN basada en Intranet, la red del departamento está físicamente conectada a la intranet de la organización pero se mantiene separada gracias a un servidor VPN. El servidor VPN no proporciona una conexión enrutada directa entre la intranet de la organización y la red del departamento. Los usuarios de la intranet de la organización que disponen de los permisos apropiados pueden establecer una conexión VPN de acceso remoto con el servidor VPN y tener acceso a los recursos protegidos de la red confidencial del departamento. (Cedillo Durán & Molina Michalo, 2006, pág. 5)

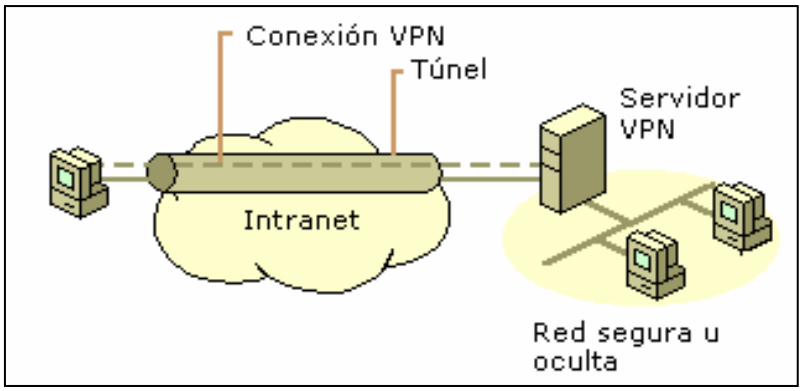


Figura 7-2: Acceso remoto a través de Intranet

Fuente: (Microsoft, 2005, pág. 5), VPN basadas en Internet

Se puede también conectar dos redes a través de una intranet mediante una conexión VPN de enrutador a enrutador. Este tipo de conexión es ideal para las organizaciones que poseen departamentos en diferentes ubicaciones, cuyos datos son confidenciales, únicamente el administradores el que maneja esta información, (Ayare, 2010, pág. 8)

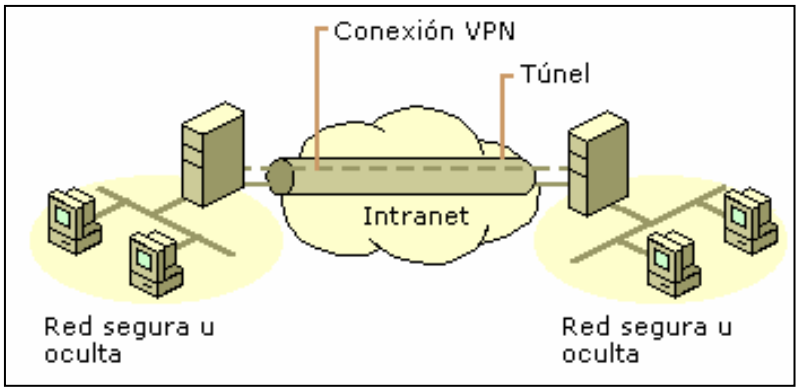


Figura 8-2: Conexión de redes a través de una intranet

Fuente: (Microsoft, 2005, pág. 8), VPN basadas en Internet

2.9. Análisis de protocolos

2.9.1. *Protocolos usados por las VPNs*

Existen variedad de protocolos de red para el uso de las VPNs que han sido implementados, estos protocolos intentan ofrecer la mayor seguridad posible en una VPN así tenemos algunos de ellos: SSH, SSL, IPSec, entre otros.

2.9.1.1. *Secure Shell (SSH)*

SSH también ofrece una comunicación segura para la transmisión de datos a través de una red no segura, como internet. SSH la función básica es de brindar comunicaciones seguras entre las oficinas remotas, hay algunas diferencias entre ellos. La diferencia principal es que SSH es un protocolo de capa de aplicación y VPN IPSec es una solución de la capa IP. Esto significa que un protocolo tal vez el más apropiado dependiendo de lo que estamos tratando de lograr. El servidor de la empresa sólo se puede acceder a través del servidor que está conectado a internet. Dado que la información que se transmite es confidencial, SSH modelo cliente / servidor puede cifrar los datos de un punto a otro con facilidad. (Romero Temero, 2004, pág. 30)Seguridad en redes y protocolos asociados.

- De seguridad para aplicaciones específicas SSH puede encriptar todas las solicitudes de la duración de la sesión siempre que la solicitud tiene un puerto conocido. Las aplicaciones que cumplen con este criterio incluyen correo electrónico, conexiones de base de datos. La ventaja de la encriptación es que sólo algunas aplicaciones se reducen el potencial de creación de sobrecarga de la red innecesarios asociados con la encriptación de todas las aplicaciones como se hace con VPN. (CISCO, 2013, pág. 10)

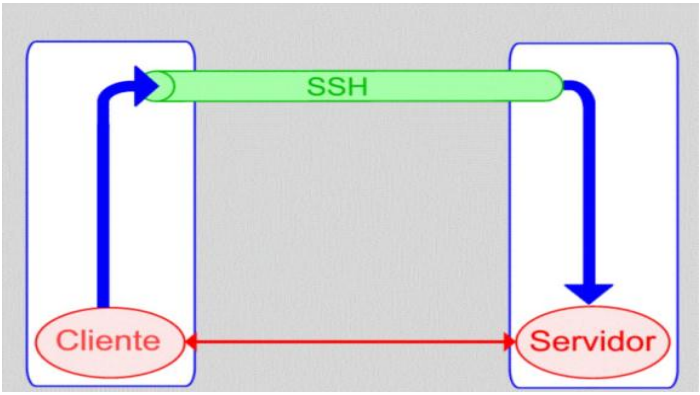


Figura 9-2: Conexión segura de SSH

Fuente: (CISCO, 2013, pág. 10), Mejora de seguridad de los routers de Cisco

2.9.1.2. *Secure Sockets Layer (SSL)*

SSL trabaja sobre el protocolo TCP (Protocolo de Control de Trasmisión) y por debajo de protocolos como HTTP (Protocolo de Transferencia de Hipertexto), IMAP (Protocolo de Acceso de Mensajes de Internet), LDAP (Protocolo Ligero de Acceso a Directorios) puede ser

usado por todos ellos de forma transparente para el usuario. Opera entre la capa de transporte y la de sesión del modelo OSI o entre la capa de transporte y la de aplicación del modelo TCP y está formado, a su vez, por dos capas y cuatro componentes bien diferenciados:

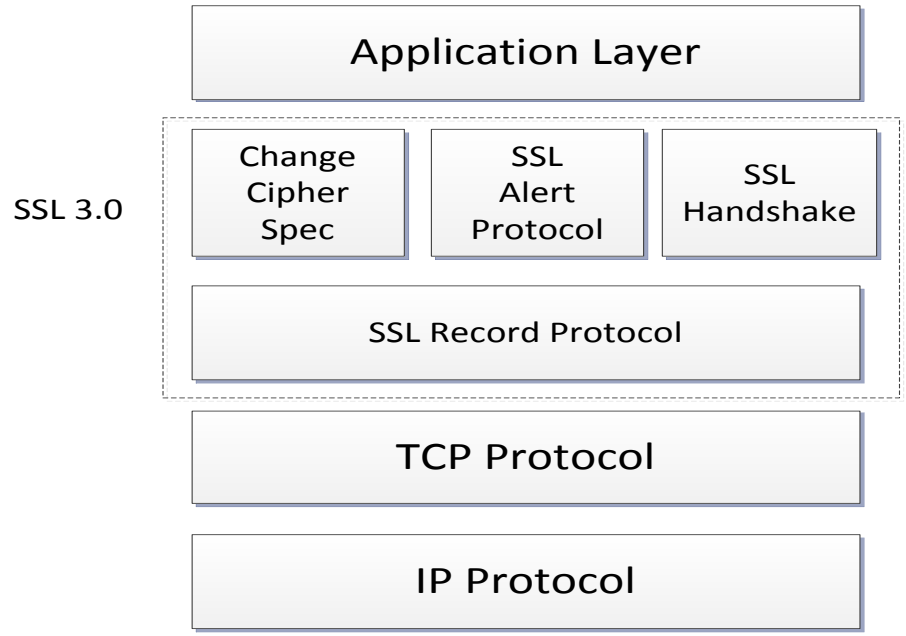


Figura 10-2: Componentes de SSL

Fuente: (Morales Vasquez, 2002)**, SSL,** Secure Sockets Layer y otros protocolos seguros para el comercio electrónico

a. **El Protocolo de registro:** se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos objeto de la comunicación.
b. **El protocolo de handshake:** el verdadero corazón de SSL está en intercambiar la clave que se utilizará para crear un canal seguro mediante un algoritmo eficiente de cifrado simétrico. También es responsabilidad de este protocolo coordinar los estados de ambos extremos de la transmisión.
c. **El protocolo de alerta:** es el encargado de señalizar problemas y errores concernientes a la sesión SSL establecida.
d. **Protocolo especial de cambio de cifrado:** Está formado por un único mensaje consistente en un único byte de valor 1 y se utiliza para notificar un cambio en la estrategia de cifrado. (Morales Vasquez, 2002)

2.10. Seguridad del protocolo internet (IPSec)

El protocolo IP, es uno de los más usados para la interconexión de redes tanto en ambientes académicos como corporativos, naturalmente lo es también en la internet pública.
Su flexibilidad y sus poderosas capacidades lo han impuesto como un vehículo de interconectividad por un largo tiempo; sin embargo, IP presenta ciertas debilidades, la forma en que el protocolo enruta los paquetes hace que las grandes redes IP sean vulnerables a ciertos riesgos bien conocidos de seguridad. (Espinoza García & Morale Luna, 2007, pág. 2)

Debido a que estas vulnerabilidades limitan y complican el uso de las grandes redes IP (incluyendo por supuesto a toda Internet), un grupo internacional organizado) bajo el grupo especial sobre ingeniería de internet (IEFT) desarrolló el IPSec, como un conjunto de extensiones para IP que ofrecen servicios de seguridad en el nivel de red (de acuerdo con el modelo de capas de ISO de OSI). La tecnología de IPSec, se basa en la criptografía moderna lo que garantiza por un lado, la privacidad y por otro una autentificación fuerte de datos. IPSec ofrece tres facilidades principales:

a) Una función de autentificación, referida como *Authentication Header* (AH).
b) Una función combinada de autentificación/encriptación llamada e*ncapsulating Security Payload* (ESP).
c) Una función de intercambio de llaves (Lujan Montes, 2005, pág. 3).

2.11. ¿Qué es una videoconferencia?

La videoconferencia es una tecnología que proporciona un sistema de comunicación bidireccional de audio, video y datos que permite que las sedes receptoras y emisoras mantengan una comunicación simultánea interactiva en tiempo real. Para ello se requiere utilizar equipo especializado que te permita realizar una conexión a cualquier parte del mundo sin la necesidad de trasladarnos a un punto de reunión. La videoconferencia involucra la preparación de la señal digital, la transmisión digital y el proceso de la señal que se recibe. Cuando la señal es digitalizada esta se transmite vía terrestre o por satélite a grandes velocidades (RIV UAEH, 2009, pág. 50).

Hoy en día la videoconferencia es una parte muy importante de las comunicaciones es por esa razón que día con día se van descubriendo nuevas aplicaciones de esta tecnología entre las aplicaciones más comunes tenemos:

- Educación a distancia
- Investigación y vinculación
- Reuniones de academia
- Formación continua

2.11.1. *Los estándares*

El mercado estuvo restringido por muchos años porque las unidades de videoconferencia manufacturadas por diferentes vendedores no eran compatibles. Es claro que la explosión que ahora experimentamos está directamente relacionada al estándar desarrollado por el grupo tres del Comité Consultivo Internacional para la Telefonía y Telegrafía (CCITT), el cual hace posible que las unidades de videoconferencia de diferentes fabricantes sean compatibles. (Morales Salcedo, 2008, pág. 63)

El primer factor es mediante la combinación de las técnicas de la codificación predictiva, la transformada discreta del coseno (DCT), compensación de movimiento y la codificación de longitud variable, el estándar hace posible el transmitir imágenes de TV de calidad aceptable con bajos requerimientos de ancho de banda, anchos de banda que se han reducido para lograr comunicaciones de bajo costo sobre redes digitales conmutadas. (RIV UAEH, 2009, http://virtual.uaeh.edu.mx/riv/videoconferencia.php)

El segundo factor que ha influido es el desarrollo de la tecnología VLSI (Very Large System Integration), la cual redujo los costos de los códec de video. Ahora en el mercado se encuentran chips mediante los cuales se pueden implantar las tecnologías DCT y de compensación de movimiento, partes del estándar. El tercer factor es el desarrollo de ISDN (Integrated Services Data Network; Red Digital de Servicios Integrados), la cual promete proveer de servicios de comunicaciones digitales conmutados de bajo costo. (RIV UAEH, 2009. http://virtual.uaeh.edu.mx/riv/videoconferencia.php)

El acceso básico de ISDN consiste de dos canales full dúplex de 64 kbps denominados canales B y un canal también full dúplex de 16 kbps. El estándar H.261 está basado en la estructura básica de 64 kbps de ISDN. Esta da nombre al título de la recomendación H.261 “Video Códec

para servicios audiovisuales a PX64 Kbps". Aunque tomará varios años para que ISDN esté disponible globalmente, los videos códec que cumplen con el estándar H.261 pueden ya operar sobre las redes de comunicaciones actualmente disponibles. (Oñate, 2009, pág. 34)

Los Estándares de la videoconferencia comúnmente utilizados:

- **Estándar H.320:** El H.320 describe normas para la videoconferencia punto a punto y multipunto en las Redes Digitales de Servicios Integrados ISDN. Este estándar gobierna los conceptos básicos para el intercambio de audio y vídeo en el proceso de comunicación.
- **Estándar H.323:** La norma H.323 proporciona una base para las comunicaciones basado en el protocolo de internet IP, definiendo la forma cómo los puntos de la red transmiten y reciben llamadas, compartiendo las capacidades de transmisión de audio, vídeo y datos.
- **Estándar H.263:** H.263 ha encontrado muchas aplicaciones en internet: gran parte del contenido en flash video (usado en sitios como YouTube, Google Video, MySpace, etc.) está codificado en formato Sorenson Spark (una implementación incompleta de H.263), aunque muchos sitios usan ahora codificación VP6 o H.264. La versión original del códec Real Video estaba basada en H.263 hasta la publicación de Real Video" (Marcellino & Mollo , 2007, pág. 67)

Las redes digitales que soportan videoconferencia son:

- RDSI: Red Digital de Servicios Integrados (1 acceso básico = 2 x 64 Kbps.= 1 BRI)
- IBERCOM: Línea digital de alta velocidad (64 Kbps. por línea)
- Satélite: Retevisión-Hispasat u otros (n x 64 Kbps. por canal)
- Punto a Punto: Líneas digitales de 64 Kbps. o 2 Mbps
- Multipunto: Líneas digitales de 64 Kbps. o 2 Mbps

Protocolos utilizados en la videoconferencia:

- **UDP (Protocolo de datagramas de usuario):** Es un protocolo que proporciona un servicio orientado a datagramas, no asegurando que los paquetes lleguen a su destino, y si llegaran no garantizando su orden. UDP es un protocolo más simple que TCP (Protocolo de Control de Transmisión), y mucho menos fiable aunque más rápido. Es útil para aplicaciones que sean simples que no necesiten de una transmisión fiable de datos, o incluso que necesiten que sus datos sean transmitidos lo más rápidamente posible. Un ejemplo de aplicaciones que utilizan UDP son aquellas aplicaciones que realizan tareas simples, TIME; que sincronizan y monitorizan redes usando SNTP (Protocolo Simple de Tiempo de Red) o SNMP (Protocolo Simple de Administración de Red), o que realizan transmisión de audio/video, usando RTP

(Protocolo de Transporte en Tiempo Real)" Introducción de Aplicaciones UDP en Redes Privadas Virtuales" (Davila , Lopez, & Román, 2010, https://www.nics.uma.es/sites /files/papers/JorgeDavila2001.pdf),

- **SIP (Protocolo de Inicio de Sesión):** Es un protocolo de internet para comunicaciones utilizados en las comunicaciones para llamadas de voz o video, permite la señalización útil para crear, modificar, finalizar sesiones de uno o más usuarios en una red IP (Protocolo de Internet), una sesión de simple llamada telefónica en dos sentidos o una sesión de videoconferencia con varios usuarios participantes.

2.12. Videoconferencia a través de VPN

Uno de los nuevos usos de las redes privadas virtuales en el área de la videoconferencia. Al igual que otros servicios de videoconferencia, esto permite a los usuarios en varios lugares llamar a un punto nodal, un código de acceso para su conferencia, y permitir que la VPN interconecte. Se trata de una "baja demanda" de servicios, lo que significa que la conexión de videoconferencia previa no requiere reservaciones. Este es un gran avance para los servicios de videoconferencia, permitiendo a los clientes la seguridad de una VPN, utilizando diferentes protocolos de red. (Sierra Rodríguez, 2008, pág. 38)

La red privada virtual permite que a través de infraestructura pública "Internet". Este servicio puede ser una gran ayuda para las empresas, con el potencial de proporcionar un enorme ahorro en los gastos de viaje, tanto entre distintos lugares de una empresa y para visitar a los vendedores. Dado que el sistema se comunica con facilidad cualquier sistema de los clientes están utilizando las videoconferencias no se limita a los sitios sólo que están en el mismo sistema.

Para cualquier empresa que necesita mantener la seguridad una VPN puede ser una alternativa económica, eficiente, para entablar una videoconferencia brindando a los clientes la velocidad y la comodidad de las VPNs estas se convierten en una excelente opción en educación, negocios.

2.13. Rendimiento de una red

El rendimiento de una red es evaluada constantemente la cual proporciona información necesaria para la toma de decisiones técnicas, empresariales, técnicas, etc., adecuadas acerca de

actualizaciones, modificaciones y ampliaciones. Los análisis que se realicen entregaran información acerca de diferentes factores que intervienen en el rendimiento, tales como colisiones, paquetes perdidos, retardos, interferencia. (Lemus Bernal , Estupiñan Cuesta, & Guillén Pinto, 2013, pág. 46)

2.13.1. *Autenticación o autentificación*

Un servicio de seguridad que permite identificar la identidad. En la seguridad de conexión, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse (García Collin, 2012, pág. 35)

2.14. Características del rendimiento de una red

Es necesario realizar supervisiones periódicas para determinar el rendimiento de la red por las siguientes razones:

- Para mejorar el rendimiento basándose en la configuración existente
- Para ofrecer capacidades de diseño y previsión
- Para obtener información del desempeño de los equipos.

El rendimiento de una red de computadores básicamente es medido de acuerdo a diferentes criterios cuantificación basados en.

- *Velocidad de transmisión,* una medida concreta de fácil cálculo la cual permite determinar si está en forma óptima trabajando.
- *Cantidad de paquetes,* la cantidad de paquetes de datos que llegan de forma íntegra desde un nodo a otro. Dado que en el traslado por el canal de conexión los datos pueden ser alterados, modificados.
- *Tiempo de respuesta,* la velocidad de traslado de la información puede ser alta pero el tiempo que demora en conectarse puede demorarse mucho. (Cevallos Rodriguez, 2006, pág. 2)

2.15. Rendimiento en redes LAN

La proximidad del diseño habitual de redes de computadora sigue un análisis de sistemas estructurados y el proceso de diseño como tal, tiene similitudes al utilizado para elaborar sistemas de aplicación los cuales siguen los siguientes pasos.

- El análisis de la red se reúne con los usuarios para determinar las necesidades y las aplicaciones que se fueran a utilizar.
- El analista realiza una proximidad del tráfico de datos en cada parte de la red. Él analista de la red diseña los circuitos necesarios para soportar este tráfico y obtener costos estimados. (Villacis Mendoza, 2009, pág. 6)

2.16. Software para realizar videoconferencia Linphone

Es una aplicación para la trasmisión de voz sobre el protocolo de internet (VoIP), para sistemas Linux, Windows, Mac, Andorid, telefonía móvil iPhone compatible con SIP (protocolo de señalización para conferencias) útil para la realización de la comunicación es de licencia GLP. Para el funcionamiento de Linphone sobre Linux, utiliza GTK+GUI puede también utilizarse desde modo consola.

2.16.1. *Códec de audio*

Speex (banda estrecha y banda ancha), G.711 (u-ley, una ley-), GSM, iLBC(a través de plug-in opcional).

- ***SPEEX:*** Transmisión de voz basada en códec libre sin patentes de software, diseñado para comprimir la voz desde 2 a 44 kbps en algo diferente a los otros códec de voz como intensidad estéreo, integrar varias frecuencias de muestreo en el mismo bitstream.
- ***G711:*** Para la codificación de audio utilizado básicamente en telefonía de código libre desde 1972, estándar digital en frecuencia de la voz humana con palabras de 8 bits, con taza de 8000 muestras por segundo, aportando un flujo de 64 kbits/s.
- ***iLBC:*** Codificador de voz gratis de banda corta creado para aplicaciones VoIP, para envíos de audio, para archivos de mensaje protocolo que puede ser transportado por RTP.

2.16.2. *Códec de video*

Linphone soporta los siguientes estándares de video: H263-1998, MPGE-4, Theora y H0.264 (plugin basado en x264), con resoluciones de QCIF (176x144) a SVGA (800x600), conforme al ancho de banda y capacidad del rendimiento CPU(Unidad Central de Proceso).

2.17. OpenVPN

Es una solución de conectividad basada en software libre: SSL (Secure Sockets Layer) VPN, OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías WiFi (redes inalámbricas IEEE 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre. (López Jimenez, 2009, http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P1)

2.18. OpenSSH

"La seguridad informática definitivamente es la parte fundamental para el buen manejo y flujo de la información, es ahí en donde en redes informáticas hablamos de protocolos en cada una de las capas del modelo TCP/IP que nos ayuden a manejar esa seguridad, uno de los protocolos que nos ofrecen seguridad y que incluyen servicios de: manejo de claves, confidencialidad, privacidad, no repudio, integridad, autenticación y autorización es OpenSSH". (Torres Carrión, 2010, pág. 3, http://dspace.ucuenca.edu.ec/handle/123456789/2535)

"SSH intenta proveer una fuerte seguridad, empleando métodos de criptografía, de forma transparente al usuario. SSH1 ofrece cuatro algoritmos de cifrado: DES, 3DES, IDEA y Blowfish. SSH2 elimina el soporte para DES (algoritmo roto) e IDEA (problemas de patentes), y añade tres nuevos algoritmos: AES, SSH1 emplea el algoritmo de autentificación RSA, mientras que SSH2 lo ha cambiado por DSA. Estos cambios fueron realizados para eliminar los problemas de patentes, IDEA y RSA, e incrementar el nivel de seguridad en SSH2 empleando algoritmos más fuertes. Además, los algoritmos de hash MD5 y SHA se emplean para asegurar la integridad de los datos, en vez del tradicional CRC empleado por SSH1" (González, Gómez, & López , 2006, https://repositorio.uam.es//implementacion_gonzalez_JCRA_2006.pdf).

2.19. OpenSwan IPSec

OPENSwan es una alternativa de software libre para crear VPN con IPSec, IPSec actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos participantes en la comunidad IPSec. No está ligado a ningún algoritmo de encriptación o autenticación, tecnología de claves o algoritmos de seguridad específico. Es más, IPSec es un marco de estándares que permite que cualquier nuevo algoritmo sea introducido sin necesitar de cambiar los estándares. IPSec está formado por un conjunto de protocolos de cifrado por securing packet flows que es el primer proceso y por el segundo proceso que key Exchange de igual manera se realiza la encapsulación y autenticación, integridad de la información.

- Encapsulating Security Payload (ESP), el cual provee autenticación, confidencialidad de datos e integridad del mensaje.
- Authentication Header (AH), provee de autenticación e integridad de datos, pero no de confidencialidad.

Por sus características es el protocolo estándar para la construcción de redes privadas virtuales, su uso es común por la seguridad que este brinda.

2.20. ¿Qué es y para qué sirve GNS3?

Simulador gráfico para el diseño de topologías de red complejas es de uso libre básicamente para la interconexión en lo permisible a un entorno real sin la implementación de hardware que puede ser costoso la adquisición de estos equipos.
Permite instalar router por medio de IOS (sistema operativo para redes), para ser configurados útil para la realización de prácticas con equipos ciertamente apegados a la realidad, al igual que permite añadir dispositivos, crear topologías, en general para habituarse al funcionamiento el GNS3 con equipos Cisco, incluso a sus errores habituales. (Microsoft, 2005, https://msdn.microsoft.com/es-es/library/cc778605%28v=ws.10%29.aspx).

Se puede descargar directamente de la red, los enlaces para descargas son variados, sitios de entrenamiento que colaboran con diferentes IOS para la creación de topologías.

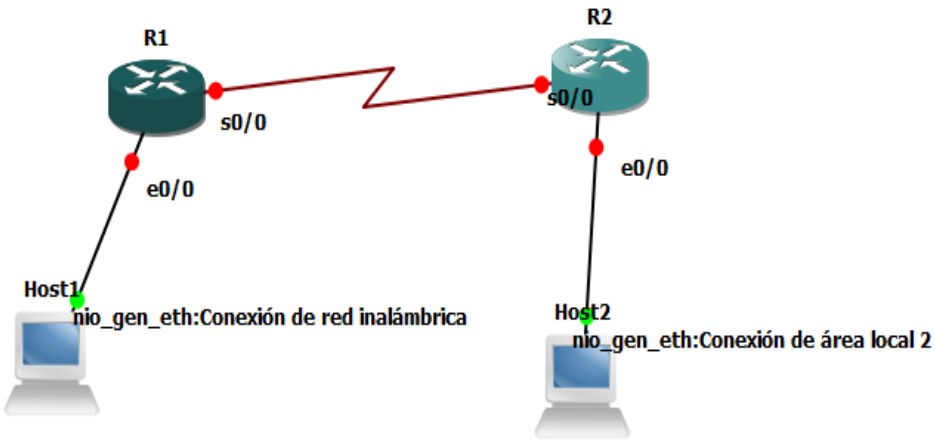


Figura 11-2: Simulador GNS3

Realizado por: Javier E. Solano Y. 2016

CAPITULO III

3. MATERIALES Y MÉTODOS

3.1. Diseño de la investigación

Por la naturaleza de la investigación se considera que el tipo de estudio es experimental, el cual se encarga del monitoreo del rendimiento: latencia, jitter, ancho de banda, porcentaje de datagramas recibidos, en cada ambiente de simulación propuesta con el uso de las arquitecturas o protocolos planteadas; SSL, SSH, IPSec, y sus efectos que se demostrará para determinar si IPSec es el mejor protocolo que se deberá implementar para la realización de videoconferencia en una VPN.

De manera experimental, partiendo de la creación de ocho ambientes de simulación de manera individual con cada protocolo, cuatro con software libre y cuatro con GNS3, teniendo en cuenta que en se implementara dos ambientes sin ningún tipo de conexión VPN únicamente interconectados. La realización de videoconferencia en tiempo real, permitirá analizar y determinar el mejor protocolo de arquitectura VPN para lo cual se plantea los siguientes:

- Establecer la videoconferencia con Linphone en Linux (Centos).
- Los objetivos de la investigación están constituidos para el análisis del rendimiento de los protocolos establecidos en los ambientes de prueba.
- Elaboración del marco teórico con la recopilación de información de cada uno de los protocolos o arquitecturas, la configuración y establecimiento de las conexiones en las VPNs.
- La hipótesis planteada busca la aceptación o no del problema de investigación con su comprobación, si la arquitectura IPSec, es la más adecuada para ser implementada en la VPN utilizada para la transmisión de videoconferencia este contraste será de manera descriptiva.
- La operacionalización de las variables están sujetas a la hipótesis expuesta.
- La recopilación de datos de las arquitecturas utilizadas en los ambientes de simulación propuestos, la recopilación de datos de las pruebas establecidos para determinar la arquitectura de mejor rendimiento utilizando software libre y con GNS3.
- Se realizará la prueba de la hipótesis con datos obtenidos en la simulación.
- Conclusiones y recomendaciones de las pruebas realizadas de las arquitecturas.

3.2. Tipo de investigación

La investigación propuesta para el análisis de las arquitecturas de conexión VPN, será del tipo; "*descriptiva y aplicada*", este tipo de investigación permitirá determinar cuáles son los efectos que tiene el rendimiento en los diferentes ambientes de simulación VPN de la videoconferencia, con software libre, GNS3 Cisco.

3.3. Métodos

Para el desarrollo del presente proyecto de investigación se utiliza los siguientes métodos de investigación:

- ***Método Científico:*** Su aplicación fundamentada en la observación de cada uno de los escenarios planteados para VPN con software libre y con GNS3, en el establecimiento de la hipótesis sí; "IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar rendimiento en la transmisión de videoconferencia". Para la comprobación de la hipótesis se plantea la realización de pruebas de cada una de las arquitecturas en seis ambientes similares con trasmisión de videoconferencia, de cada arquitectura se medirá el rendimiento de la red, al finalizar la etapa de pruebas y la recolección de la información se procederá al análisis comparativo, estadístico para emitir las conclusiones necesarias de cuál es la arquitectura de mejor rendimiento.

- ***Método Comparativo*:** Para comparar cada uno de los procesos y determinar la arquitectura de mayor rendimiento en base a la latencia (ms), jitter (ms), ancho de banda (MB/s), porcentaje de datagramas recibidos.

- ***Método Experimental, Estadístico:*** En el análisis estadístico con la prueba de la varianza ANOVA de un solo factor y la presentación de resultados en la comparación entre los diferentes protocolos de conexión VPN con una prueba complementaria post hoc de Hds de Tukey, dado que se realizará múltiples comparaciones de cada arquitectura con cada indicador de rendimiento.

3.4. Técnicas a utilizarse

Se utilizan para la recolección de información las siguientes técnicas que se detallan a continuación:

- Observación
- Revisión y estudio de documentación
- Recopilación de información
- Análisis comparativo

3.5. Validación de instrumentos

Para cuantificar los indicadores de rendimiento utilizaremos Iperf, que es una herramienta de software de tipo cliente-servidor útil para medir el jitter, ancho de banda, porcentaje de datagramas recibidos, ideal para la trasmisión de videoconferencia con protocolos de comunicación TCP, UDP, este software puede ser instalado en Linux y Windows, ejecutado desde consola los comandos son comunes en los dos sistemas operativos, los datos que entrega Iperf son cuantitativos datos numéricos lo que permitirá realizar las múltiples comparaciones de los indicadores.

Los comandos que se deben ejecutarán desde el terminal. Para el servidor de Centos o Windows:

- #iperf –s –u –f Mb –t 30 –i 1 ;

-s: identifica que esta terminal es el servidor
-u: para transmisión de videoconferencia por el protocolo UDP
-f: el ancho de banda será de Megabytes
-t: número de muestras que se desean obtener, en este caso será de treinta (30).
-i: el tiempo de demora entre cada dato en segundos es de uno (1).

El (Gráfico 1-3), presenta las capturas con el software Iperf desde el servidor en el que se identifica la el intervalo de entre las treinta muestras que es de un segundo la taza de transferencia en Kbyte, el ancho de banda por Mbyte, la interferencia o jitter esta medida por milisegundos y el porcentaje de datagramas transferidos por intervalo de tiempo.

[ID]	Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[5]	0.00-1.00 sec	64.0 KBytes	0.06 MBytes/sec	1132.235 ms	83/91 (91%)
[5]	1.00-2.00 sec	0.00 Bytes	0.00 MBytes/sec	1132.235 ms	0/0 (nan%)
[5]	2.00-3.00 sec	8.00 KBytes	0.01 MBytes/sec	1169.869 ms	229/230 (1e+02%)
[5]	3.00-4.00 sec	16.0 KBytes	0.02 MBytes/sec	1107.063 ms	0/2 (0%)
[5]	4.00-5.00 sec	8.00 KBytes	0.01 MBytes/sec	1071.074 ms	0/1 (0%)
[5]	5.00-6.00 sec	16.0 KBytes	0.02 MBytes/sec	1016.081 ms	0/2 (0%)
[5]	6.00-7.00 sec	8.00 KBytes	0.01 MBytes/sec	987.732 ms	0/1 (0%)
[5]	7.00-8.00 sec	0.00 Bytes	0.00 MBytes/sec	987.732 ms	0/0 (nan%)
[5]	8.00-9.00 sec	16.0 KBytes	0.02 MBytes/sec	1007.467 ms	47/49 (96%)

Figura 1-3: Captura de datos con Iperf servidor

Realizado por: Javier E. Solano Y. 2016

Para el cliente de Centos o Windows:

- #iperf –c <ipservidor> -u –r –f Mb –t 30 –i 1

  -c: identifica que es el cliente

  -<ip servidor>: es la dirección ip del servidor

  -r: ancho de banda bidireccional

El (Gráfico 2-3), presenta las capturas del ancho de banda, jitter, porcentaje de datagramas recibidos con Iperf del cliente, con el comodín –r, permite la captura del rendimiento en ambas direcciones.

[ID]	Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[3]	0.0- 1.0 sec	0.02 MBytes	0.02 MBytes/sec	39.019 ms	1/ 15 (6.7%)
[3]	1.0- 2.0 sec	0.02 MBytes	0.02 MBytes/sec	52.918 ms	0/ 15 (0%)
[3]	2.0- 3.0 sec	0.02 MBytes	0.02 MBytes/sec	54.170 ms	0/ 16 (0%)
[3]	3.0- 4.0 sec	0.02 MBytes	0.02 MBytes/sec	55.166 ms	0/ 15 (0%)
[3]	4.0- 5.0 sec	0.02 MBytes	0.02 MBytes/sec	55.613 ms	0/ 15 (0%)
[3]	5.0- 6.0 sec	0.02 MBytes	0.02 MBytes/sec	54.916 ms	0/ 15 (0%)
[3]	6.0- 7.0 sec	0.01 MBytes	0.01 MBytes/sec	51.906 ms	30/ 40 (75%)
[3]	7.0- 8.0 sec	0.01 MBytes	0.01 MBytes/sec	46.155 ms	91/ 96 (95%)
[3]	8.0- 9.0 sec	0.00 MBytes	0.00 MBytes/sec	45.257 ms	52/ 54 (96%)
[3]	9.0-10.0 sec	0.00 MBytes	0.00 MBytes/sec	45.429 ms	91/ 92 (99%)
[3]	0.0- 1.0 sec	0.02 MBytes	0.02 MBytes/sec	40.599 ms	0/ 15 (0%)

Figura 2-3: Captura de datos con Iperf cliente

Realizado por: Javier E. Solano Y. 2016

Para medir la latencia en Centos, Windows del cliente y del servidor con el comando ping. Este comando verifica la conectividad entre dos host. La latencia, es decir el retardo producido en la entrega de paquetes cuando se haya establecido la videoconferencia utilizando las arquitecturas de conexión VPN.

- Windows: >ping -n 30 -i 1 <ip destino>
- Centos: # ping -w 30 –i 1 <ip destino>
- n,w: determina el número de muestras para nuestro análisis que es de treinta(30).
- i: el intervalo de tiempo entre cada muestra que es de uno (1).

El (Gráfico 3-3), muestra la captura de la latencia con el comando ping de una de las terminales.

```
PING 192,168,1,31 (192,168,1,31) 56(84) bytes of data,
64 bytes from 192,168,1,31: icmp_seq=1 ttl=64 time=1,40 ms
64 bytes from 192,168,1,31: icmp_seq=2 ttl=64 time=1,00 ms
64 bytes from 192,168,1,31: icmp_seq=3 ttl=64 time=14,6 ms
64 bytes from 192,168,1,31: icmp_seq=4 ttl=64 time=17,6 ms
64 bytes from 192,168,1,31: icmp_seq=5 ttl=64 time=4,07 ms
64 bytes from 192,168,1,31: icmp_seq=6 ttl=64 time=0,903 ms
64 bytes from 192,168,1,31: icmp_seq=7 ttl=64 time=2,44 ms
64 bytes from 192,168,1,31: icmp_seq=8 ttl=64 time=9,15 ms
64 bytes from 192,168,1,31: icmp_seq=9 ttl=64 time=6,53 ms
64 bytes from 192,168,1,31: icmp_seq=10 ttl=64 time=22,6 ms
64 bytes from 192,168,1,31: icmp_seq=11 ttl=64 time=1,20 ms
```

Figura 3-3: Captura de latencia con el comando ping

Realizado por: Javier E. Solano Y. 2016

Se ha considerado el uso del software libre Iperf por las ventajas al ser utilizado en los dos sistemas operativos, al mismo tiempo puede ser ejecutado desde el cliente, servidor, entrega información detallada del tráfico de red referente a los indicadores planteados en el estudio de cada una de las arquitecturas VPNs propuesto. El comando ping para la obtención de la latencia desde los terminales de Windows y Centos.

3.6. Planteamiento de la hipótesis

“IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar el rendimiento en la transmisión de videoconferencia”.

3.7. Determinación de las variables

Las variables que serán objeto de estudio se detallan a continuación:

- **Variable Independiente:** Arquitecturas o protocolos para la conexión VPN.
- **Variable Dependiente:** Rendimiento en la transmisión de videoconferencia.

3.8. Operacionalización de variables

- **Operacionalización Conceptual**

  La (Tabla 1-3), describe la definición conceptual de las variable Independiente, Dependiente utilizadas en esta investigación.

Tabla 1-3: Operacionalización conceptual

Variable	Tipo	Definición
Arquitecturas o protocolos para la conexión VPN.	Independiente	Las Arquitecturas o Protocolos VPN permiten crear túneles y esto permite la encapsulación de la información que es transmitida.
Rendimiento	Dependiente	Generalmente el rendimiento es cuantificado, dada por la velocidad de transmisión de datos, entre las diferentes conexiones de red, otros factores influyen en el rendimiento como jitter, ancho de banda, en la videoconferencia específicamente el porcentaje de datagramas recibidos al realizarse por el protocolo UDP.

Realizado por: Javier E. Solano Y. 2016

- **Operacionalización Metodológica**

La (Tabla 2-3) describe la operacionalización metodológica de la hipótesis.

Tabla 2-3: Operacionalización metodológica

Hipótesis	Variables	Indicadores	Instrumentos
IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar el rendimiento en la transmisión de videoconferencia.	**V. Independiente** Arquitecturas o protocolos para la conexión VPN	**Protocolos SSH, SSL, IPSec**	- Guías - Manuales técnicos - OpenVPN SSL - OpenSSH SSH - OPENSwan IPSec - GNS3
	V. Dependiente Rendimiento	I.1 Latencia	- Iperf - Comando Ping - Wireshark
		I.2 Jitter	
		I.3 Ancho de banda	
		I.4 Porcentaje de datagramas recibidos	

Realizado por: Javier E. Solano Y. 2016

A continuación se detallan los indicadores de rendimiento que se utilizarán para cada arquitectura:

- *Latencia:* es el tiempo promedio de retardos temporales en la red medidos en milisegundos (ms).
- *Jitter:* es la variabilidad de tiempo en la transmisión de paquetes medido en (ms).
- *Ancho de Banda:* cantidad de información que soporta el canal de comunicación, datos que se puede enviar en una conexión de red en Mbyte/sec.
- *Datagramas recibidos:* específicamente en el uso del protocolo UDP este, no orientado a la conexión que permite obtener el porcentaje de paquetes enviados y si existe o no perdida de paquetes en la transmisión de videoconferencia.

3.9. Procesamiento de la información

Para la realización del este estudio comparativo entre los indicadores de rendimiento de las arquitecturas VPNs planteadas, se elaboran tres escenarios VPN con Linux y tres escenarios VPN con GNS3 Cisco. De cada uno de los escenarios se obtendrán datos numéricos que posteriormente serán comparados entre sí. Se validará la variable dependiente a través del monitoreo, captura del tráfico de la red, con una totalidad de treinta muestras obtenidas de cada

indicador, tomados desde el servidor y cliente a través de la transmisión de videoconferencia en tiempo real mediante el protocolo UDP (Protocolo de Datagramas de Usuario) con el comando ping y el software Iperf, estos datos serán valorados, ponderados, comparados mediante el análisis de la varianza ANOVA de un solo factor con la prueba Post hoc, HSD de tukey. Dado que el número de comparaciones a realizarse es de doce por treinta muestras de cada indicador de rendimiento.

Los escenarios de pruebas a ser desarrollados se detallan en el (ítem 3.10.3), donde se contempla el proceso de instalación, configuraciones necesarias que se deben realizar para cada escenario.

3.10. Población y muestra

A continuación se describen la población y el tamaño de la muestra utilizadas para la investigación.

3.10.1. *Población*

Para la realización de la presente investigación se consideran las arquitecturas de conexión VPNs que serán comparadas en su rendimiento con la realización de la transmisión de videoconferencia. Para lo cual es necesario establecer dos grupos de VPNs, uno con software libre y otro con GNS3 para equipos cisco, como se detallan en la (Gráfica 4-3).

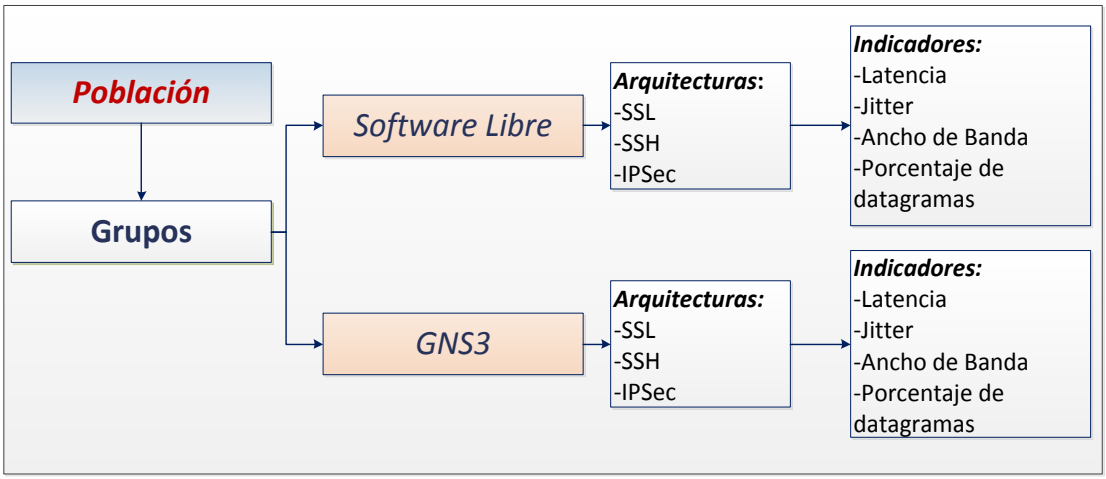


Figura 4-3: Grupos e indicadores

Realizado por: Javier E. Solano Y. 2016

3.10.2. *Muestra*

La muestra será ponderada con treinta datos numéricos obtenidas de la captura del tráfico en base al rendimiento de los diferentes indicadores la latencia, jitter, ancho de banda, porcentaje de datagramas recibidos de cada una de las arquitecturas en los ocho ambientes de simulación propuestos tres para VPN con software libre, tres con VPN GNS3, dos escenarios con videoconferencia para ser referenciados en cada grupo.

3.10.3. *Escenarios para las pruebas*

a. Los escenarios del uno al cuatro planteados en la investigación con la utilización de software libre para establecer la conexión VPN son:

- **Escenario 1.** Se establece la conexión de red y la videoconferencia sin ningún tipo de arquitectura VPN, permitiendo obtener datos referenciales de cada uno de los indicadores.

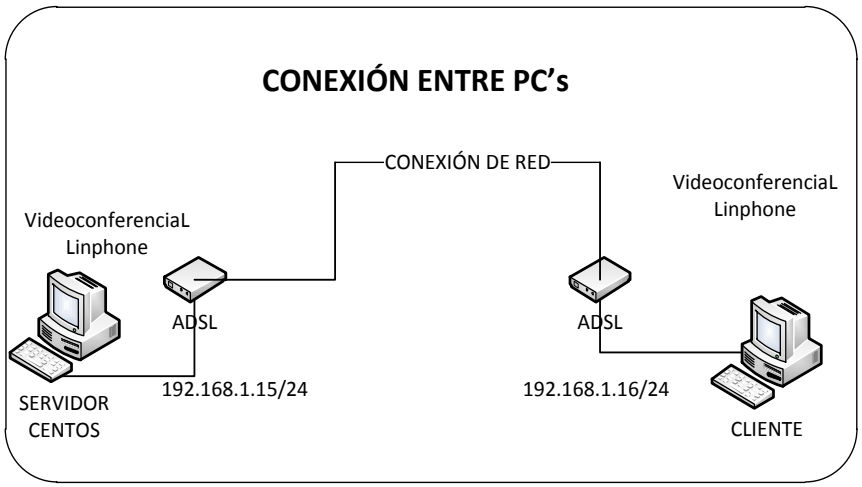


Figura 5-3: Videoconferencia software libre

Realizado por: Javier .E. Solano Y.

- **Escenario 2.** Establecimiento de la VPN con videoconferencia utilizando OpenVPN para SSL sobre Centos, permitiendo obtener datos referentes al rendimiento: la latencia, jitter, ancho de banda, porcentaje de datagramas recibidos.

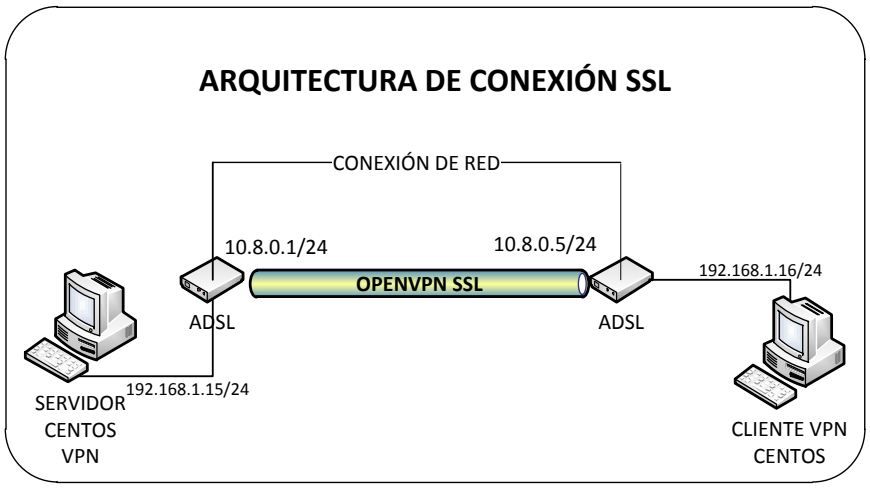


Figura 6-3: Escenario de configuración OpenVPN SSL

Realizado por: Javier E. Solano Y. 2016

- **Escenario 3.** Establecimiento de la videoconferencia con servicio VPN, utilizando OpenSSH sobre Centos, permitiendo obtener datos referentes al rendimiento: la latencia, jitter, ancho de banda, porcentaje de datagramas recibidos, evaluados con el uso de los protocolos TCP, UDP que es utilizado para la transmisión de la videoconferencia.

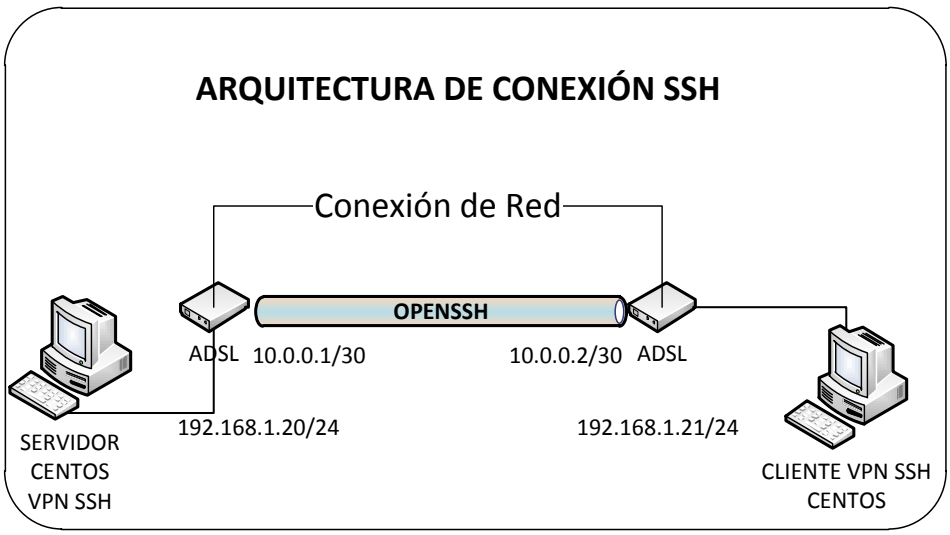


Figura 7-3: Escenario de configuración OpenSSH-Server

Realizado por: Javier E. Solano Y. 2016

- **Escenario 4.** Establecimiento de la videoconferencia con servicio VPN, utilizando OpenSwan IPSec sobre Centos, para obtener datos referentes al rendimiento.

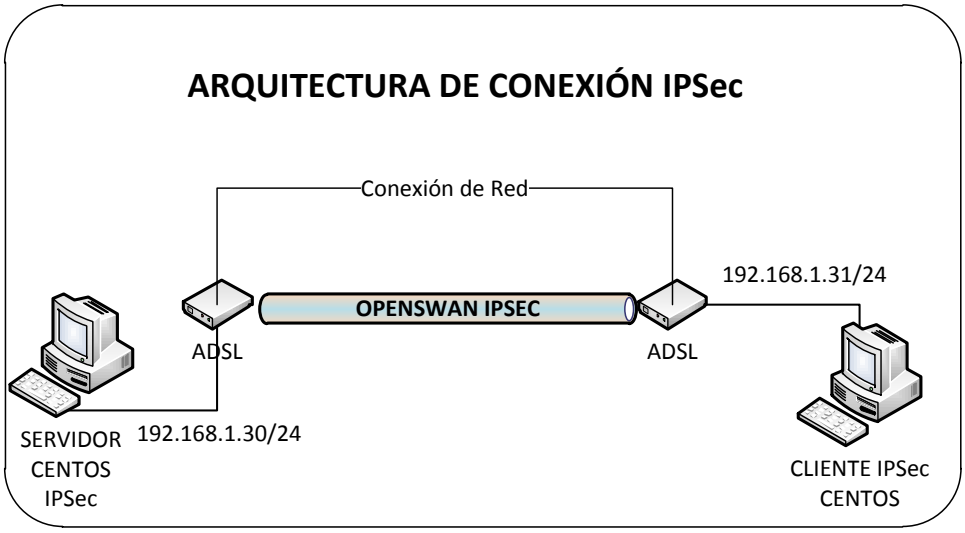


Figura 8-3: Escenario de configuración OpenSwan IPSec

Realizado por: Javier E. Solano Y. 2016

b. Los escenarios del cinco al ocho corresponden a GNS3 para establecer la conexión VPN con equipos cisco:

- **Escenario 5.** Escenario con videoconferencia sin ningún tipo de arquitectura VPN, permitiendo obtener datos referenciales de cada uno de los indicadores de rendimiento.

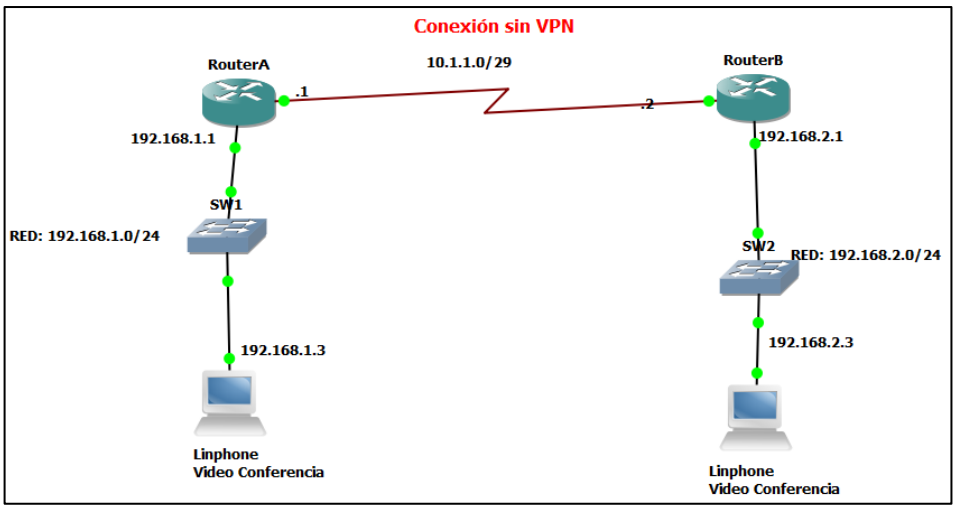


Figura 9-3: Videoconferencia con GNS3

Realizado por: Javier E. Solano Y. 2016

- **Escenario 6.** Establecimiento de la videoconferencia con servicio VPN, utilizando SSL sobre GNS3, permitiendo obtener datos referentes al rendimiento: la latencia, jitter, ancho de banda, porcentaje de datagramas recibidos que posteriormente serán analizados.

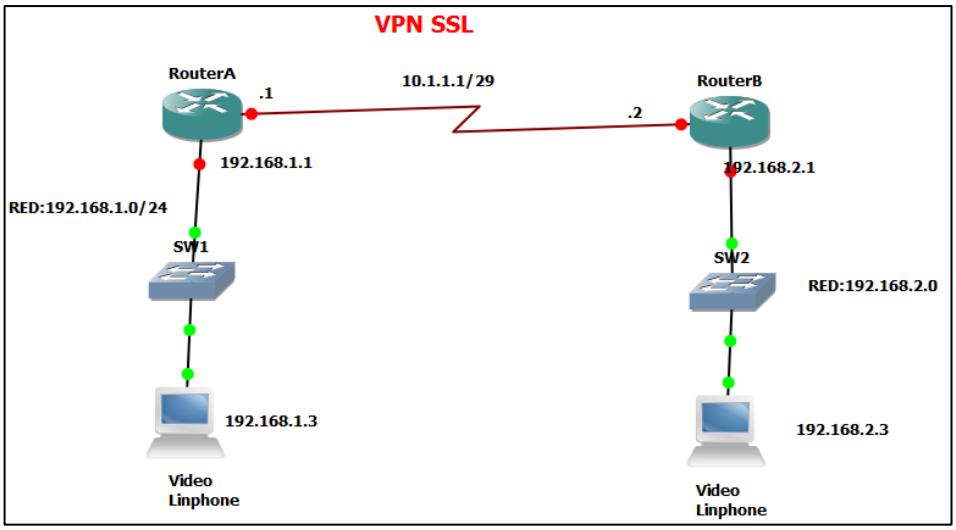


Figura 10-3: Escenario de conexión VPN SSL GNS3

Realizado por: Javier E. Solano Y. 2016

- **Escenario 7.** Establecimiento de la videoconferencia con servicio VPN, utilizando SSH sobre GNS3, permitiendo obtener datos referentes al rendimiento: la latencia, jitter, ancho de banda, porcentaje de datagramas recibidos que posteriormente serán analizados.

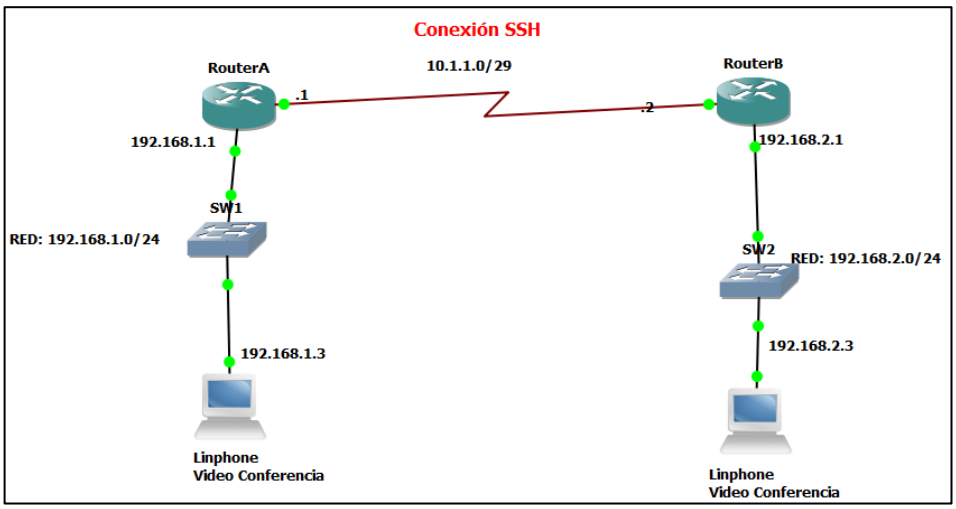


Figura 11-3: Escenario de conexión VPN SSH GNS3

Realizado por: Javier E. Solano Y. 2016

- **Escenario 8.** Establecimiento de la videoconferencia con servicio VPN, utilizando IPSec sobre GNS3, permitiendo obtener datos referentes al rendimiento: la latencia, jitter, ancho de banda, porcentaje de datagramas recibidos que posteriormente serán analizados.

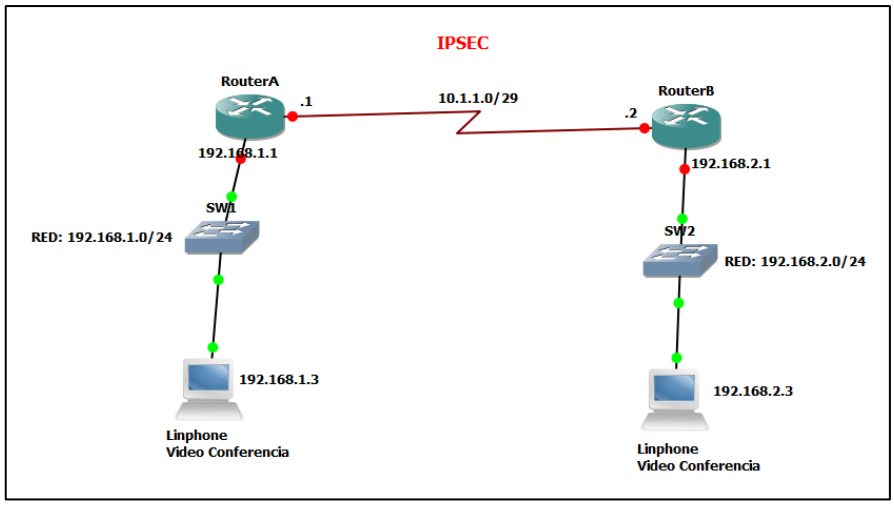


Figura 12-3: Escenario de conexión IPSec

Realizado por: Javier E. Solano Y. 2016

3.11. Implementación de los ambientes de pruebas

Se establecen los ambientes de pruebas para las diferentes arquitecturas de conexión de redes VPN con transmisión de videoconferencia, en cada uno de los escenarios propuestos (SSL, SSH, IPSec) en VPN software libre y VPN GNS3 cisco, de cada uno de ellos se obtendrá datos cuantitativos para su posterior análisis y comparación en función del rendimiento, es decir con los indicadores latencia, el jitter, ancho de banda que ocupan y porcentaje de datagramas recibidos.

Es necesario realizar configuraciones para implementar el software libre VPN sobre Centos al igual que en los router en el simulador de redes GNS3, determinar herramientas de software y hardware que permitan crear los ambientes de pruebas, estas herramientas, configuraciones permitirán efectuar estos escenarios de pruebas, los que se describen a continuación.

3.12. Requerimientos para los escenarios de pruebas

3.12.1. *Software utilizado*

a. Para los equipos de conexión en el entorno LAN

- Centos versión 6.6

- Win XP (home edition sp3)

b. Software libre para el establecimiento de la Videoconferencia

- Linphone versión 3.5.2

c. Software Libre para la creación de las VPN.

- OpenVPN SSL versión 2.2.2
- OpenVPN SSH versión 5.3p1
- OpenSwan IPSec versión 2.6.32

d. El siguiente Software será utilizado para las pruebas

- Wireshark versión 1.12.1
- Iperf-2.0.5-2-win32 para Windows, Iperf_2.0.2-4_i386.tar para Centos
- Comando ping

3.12.2. *IOS equipos utilizados para los escenarios con equipos Cisco GNS3*

Para el levantamiento de cada uno de los servicios con el simulador de redes es necesario contar con los sistemas operativos en los router que a continuación se detallan:

- Para la creación de VPN SSL se utiliza en GNS3 lo siguiente; Router Cisco 3725, con (IOS: 3725-adventerprisexa-mz124-15.bin); para generar las credenciales de autenticación SSL se utiliza: (Cliente SSL: sslclient-win-1.1.4.176.pkg).
- Para la creación de VPN SSH y IPSec se utiliza: Router Cisco 2691 con (IOS: c2691-adventerprisek9_sna-mz.124-13b.bin).
- Para el entorno de interconexión Switch 2960
- 2 Pc para el entono LAN (Local Area Network) instalados Linphone para la videoconferencia
- 1 Pc con instalación de GNS3_0.8.7.

3.13. Pasos para la creación de escenarios de pruebas software libre

3.13.1. *Escenario Nº 1; videoconferencia con conexión LAN*

a. Instalar repositorios rpmforge

Para la validación de llaves de los paquetes necesarios que serán instalados en el servidor-cliente de Centos se lo realiza con rpm-gpg-key.
Posteriormente se realiza la actualización de los repositorios con los siguientes comandos:
#wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.i686.rpm
#rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
#rpm -i rpmforge-release-0.5.2-2.el6.rf.i686.rpm

b. Instalación de paquetes complementarios

Previa la instalación de Linphone son necesarios varios paquetes que a continuación se detallan:

#yum groupinstall basic-desktop desktop-platform x11 fonts
#yum install gcc-c++ intltool gtk2-devel libosip2-devel speex- vel ffmpeg-evel libXv-devel libv4l-devel
#wget http://download.savannah.gnu.org/releases/exosip/libeXosip2-3.5.0.tar.gz
#tar vxzf libeXosip2-3.5.0.tar.gz
#cd libeXosip2-3.5.0
#./configure
#make
#make install

c. Descarga instalación de Linphone

Con los siguientes comandos procedemos a la descarga e instalación de Linphone 3.5.2.

#wget http://download-mirror.savannah.gnu.org/releases/linphone/3.5.x/sources/linphone-3.5.2.tar.gz
#tar vxzf linphone-3.5.2.tar.gz

#cd linphone-3.5.2
#./configure
#make
#make install

d. Ejecutar Linphone

Una vez instalado procedemos a la ejecución de Linphone desde la consola con el siguiente comando #linphone, de no existir problema en la instalación se ejecutará el programa como se visualiza en la (Figura 13-3):

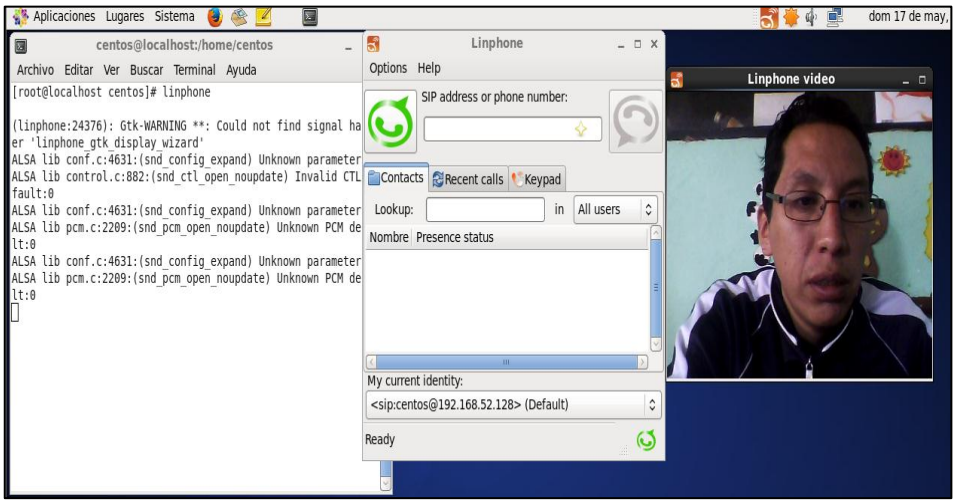


Figura 13-3: Videoconferencia con Linphone

Realizado por: Javier E SolanoY. 2016

3.13.2. *Escenario Nº 2; instalación, configuración OpenVPN SSL en Centos*

Para la instalación, configuración de OpenVPN para la arquitectura SSL se realizan los siguientes pasos:

a. Repositorios RHEL EPEL

Con los siguientes comandos actualizamos los repositorios necesarios para la descargar, instalar OpenVPN:

#wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
#wget http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
#rpm -Uvh remi-release-6*.rpm epel-release-6*.rpm
#yum install gcc make rpm-build autoconf.noarch zlib-devel pam-devel openssl-devel-y

b. Descarga de LZO-RPM

Actualización de los repositorios para OPENVPN.
#wget http://OpenVPN.net/release/lzo-1.08-4.rf.src.rpm

c. Descarga de RPMForge Repo

Actualización y descarga de repositorios RPMForge Repo
#wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.i686.rpm
#rpmbuild --rebuild lzo-1.08-4.rf.src.rpm
#rpm -Uvh lzo-*.rpm
#rpm -Uvh rpmforge-release*

d. Instalación de OpenVPN; para el servidor y el cliente
Con el siguiente comando procedemos a la instalación de OpenVPN.
#yum install OpenVPN

e. Descarga de easy-rsa-2.2.2

Realizamos la descarga y copia en el directorio cd/OpenVPN; de archivos de configuración previamente generados de certificados, llaves con contenido de ayuda de creación:

#cd /etc/OpenVPN
#wget https://github.com/OpenVPN/easy-rsa/releases/download/2.2.2/EasyRSA-2.2.2.tgz
#tar -zxvf EasyRSA-2.2.2.tgz
#cd EasyRSA-2.2.2
#cp openssl-1.0.0.cnf openssl.cnf

f. Para la creación de certificados y llaves en el servidor

Es necesario crear el siguiente el directorio que contendrá las llaves generadas para el servidor y el cliente, ya que OpenVPN crear llaves compartidas, que en lo posterior serán entregadas al cliente en forma digital. Al igual que este directorio contendrá las llaves privadas (.key), archivos de certificado (.csr) y los certificados (.crt).

#mkdir -p /etc/OpenVPN/EasyRSA-2.2.2/keys

g. Activar IP forwarding

Ponemos a Linux en modo de ruteo editando el siguiente archivo de configuración:

#vi /etc/sysctl.conf
Buscar; net.ipv4.ip_forward = 0 cambiar por; net.ipv4.ip_forward = 1

h.Generar credenciales para el servidor y el cliente

Procedemos a modificar KEY_COUNTRY, KEY_PROVINCE_, KEY_CITY, KEY_ORG Y KEY_MAIL, como se muestran en la (Figura 3-10), información necesaria referente a la ubicación de la empresa como ciudad, provincia, etc. También aquí modificamos la ruta de las llaves (KEYS), es decir la ubicación del directorio; /etc/OpenVPN/EasyRSA-2.2.2/keys.

En el caso de nuestra VPN se utilizara llave RSA que está controlada por la variable KEYSIZE, del archivo /etc/OpenVPN/EasyRSA-2.2.2/vars, utilizaremos de 2048 (bits), el archivo que contiene los permisos es: dh2048.pem, el cual contendrá las opciones del protocolo Diffie-Hellman de 2048 bits, tamaño de las llaves de encriptación tanto del servidor como del cliente, para lo cual procederemos con el siguiente comando a editar el siguiente archivo:

#vi /etc/OpenVPN/EasyRSA-2.2.2/vars

```
export KEY_SIZE=2048

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="EC"
export KEY_PROVINCE="CH"
export KEY_CITY="Riobamba"
export KEY_ORG="Maestria"
export KEY_EMAIL="maestria@hotmail.com"
export KEY_OU="Maestria"

# X509 Subject Field
```

Figura 14-3: Configuración de archivo /etc/OpenVPN/EasyRSA-2.2.2/vars

Realizado por: Javier E. Solano Y. 2016

i. Limpieza del directorio que contendrá las llaves del servidor y del cliente

Ejecutamos las siguientes comandos para limpiar todos los archivos que hayan en el directorio /keys; es decir si existieran llaves, certificados generadas para el servidor y los clientes.

#cd /etc/OpenVPN/EasyRSA-2.2.2

#chmod 755*

#source ./vars

#./clean-all

#./build-ca

```
[centos@localhost EasyRSA-2.2.2]$ source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/EasyRSA-
[centos@localhost EasyRSA-2.2.2]$ ./clean-all
[centos@localhost EasyRSA-2.2.2]$ ./build-ca
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) [EC]:
State or Province Name (full name) [CH]:
Locality Name (eg, city) [Riobamba]:
Organization Name (eg, company) [Maestria]:
Organizational Unit Name (eg, section) [Maestria]:
```

Figura 15-3: Información para generar de las credenciales

Realizado por: Javier E. Solano Y. 2016

j. Para generar el certificado del servidor

Para la generar los certificados de servidor (server) ejecutamos el siguiente comando:

./build-key-server server

En el caso de ser necesario cambiamos la información solicitada de la ciudad, estado, organización, nombre del servidor, correo electrónico como se muestra en la (Figura 16-3).

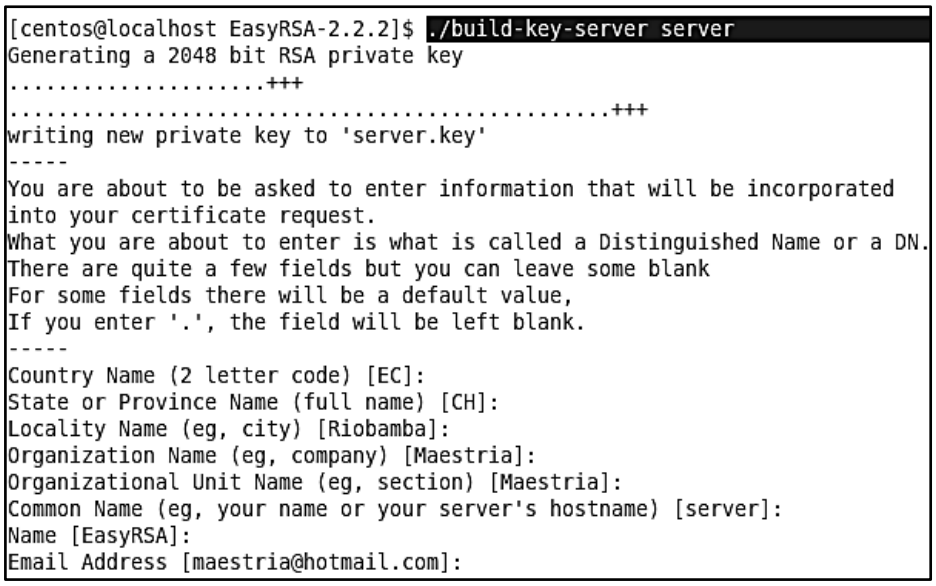


Figura 16-3: Generar certificados para el servidor

Realizado por: Javier E. Solano Y. 2016

k. Para generar los certificados de los clientes en este caso se genera cliente1

Para generar los certificados de los clientes utilizamos el siguiente comando:

#./build-key cliente1

De ser necesario cambiaremos la información requerida, caso contrario presionamos la tecla enter para aceptar los datos que se encuentran previamente atribuidos.

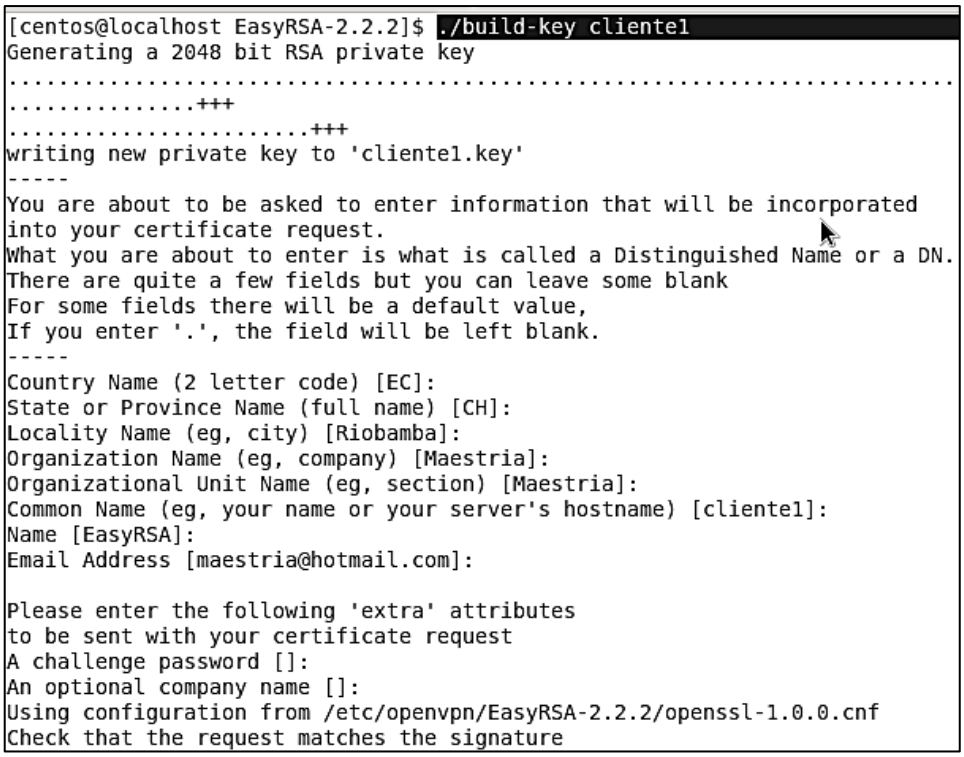


Figura 17-3: Generar certificados para el cliente

Realizado por: Javier E. Solano Y. 2016

l. Establecemos el protocolo criptográfico Diffie- Hellman de 2048bits

Para la creación de las llaves encriptadas tanto para el servidor como para el cliente lo realizamos con el comando: #./buid-dh

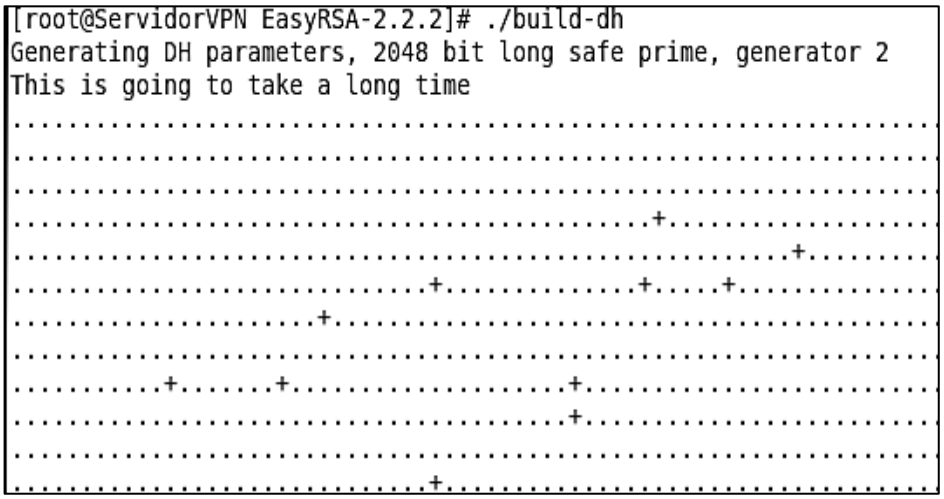


Figura 18-3: Generar llaves para el cliente

Realizado por: Javier E. Solano Y. 2016

m. Llaves generadas para los clientes y el servidor

Los archivos que contienen información para la conexión VPN del cliente son; ca.crt, cliente1.crt, cliente1.key estos archivos deben ser compartidos, copiados en el cliente, de igual manera se encuentran los archivos de configuración del servidor que son las credenciales de autenticación entre el cliente-servidor, estas llaves y los certificados del cliente-servidor se encuentran generados en el siguiente directorio (Figura 19-3).

- /etc/OpenVPN/EasyRSA-2.2.2/keys

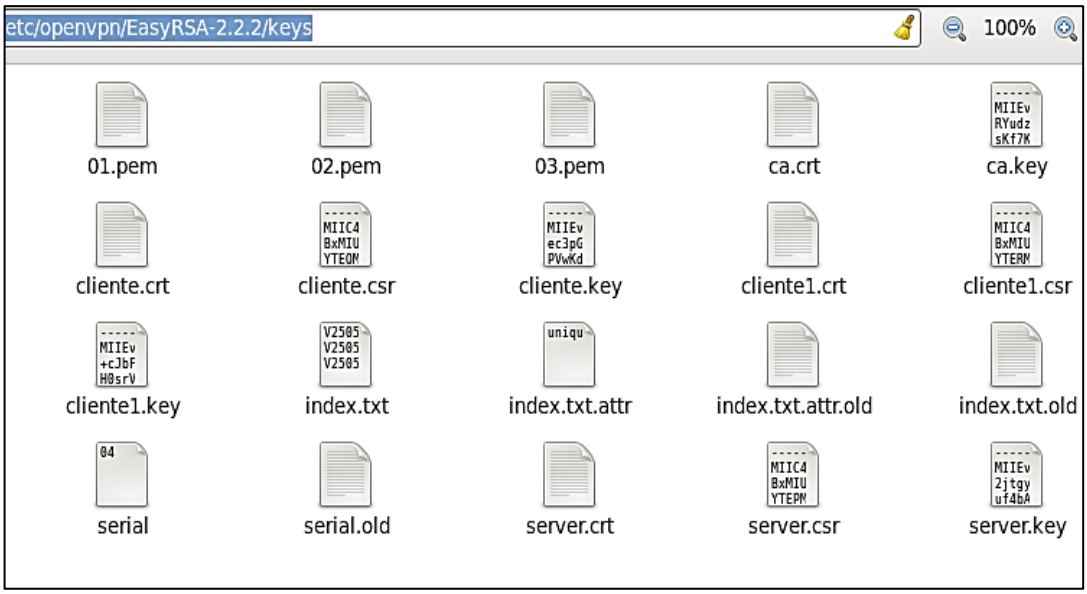


Figura 19-3: Generar llaves para el servidor

Realizado por: Javier E. Solano Y. 2016

n. Archivo de configuración del servidor OpenVPN

El archivo de configuración server.conf es el que contiene la información para la creación del túnel descrito en la (Figura 20-3), a continuación se describirá algunas de las líneas de código que contiene el archivo de configuración, el puerto que utilizara es el 1191, se debe habilitar los puertos para transmisión UDP y TCP; en modo túnel por dev TUN; la ubicación de los certificas y llaves del servidor. El rango de las IP que serán asignadas a los túneles creados por 10.8.0.0 y la red que utilizara es 192.168.161.1/24, que soporta máximo tres (3) clientes, para la edición del archivo server.conf utilizamos el siguiente comando;

vi /etc/OpenVPN/server.conf

```
#ARCHIVO DE CONFIGURACION DEL SERVIDOR /etc/openvpn/server.conf
;local a.b.c.d
port 1194
# Uso de protocol UDP o TCP
proto udp
the TUN/TAP interface.
;dev tap
dev tun
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap
# Localización de certificados
ca /etc/openvpn/EasyRSA-2.2.2/keys/ca.crt
cert /etc/openvpn/EasyRSA-2.2.2/keys/server.crt
key /etc/openvpn/EasyRSA-2.2.2/keys/server.key
# clave compartida de 2048 bit keys.
dh /etc/openvpn/EasyRSA-2.2.2/keys/dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
route 192.168.0.1 255.255.255.0
;client-to-client
keepalive 10 120
comp-lzo
max-clients 3
user nobody
group nobody
persist-key
persist-tun
log-append  /var/log/openvpn.log
verb 3
;mute 20
```

Figura 20-3: Archivo de configuración del servidor OpenVPN

Realizado por: Javier E. Solano Y. 2016

o. Configuración del cliente OpenVPN

La terminal que se utilizará como cliente debe tener previamente instalado OpenVPN. El archivo de configuración del cliente se identifica con el nombre client al inicio, además deben estar habilitados los puertos UDP, TCP, la dirección ip del servidor el número de puerto por el que se comunicaran es 1194, la ubicación del directorio de los certificados y las llaves del cliente OpenVPN.

Para editar el archivo de configuración del cliente lo realizamos con el siguiente comando:
#vi /etc/OpenVPN/cliet.conf

```
# Archivo de configuración Cliente VPN
client
;dev tap
dev tun
proto udp
proto tcp
;remote server
remote 192.168.1.15 1194
;remote-random
resolv-retry infinite
nobind
;# nobody
;#group nobody
persist-key
persist-tun
;mute-replay-warnings
# SSL/TLS parms.
ca /etc/openvpn/ca.crt
cert /etc/openvpn/client1.crt
key /etc/openvpn/client1.key
ns-cert-type server
;tls-auth ta.key 1
;cipher x
comp-lzo
verb 3
;mute 20
```

Figura 21-3: Archivo de configuración del cliente OpenVPN

Realizado por: Javier E. Solano Y. 2016

p. Reiniciar los servicios de OpenVPN

Con los siguientes comandos procedemos a reiniciar los servicios en el cliente y en el servidor.

#service OpenVPN restart

Para el servicio OpenVPN se ejecute cada inicio del servidor o cliente con el siguiente comando:

#chkconfig OpenVPN on

q. Establecimiento del túnel VPN

Una vez que se han reiniciado el servidor como el cliente verificamos la creación del túnel, este añade una interfaz temporal en nuestro equipo como se muestra en la (Figura 22-3) para el servidor tun0 con dirección ip 10.8.0.1, para el cliente en la (Figura 23-3) tun0 con dirección ip 10.8.06.

Aplicamos el siguiente comando para verificar las interfaces virtuales de red en el cliente y el servidor.

#ifconfig -a

```
[root@ServidorVPN EasyRSA-2.2.2]# ifconfig -a
eth2      Link encap:Ethernet  HWaddr 00:0C:29:EF:F2:D6
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feef:f2d6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28819 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21176 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39065897 (37.2 MiB)  TX bytes:1448385 (1.3 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:816 (816.0 b)  TX bytes:816 (816.0 b)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[root@ServidorVPN EasyRSA-2.2.2]#
```

Figura 22-3: Interfaz del túnel OpenVPN SSL servidor

Realizado por: Javier E. Solano Y. 2016

```
[root@ClienteVPN centos]# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0C:29:53:30:76
          inet addr:192.168.1.16  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe53:3076/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:652 errors:0 dropped:0 overruns:0 frame:0
          TX packets:602 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99613 (97.2 KiB)  TX bytes:67465 (65.8 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.6  P-t-P:10.8.0.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:200 (200.0 b)

[root@ClienteVPN centos]#
```

Figura 23-3: Interfaz del túnel OpenVPN SSL cliente

Realizado por: Javier E. Solano Y. 2016

r. Prueba de conectividad

Para la prueba de conectividad entre el servidor y cliente VPN SSL, utilizamos el comando ping, el resultado obtenido se muestra en la (Figura 24-3):

#ping 10.8.0.6 ; del servidor hacia el cliente

```
[root@ServidorVPN EasyRSA-2.2.2]# ping 10.8.0.6
PING 10.8.0.6 (10.8.0.6) 56(84) bytes of data.
64 bytes from 10.8.0.6: icmp_seq=1 ttl=64 time=2.44 ms
64 bytes from 10.8.0.6: icmp_seq=2 ttl=64 time=1.98 ms
64 bytes from 10.8.0.6: icmp_seq=3 ttl=64 time=1.76 ms
64 bytes from 10.8.0.6: icmp_seq=4 ttl=64 time=1.59 ms
64 bytes from 10.8.0.6: icmp_seq=5 ttl=64 time=1.94 ms
64 bytes from 10.8.0.6: icmp_seq=6 ttl=64 time=1.75 ms
^C
--- 10.8.0.6 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5454ms
rtt min/avg/max/mdev = 1.598/1.914/2.447/0.276 ms
[root@ServidorVPN EasyRSA-2.2.2]#
```

Figura 24-3: Prueba de conectividad servidor-cliente

Realizado por: Javier E. Solano Y. 2016

3.13.3. *Escenario N°3; instalación, configuración OpenSSH*

a. Instalación OpenSSH-Server

En la mayoría de las distribuciones de Centos ya se encuentra instalado OpenSSH-Server, para lo cual verificamos con el siguiente comando:

#yum list | grep OpenSSH-Server; si está instalado nos deberá mostrar lo siguiente:

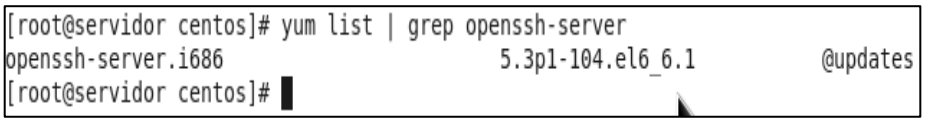


Figura 25-3: Verificación de la instalación de OpenSSH Server en Centos.

Realizado por: Javier E. Solano Y. 2016

En caso de que no esté instalado ejecutamos lo siguiente desde el terminal;
#yum install –y OpenSSH-Server.

Levantamos el demonio de OpenSSH con; #service sshd restart

b.Activar IP forwarding ; editar el archivo

Activamos en Linux el modo de ruteo editando el siguiente archivo de configuración:

- vi /etc/sysctl.conf
Cambiar;
- net.ipv4.ip_forward = 0
Por;
- net.ipv4.ip_forward = 1

c. Permisos de creación del Túnel VPN (TUN).

Para crear interfaces **TUN** será necesario que en el cliente como en el Servidor estén como root se debe editar el siguiente archivo de configuración:

#vi /etc/ssh/sshd.conf; cambiando la línea PermitTunnet yes.

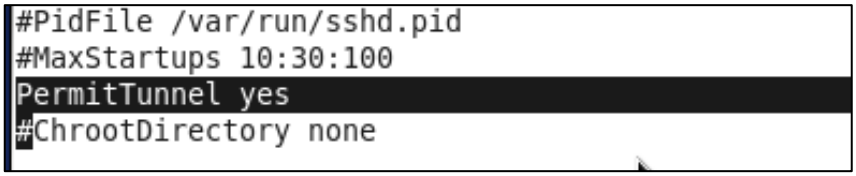


Figura 26-3: Habilitar el túnel VPN OpenSSH server.

Realizado por: Javier E. Solano Y. 2016

d. Crear la conexión OpenSSH desde el cliente hacia el servidor

Para la conexión SSH utilizamos; "-w 1:0" desde el cliente, enviando la solicitud para que se cree un túnel entre la interface virtual tun1 del cliente SSH y el interfaz virtual tun0 del servidor SSH.

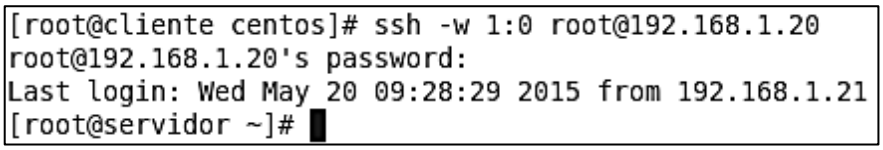


Figura 27-3: Establecer conexión SSH

Realizado por: Javier E. Solano Y. 2016

e. Interfaces virtuales VPN OpenSSH

Procedemos a la verificación de la creación del túnel en el servidor con la interfaz virtual tun0 para lo cual ejecutamos el siguiente comando:
#ifconfig tun0

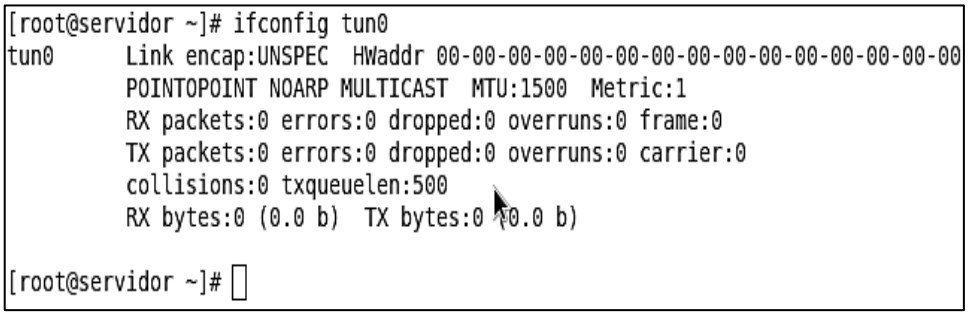


Figura 28-3: Interfaz virtual VPN tun0 en el servidor OpenSSH

Realizado por: Javier E. Solano Y. 2016

Procedemos a la verificación de la creación del túnel en el cliente en la interfaz tun1 para lo cual ejecutamos el siguiente comando: #ifconfig tun1

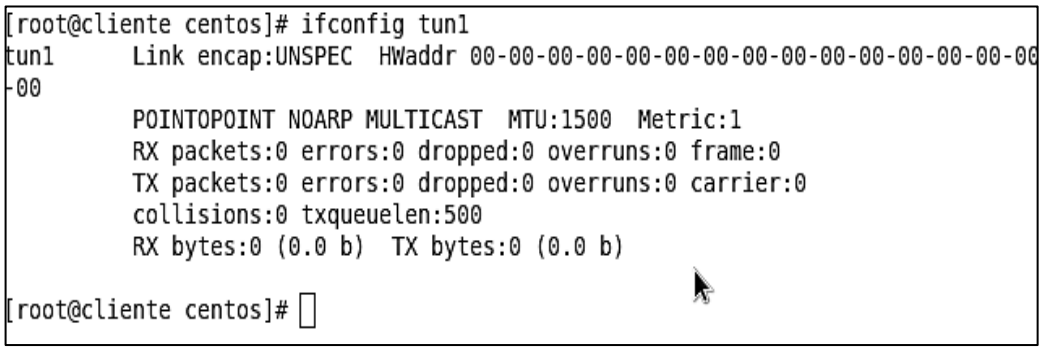


Figura 29-3: Interfaz virtual VPN tun1 en el cliente OpenSSH

Realizado por: Javier E. Solano Y. 2016

f. Asignación de direcciones IP a las interfaces virtuales

La (Figura 30-3) indica el proceso de asignación de las direcciones ip a las interfaces del túnel para el servidor la dirección ip es 10.0.0.1 con interfaz de red virtual tun0, para el cliente la dirección ip es 10.0.0.2 con interfaz de red virtual 10.0.0.1.

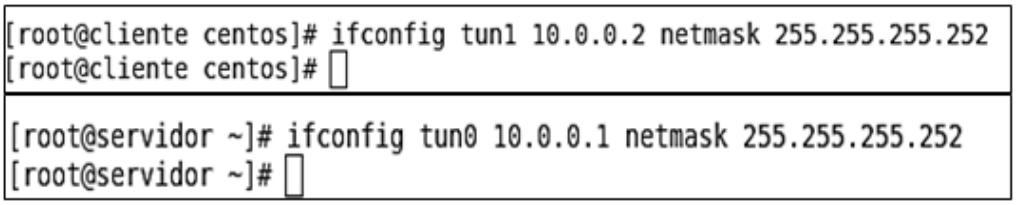


Figura 30-3: Asignación de direcciones IP a las interfaces virtuales OpenSSH

Realizado por: Javier E. Solano Y. 2016

g. Prueba de conectividad de los túneles VPN

Para la prueba de conectividad entre las interfaces virtuales del túnel tun1 que corresponde al servidor hacia la interfaz tun0 del cliente lo realizamos con los siguientes comandos:

#ping 10.0.0.1; ejecutado desde el cliente hacia el servidor
#ping 10.0.0.6; ejecutado desde el servidor hacia el cliente

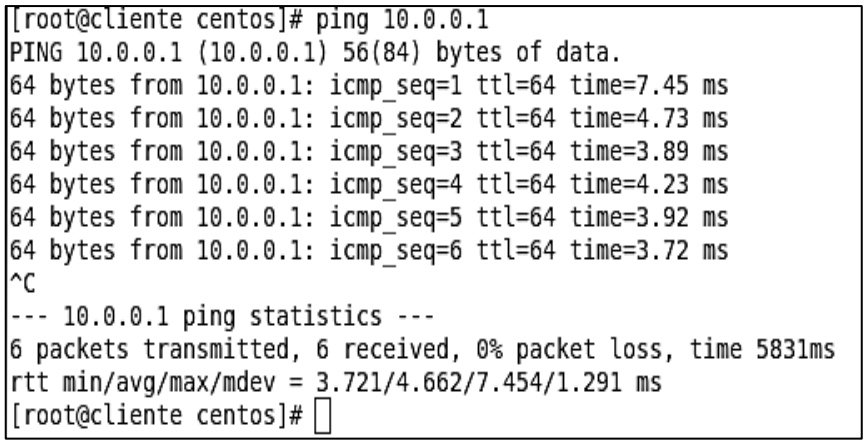


Figura 31-3: Prueba de conectividad cliente-servidor VPN OpenSSH

Realizado por: Javier E. Solano Y. 2016

3.13.4. *Escenario N°4; instalación, configuración OPENSwan IPSec*

a. Instalación de OPENSwan

La instalación de OPENSwan lo realizamos en el Cliente y en el Servidor con el siguiente comando:

#yum -y install OPENSwan

b. Configuración de IPSec con PSK (claves compartidas)

Para el escenario OPENSwan con arquitectura IPSec, utilizaremos llaves compartidas el cual consiste que en el servidor y en el cliente vamos a asignar una contraseña PSK similar la cual es "pruebaipsec" con la dirección ip del servidor 192.168.1.30 y la dirección ip del cliente 192.168.1.31 (Figura 32-3), editando el siguiente archivo:

#nano /etc/IPSec.secrets

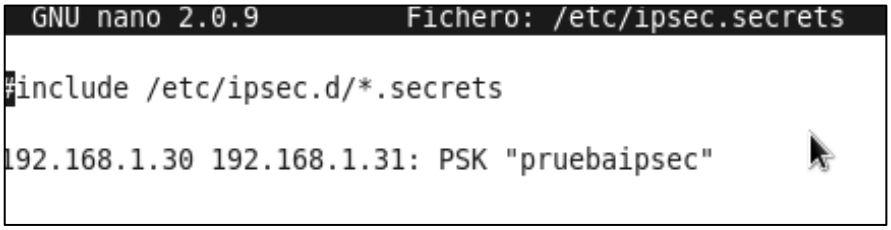


Figura 32-3: Asignar contraseña en el servidor OPENSwan

Realizado por: Javier E. Solano Y. 2016

En el cliente de igual forma ejecutamos el siguiente comando y asignamos la contraseña con la dirección ip del cliente 192.168.1.31 y la del servidor 192.168.1.30; #nano /etc/IPSec.secrets

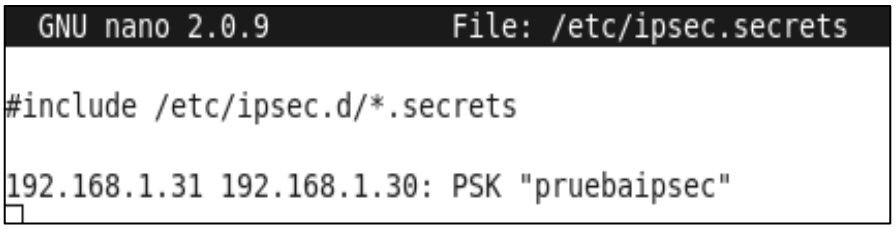


Figura 33-3: Asignar contraseña en el cliente OPENSwan

Realizado por: Javier E. Solano Y. 2016

c. Archivo de Configuración en el servidor

La (Figura 34-3) contiene la configuración del archivo del servidor OPENSwan conectado con el cliente, el algoritmo de encriptación (esp=3des-md5-modp1024), direccionado hacia la dirección IP local correspondiente al servidor (left=192.168.1.30), conectada con la dirección, IP remota correspondiente al cliente (right=192.168.1.31). Para editar el archivo de configuración en el servidor utilizamos la siguiente línea de código; #nano /etc/IPSec.conf

```
# /etc/ipsec.conf - Openswan IPsec configuration file
config setup
        # interfaces fisicas
        interfaces=%defaultroute
        # For Red Hat Enterprise Linux and Fedora, leave
        protostack=netkey
conn %default
        # Aqui ira el nombre del cliente o host
conn Cliente
        # Para empezar la conexión automáticamente
        auto=start
        # autenticación mediante clave PSK
        authby=secret
        # algoritmos de cifrado y autenticacion
        esp=3des-md5
        # algoritmos de cifrado y autenticación(fase1)
        ike=3des-md5-modp1024
# Dirección IP local
        left=192.168.1.30
# Subred local
        leftsubnet=192.168.1.0/24
# Dirección IP remota
        right=192.168.1.31
# Subred remota
        rightsubnet=192.168.1.0/24
#include /etc/ipsec.d/*.conf
```

Figura 34-3: Archivo de configuración servidor OPENSwan IPSec

Realizado por: Javier E. Solano Y. 2016

d. Archivo de Configuración del Cliente

La (Figura 35-3) contiene la configuración del cliente que se conectara con el servidor (conn Servidor), utilizando el algoritmo de encriptación (esp=3des-md5-modp1024), direccionado hacia IP local (left=192.168.1.31), conectada con la dirección IP remota (right=192.168.1.30). Para editar el archivo de configuración del cliente del servidor utilizamos la siguiente línea de código;

#nano /etc/IPSec.conf

```
# /etc/ipsec.conf - Openswan IPsec configuration file
config setup
        # interfaces fisicas
        interfaces=%defaultroute
        # For Red Hat Enterprise Linux and Fedora, leave
        protostack=netkey
conn %default
        # Para la conexión con el Servidor o nombre del host
Con Servidor
        # Para empezar la conexión automáticamente
        auto=start
        # autenticación mediante clave PSK
        authby=secret
        # algoritmos de cifrado y autenticacion
        esp=3des-md5
        # algoritmos de cifrado y autenticación(fase1)
        ike=3des-md5-modp1024
# Dirección IP local
        left=192.168.1.31
# Subred local
        leftsubnet=192.168.1.0/24
# Dirección IP remota
        right=192.168.1.30
# Subred remota
        rightsubnet=192.168.1.0/24
#include /etc/ipsec.d/*.conf
```

Figura 35-3: Archivo de configuración cliente OPENSwan IPSec

Realizado por: Javier E. Solano Y. 2016

e. Reinicio del servicio de IPSec

Reiniciamos IPSec con la siguiente línea de código:

#service ipsec restart

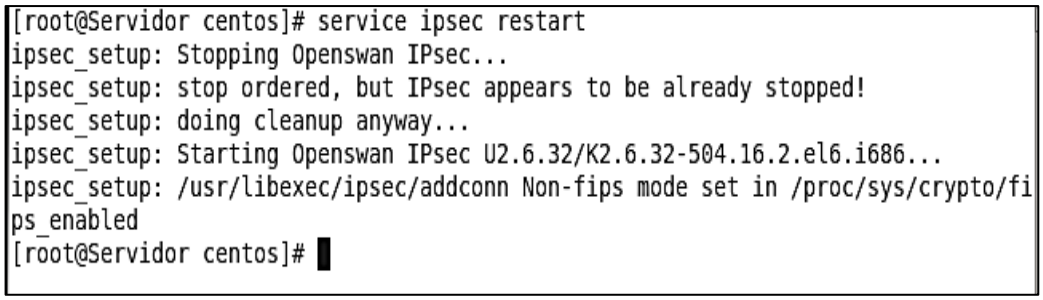


Figura 36-3: Inicio de Servicio del VPN IPSec

Realizado por: Javier E. Solano Y. 2016

f. Registro de la nueva configuración y validación de la contraseña en el servidor

Se debe Registrar en el demonio (programa que se ejecuta en segundo plano), la nueva configuración, la clave compartida PSK, del cliente en el servidor y también agregamos el nombre del cliente, levantamos el túnel con las siguientes líneas de código:

#ipsec auto --rereadsecrets
#ipsec auto -- add Cliente
ipsec auto – up Cliente

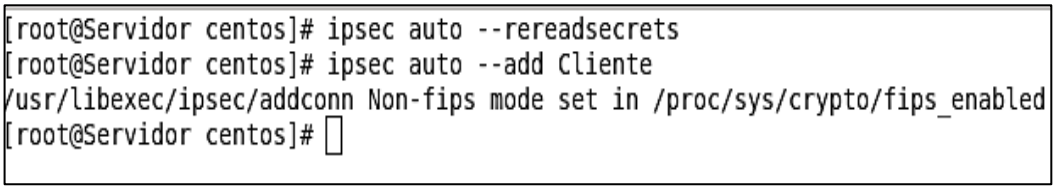


Figura 37-3: Validar clave compartida en el servidor

Realizado por: Javier E. Solano Y. 2016

g. Registro de la nueva configuración, validación de la contraseña en el cliente

Se debe registrar en el demonio, la nueva configuración, la clave compartida PSK, del servidor en el cliente y también agregamos el nombre del servidor, levantamos el túnel con las siguientes líneas de código:

#IPSec auto --rereadsecrets
#IPSec auto --add Servidor
IPSec auto --up Servidor

```
[root@cliente centos]# ipsec auto --rereadsecrets
[root@cliente centos]# ipsec auto --add Servidor
/usr/libexec/ipsec/addconn Non-fips mode set in /proc/sys/crypto/fips_enabled
[root@cliente centos]# ipsec auto --up Servidor
104 "Servidor" #7: STATE_MAIN_I1: initiate
003 "Servidor" #7: received Vendor ID payload [Openswan (this version) 2.6.32 ]
003 "Servidor" #7: received Vendor ID payload [Dead Peer Detection]
106 "Servidor" #7: STATE_MAIN_I2: sent MI2, expecting MR2
108 "Servidor" #7: STATE_MAIN_I3: sent MI3, expecting MR3
003 "Servidor" #7: received Vendor ID payload [CAN-IKEv2]
004 "Servidor" #7: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_PRESHARED_K
EY cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp1024}
117 "Servidor" #8: STATE_QUICK_I1: initiate
004 "Servidor" #8: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {E
SP=>0xde674c77 <0xb2dfaede xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=none DPD=none}
[root@cliente centos]#
```

Figura 38-3: Validar clave compartida en el cliente.

Realizado por: Javier E. Solano Y. 2016

h. Prueba de conectividad entre el servidor

Con *#tail -f /var/log/secure;* despliega la información de las acciones que realiza en el servidor; es así que con este comando se puede visualizar en la (Figura 39-3) que se encuentra establecida la comunicación con el cliente; la (Figura 40-3) se identifica que el servidor se encuentra levantado con el PID(identificador de proceso) pluto.

```
[root@servidor centos]# tail -f /var/log/secure
May 25 09:30:13 servidor pluto[3711]: "cliente" #1: received Vendor ID payload [CAN-IKEv2]
May 25 09:30:13 servidor pluto[3711]: "cliente" #1: Main mode peer ID is ID_IPV4_ADDR: '192.168.1.31'
May 25 09:30:13 servidor pluto[3711]: "cliente" #1: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4
May 25 09:30:13 servidor pluto[3711]: "cliente" #1: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_PRESHARED
akley_3des_cbc_192 prf=oakley_md5 group=modp1024}
May 25 09:30:13 servidor pluto[3711]: "cliente" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+
sing isakmp#1 msgid:0bba81c5 proposal=3DES(3)_192-MD5(1)_128 pfsgroup=OAKLEY_GROUP_MODP1024}
May 25 09:30:13 servidor pluto[3711]: "cliente" #2: transition from state STATE_QUICK_I1 to state STATE_QUICK_I
May 25 09:30:13 servidor pluto[3711]: "cliente" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode
549 <0x261bc4c7 xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=none DPD=none}
May 25 09:31:03 servidor pluto[3711]: "cliente" #3: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+
sing isakmp#1 msgid:562e2c1b proposal=3DES(3)_192-MD5(1)_128 pfsgroup=OAKLEY_GROUP_MODP1024}
May 25 09:31:03 servidor pluto[3711]: "cliente" #3: transition from state STATE_QUICK_I1 to state STATE_QUICK_I
May 25 09:31:03 servidor pluto[3711]: "cliente" #3: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode
be9 <0x947585c8 xfrm=3DES_0-HMAC_MD5 NATOA=none NATD=none DPD=none}
```

Figura 39-3: Prueba de conectividad servidor-cliente

Realizado por: Javier E. Solano Y. 2016

```
[root@servidor centos]# service ipsec --status
IPsec running  - pluto pid: 2859
pluto pid 2859
1 tunnels up
```

Figura 40-3: Estado del servicio IPSec en el servidor

Realizado por: Javier E. Solano Y. 2016

i. Prueba de conectividad entre el cliente

Con *#tail -f /var/log/secure;* despliega la información de las acciones que realiza en el cliente; es así que con este comando se puede visualizar en la (Figura 41-3) que se encuentra establecida la comunicación con el servidor; en la (Figura 42-3) se identifica que el servidor se encuentra levantado con el PID(identificador de proceso) pluto.

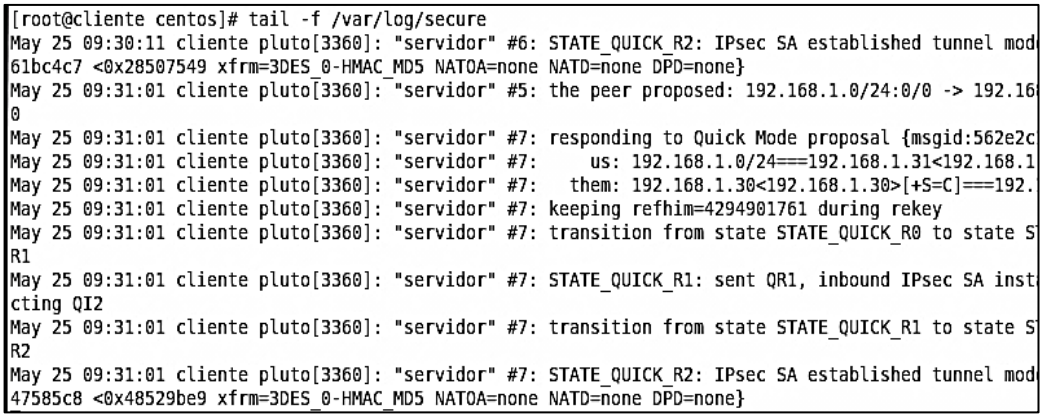


Figura 41-3: Prueba de conectividad IPSec cliente

Realizado por: Javier E. Solano Y. 2016

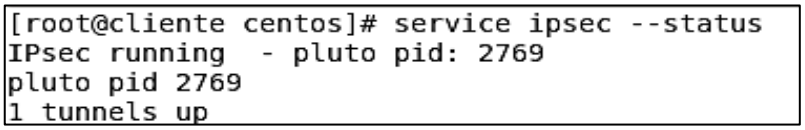


Figura 42-3: Estado de servicio IPSec cliente

Realizado por: Javier E. Solano Y. 2016

3.14. Proceso para la creación de los escenarios de pruebas GNS3 cisco

3.14.1. *Escenario Nº 5; conexión, conectividad de la red*

a. Configuraciones de los Router A y B

Las primeras configuraciones a desarrollarse son similares en los escenarios seis, siete, ocho para tener conectividad entre los Routers A y B con la instrucción (ip route) como se describen en la siguiente (Figura 43-3), (Figura 44-3):

```
RouterA#conf t
RouterA(config)#int s0/0
RouterA(config-if)#ip address 10.1.1.1 255.255.255.248
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config-if)#int f0/0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config-if)#ip route 192.168.2.0 255.255.255.0 s0/0
```

Figura 43-3: Direccionamiento ip, ruteo RouterA

Realizado por: Javier E. Solano Y. 2016

```
RouterB#conf t
RouterB(config)#int s0/0
RouterB(config-if)#ip address 10.1.1.2 255.255.255.248
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config-if)#int f0/0
RouterB(config-if)#ip address 192.168.2.1 255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config-if)#ip route 192.168.1.0 255.255.255.0 s0/0
```

Figura 44-3: Direccionamiento ip, ruteo RouterB

Realizado por: Javier E. Solano Y. 2016

3.14.2. *Escenario N°6; configuración VPN SSL cisco GNS3*

Para VPN SSL es necesario crear conexión SSH para la autenticación, instalación del archivo Winssl para el cliente Windows, esto permitirá llevar a cabo la autenticación del acceso remoto.

a. Configuraciones SSH en el ROUTER A

- Creamos el usuario vpnssl con modo de acceso privilegiado alto identificado con quince y con password prueba123.
- Habilitar el router http , el servidor https con los comandos ip http:
- Configurar SSH para la conexión local y el nivel de privilegio quince (15).

```
RouterA(config)#username vpnssl privilege 15 password prueba123
RouterA(config)#ip http server
RouterA(config)#ip http secure-server
RouterA(config)#ip http authentication local
RouterA(config)#line vty 0 4
RouterA(config-line)#login local
RouterA(config-line)#transport input ssh
RouterA(config-line)#exit
```

Figura 45-3: Configuración del SSH en el Router A

Realizado por: Javier E. Solano Y. 2016

b. Configuración WEBVPN SSL

```
RouterA(config)#ip local pool sslpool 192.168.1.21 192.168.1.31
RouterA(config)#aaa new-model
RouterA(config)#aaa authentication login webssl local
RouterA(config)#webvpn gateway maestria-gateway
RouterA(config-webvpn-gateway)#ip address 192.168.1.1 port 443
RouterA(config-webvpn-gateway)#ssl encryption rc4-md5
RouterA(config-webvpn-gateway)#do show run | b crypto
RouterA(config-webvpn-gateway)#do show run | b crypto
crypto pki certificate chain TP-self-signed-4279256517
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 34323739 32353635 3137301E 170D3032 30333031 30303034
  33335A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
RouterA(config-webvpn-gateway)#ssl trustpoint TP-self-signed-4279256517
RouterA(config-webvpn-gateway)#inservice
RouterA(config-webvpn-gateway)#exit
RouterA(config)#webvpn context maes-webvpn
RouterA(config-webvpn-context)#title "maestria-webvpn"
RouterA(config-webvpn-context)#login-message "webvpn login"
RouterA(config-webvpn-context)#aaa authentication list webssl
RouterA(config-webvpn-context)#gateway maestria-gateway
RouterA(config-webvpn-context)#max-users 10
RouterA(config-webvpn-context)#url-list "MisPaginas"
RouterA(config-webvpn-url)#heading "MisPaginas"
RouterA(config-webvpn-url)#url-text maestriaweb url-value "http://maestriaweb.local"
RouterA(config-webvpn-url)#acl webvpn-acl
RouterA(config-webvpn-acl)#permit ip 192.168.1.0 255.255.255.0 192.168.1.0
255.255.255.0
```

Figura 46-3: Configuración SSL GNS3.

Realizado por: Javier E. Solano Y. 2016

- Con ip local pool; se configura un grupo de direcciones válidas que serán asignadas a los túneles VPN.
- Con aaa asignamos direcciones de VPN a clientes de acceso remoto.
- Webvpn permite a los usuarios establece un acceso remoto VPN túnel seguro utilizando un navegador web.
- En la siguiente (Figura 46-3) con el comando: trustpoint *TP-self-signed-4279256517* se establece la contraseña cifrada de acceso web hacia al router; el comando inservice para activar el usuario: vpnssl y contraseña: prueba123
- Instalación de sslclient-win-1.1.4.176.pkg; para activar del cliente SSL, para que sea generado el certificado del cliente VPN SSL.

c. Configuraciones necesarias en el ROUTER B

En el ROUTER B solo es necesario una configuración básica de conexión y direccionamiento IP en la interfaces al igual que crear una ruta con el comando ip route como se muestra en la (Figura 47-3).

```
RouterB#conf t
RouterB(config)#int s0/0
RouterB(config-if)#ip address 10.1.1.2 255.255.255.248
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#int f0/0
RouterB(config-if)#ip address 192.168.2.1 255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config)#ip route 192.168.1.0 255.255.255.255.0 s0/0
```

Figura 47-3: Configuración del RouterB.

Realizado por: Javier E. Solano Y. 2016

d. Configuraciones Clientes VPN SSL

- Para accede a la aplicación Webvpn SSL lo hacemos desde el navegador con https://192.168.1.1. Que es la puerta de enlace del ROUTERA.
- Para lo cual es necesario registrar el nombre de usuario: vpnssl y la contraseña: prueba123 como se identifica en la siguiente figura.

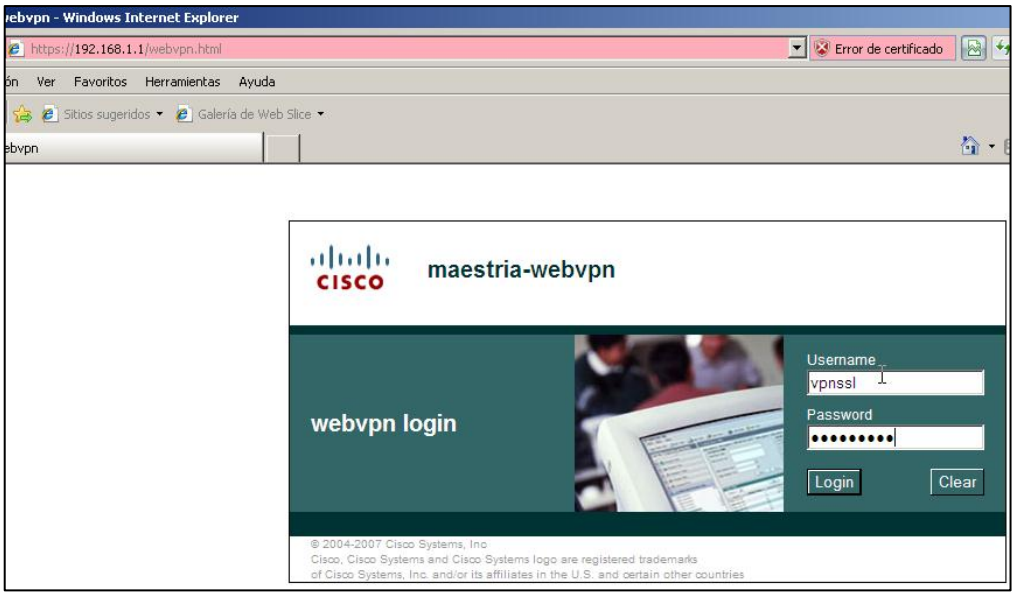


Figura 48-3: Conexión web con el servidor Webvpn

Realizado por: Javier E. Solano Y. 2016

- Luego que las credenciales de autenticación se hayan validado ingresamos a la interface de creación del tunel para la activación damos un clic en (Tunnel Connection clic botón Start), esto permitirá que se inicie el túnel.

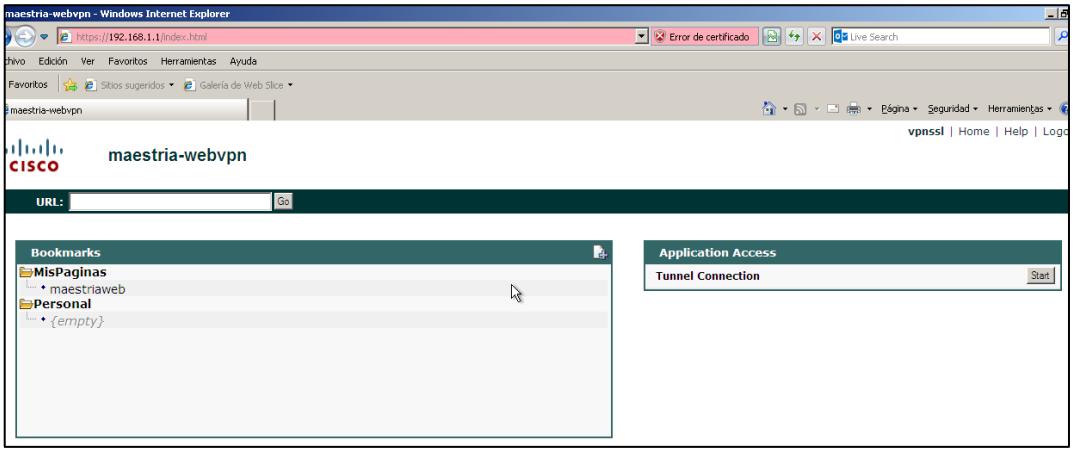


Figura 49-3: Ventana de configuración web de inicio del túnel cliente SSL

Realizado por: Javier E. Solano Y. 2016

- La conexión del túnel empieza con la validación de las credenciales (Figura 50-3), desde el cliente el cual permitirá la instalación de los certificados:

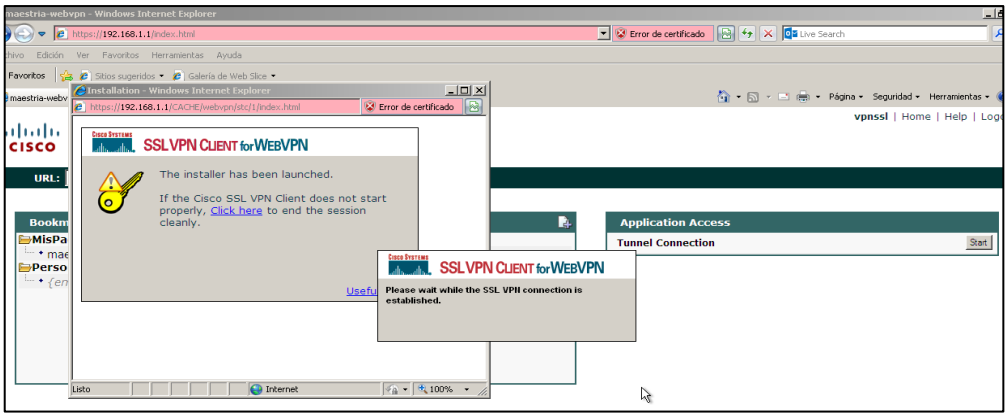


Figura 50-3: Validación de credenciales del cliente para inicio de sesión SSL

Realizado por: Javier E. Solano Y. 2016

- La (Figura 51-3), proceso de instalar certificados, SSL VPN Client for Webvpn en el cliente VPN Windows, +correspondientes al certificado de conexión: *TP-self-signed-4279256517*, para el establecimiento de la conexión SSL VPN cliente

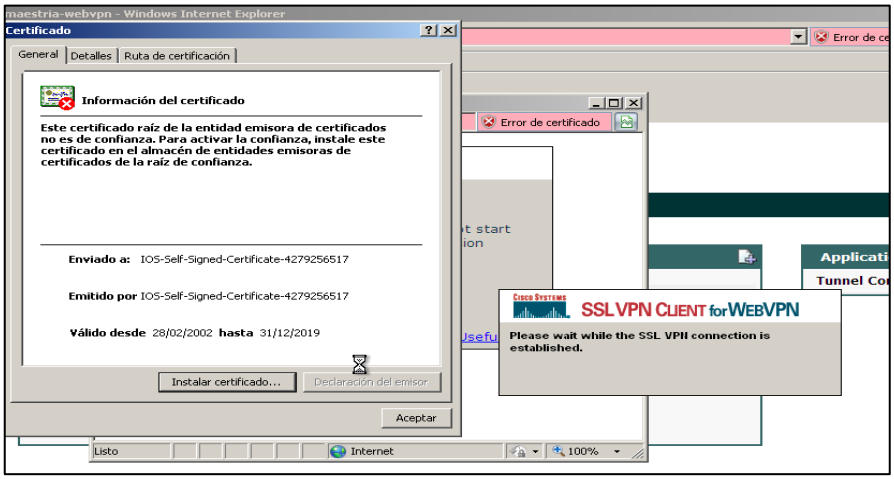


Figura 51-3: Instalar credenciales de autenticación cliente Webvpn SSL

Realizado por: Javier E. Solano Y. 2016

e. Si todo está correctamente configurado y validado en la barra de tareas del cliente se mostrara el mensaje de la conexión establecida y aparece una llave (Figura 52-3).

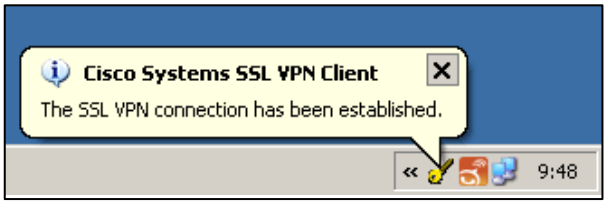


Figura 52-3: Establecimiento de la conexión

Realizado por: Javier E. Solano Y. 2016

f. Para verificar la creación de la interfaz virtual cisco SSL VPN, desde el terminal con el comando >ipconfig; el cual permite visualizar la nueva interfaz se encuentra creada y activa, sino se muestra una nueva interface de red quiere decir que el túnel no se ha establecido en el cliente, en la (Figura 53-3) se identifica la dirección 192.168.1.21 que le corresponde al túnel VPN SSL del cliente 1.

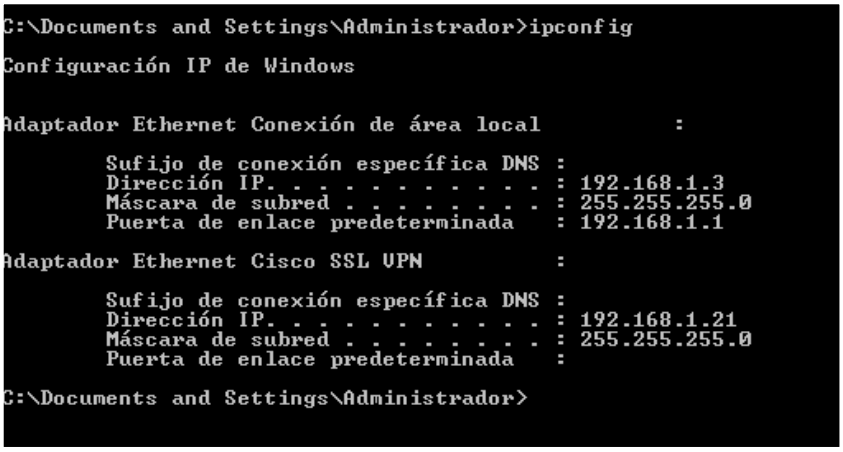


Figura 53-3: Verificación adaptador SSL del cliente uno.

Realizado por: Javier E. Solano Y. 2016

Con el comando ipconfig se identifica en (Figura 54-3) que la dirección correspondiente al túnel VPN SSL le corresponde la dirección ip 192.168.1.22, también se identifica que la dirección ip de la interfaz física le corresponde 192.168.2.3, en donde se interpreta que VPN SSL cisco crea una interfaz virtual adicional a la interfaz física del terminal cliente, por la que la información será enviada y receptada.

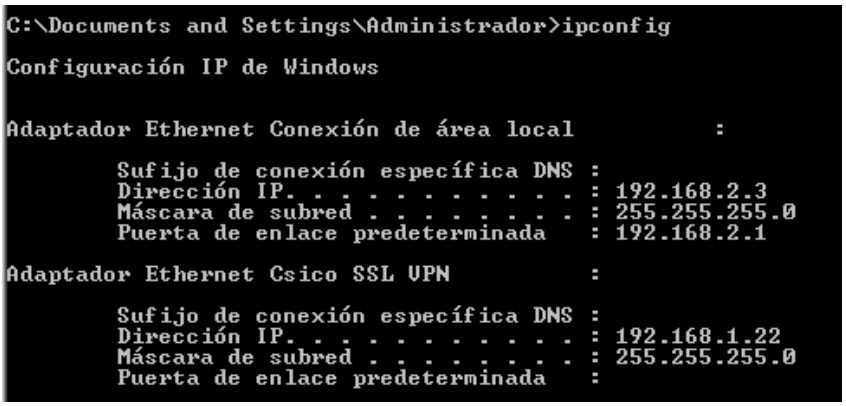


Figura 54-3: Verificación adaptador SSL del cliente dos

Realizado por: Javier E. Solano Y. 2016

g. Se puede verificar la creación de la interfaces desde el administrador de configuraciones de red, se visualiza el adaptador de red conectado y perteneciente al adaptador SSL VPN en el cliente1 y cliente2.

Figura 55-3: Interfaz de red VPN SSL conectada

Realizado por: Javier E. Solano Y. 2016

3.14.3. *Escenario N°7; configuración VPN SSH cisco GNS3*

a. Configuraciones SSH ROUTER A

Creamos el usuario vpnssh en modo de acceso privilegiado alto identificado con quince y con password prueba123. Con ip hhtp secure-server; se genera la contraseña RSA de 1024 bits. Habilitar el router http o el servidor https con los siguientes comandos (Figura 56-3), para verificar conectividad utilizamos el comando ping a la dirección ip del RouterB 10.1.1.2.

```
RouterA(config)#username vpssh privilege 15 password prueba123
RouterA(config)#ip http server
RouterA(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar  1 00:32:37.455: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Mar  1 00:32:39.099: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new certificate
RouterA(config)#ip http authentication local
RouterA(config)#line vty 0 4
RouterA(config-line)#login local
RouterA(config-line)#transport input ssh
```

Figura 56-3: Configuración de SSH GNS3 cliente uno

Realizado por: Javier E. Solano Y. 2016

b. Configuraciones SSH ROUTER B

Creamos el usuario vpnssh1 con modo de acceso privilegiado alto identificado con quince y con password prueba123. Con ip hhtp secure-server; se genera la contraseña RSA de 1024 bits.

Configurar SSH para la conexión local y el nivel de privilegio quince, este proceso lo repetimos similar a la configuración del RouterA (Figura 57-3).

```
RouterB(config)#username vpssh1 privilege 15 password prueba123
RouterB(config)#ip http server
RouterB(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar  1 00:40:40.455: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Mar  1 00:42:09.099: %PKI-4-NOAUTOSAVE: Configuration was
RouterB(config)#ip http authentication local
RouterB(config)#line vty 0 4
RouterB(config-line)#login local
```

Figura 57-3: Configuración de SSH GNS3 cliente dos

Realizado por: Javier E. Solano Y. 2016

3.14.4. *Escenario N°8; configuración VPN IPSec cisco con GNS3*

a. Configuración de IPSec ROUTER A

```
RouterA(config)#crypto isakmp policy 10
RouterA(config-isakmp)#authentication pre-share
RouterA(config-isakmp)#hash sha
RouterA(config-isakmp)#encryption aes 256
RouterA(config-isakmp)#group 5
RouterA(config-isakmp)#lifetime 3600
RouterA(config-isakmp)#exit
RouterA(config)#crypto isakmp key 0 prueba123 address 10.1.1.2
RouterA(config)#crypto isakmp keepalive 10 2 periodic
RouterA(config)#end
RouterA#configure terminal
RouterA(config)#crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
RouterA(cfg-crypto-trans)#mode tunnel
RouterA(cfg-crypto-trans)#end
RouterA#configure terminal
RouterA(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
RouterA(config)#end
RouterA(config)#crypto map RouterA_to_RouterB 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
RouterA(config-crypto-map)#set peer 10.1.1.2
RouterA(config-crypto-map)#match address 101
RouterA(config-crypto-map)#set transform-set myset
RouterA(config-crypto-map)#end
RouterA#configure terminal
RouterA(config)#interface serial 0/0
RouterA(config-if)#crypto map RouterA_to_RouterB
*Mar  1 00:42:39.887: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
RouterA(config-if)#exit
```

Figura 58-3: Configuración de IPSec en el RouterA

Realizado por: Javier E. Solano Y. 2016

La (Figura 58-3) visualiza las instrucciones para la creación del túnel VPN IPSec; con isakmp policy; configuramos los parámetros IKE que serán utilizados mediante el intercambio secreto de claves de tipo Diffie-Hellman, con contraseñas compartidas. transform-set configura los parámetros necesarios que serán utilizados IKE para la creación del túnel. ACL crea o define que direcciones IP permitirá el acceso a la VPN. crypto map configura los parámetros de conexión entre el ROUTERA to ROUTERB, en las interfaces de red, la misma configuración se realiza en el RouterB.

b. Prueba de conectividad IPSec

Para la prueba de creación del túnel IPSec lo hacemos desde el terminal del RouterB con show crypto sesión, estas instrucciones permiten visualizar si la sesión túnel VPN se encuentra activa (Figura 59-3).

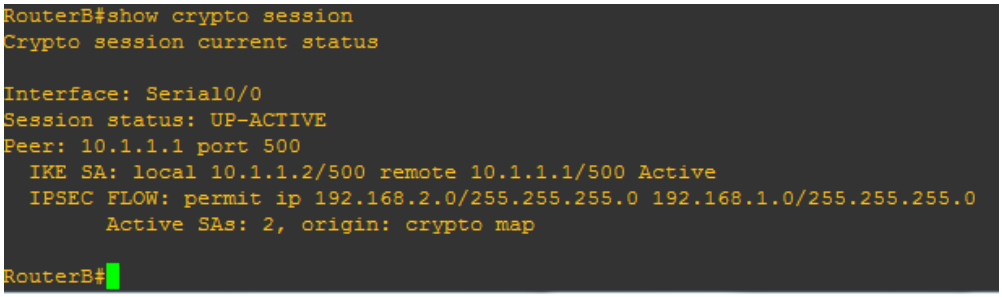


Figura 59-3: Establecimiento, inicio de sesión IPSec.

Realizado por: Javier E. Solano Y. 2016

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

Esta investigación está enfocada en el estudio del rendimiento de varias de las arquitecturas utilizadas en la conectividad VPN (SSL, SSH, IPSec), estas arquitecturas o protocolos son implementadas con software libre y con el simulador de equipos Cisco GNS3, para la transmisión de videoconferencia mediante el software Linphone.

Los escenarios dos, tres y cuatro son creados con software libre (OpenVPN para SSL, OpenSSH para SSH, OPENSwan para IPSec). Los escenarios seis, siete, ocho, implementados en el simulador de redes GNS3 de equipos Cisco. Los escenarios uno, cinco tendrán una conexión de enrutamiento básica es decir lo único que permiten realizar es videoconferencia; en lo posterior para referirnos a estos dos escenarios lo aremos como conexión.

El rendimiento será analizado en los diferentes escenarios con treinta muestras, tomados de la transmisión de videoconferencia en tiempo real de cliente-servidor de cada indicador plateado, estos escenarios serán ponderados, analizados y comparados a través de datos cuantificando su rendimiento lo que permitirá demostrar la hipótesis planteada.

Por lo tanto se mide los efectos que la variable independiente produce sobre la variable dependiente. Los parámetros de verificación de rendimiento que se establecen como indicadores son:

- I1. Latencia: el tiempo promedio de retardos temporales en la red.
- I2. Jitter: variabilidad de tiempo en la transmisión de paquetes.
- I3. Ancho de Banda: Cantidad de información, datos que se puede enviar en una conexión de red.
- I4. Datagramas recibidos: específicamente este validará el uso del protocolo UDP el que permite determinar el porcentaje de paquetes enviados en la transmisión de videoconferencia.

Se realizara la tabulación de cada uno de los indicadores al igual que se compara cada indicador estos datos están representados en las tablas, graficas que a continuación se detallan, la

validación de la hipótesis está dada por el análisis de la varianza ANOVA de un factor con la prueba post hoc HSD de Tukey.

4.1. Análisis de la variable dependiente rendimiento

Luego de obtener datos cuantitativos de los parámetros establecidos del rendimiento, se mide la latencia con el comando ping, con el software libre Iperf se mide el jitter, ancho de banda y el porcentaje de datagramas recibidos. Procedemos a las comparaciones para establecer el mejor protocolo de conexión VPN en la realización de videoconferencia con Linphone, con software libre y con GNS3 por separado.

4.2. Muestras, análisis comparativo entre el servidor-cliente de los diferentes indicadores de rendimiento con software libre

4.2.1. *Indicador I.1: Latencia*

Para el análisis de *latencia* se tomaron treinta (30) muestras de los escenarios uno, dos, tres, cuatro del servidor y del cliente para realizar el análisis comparativos entre las diferentes arquitecturas de conexión VPN en la (Tabla 1-4).

Tabla 1-4: Latencia con software libre para la conexión VPN servidor-cliente

TOMA DE 30 MUESTRAS LATENCIA (ms)								
N° DE MUESTRAS	CONEXION		OPENVPN SSL		OPENSSH SSH		OPENSWAN IPSEC	
	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente
1	3,17	13,6	13,6	7,38	2,03	2,25	1,4	5,42
2	1,62	3,17	13,5	1,68	1,18	1,31	1	3,6
3	4,61	27,4	6,92	2,1	8,83	3,27	7	2,41
4	11	4,36	11,7	5,11	1,47	1,5	6	2,88
5	10	2,09	5,6	4,02	1,16	2,26	4,07	5,7
6	3,9	2,6	1,6	1,74	12,3	4,39	0,903	2,62
7	2,61	1,41	3,35	3,74	1,33	1,99	2,44	7,19
8	4,85	5,04	4,93	9,3	10,1	1,42	9,15	0,67
9	2,62	4,28	1,85	2,79	1,75	1,46	12,53	3,87
10	0,482	1,49	3,72	4,05	2,97	3,22	8	8,7
11	1,14	3,15	5,53	1,57	1,81	1,29	1,2	5,04

12	13,9	11,2	11,7	2,93	1,71	1,62	3,29	8,4
13	5,49	1,17	7,13	6,23	4,61	1,64	2,34	5,26
14	1,16	7,58	9,51	8,07	8,48	2,02	7,17	4,01
15	3,69	6,41	8,68	7,22	1,04	3	2,59	6,15
16	3,77	1,89	5,99	2,38	1,24	2,94	5,1	1,24
17	3,17	0,983	6,46	7,25	1,85	9,72	10,2	11,2
18	4,24	2,19	1,32	2,16	6,35	1,63	2,65	5,95
19	26,5	24,9	9,87	2,9	8,23	2,88	11	3,76
20	2,46	7,85	3,85	3,16	1,85	15,1	4,42	3,34
21	0,934	14,6	2,48	5,31	2,55	3,1	20,32	1,24
22	1,19	24,5	1,46	7,05	1,81	1,25	1,56	7,61
23	11,2	1,74	5,72	1,41	1,08	2,83	3,53	10,6
24	17,5	0,63	12,1	6,42	2,28	5,48	0,998	3,61
25	6,57	1,61	4,16	7,32	0,916	2	3,87	0,557
26	3,78	0,941	15,9	5,6	1,59	4,04	3,1	3,23
27	5,07	1,13	1,56	9,03	7,23	8,07	9,9	1,7
28	25,9	0,844	15,3	4,6	1,4	1,29	4,19	1,44
29	6,65	4,11	6,56	6,26	2,34	2,01	1,59	11,6
30	0,627	6,27	5,52	3,97	2,5	4,08	1,21	2,49
Suma	189,80	189,14	207,57	142,75	103,99	99,06	152,72	141,49
Mínimo	0,48	0,63	1,32	1,41	0,92	1,25	0,90	0,56
Máximo	26,5	27,4	15,9	9,3	12,3	15,1	20,32	11,6
Promedio	6,33	6,30	6,92	4,76	3,47	3,30	5,09	4,72
Desviación estándar	6,77	7,51	4,34	2,38	3,19	2,96	4,41	3,10
Coeficiente de variación	107,02%	119,14%	62,70%	50,05%	92,15%	89,74%	86,70%	65,63%

Realizado por: Javier E. Solano Y. 2016

La desviación estándar de la (Tabla 1-4), permite determinar que el promedio de la fluctuación entre los diferentes escenarios de los servidores es de tres coma diecinueve (3,19) y corresponde a OpenSSH, entre los clientes es de dos coma noventa y seis (2,96) y también corresponde a OpenSSH, se identifica que el menor tiempo de latencia es OpenSSH.

El (Gráfico 1-4), marca claramente la diferencia de la latencia que tiene el servidor OpenSSH ya que sus picos son bajos referentes a las otras tres (3) conexiones.

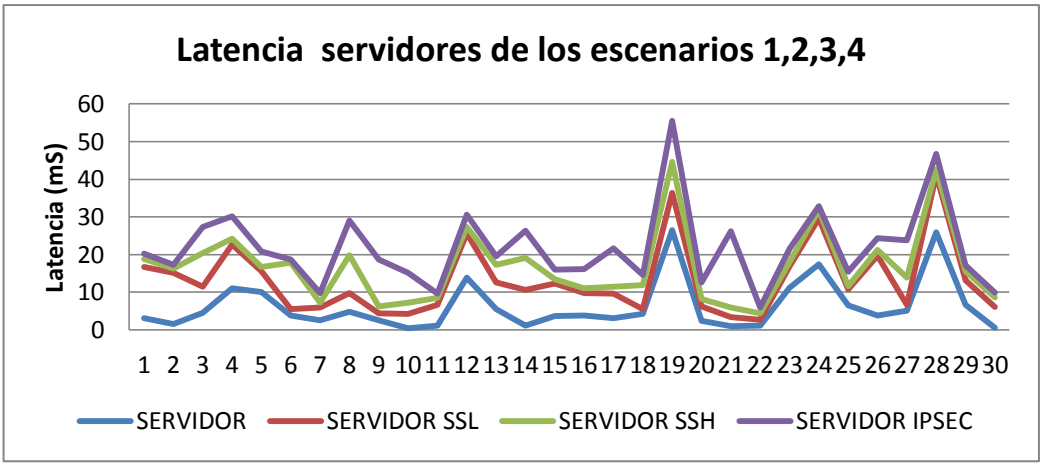


Gráfico 1-4: Latencia de los servidores escenario 1, 2, 3, 4 software libre

Realizado por: Javier E. Solano Y. 2016

El (Gráfico 2-4), la diferencia de la latencia que tiene el cliente OpenSSH ya que sus picos son bajos referentes a las otras tres (3) conexiones.

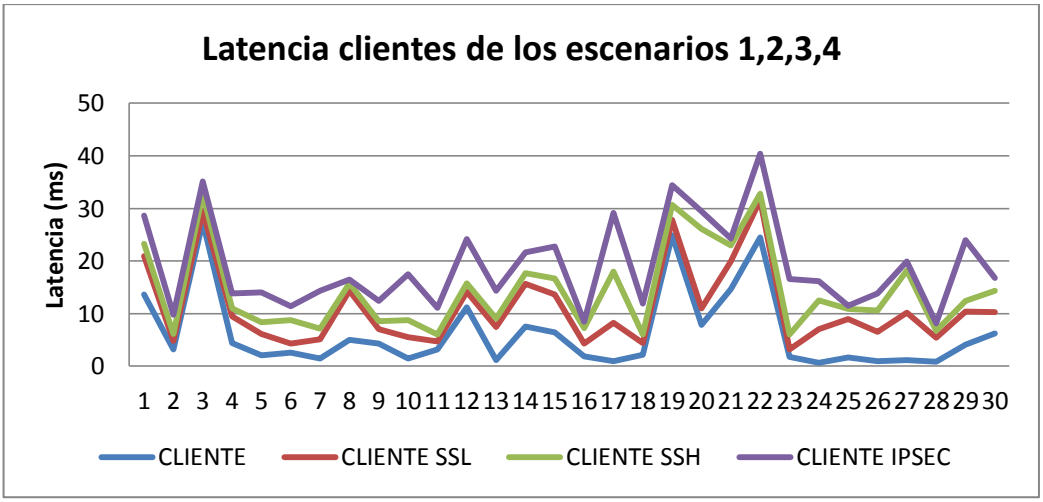


Gráfico 2-4: Latencia de los clientes escenario 1, 2, 3, 4 software libre

Realizado por: Javier E. Solano Y. 2016

4.2.2. *Indicador I.2: Jitter*

Para el análisis del *jitter* se tomaron treinta (30) muestras de los escenarios uno, dos, tres, cuatro del servidor y del cliente para realizar el análisis comparativos entre las diferentes arquitecturas de conexión VPN que se muestran en la (Tabla 2-4).

Tabla 2-4: Jitter con software libre para la conexión VPN servidor-cliente

TOMA DE MUESTRAS JITTER (ms)								
N° DE MUESTRAS	**CONEXIÓN**		**OPENVPN SSL**		**OPENSSH SSH**		**OPENSWAN IPSEC**	
	Servidor	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**
1	2,53	0,74	5,36	4,15	1,58	0,89	3,85	0,57
2	1,70	0,37	4,40	4,30	1,38	0,57	2,76	0,88
3	2,45	0,44	4,66	3,88	2,43	0,88	4,31	0,54
4	2,77	0,49	4,78	4,42	0,79	0,54	3,00	0,85
5	2,45	0,36	5,02	4,62	0,94	0,85	3,00	0,64
6	2,85	0,33	5,18	3,09	1,80	0,64	5,18	0,61
7	2,93	0,38	4,09	3,93	2,15	0,61	5,05	0,98
8	3,12	0,81	4,82	7,55	1,34	0,98	2,65	0,58
9	3,29	0,48	5,66	2,54	1,41	0,58	4,86	0,47
10	3,40	0,71	5,38	5,16	0,92	0,47	4,62	0,72
11	5,00	0,45	4,18	5,52	2,29	0,72	6,23	0,48
12	3,23	0,49	3,51	2,65	1,28	0,48	2,81	0,72
13	2,99	0,47	3,86	3,40	1,53	0,72	3,22	1,07
14	3,43	0,21	4,63	3,92	1,98	1,07	3,29	0,63
15	1,83	0,29	4,85	5,32	2,41	0,63	3,97	0,49
16	2,36	0,48	4,26	5,93	1,95	0,45	4,30	0,47
17	3,41	0,44	4,59	5,30	2,35	0,79	3,92	0,21
18	4,81	0,42	5,53	3,80	1,36	0,41	5,04	0,29
19	2,44	0,56	4,17	4,68	1,83	0,47	3,11	0,48
20	2,82	0,50	4,87	3,53	1,32	1,00	4,59	0,44
21	2,50	0,34	5,35	3,37	0,98	0,37	3,20	0,42
22	2,75	0,67	4,46	5,77	2,44	1,07	4,38	0,56
23	2,38	0,42	3,89	2,76	2,16	0,75	5,11	0,50
24	2,94	0,49	4,34	3,70	0,94	1,00	3,86	0,34
25	2,75	0,46	5,04	5,29	3,27	0,42	1,12	0,67
26	2,06	0,28	5,09	3,62	1,24	0,68	4,02	0,42
27	3,66	0,42	3,73	4,54	0,97	0,71	0,46	0,49
28	4,29	0,79	2,67	5,96	3,19	1,37	0,30	0,46
29	2,38	0,98	4,65	2,55	1,07	0,42	0,25	0,43
30	4,46	0,30	4,15	2,76	2,45	0,54	0,39	0,40
Suma	89,98	14,53	137,16	128,02	51,73	21,06	102,82	16,78
Mínimo	1,70	0,21	2,67	2,54	0,79	0,37	0,25	0,21
Máximo	5,004	0,978	5,658	7,551	3,268	1,365	6,23	1,07
Promedio	3,00	0,48	4,57	4,27	1,72	0,70	3,43	0,56
Desviación estándar	0,81	0,18	0,66	1,21	0,68	0,25	1,58	0,19
Coeficiente de variación	26,96%	36,15%	14,45%	28,42%	39,17%	34,94%	46,23%	34,58%

Realizado por: Javier E. Solano Y. 2016

La desviación estándar de la (Tabla 2-4), permite determinar que el promedio de la fluctuación entre los diferentes escenarios de los servidores es de cero coma sesenta y ocho (0,68) que corresponde a OpenSSH, entre los clientes es de cero coma veinte y cinco (0,19) que corresponde a OPENSwan.

El (Gráfico 3-4), marca claramente la diferencia del jitter que tiene el servidor OpenSSH ya que sus picos son bajos referentes a las otras tres (3) conexiones.

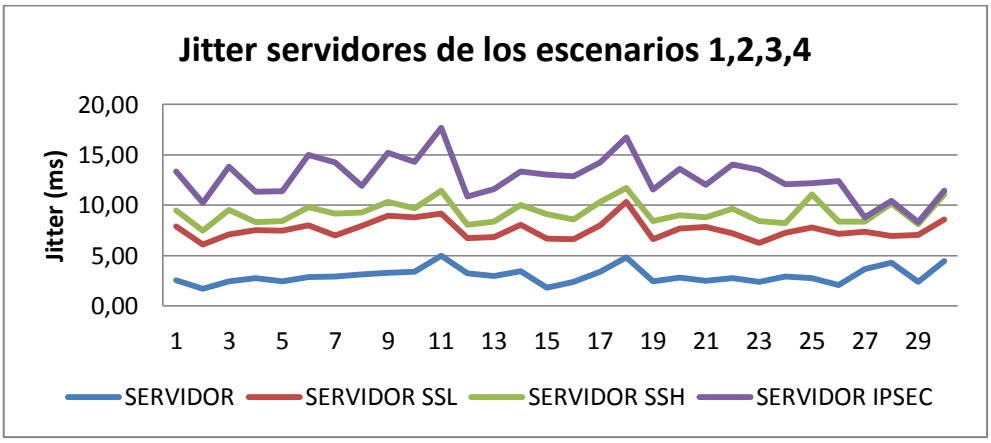


Gráfico 3-4: Jitter de los servidores escenarios 1, 2, 3, 4 software libre

Realizado por: Javier E. Solano Y. 2016

El (Gráfico 4-4), marca claramente la diferencia del jitter que tiene el cliente OPENSwan ya que sus picos son bajos referentes a las otras tres (3) conexiones.

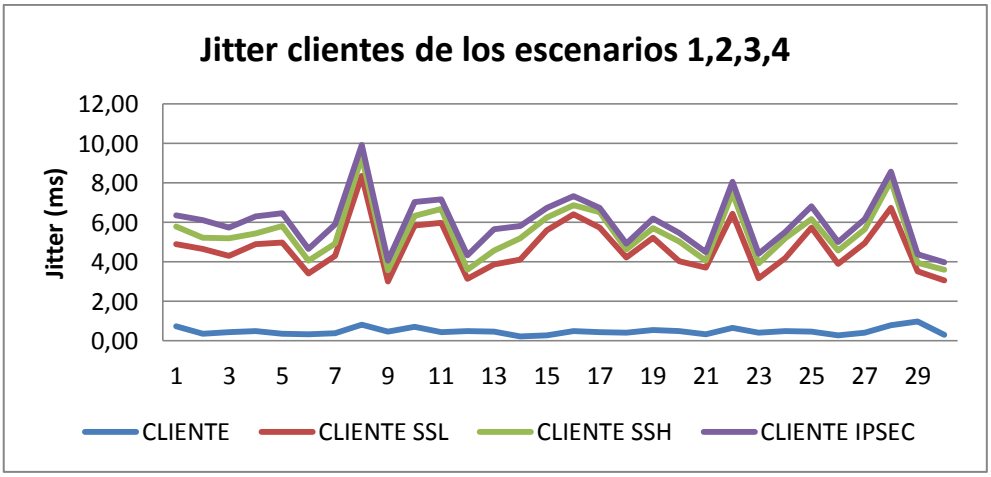


Gráfico 4-4: Jitter de los clientes escenarios 1, 2, 3, 4 software libre

Realizado por: Javier E. Solano Y. 2016

4.2.3. *Indicador I.3: Ancho de Banda*

Para el análisis del *Ancho de banda* se tomaron treinta (30) muestras de los escenarios uno, dos, tres, cuatro del servidor y del cliente para realizar el análisis comparativo entre las diferentes arquitecturas de conexión VPN que en la (Tabla 3-4) se visualiza.

Tabla 3-4: Ancho de banda, software libre, conexión VPN servidor-cliente

TOMA DE MUESTRAS ANCHO DE BANDA (MB)								
N° DE MUESTRAS	**CONEXIÓN**		**OPENVPN SSL**		**OPENSSH**		**OPENSWAN IPSEC**	
	Servidor	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**
1	0,13	0,12	0,12	0,12	0,13	0,12	0,12	0,12
2	0,12	0,13	0,12	0,12	0,12	0,12	0,12	0,12
3	0,12	0,12	0,13	0,13	0,12	0,13	0,12	0,12
4	0,13	0,12	0,12	0,12	0,12	0,12	0,13	0,12
5	0,12	0,13	0,12	0,13	0,13	0,13	0,12	0,13
6	0,12	0,12	0,13	0,13	0,12	0,12	0,12	0,12
7	0,13	0,13	0,12	0,12	0,12	0,12	0,12	0,13
8	0,13	0,12	0,12	0,12	0,12	0,13	0,13	0,12
9	0,12	0,13	0,13	0,13	0,12	0,12	0,12	0,12
10	0,12	0,12	0,12	0,13	0,12	0,12	0,12	0,12
11	0,12	0,12	0,13	0,12	0,13	0,12	0,13	0,13
12	0,12	0,13	0,12	0,12	0,12	0,13	0,12	0,12
13	0,12	0,12	0,12	0,12	0,12	0,12	0,12	0,12
14	0,12	0,12	0,13	0,13	0,12	0,13	0,12	0,12
15	0,13	0,12	0,12	0,12	0,12	0,13	0,13	0,13
16	0,12	0,12	0,12	0,12	0,12	0,12	0,12	0,12
17	0,12	0,13	0,12	0,13	0,13	0,12	0,12	0,12
18	0,12	0,12	0,12	0,12	0,12	0,13	0,12	0,12
19	0,13	0,12	0,13	0,12	0,12	0,12	0,12	0,12
20	0,12	0,12	0,12	0,13	0,13	0,12	0,12	0,12
21	0,12	0,12	0,12	0,12	0,12	0,12	0,12	0,12
22	0,13	0,12	0,12	0,12	0,13	0,13	0,12	0,12
23	0,12	0,13	0,13	0,13	0,12	0,12	0,12	0,12
24	0,13	0,12	0,12	0,12	0,13	0,12	0,13	0,12
25	0,12	0,13	0,12	0,13	0,12	0,13	0,12	0,13
26	0,13	0,12	0,12	0,12	0,12	0,13	0,12	0,12
27	0,13	0,12	0,13	0,12	0,12	0,12	0,13	0,12
28	0,12	0,13	0,12	0,13	0,12	0,12	0,11	0,12
29	0,12	0,12	0,12	0,12	0,13	0,13	0,12	0,12
30	0,12	0,13	0,12	0,12	0,13	0,12	0,12	0,12
SUMA	3,7	3,7	3,68	3,71	3,69	3,71	3,65	3,65
MINIMIMO	0,12	0,12	0,12	0,12	0,12	0,12	0,11	0,12
MAXIMO	0,13	0,13	0,13	0,13	0,13	0,13	0,13	0,13

PROMEDIO	0,12	0,12	0,12	0,12	0,12	0,12	0,12	0,12
DESVIACIÓN ESTANDAR	0,00479	0,00479	0,00450	0,00490	0,00466	0,00490	0,00461	0,00379
COEFICIENTE DE VARIACIÓN	3,89%	3,89%	3,67%	3,96%	3,79%	3,96%	3,79%	3,12%

Realizado por: Javier E. Solano Y. 2016

Con la desviación estándar de la (Tabla 4-3), determinamos que no hay diferencia significativa del uso de ancho de banda de todos los escenarios.

El (Gráfico 5-4), muestra que no hay una diferencia significativa de las arquitecturas VPN en los servidores.

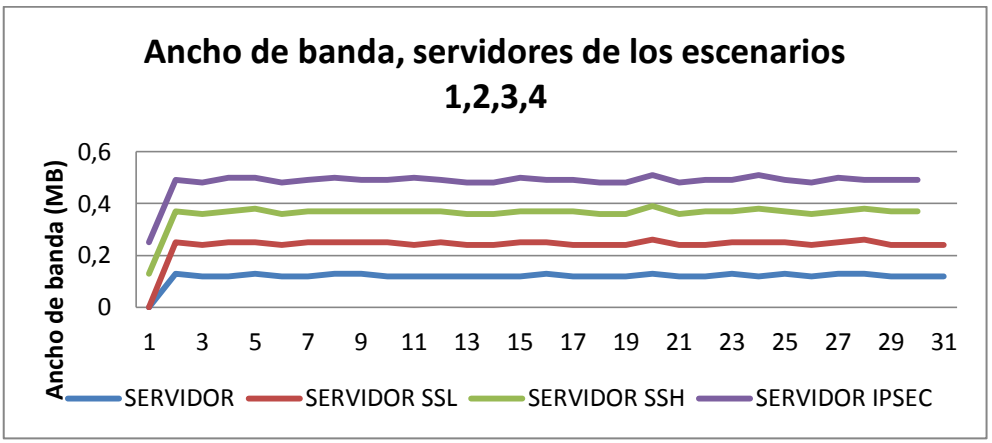


Gráfico 5-4: Ancho de banda de los servidores escenarios 1, 2, 3,4 software libre

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 6-4), no se identifica diferencia de ancho de banda entre las arquitecturas VPN de los clientes.

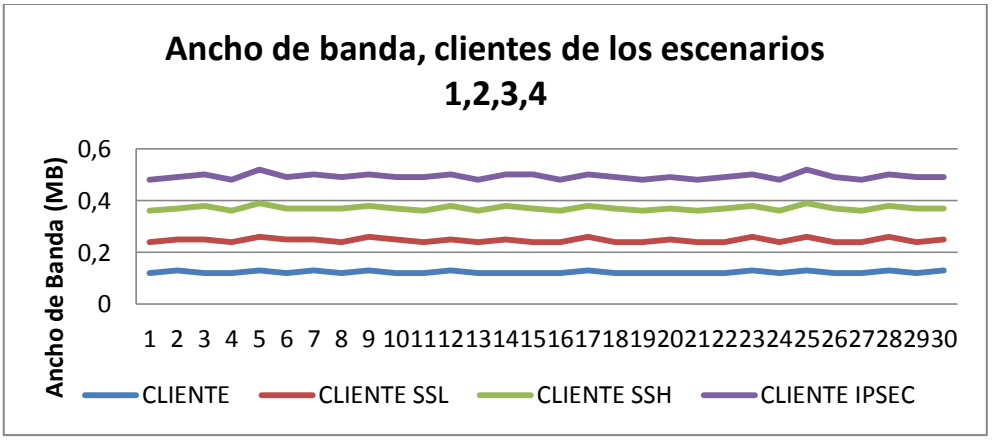


Gráfico 6-4: Ancho de Banda de los clientes escenarios 1, 2, 3, 4 software libre

Realizado por: Javier E. Solano Y. 2016

4.2.4. *Indicador I.4: Porcentaje de datagramas recibidos*

Para el análisis del *porcentaje de datagramas recibidos*, se tomaron treinta (30) muestras de los escenarios uno, dos, tres, cuatro del servidor y del cliente para realizar el análisis comparativo entre las diferentes arquitecturas de conexión VPN (Tabla 4-4).

Tabla 4-4: Datagramas recibidos, software libre, conexión VPN servidor-cliente

TOMA DE MUESTRAS PORCENTAJE DE DATAGRAMAS RECIBIDOS								
N° DE MUESTRAS	**CONEXIÓN**		**OPENVPN SSL**		**OPENSSH**		**OPENSWAN IPSEC**	
	Servidor	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**
1	0,9	0,89	0,89	0,88	0,9	0,89	0,88	0,88
2	0,86	0,9	0,88	0,89	0,89	0,88	0,89	0,83
3	0,89	0,89	0,91	0,9	0,89	0,9	0,84	0,86
4	0,91	0,87	0,89	0,88	0,89	0,88	0,92	0,85
5	0,89	0,91	0,88	0,9	0,9	0,91	0,87	0,88
6	0,89	0,88	0,9	0,9	0,89	0,89	0,85	0,86
7	0,9	0,9	0,89	0,89	0,89	0,88	0,88	0,94
8	0,9	0,88	0,89	0,88	0,89	0,9	0,9	0,89
9	0,88	0,9	0,9	0,9	0,89	0,89	0,86	0,86
10	0,89	0,89	0,88	0,9	0,89	0,89	0,86	0,91
11	0,89	0,89	0,9	0,88	0,9	0,89	0,91	0,81
12	0,87	0,9	0,89	0,89	0,89	0,9	0,86	0,86
13	0,89	0,89	0,88	0,89	0,89	0,88	0,88	0,88
14	0,89	0,89	0,91	0,9	0,89	0,9	0,86	0,8746667
15	0,9	0,89	0,89	0,89	0,89	0,9	0,92	0,9
16	0,88	0,89	0,89	0,89	0,89	0,89	0,87	0,9
17	0,89	0,9	0,89	0,9	0,9	0,87	0,88	0,89
18	0,89	0,89	0,89	0,87	0,89	0,91	0,88	0,88
19	0,9	0,89	0,9	0,89	0,88	0,89	0,83	0,9
20	0,88	0,89	0,88	0,91	0,9	0,88	0,86	0,9
21	0,89	0,89	0,89	0,89	0,89	0,89	0,85	0,88
22	0,9	0,87	0,89	0,87	0,9	0,91	0,88	0,89
23	0,89	0,9	0,9	0,92	0,88	0,89	0,86	0,89
24	0,9	0,89	0,89	0,88	0,9	0,88	0,94	0,9
25	0,87	0,91	0,89	0,9	0,89	0,9	0,89	0,89
26	0,91	0,88	0,87	0,89	0,89	0,9	0,86	0,89
27	0,9	0,89	0,92	0,89	0,89	0,88	0,91	0,9
28	0,88	0,9	0,89	0,9	0,89	0,89	0,81	0,87
29	0,87	0,89	0,89	0,89	0,9	0,9	0,86	0,89
30	0,9	0,9	0,89	0,89	0,9	0,89	0,88	0,88
Suma	26,70	26,75	26,75	26,75	26,77	26,75	26,24	26,43
Mínimo	0,86	0,87	0,87	0,87	0,88	0,87	0,81	0,81

Máximo	0,91	0,91	0,92	0,92	0,9	0,91	0,94	0,94
Promedio	0,89	0,89	0,89	0,89	0,89	0,89	0,87	0,88
Desviación estándar	0,0120	0,0095	0,0102	0,0109	0,0057	0,0102	0,0279	0,0246
Coeficiente de variación	1,35%	1,07%	1,14%	1,22%	0,64%	1,14%	3,19%	2,79%

Realizado por: Javier E. Solano Y. 2016

La desviación estándar de la (Tabla 4-4), permite determinar que no hay una marcada diferencia en el porcentaje de datagramas recibidos, se puede determinar que el de menor perdida en cuanto al servidor es de cero coma cero doscientos setenta y nueve (0,0279) y del cliente cero coma cero doscientos cuarenta y seis (0,0246) que corresponde a OPENSwan.

En el (Gráfico 7-4), se visualiza que no hay una diferencia significativa entre las diferentes arquitecturas en cuanto a los datagramas entre servidores pero si existe uno que tiene menor significancia que es OPENSwan.

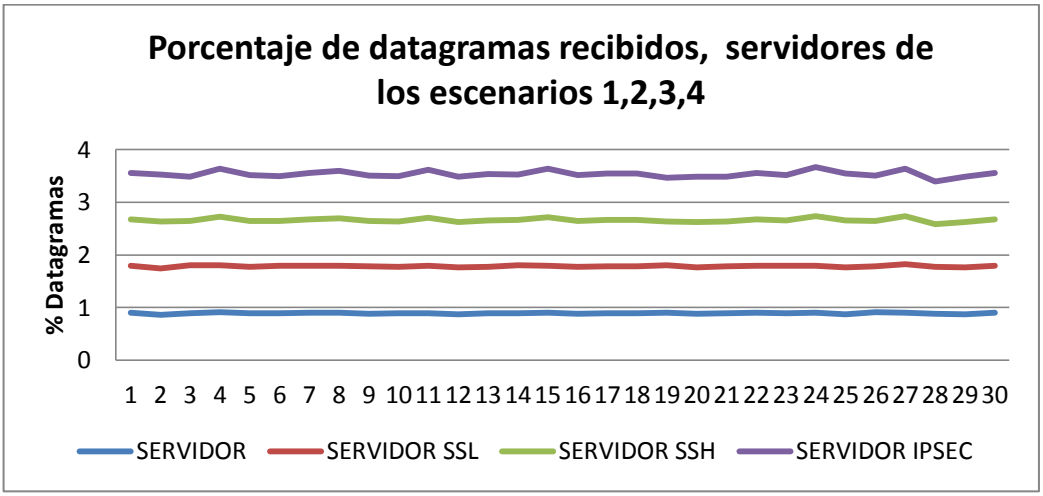


Gráfico 7-4: Datagramas servidores escenarios 1, 2, 3, 4 software libre

Realizado por: Javier E. Solano Y. 2016

El (Gráfico 8-4), muestra que no hay una diferencia significativa entre las diferentes arquitecturas en cuanto a los datagramas entre servidores pero si el de menor significancia es el OPENSwan.

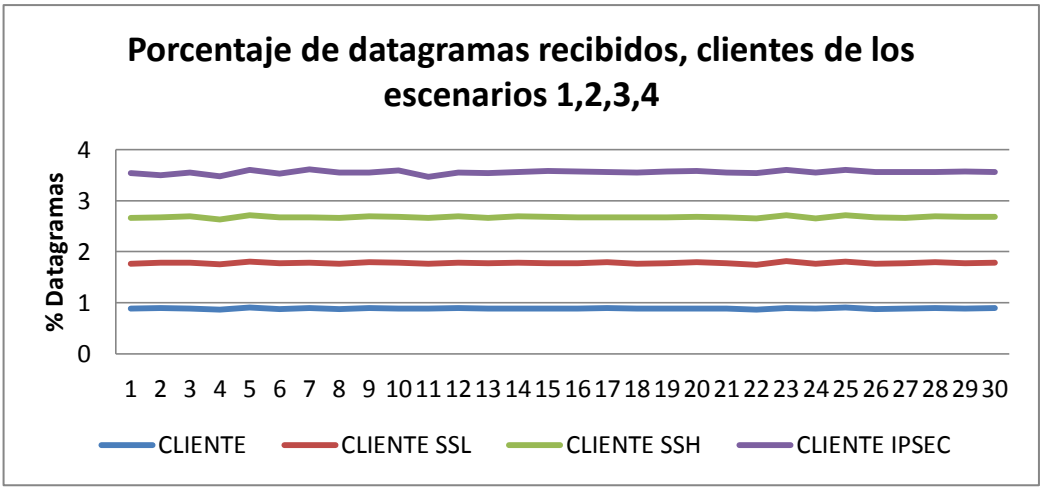


Gráfico 8-4: Datagramas clientes escenarios 1, 2, 3,4 software libre

Realizado por: Javier E. Solano Y. 2016

4.2.5. *Resumen de la variable dependiente: rendimiento de los promedios obtenidos de las VPNs con software libre de los servidores.*

La (Tabla 5-4), describe los promedios obtenidos de treinta (30) muestras obtenidas de los escenarios uno, dos, tres, cuatro de los diferentes indicadores de rendimiento previamente establecido en la transmisión de la videoconferencia en las diferentes arquitecturas VPN, cliente-servidor.

Tabla 5-4: Tabla comparativa de los indicadores de rendimiento con software libre

PROMEDIO DEL RENDIMIENTO DE LAS VPN DE 30 MUESTRAS OBTENIDAS								
Rendimiento / VPN	LATENCIA (ms)		JITTER(ms)		ANCHO DE BANDA (MB/seg)		PORCENTAJE DATAGRAMAS RECIBIDOS	
	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente
CONEXIÓN	6,33	6,30	3,00	0,48	0,12	0,12	89	89,17
OpenVPN SSL	6,92	4,76	4,57	4,27	0,12	0,13	89	89,17
OpenSSH	3,47	3,30	1,72	0,70	0,12	0,12	89	89,17
OPENSwan IPSec	5,09	4,72	3,43	0,56	0,12	0,12	87	88,12

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 9-4), del promedio obtenido de latencia, se puede determinar que los menores tiempos de retraso del servidor es tres coma cuarenta y siete (3,47) correspondiente a la arquitectura OpenSSH.

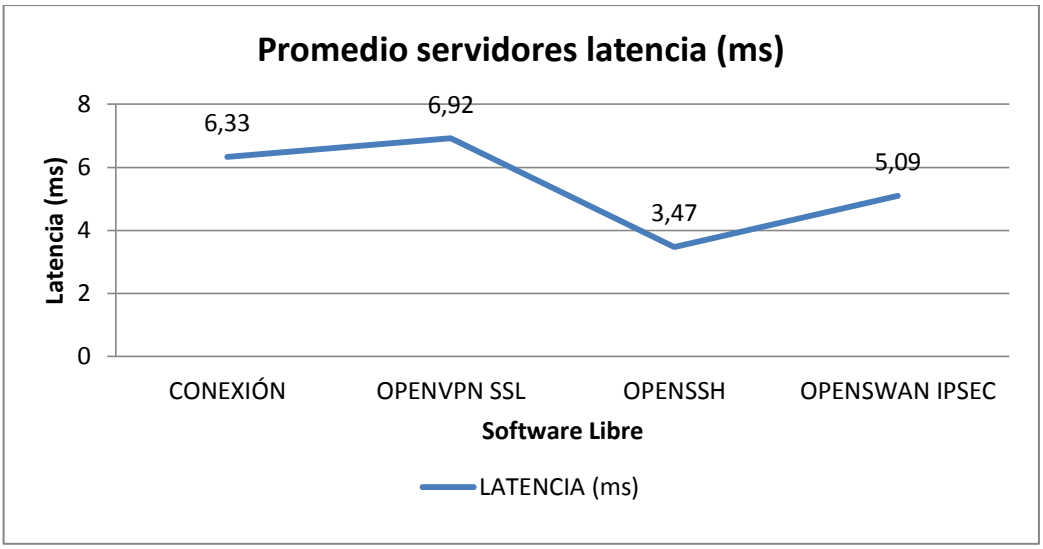


Gráfico 9-4: Promedio latencia servidores escenarios 1, 2, 3, 4 software libre

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 10-4), de la media de datos obtenidos del jitter, se puede determinar que l menor tiempo del servidor es uno coma setenta y dos (1,72) que corresponden a la arquitectura OpenSSH.

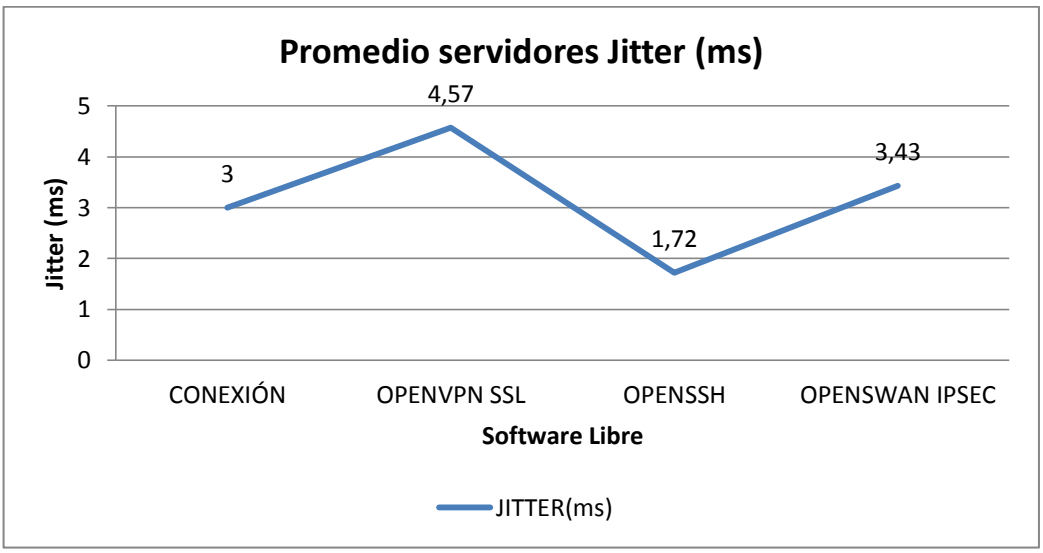


Gráfico 10-4: Promedio jitter servidores escenarios 1, 2, 3,4 software libre

Realizado por: Javier E. Solano Y. 2016

El (Gráfico 11-4), visualiza que de los promedios obtenidos de ancho de banda, se puede determinar que el número de Mbytes que utilizan los servidores es de cero coma doce (0,12) en todas las arquitecturas.

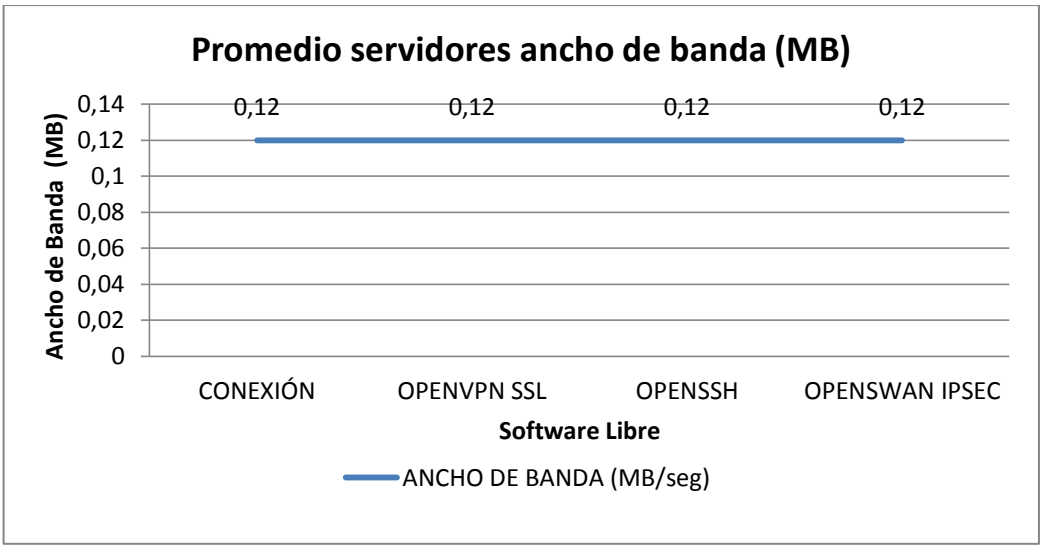


Gráfico 11-4: Promedio ancho de banda servidores escenarios 1, 2, 3,4 software libre

Realizado por: Javier E. Solano Y. 2016

El (Gráfico 12-4), de los promedios obtenidos del porcentaje de datagramas recibidos, se puede determinar que el porcentaje menor perdida del servidor es de ochenta y siete (87), corresponde a OPENSwan.

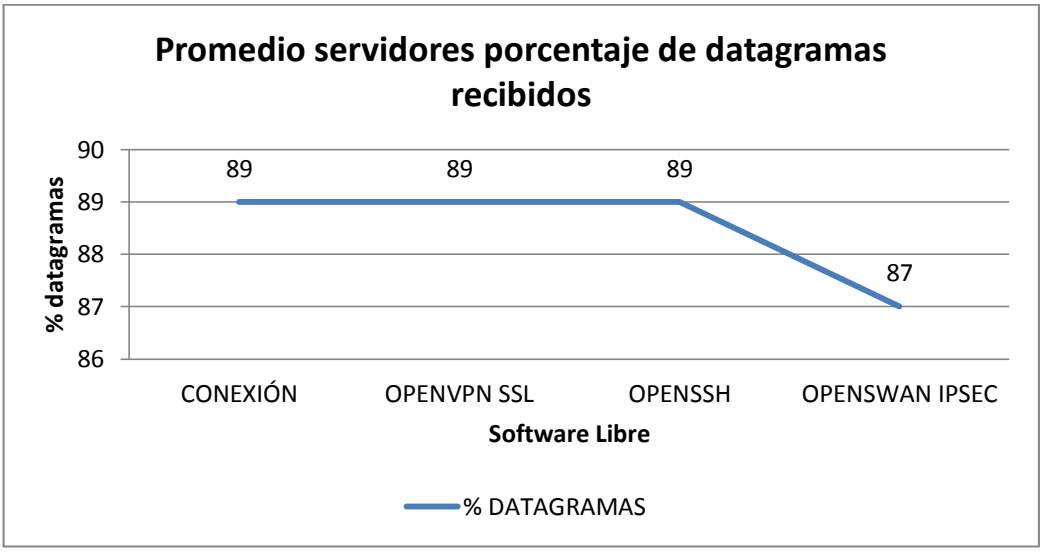


Gráfico 12-4: Promedio datagramas servidores escenarios 1, 2, 3,4 software libre

Realizado por: Javier E. Solano Y. 2016

4.2.6. *Wireshark captura de los protocolo de Conexión, OpenVPN SSL, OpenSSH SSH, OpenSwan IPSec*

En la (Figura 1-4), con el software Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante los protocolos RTP, SIP.

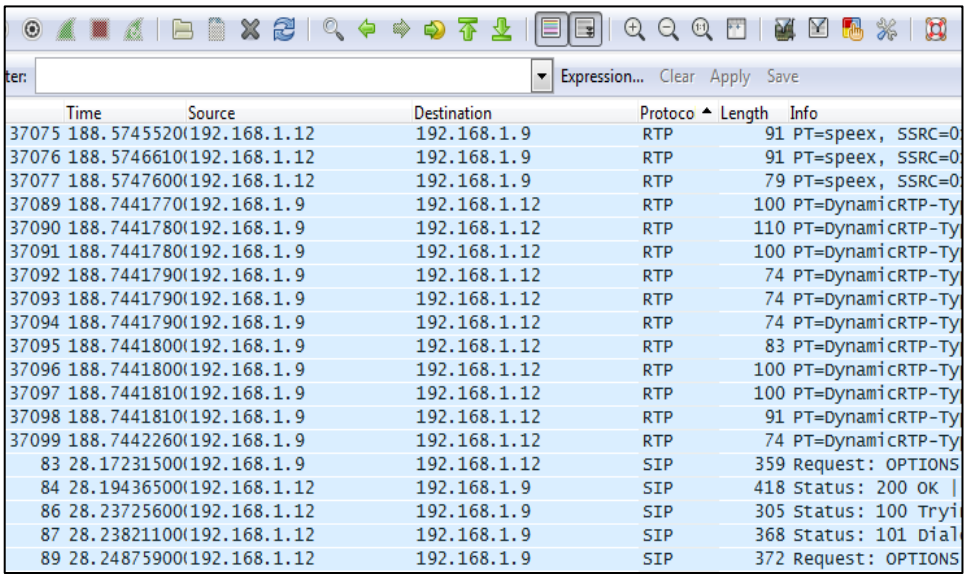


Figura 1-4: Transmisión videoconferencia RTP, SIP con Linphone

Realizado por: Javier E. Solano Y. 2016

La (Figura 2-4), con Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante el túnel OPENVPN SSL.

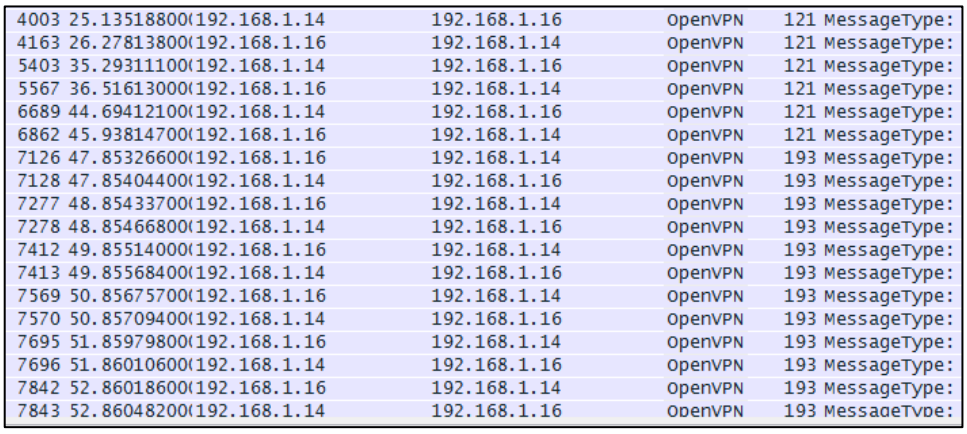
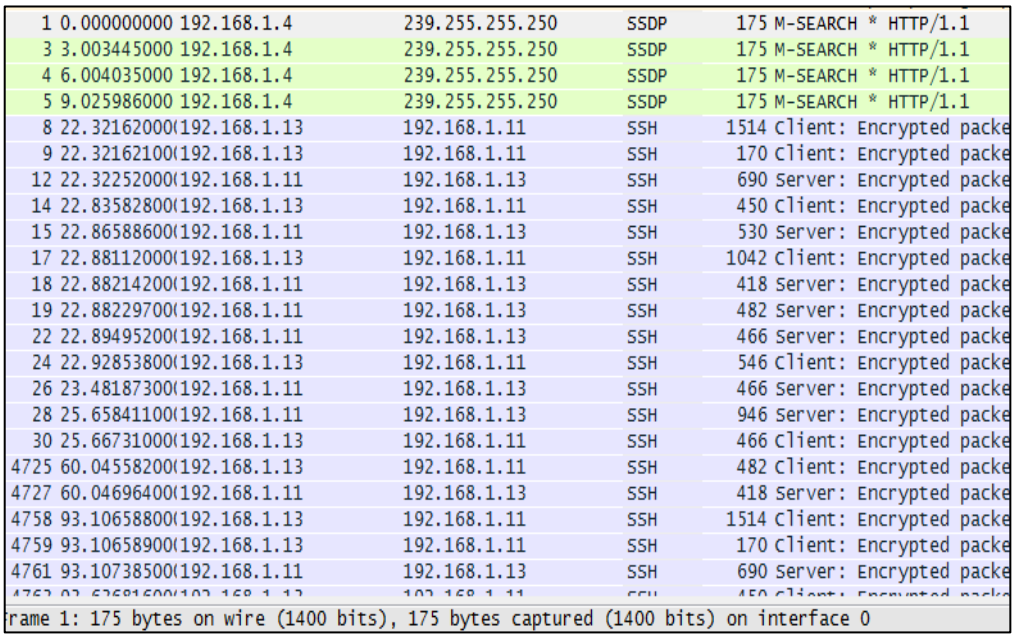


Figura 2-4: Túnel OPENVPN SSL Linphone

Realizado por: Javier E. Solano Y. 2016

La (Figura 3-4), con Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante el túnel OPENSSH SSH.



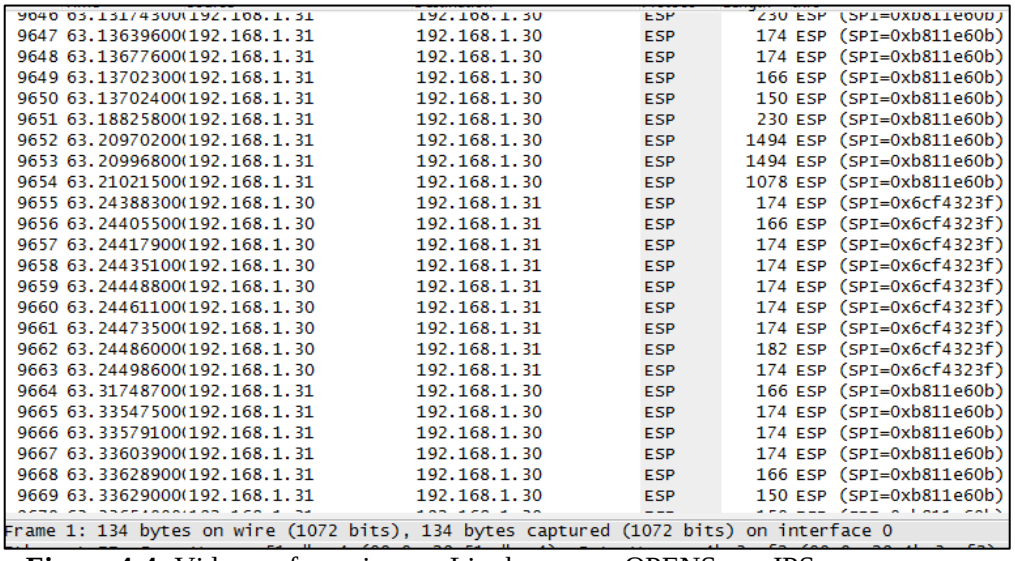
1	0.000000000	192.168.1.4	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
3	3.003445000	192.168.1.4	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
4	6.004035000	192.168.1.4	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
5	9.025986000	192.168.1.4	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
8	22.32162000	192.168.1.13	192.168.1.11	SSH	1514 Client: Encrypted packe
9	22.32162100	192.168.1.13	192.168.1.11	SSH	170 Client: Encrypted packe
12	22.32252000	192.168.1.11	192.168.1.13	SSH	690 Server: Encrypted packe
14	22.83582800	192.168.1.13	192.168.1.11	SSH	450 Client: Encrypted packe
15	22.86588600	192.168.1.11	192.168.1.13	SSH	530 Server: Encrypted packe
17	22.88112000	192.168.1.13	192.168.1.11	SSH	1042 Client: Encrypted packe
18	22.88214200	192.168.1.11	192.168.1.13	SSH	418 Server: Encrypted packe
19	22.88229700	192.168.1.11	192.168.1.13	SSH	482 Server: Encrypted packe
22	22.89495200	192.168.1.11	192.168.1.13	SSH	466 Server: Encrypted packe
24	22.92853800	192.168.1.13	192.168.1.11	SSH	546 Client: Encrypted packe
26	23.48187300	192.168.1.11	192.168.1.13	SSH	466 Server: Encrypted packe
28	25.65841100	192.168.1.11	192.168.1.13	SSH	946 Server: Encrypted packe
30	25.66731000	192.168.1.13	192.168.1.11	SSH	466 Client: Encrypted packe
4725	60.04558200	192.168.1.13	192.168.1.11	SSH	482 Client: Encrypted packe
4727	60.04696400	192.168.1.11	192.168.1.13	SSH	418 Server: Encrypted packe
4758	93.10658800	192.168.1.13	192.168.1.11	SSH	1514 Client: Encrypted packe
4759	93.10658900	192.168.1.13	192.168.1.11	SSH	170 Client: Encrypted packe
4761	93.10738500	192.168.1.11	192.168.1.13	SSH	690 Server: Encrypted packe

rame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0

Figura 3-4: Túnel SSH Encrypted Linphone OPENSSH.

Realizado por: Javier E. Solano Y. 2016

La (Figura 4-4), con Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante el túnel de OPENSwan IPSec.



9647	63.13639600	192.168.1.31	192.168.1.30	ESP	174 ESP (SPI=0xb811e60b)
9648	63.13677600	192.168.1.31	192.168.1.30	ESP	174 ESP (SPI=0xb811e60b)
9649	63.13702300	192.168.1.31	192.168.1.30	ESP	166 ESP (SPI=0xb811e60b)
9650	63.13702400	192.168.1.31	192.168.1.30	ESP	150 ESP (SPI=0xb811e60b)
9651	63.18825800	192.168.1.31	192.168.1.30	ESP	230 ESP (SPI=0xb811e60b)
9652	63.20970200	192.168.1.31	192.168.1.30	ESP	1494 ESP (SPI=0xb811e60b)
9653	63.20996800	192.168.1.31	192.168.1.30	ESP	1494 ESP (SPI=0xb811e60b)
9654	63.21021500	192.168.1.31	192.168.1.30	ESP	1078 ESP (SPI=0xb811e60b)
9655	63.24388300	192.168.1.30	192.168.1.31	ESP	174 ESP (SPI=0x6cf4323f)
9656	63.24405500	192.168.1.30	192.168.1.31	ESP	166 ESP (SPI=0x6cf4323f)
9657	63.24417900	192.168.1.30	192.168.1.31	ESP	174 ESP (SPI=0x6cf4323f)
9658	63.24435100	192.168.1.30	192.168.1.31	ESP	174 ESP (SPI=0x6cf4323f)
9659	63.24448800	192.168.1.30	192.168.1.31	ESP	174 ESP (SPI=0x6cf4323f)
9660	63.24461100	192.168.1.30	192.168.1.31	ESP	174 ESP (SPI=0x6cf4323f)
9661	63.24473500	192.168.1.30	192.168.1.31	ESP	174 ESP (SPI=0x6cf4323f)
9662	63.24486000	192.168.1.30	192.168.1.31	ESP	182 ESP (SPI=0x6cf4323f)
9663	63.24498600	192.168.1.30	192.168.1.31	ESP	174 ESP (SPI=0x6cf4323f)
9664	63.31748700	192.168.1.31	192.168.1.30	ESP	166 ESP (SPI=0xb811e60b)
9665	63.33547500	192.168.1.31	192.168.1.30	ESP	174 ESP (SPI=0xb811e60b)
9666	63.33579100	192.168.1.31	192.168.1.30	ESP	174 ESP (SPI=0xb811e60b)
9667	63.33603900	192.168.1.31	192.168.1.30	ESP	174 ESP (SPI=0xb811e60b)
9668	63.33628900	192.168.1.31	192.168.1.30	ESP	166 ESP (SPI=0xb811e60b)
9669	63.33629000	192.168.1.31	192.168.1.30	ESP	150 ESP (SPI=0xb811e60b)

Frame 1: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0

Figura 4-4: Videoconferencia con Linphone por OPENSwan IPSec

Realizado por: Javier E. Solano Y. 2016

4.3. *Muestras, análisis comparativo entre el servidor-cliente de los diferentes indicadores de rendimiento con el simulador de redes GNS3.*

4.3.1. *Indicador I.1: Latencia*

Para el análisis de *latencia* se tomaron treinta (30) muestras de los escenarios cinco, seis, siete, ocho del servidor y del cliente para realizar el análisis comparativo entre las diferentes arquitecturas de conexión VPN que se muestran en la (Tabla 6-4).

Tabla 6-4: Latencia con GNS3 para la conexión VPN servidor-cliente

MUESTRAS LATENCIA								
N° DE MUESTRAS	CONEXION		SSL		SSH		IPSEC	
	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente
1	1438	7704	101	32,846	71,9	41,7	19,8	17,8
2	724	8584	102	46,725	82	58,3	17,7	14,6
3	226	8765	29	53,348	84,8	81,3	15,6	19
4	129	10234	27,6	57,827	96,7	72,6	14,6	13,4
5	132	9911	41,7	57,279	119	57,1	14,5	17,7
6	82,2	8552	39,2	57,279	84,1	58,6	13,4	13,1
7	74,6	7852	49	57,279	62,9	72	13,1	18,5
8	50	7112	44,9	57,279	89,8	84,5	22,4	12,9
9	72,1	5373	112	57,279	53,7	66,5	8,76	17,2
10	63,4	4544	41,8	35,846	51,7	81,9	76	11,6
11	41,6	3624	52,8	49,725	41,6	68,3	15,4	17
12	70,1	2014	86,1	33,348	39,4	42,7	13,7	15,6
13	76,2	1275	53,9	77,827	72,4	59,1	21,2	14,3
14	71,9	605	52,6	57,279	63,8	73,5	11,7	14,6
15	70,1	600	51,5	57,279	54,6	47,8	9,05	9,17
16	68,5	682	87,5	67,279	61,5	62,2	18,2	18,5
17	89,3	1279	122	67,279	97,5	16,6	17,1	12,9
18	87,4	1715	52,2	67,279	46,4	72,8	16	12,2
19	67,5	2083	61,7	37,846	73,3	59,3	15	7,09
20	110,32	2422	60,6	43,725	62,7	56,7	13,8	16
21	112,3	2950	69,5	53,348	63,6	28,1	12,7	20,4
22	12,89	3122	68,5	27,827	51,9	73,4	10,7	9,81
23	12,87	3747	97,3	7,279	54,7	98,9	9,11	14,1
24	11,34	4189	68	77,279	81,3	137,6	9,07	13,5
25	89,76	4783	104	89,279	109	173	7,98	17,9

26	70,1	6600	74,5	45,279	96,2	208,4	6,85	18,6
27	77,23	600	96,4	67,279	60,7	243,8	15,6	23
28	42,56	682	64,3	49,725	59,5	88,1	13,9	11
29	43,12	1279	82,5	33,348	35,43	67,6	20,5	10,2
30	134,2	1715	81,1	77,827	17,08	81,1	12,3	21,7
Suma	4350,59	124597,00	2075,20	1600,32	2039,22	2433,50	485,72	453,37
Mínimo	11,34	600,00	27,60	7,28	17,08	16,60	6,85	7,09
Máximo	1438	10234	122	89,279	119	243,8	76	23
Promedio	145,02	4153,23	69,17	53,34	67,97	81,12	16,19	15,11
Desviación estándar	274,40	3145,31	25,40	17,36	22,90	49,20	11,98	3,83
Coeficiente de variación	189,21%	75,73%	36,71%	32,53%	33,68%	60,66%	73,99%	25,35%

Realizado por: Javier E. Solano Y. 2016

La desviación estándar de la (Tabla 6-4), permite determinar que el promedio de la fluctuación entre los diferentes escenarios con arquitectura VPN correspondiente de los servidores es de once coma noventa y ocho (11,98) de los clientes es de tres coma ochenta y tres (3,83) pertenecen a IPSec.

El (Gráfico 13-4), denota levemente la diferencia de la latencia que tiene el servidor IPSec ya que sus picos son bajos referentes a las otras tres conexiones.

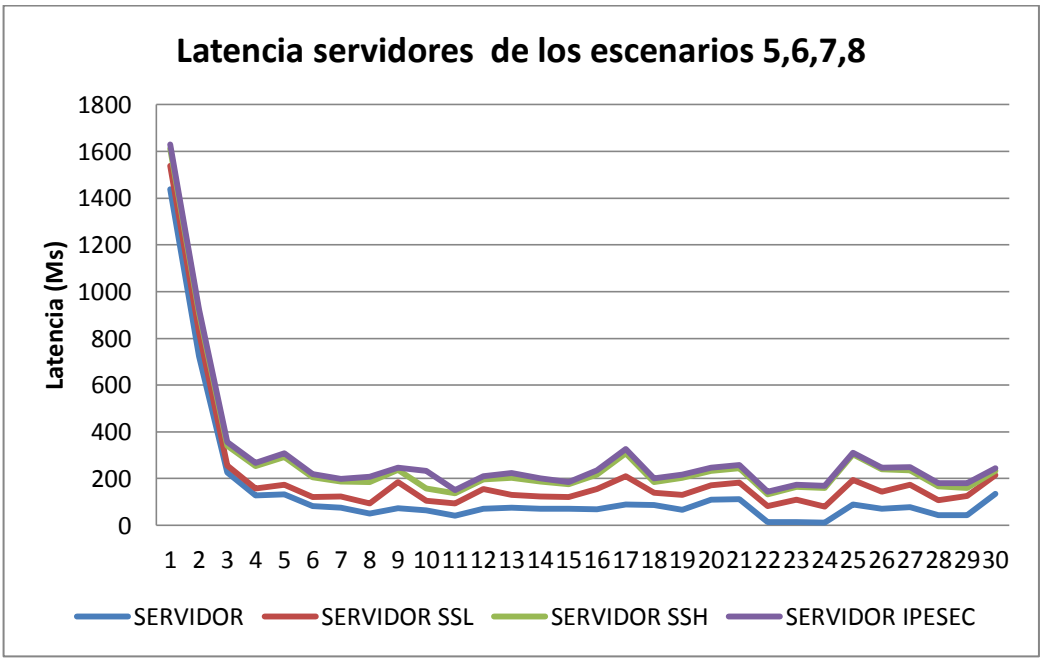


Gráfico 13-4: Latencia de los servidores, escenario 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

El (Gráfico 14-4), denota levemente la diferencia de la latencia que tiene el cliente IPSec ya que sus picos son bajos referentes a las otras tres conexiones.

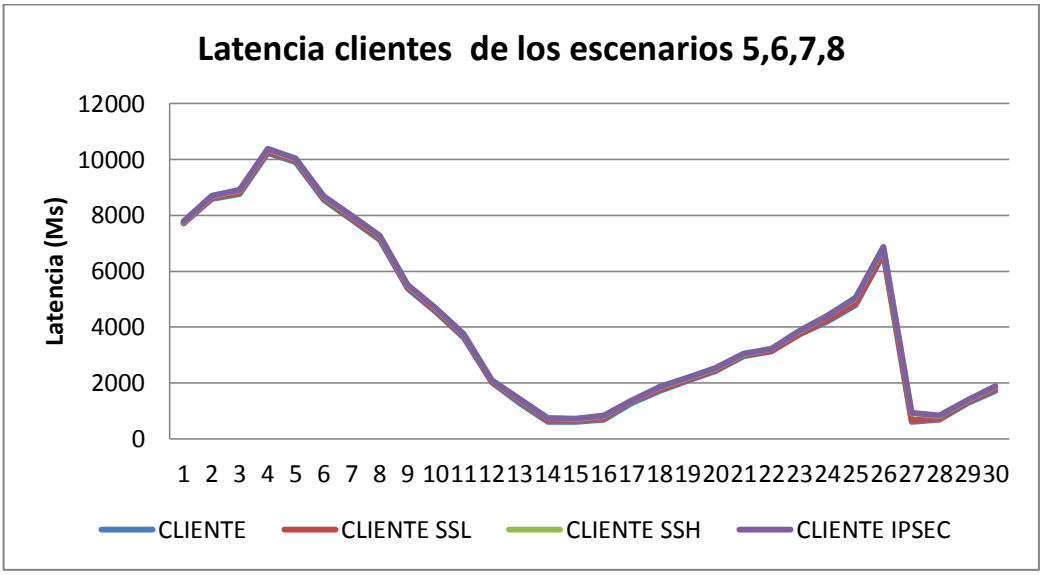


Gráfico 14-4: Latencia de los clientes, escenario 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

4.3.2. *Indicador I.2: Jitter*

Para el análisis del *jitter* se tomaron treinta (30) muestras de los escenarios cinco, seis, siete, ocho del servidor y del cliente para realizar el análisis comparativo entre las diferentes arquitecturas de conexión VPN que la (Tabla 7-4), contiene:

Tabla 7-4: Jitter con GNS3 para la conexión VPN servidor-cliente

MUESTRAS JITTER								
N° DE MUESTRAS	CONEXION		SSL		SSH		IPSEC	
	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente
1	17,70	6,84	39,02	32,85	11,12	2,86	14,72	17,80
2	22,00	3,11	52,92	46,73	11,09	2,71	16,55	14,60
3	22,83	4,25	54,17	53,35	8,65	14,94	14,83	19,00
4	22,52	5,59	55,17	57,83	10,70	20,31	15,67	13,40
5	22,34	16,11	55,61	57,28	8,74	21,00	15,94	17,70
6	22,45	20,45	54,92	57,28	10,97	21,30	18,61	13,10
7	9,65	21,00	51,91	57,28	13,10	21,16	18,29	18,50

8	27,14	21,78	46,16	57,28	8,37	22,87	16,91	12,90
9	9,38	21,18	45,26	57,28	10,20	21,72	16,61	17,20
10	8,69	21,10	45,43	35,85	10,35	21,79	18,82	11,60
11	8,53	21,01	40,60	49,73	10,12	31,55	22,35	17,00
12	9,70	5,56	53,63	33,35	9,85	7,87	18,72	15,60
13	8,27	21,86	56,48	77,83	10,50	10,48	18,68	14,30
14	8,55	2,35	55,50	57,28	9,29	8,85	18,07	14,60
15	8,85	16,22	56,21	57,28	11,46	11,57	18,83	9,17
16	8,84	20,41	56,28	67,28	11,30	11,15	18,38	18,50
17	8,31	20,95	56,26	67,28	10,83	15,09	15,90	12,90
18	10,08	20,97	55,62	67,28	11,02	22,49	19,04	12,20
19	9,54	21,15	55,62	37,85	19,06	30,21	18,00	7,09
20	8,92	21,14	45,20	43,73	24,65	5,12	18,61	16,00
21	10,22	11,80	48,25	53,35	24,73	3,48	15,78	20,40
22	9,15	6,25	39,02	27,83	24,31	3,02	14,64	9,81
23	8,55	7,46	52,92	7,28	21,32	2,47	18,19	14,10
24	10,54	10,82	54,17	77,28	23,82	19,46	21,40	13,50
25	9,22	7,76	55,17	89,28	23,25	20,94	17,10	17,90
26	19,15	11,20	55,61	45,28	21,97	22,10	19,91	18,60
27	21,50	10,48	54,92	67,28	24,53	21,54	20,91	23,00
28	22,23	9,21	51,91	49,73	17,72	21,55	17,89	11,00
29	22,27	9,72	46,16	33,35	15,13	21,51	19,52	10,20
30	25,24	7,66	45,26	77,83	10,66	9,11	19,45	21,70
Suma	432,35	405,35	1535,31	1600,32	438,78	470,19	538,31	453,37
Mínimo	8,27	2,35	39,02	7,28	8,37	2,47	14,64	7,09
Máximo	27,141	21,862	56,482	89,279	24,73	31,551	22,347	23
Promedio	14,41	13,51	51,18	53,34	14,63	15,67	17,94	15,11
Desviación estándar	6,72	6,97	5,57	17,36	5,98	8,46	1,93	3,83
Coeficiente de variación	46,64%	51,56%	10,88%	32,53%	40,90%	53,99%	10,78%	25,35%

Realizado por: Javier E. Solano Y. 2016

La desviación estándar de la (Tabla 7-4), permite determinar que el promedio de la fluctuación entre los diferentes escenarios con arquitectura VPN con el simulador de redes GNS3 entre los servidores es de uno coma noventa y tres (1,93) y entre los clientes es de tres coma ochenta y tres (3,83) estos valores corresponden a la arquitectura de conexión VPN IPSec.

El (Gráfico 15-4), visualiza que la diferencia de la latencia es decir el tiempo de respuesta del servidor con el cliente no es mayor del servidor IPSec entre los otro cuatro ya que sus picos denotan que son bajos referentes a las otras tres conexiones.

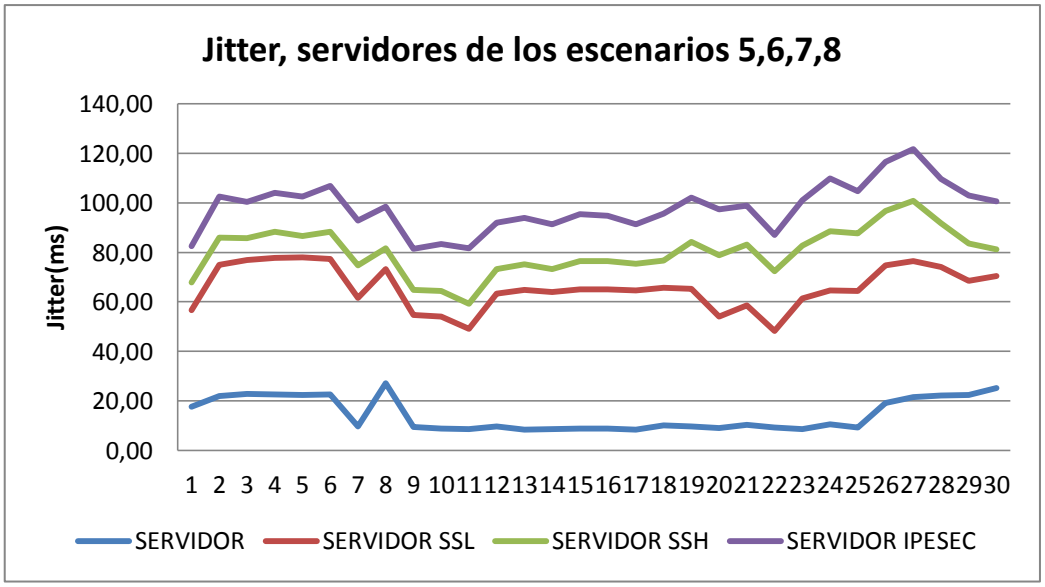


Gráfico 15-4: Jitter de los servidores escenarios 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

El (Gráfico 16-4), marca levemente la diferencia de la latencia que tiene el cliente VPN IPSec referente a las otras arquitecturas de conexión ya que sus picos no son estrechamente distantes.

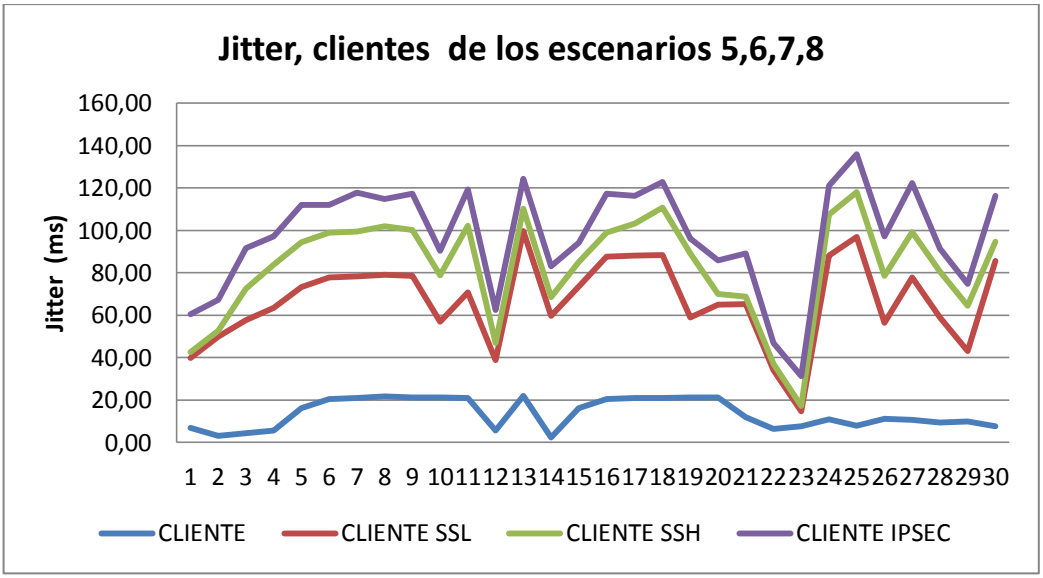


Gráfico 16-4: Jitter de los clientes escenarios 5, 6, 7, 8 GNS3.

Realizado por: Javier E. Solano Y. 2016

4.3.3. *Indicador I.3: Ancho de Banda*

Para el análisis del *ancho de banda* se tomaron treinta (30) muestras de los escenarios cinco, seis, siete, ocho del servidor y del cliente para realizar el análisis comparativo entre las diferentes arquitecturas de conexión VPN que la (Tabla 8-4), contiene:

Tabla 8-4: Ancho de banda con GNS3 para la conexión VPN servidor-cliente

TOMA DE MUESTRAS ANCHO DE BANDA								
N° DE MUESTRAS	**CONEXION**		**SSL**		**SSH**		**IPSEC**	
	Servidor	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**
1	0,04	0,11	0,02	0,02	0,11	0,12	0,07	0,07
2	0,04	0,14	0,02	0,02	0,11	0,13	0,07	0,05
3	0,04	0,12	0,02	0,02	0,12	0,09	0,05	0,04
4	0,04	0,12	0,02	0,02	0,12	0,04	0,06	0,04
5	0,04	0,09	0,02	0,02	0,12	0,04	0,06	0,04
6	0,04	0,04	0,02	0,02	0,11	0,04	0,05	0,05
7	0,09	0,04	0,01	0,02	0,11	0,04	0,06	0,04
8	0,14	0,04	0,01	0,02	0,12	0,04	0,05	0,04
9	0,13	0,04	0,02	0,02	0,11	0,04	0,06	0,04
10	0,13	0,04	0,02	0,02	0,12	0,04	0,06	0,04
11	0,13	0,04	0,02	0,02	0,12	0,03	0,06	0,04
12	0,13	0,08	0,02	0,02	0,12	0,04	0,06	0,04
13	0,14	0,14	0,02	0,02	0,11	0,04	0,05	0,04
14	0,13	0,14	0,02	0,02	0,12	0,04	0,05	0,03
15	0,14	0,07	0,02	0,02	0,12	0,04	0,06	0,04
16	0,13	0,04	0,02	0,02	0,12	0,04	0,05	0,04
17	0,14	0,04	0,02	0,02	0,12	0,04	0,05	0,05
18	0,14	0,04	0,01	0,02	0,12	0,07	0,06	0,05
19	0,13	0,04	0,01	0,02	0,05	0,14	0,06	0,04
20	0,13	0,04	0,01	0,02	0,04	0,13	0,06	0,05
21	0,13	0,04	0,01	0,02	0,04	0,13	0,06	0,04
22	0,12	0,04	0,02	0,02	0,04	0,14	0,06	0,04
23	0,13	0,04	0,02	0,02	0,04	0,13	0,06	0,04
24	0,12	0,04	0,02	0,02	0,04	0,05	0,06	0,04
25	0,14	0,04	0,02	0,02	0,04	0,04	0,06	0,04
26	0,05	0,04	0,02	0,02	0,04	0,04	0,06	0,05
27	0,04	0,04	0,02	0,02	0,04	0,04	0,06	0,04
28	0,04	0,04	0,01	0,02	0,04	0,04	0,06	0,04
29	0,04	0,04	0,01	0,02	0,04	0,04	0,06	0,04
30	0,04	0,04	0,02	0,02	0,04	0,04	0,06	0,6
Suma	2,92	1,85	0,52	0,6	2,59	1,92	1,75	1,84
Mínimo	0,04	0,04	0,12	0,02	0,04	0,03	0,05	0,03

Máximo	0,14	0,14	0,02	0,02	0,12	0,14	0,07	0,6
Promedio	0,10	0,06	0,02	0,02	0,09	0,06	0,06	0,06
Desviación estándar	0,04464	0,03649	0,00450	0,00345	0,03801	0,03944	0,00531	0,10197
Coeficiente de variación	45,86%	59,17%	25,95%	0,00%	44,03%	61,63%	9,10%	166,26%

Realizado por: Javier E. Solano Y. 2016

La desviación estándar de la (Tabla 8-4), permite determinar que el promedio de la fluctuación entre los diferentes escenarios con arquitectura VPN correspondiente de los servidores es de cero coma cero cuatrocientos cincuenta (0,0450), entre los clientes es de cero coma cero cero trecientos cuarenta y cinco (0,00345) pertenecen a SSL.

En el (Gráfico 17-4), se puede determinar la VPN con menor ancho de banda entre los servidores es SSL.

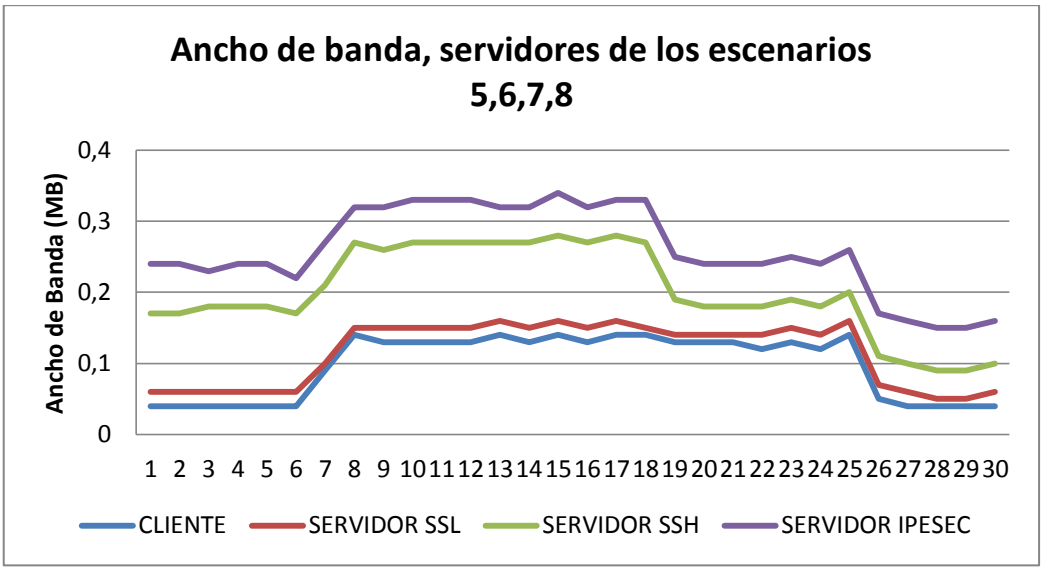


Gráfico 17-4: Ancho de banda de los servidores escenarios 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 18-4), se puede determinar que la VPN con menor Ancho de Banda entre los clientes es SSL.

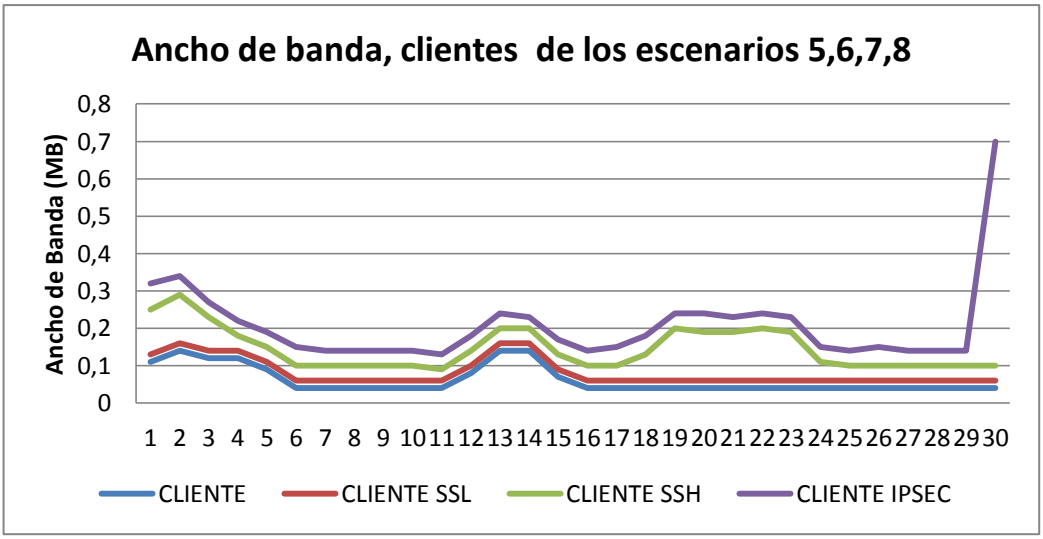


Gráfico 18-4: Ancho de Banda de los clientes escenarios 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

4.3.4. *Indicador I.4: Porcentaje de datagramas recibidos*

Para el análisis del *porcentaje de datagramas recibidos* se tomaron treinta (30) muestras de los escenarios cinco, seis, siete, ocho del servidor y del cliente para realizar el análisis comparativo entre las diferentes arquitecturas de conexión VPN que la (Tabla 9-4), contiene:

Tabla 9-4: Porcentaje de datagramas con GNS3para la conexión VPN servidor-cliente

MUESTRAS PORCENTAJE DE DATAGRAMAS RECIBIDOS								
N° DE MUESTRAS	CONEXION		SSL		SSH		IPSEC	
	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente	Servidor	Cliente
1	0,3	0,8	0,15	0,44	0,8	0,88	0,47	0,61
2	0,3	0,97	0,15	0,14	0,82	0,9	0,51	0,92
3	0,29	0,89	0,16	0,15	0,86	0,61	0,86	0,96
4	0,29	0,87	0,15	0,14	0,85	0,31	0,7	0,89
5	0,31	0,65	0,15	0,11	0,84	0,31	0,88	0,86
6	0,3	0,31	0,15	0	0,76	0,31	0,88	0,88
7	0,61	0,31	0,4	0	0,81	0,31	0,76	0,84
8	2,75	0,31	0,96	0	0,87	0,31	0,88	0,97
9	1,39	0,31	0,54	0	0,82	0,3	0,81	0,86
10	0,95	0,31	0,92	0,44	0,85	0,31	0,8	0,91
11	0,96	0,31	0,15	0,14	0,86	0,24	0,93	0,89
12	0,96	0,6	0,15	0,15	0,85	0,88	0,78	0,9
13	0,97	2,9	0,14	0,14	0,8	0,89	0,78	0,83

14	0,94	1,53	0,15	0,11	0,86	0,9	0,78	0,94
15	1	0,52	0,15	0	0,84	0,88	0,85	0,87
16	0,9	0,31	0,15	0	0,83	0,88	0,82	0,91
17	0,97	0,31	0,15	0	0,85	1,06	0,81	0,91
18	0,99	0,31	0,34	0	0,83	1,51	0,82	0,88
19	0,95	0,31	0	0,44	0,35	2,74	0,8	0,94
20	0,92	0,31	1,81	0,14	0,3	1,65	0,93	0,87
21	0,91	0,75	0,3	0,15	0,3	0,93	0,8	0,85
22	0,89	0,92	0,15	0,14	0,31	0,98	0,79	0,93
23	0,93	0,85	0,15	0,11	0,3	0,96	0,84	0,81
24	0,86	0,93	0,16	0	0,31	0,34	0,85	0,92
25	0,98	0,88	0,15	0	0,3	0,3	0,83	0,91
26	0,39	0,91	0,15	0	0,3	0,31	0,81	0,87
27	0,31	0,88	0,15	0	0,3	0,3	0,84	0,91
28	0,3	0,88	0,4	0,23	0,78	0,31	0,9	0,88
29	0,3	0,88	0,96	0,65	0,81	0,31	0,82	0,91
30	0,3	0,88	0,54	0,34	0,93	0,8	0,82	0,78
Suma	23,22	21,90	10,03	4,16	20,29	21,72	24,15	26,41
Mínimo	0,29	0,31	0,00	0,00	0,30	0,24	0,47	0,61
Máximo	2,75	2,9	1,81	0,65	0,93	2,74	0,93	0,97
Promedio	0,77	0,73	0,33	0,14	0,68	0,72	0,81	0,88
Desviación estándar	0,4977	0,5153	0,3784	0,1678	0,2474	0,5409	0,0987	0,0663
Coeficiente de variación	64,30%	70,59%	113,17%	120,99%	36,57%	74,71%	12,27%	7,53%

Realizado por: Javier E. Solano Y. 2016

La desviación estándar de la (Tabla 9-4), permite determinar que el promedio de la fluctuación entre los diferentes escenarios con arquitectura VPN correspondiente a los servidores es cero coma tres mil setecientos ochenta y cuatro (0,3784) y entre los clientes es de cero coma mil seiscientos setenta y ocho (0,1678) pertenecen a SSL.

En el (Gráfico 19-4), se visualiza que no hay una diferencia significativa entre las arquitecturas VPN, el de menor significancia es SSL.

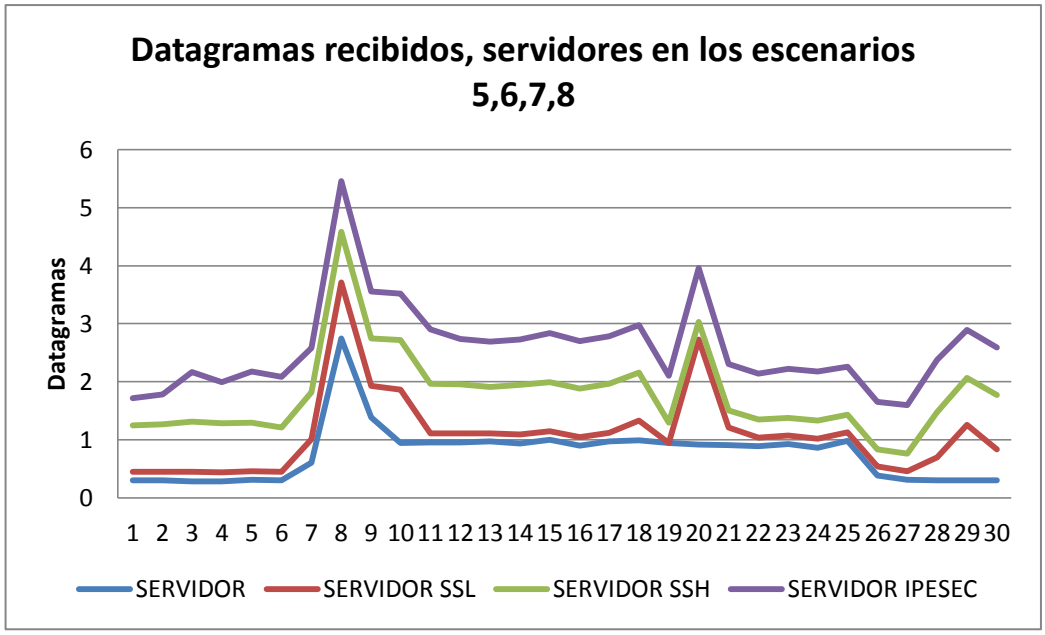


Gráfico 19-4: Datagramas servidores escenarios 5, 6, 7,8 GNS3

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 20-4), se visualiza que no hay una diferencia significativa entre las diferentes arquitecturas en cuanto a los datagramas entre clientes el de menor significancia es SSL.

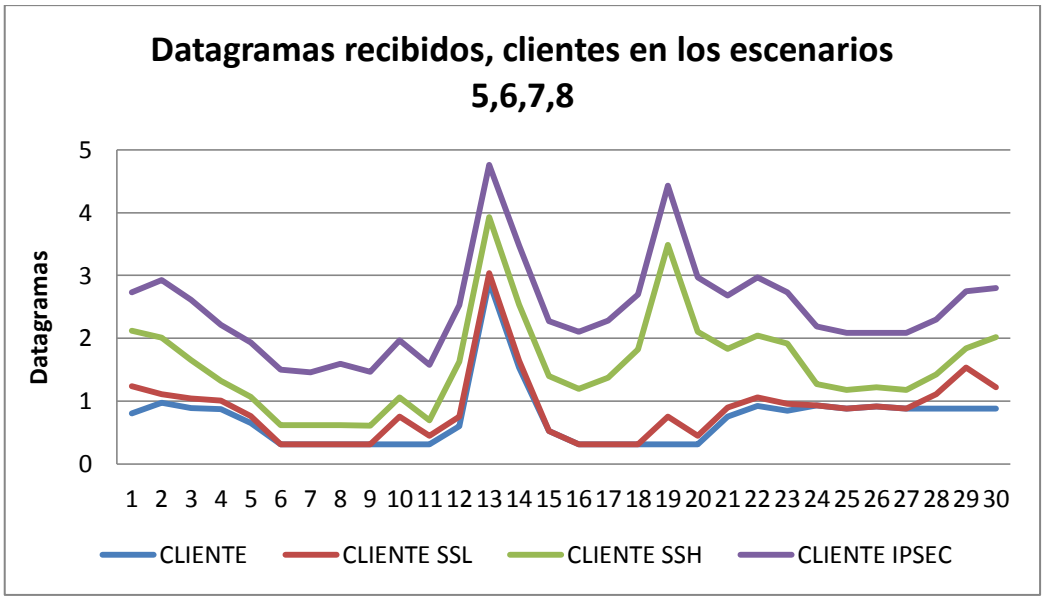


Gráfico 20-4: Datagramas clientes escenarios 5, 6, 7,8 GNS3

Realizado por: Javier E. Solano Y. 2016

4.3.5. *Resumen de la variable dependiente: rendimiento de los promedios obtenidos de las VPNs con el simulador de redes GNS3.*

La (Tabla 10-4), describe los promedios obtenidos de treinta (30) muestras obtenidas de los escenarios cinco, seis, siete, ocho con los diferentes parámetros establecidos para medir el rendimiento de la videoconferencia con las diferentes arquitecturas VPN, estos obtenidos del cliente-servidor.

Tabla 10-4: Tabla comparativa de los indicadores de rendimiento con GNS3

PROMEDIO DEL RENDIMIENTO DE LAS VPN DE 30 MUESTRAS OBTENIDAS								
Rendimiento / VPN	**LATENCIA (ms)**		**JITTER(ms)**		**ANCHO DE BANDA (MB/seg)**		**PORCENTAJE DE DATAGRAMAS RECIBIDOS**	
	Servidor	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**	**Servidor**	**Cliente**
CONEXIÓN	145,02	4153,23	14,41	13,51	0,10	0,06	0,77	0,73
SSL	69,17	53,34	51,18	53,34	0,02	0,02	0,33	0,14
SSH	67,97	81,12	14,63	15,67	0,09	0,06	0,68	0,72
IPSEC	16,19	15,11	17,94	15,11	0,06	0,06	0,81	0,88

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 21-4), se puede observar que del promedio obtenido de latencia, los menores tiempos del Servidor es de dieciséis coma diecinueve (16,19) correspondiente a la arquitectura IPSec.

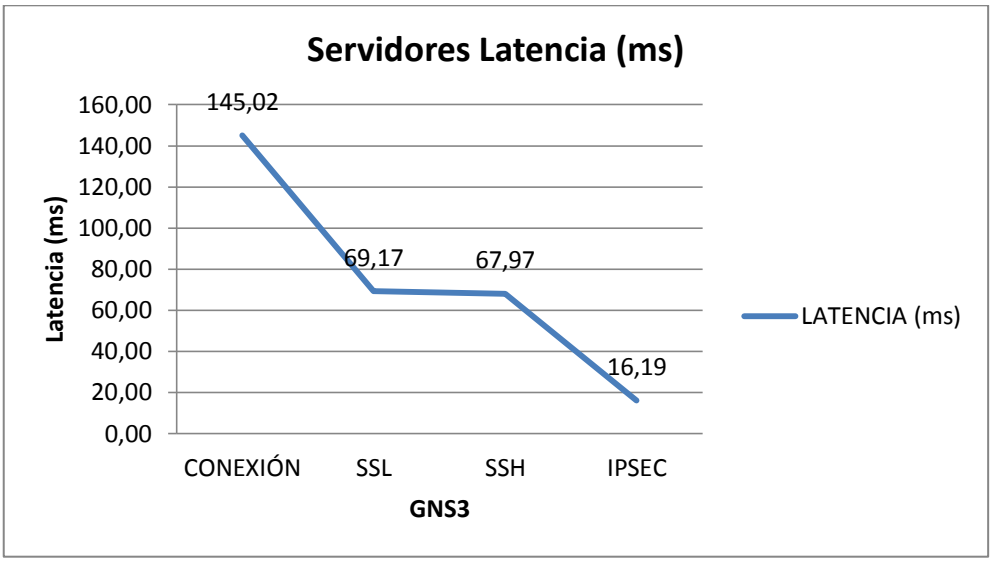


Gráfico 21-4: Latencia servidores escenarios 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 22-4), de los promedios obtenidos de jitter, se puede determinar que los menores tiempos de interferencia corresponde al servidor SSH con valor de catorce coma sesenta y tres (14,63).

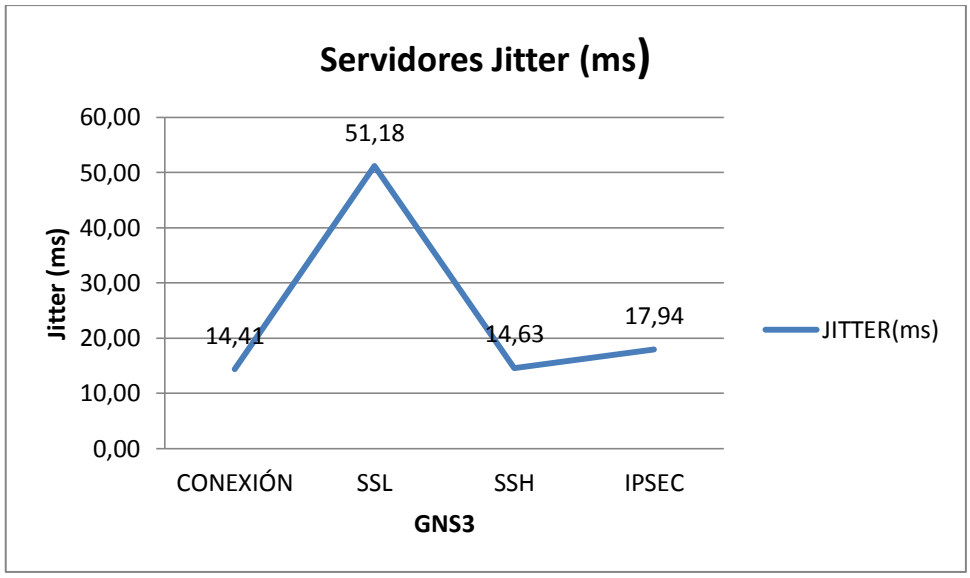


Gráfico 22-4: Jitter servidores escenarios 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 23-4), de los promedios obtenidos del uso de ancho de Banda, se puede determinar que el número de Mbyte menor que utiliza es el servidor SSL con valores de cero coma cero dos (0,02).

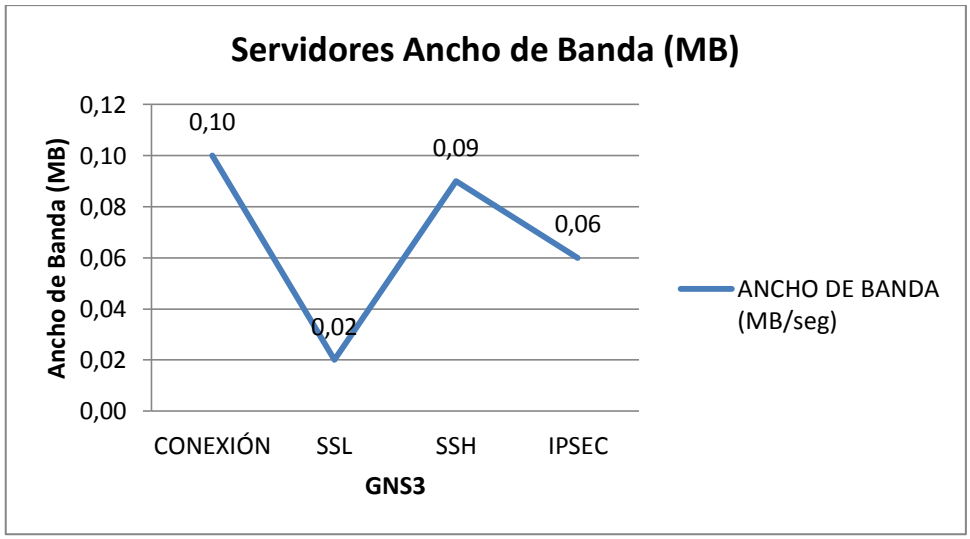


Gráfico 23-4: Ancho de banda servidores escenarios 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

En el (Gráfico 24-4), de los promedios obtenidos del porcentaje de datagramas recibidos se puede determinar que el porcentaje de menor perdida de paquetes corresponde al servidor SSL con valor de cero coma treinta y tres (0,33) que en porcentaje es el de treinta y tres por ciento (33%).

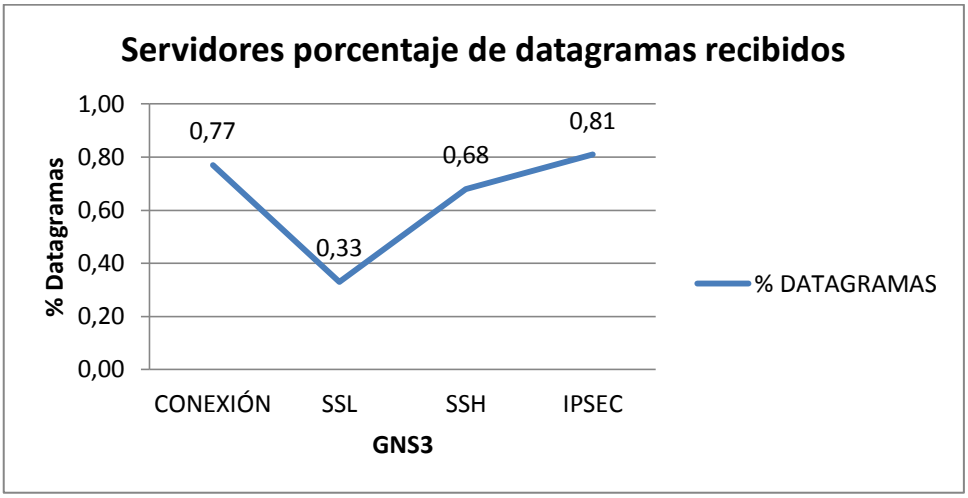


Gráfico 24-4: Datagramas servidores escenarios 5, 6, 7, 8 GNS3

Realizado por: Javier E. Solano Y. 2016

4.3.6. *Wireshark captura de protocolos SSL, SSH, IPSec*

En la (Figura 5-4), con Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante los protocolos SIP, UDP.

192.168.2.3	192.168.1.3	SIP/XML	575	Request: INFO s
192.168.2.3	192.168.1.3	SIP/XML	575	Request: INFO s
192.168.2.3	192.168.1.3	SIP/XML	575	Request: INFO s
192.168.2.3	192.168.1.3	SIP/XML	575	Request: INFO s
192.168.2.3	192.168.1.3	SIP/XML	575	Request: INFO s
192.168.2.3	192.168.1.3	SIP/XML	575	Request: INFO s
192.168.2.2	239.255.255.250	SSDP	175	M-SEARCH * HTTP
169.254.148.252	239.255.255.250	SSDP	175	M-SEARCH * HTTP
192.168.2.2	239.255.255.250	SSDP	175	M-SEARCH * HTTP
192.168.2.2	239.255.255.250	SSDP	175	M-SEARCH * HTTP
192.168.1.3	192.168.2.3	UDP	101	Source port: 70
192.168.2.3	192.168.1.3	UDP	97	Source port: 70
192.168.2.3	192.168.1.3	UDP	99	Source port: 70
192.168.1.3	192.168.2.3	UDP	98	Source port: 70
192.168.2.3	192.168.1.3	UDP	270	Source port: 90
192.168.2.3	192.168.1.3	UDP	104	Source port: 70
192.168.2.3	192.168.1.3	UDP	104	Source port: 70
192.168.2.3	192.168.1.3	UDP	106	Source port: 70
192.168.1.3	192.168.2.3	UDP	279	Source port: 90

Figura 5-4: Transmisión de videoconferencia por RTP Y SIP Linphone

Realizado por: Javier E. Solano Y. 2016

En la (Figura 6-4), con Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante el túnel SSL.

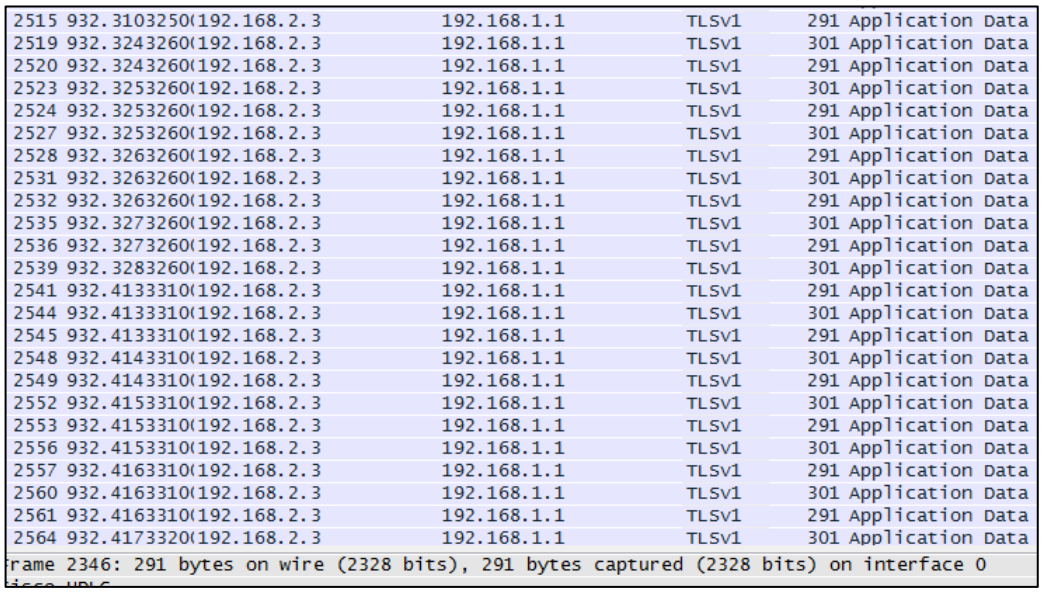


Figura 6-4: Transmisión por el Túnel SSL con Linphone

Realizado por: Javier E. Solano Y. 2016

En la (Figura 7-4), con Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante el túnel SSH.

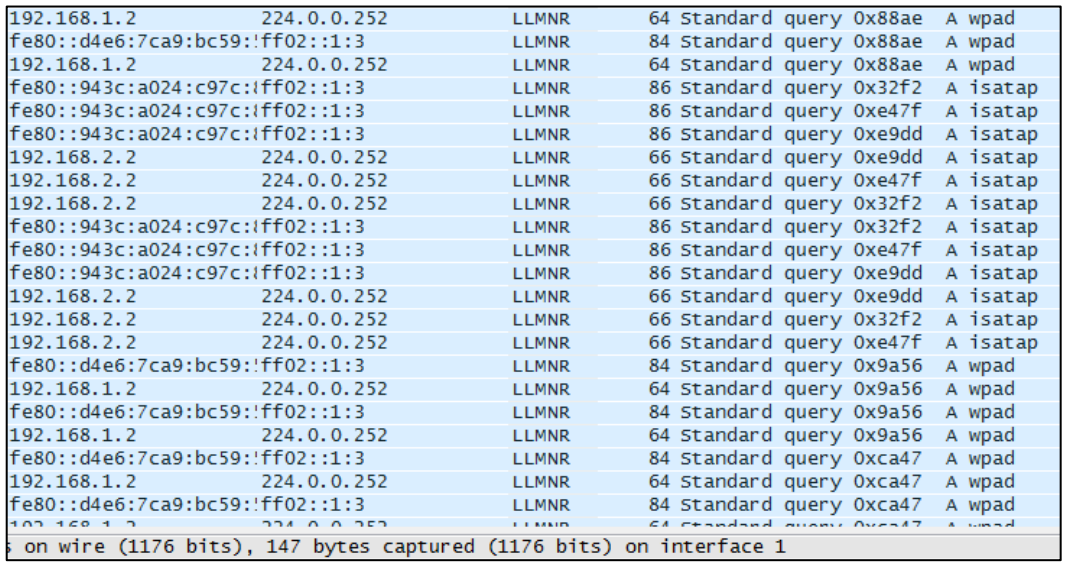


Figura 7-4: Transmisión por el túnel SSH con Linphone.

Realizado por: Javier E. Solano Y. 2016

En la (Figura 8-4), con Wireshark se puede identificar que la trasmisión de la videoconferencia se realiza mediante el túnel ESP de IPSec.

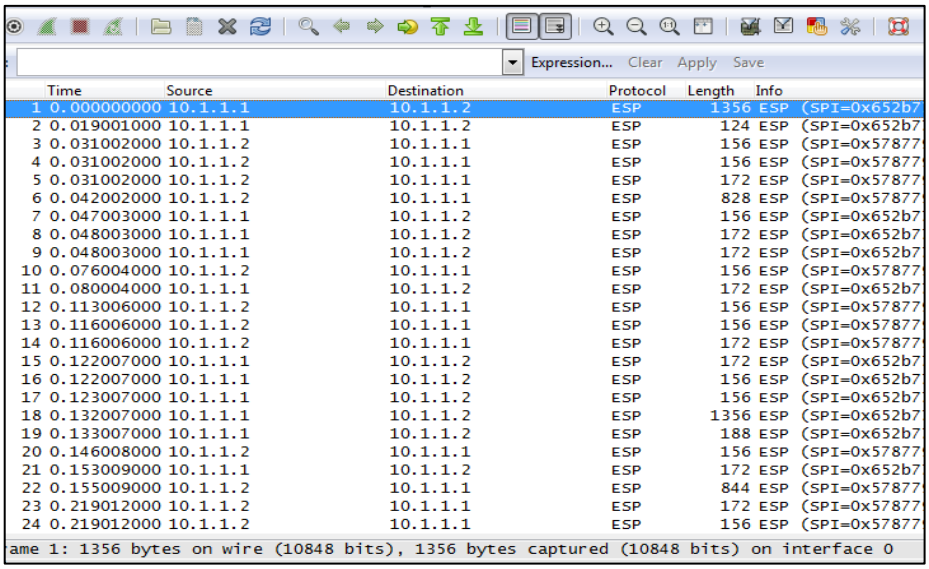


Figura 8-4: Transmisión por el túnel IPSec con Linphone

Realizado por: Javier E. Solano Y. 2016

4.4. Comprobación de la hipótesis de la investigación

Se han establecido diferentes parámetros para la comprobación de la hipótesis en base al rendimiento de cada una de las arquitecturas en los escenarios propuestos con software libre y con el simulador de equipos cisco GNS3.

Los parámetros establecidos para el rendimiento son la latencia, jitter, ancho de banda y porcentaje de datagramas cada uno de estos tabulados con treinta (30) muestras. Para lo cual se utiliza la prueba de la varianza ANOVA de un solo Factor con el propósito de comparar los protocolos o arquitecturas, al igual que comprobar la existencia de diferencias significativas entre las arquitecturas con la comprobación de la hipótesis, dado que el número de comparaciones es alta de cada indicador en las arquitecturas, se ha aplicado la prueba complementaria post hoc de HSD de Tukey.

4.4.1. *Comprobación de hipótesis para software libre*

Las pruebas que se realizaron con software libre para evaluar las arquitecturas de conexión VPN son SSH, SSL, IPSec en los escenarios uno, dos, tres y cuatro que a continuación se detallan.

4.4.1.1. *Anova de un factor para la latencia I.1 con software libre*

Tabla 11-4: Datos descriptivos prueba latencia.

	N° de muestras	Media	Desviación típica	Error típico	Intervalo de confianza para la media al 95%		Mínimo	Máximo
					Límite inferior	Límite superior		
Conexión	30	6,3268	6,77073	1,23616	3,7985	8,8550	,48	26,50
OPENVPN SSL	30	6,9190	4,33810	,79203	5,2991	8,5389	1,32	15,90
OPENSSH	30	3,4662	3,19405	,58315	2,2735	4,6589	,92	12,30
OPENSWAN IPSEC	30	5,0907	4,41379	,80584	3,4426	6,7388	,90	20,32
Total	120	5,4507	4,97536	,45419	4,5513	6,3500	,48	26,50

Realizado por: Javier E. Solano Y. 2016

Tabla 12-4: Prueba ANOVA de un factor latencia

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	209,737	3	69,912	2,964	,035
Intra-grupos	2736,018	116	23,586		
Total	2945,755	119			

Realizado por: Javier E. Solano Y. 2016

Aplicada la prueba de Anova de un factor con un valor alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad, se ha obtenido como resultado un nivel de significancia de cero coma cero treinta y cinco (0,035) esto permite afirmar que entre las arquitecturas establecidas para la conexión VPN, en el indicador I.1, existe una diferencia significativa entre las arquitecturas.

Tabla 13-4: Prueba post hoc de comparaciones múltiples HSD de Tukey para latencia

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	OPENVPN SSL	-,59223	1,25396	,965	-3,8609	2,6764
	OPENSSH	2,86057	1,25396	,108	-,4081	6,1292
	OPENSWAN IPSEC	1,23607	1,25396	,758	-2,0326	4,5047
OPENVPN SSL	Conexión	,59223	1,25396	,965	-2,6764	3,8609
	OPENSSH	3,45280*	1,25396	,034	,1841	6,7215
	OPENSWAN IPSEC	1,82830	1,25396	,466	-1,4404	5,0970
OPENSSH	Conexión	-2,86057	1,25396	,108	-6,1292	,4081
	OPENVPN SSL	-3,45280*	1,25396	,034	-6,7215	-,1841
	OPENSWAN IPSEC	-1,62450	1,25396	,568	-4,8932	1,6442
OPENSWAN IPSEC	Conexión	-1,23607	1,25396	,758	-4,5047	2,0326
	OPENVPN SSL	-1,82830	1,25396	,466	-5,0970	1,4404
	OPENSSH	1,62450	1,25396	,568	-1,6442	4,8932

*. La diferencia de medias es significativa al nivel 0.05.

Realizado por: Javier E. Solano Y. 2016

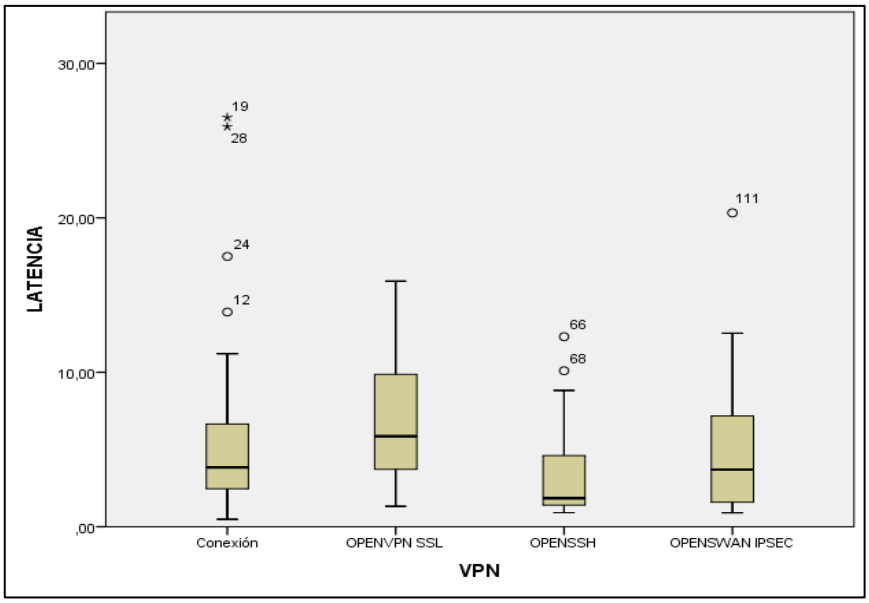


Gráfico 25-4: Representación de caja del indicador I.1 software libre

Realizado por: Javier E. Solano Y. 2016

Como resultado de la prueba post hoc de HSD de Tukey se ha podido determinar a través de la comparación de la prueba testigo (conexión normal para videoconferencia) con los tres protocolos VPN, que no existen diferencias significativas entre la mayoría de ellos.

Con respecto a la hipótesis propuesta que asegura que IPSEC es la mejor arquitectura o protocolo que se debería implementar en una VPN para mejorar el rendimiento en la

transmisión de videoconferencia, se ha comprobado que solamente existen diferencias significativas en la prueba de latencia entre las arquitecturas SSH y SSL con un grado de significancia de cero coma cero treinta y cuatro (0,034). Lo que significa que la hipótesis del investigador se rechaza, ya que la arquitectura IPSec no ha demostrado diferencias con las otras arquitecturas, como se puede observar en la (Tabla 13-4) y el (Gráfico 25-4).

4.4.1.2. *Anova de un factor para el jitter I.2 software libre*

Tabla 14-4: Datos descriptivos prueba de jitter.

	N° de Muestras	Media	Desviación típica	Error típico	Intervalo de confianza para la media al 95%		Mínimo	Máximo
					Límite inferior	Límite superior		
Conexión	30	2,9993	,80780	,14748	2,6977	3,3010	1,70	5,00
OPENVPN SSL	30	4,5723	,66104	,12069	4,3255	4,8192	2,67	5,66
OPENSSH	30	1,7250	,67500	,12324	1,4730	1,9770	,79	3,27
OPENSWAN IPSEC	30	3,4283	1,58398	,28919	2,8369	4,0198	,25	6,23
Total	120	3,1813	1,42625	,13020	2,9234	3,4391	,25	6,23

Realizado por: Javier E. Solano Y. 2016

Tabla 15-4: Prueba ANOVA de un factor jitter

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	124,498	3	41,499	40,945	,000
Intra-grupos	117,570	116	1,014		
Total	242,068	119			

Realizado por: Javier E. Solano Y. 2016

Para la prueba de Anova de un factor de jitter con un valor alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad se ha obtenido un valor de cero coma cero cero (0,00) lo que quiere decir que existe una diferencia significativa entre las arquitecturas para este indicador I.2.

Tabla 16-4: Prueba post hoc de comparaciones múltiples HSD de Tukey para jitter

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	OPENVPN SSL	-1,57300*	,25994	,000	-2,2506	-,8954
	OPENSSH	1,27433*	,25994	,000	,5968	1,9519
	OPENSWAN IPSEC	-,42900	,25994	,355	-1,1066	,2486
OPENVPN SSL	Conexión	1,57300*	,25994	,000	,8954	2,2506
	OPENSSH	2,84733*	,25994	,000	2,1698	3,5249
	OPENSWAN IPSEC	1,14400*	,25994	,000	,4664	1,8216
OPENSSH	Conexión	-1,27433*	,25994	,000	-1,9519	-,5968
	OPENVPN SSL	-2,84733*	,25994	,000	-3,5249	-2,1698
	OPENSWAN IPSEC	-1,70333*	,25994	,000	-2,3809	-1,0258
OPENSWAN IPSEC	Conexión	,42900	,25994	,355	-,2486	1,1066
	OPENVPN SSL	-1,14400*	,25994	,000	-1,8216	-,4664
	OPENSSH	1,70333*	,25994	,000	1,0258	2,3809

*. La diferencia de medias es significativa al nivel 0.05.

Realizado por: Javier E. Solano Y. 2016

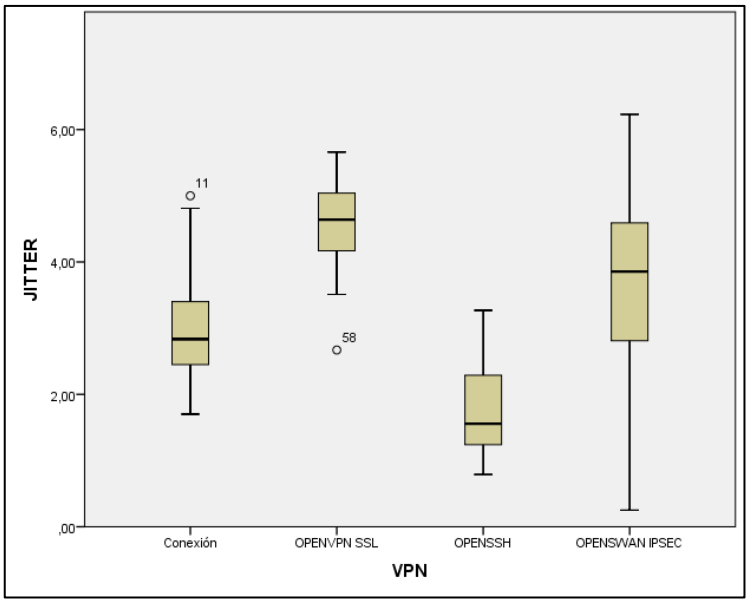


Gráfico 26-4: Representación de caja del indicador I.2 software libre

Realizado por: Javier E. Solano Y. 2016

La prueba de diferencias de medias de HSD de Tukey para el jitter, comparando la prueba testigo (conexión normal para la videoconferencia) con las otras arquitecturas establece que existen diferencias significativas con SSH e IPSec. Con respecto a la hipótesis propuesta que asegura que IPSec es el mejor protocolo que se debería implementar en una VPN para mejorar el rendimiento en la transmisión de videoconferencia, se establece que la diferencia entre IPSec con SSH y SSL es significativa, de acuerdo a la (Tabla 16-4) y el (Gráfico 26-4), que el protocolo con menor interferencia es SSH, por lo que la hipótesis del investigador se rechaza.

4.4.1.3. *Anova de un factor para de banda I.3 con software libre*

Tabla 17-4: Datos descriptivos prueba de ancho de Banda

	N° de Muestras	Media	Desviación típica	Error típico	Intervalo de confianza para la media al 95%		Mínimo	Máximo
					Límite inferior	Límite superior		
Conexión	30	,1233	,00479	,00088	,1215	,1251	,12	,13
OPENVPN SSL	30	,1227	,00450	,00082	,1210	,1243	,12	,13
OPENSSH	30	,1230	,00466	,00085	,1213	,1247	,12	,13
OPENSWAN IPSEC	30	,1217	,00461	,00084	,1199	,1234	,11	,13
Total	120	,1227	,00463	,00042	,1218	,1235	,11	,13

Realizado por: Javier E. Solano Y. 2016

Tabla 18-4: Prueba ANOVA de un factor del ancho de banda

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	,000	3	,000	,722	,541
Intra-grupos	,003	116	,000		
Total	,003	119			

Realizado por: Javier E. Solano Y. 2016

De acuerdo a los resultados obtenidos de la prueba Anova de un factor para el análisis de ancho de banda con un nivel alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad se establece que entre los tres protocolos y la conexión no existen diferencias significativas, como se puede apreciar en la (Tabla 17-4).

Tabla 19-4: Prueba post hoc comparaciones múltiples HSD de Tukey para ancho de banda

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	OPENVPN SSL	,00067	,00120	,945	-,0025	,0038
	OPENSSH	,00033	,00120	,992	-,0028	,0035
	OPENSWAN IPSEC	,00167	,00120	,508	-,0015	,0048
OPENVPN SSL	Conexión	-,00067	,00120	,945	-,0038	,0025
	OPENSSH	-,00033	,00120	,992	-,0035	,0028
	OPENSWAN IPSEC	,00100	,00120	,838	-,0021	,0041
OPENSSH	Conexión	-,00033	,00120	,992	-,0035	,0028
	OPENVPN SSL	,00033	,00120	,992	-,0028	,0035
	OPENSWAN IPSEC	,00133	,00120	,683	-,0018	,0045
OPENSWAN IPSEC	Conexión	-,00167	,00120	,508	-,0048	,0015
	OPENVPN SSL	-,00100	,00120	,838	-,0041	,0021
	OPENSSH	-,00133	,00120	,683	-,0045	,0018

Realizado por: Javier E. Solano Y. 2016

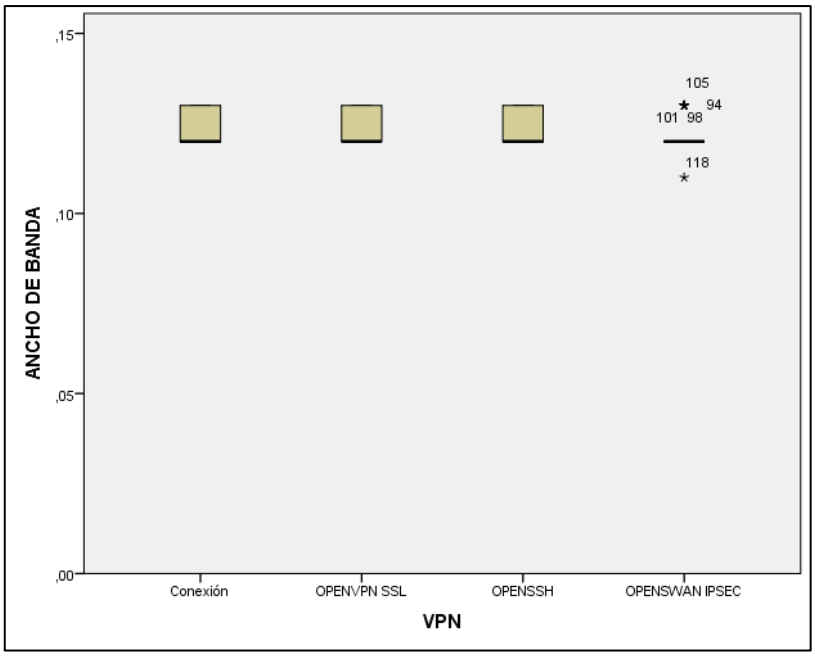


Gráfico 27-4: Representación de caja del indicador I.3 software libre

Realizado por: Javier E. Solano Y. 2016

Como se puede observar en la (Tabla 19-4), luego de la aplicación de la prueba ce HSD de Tukey ningún de los valores obtenidos son significativos, estableciéndose que la hipótesis planteada por el investigador que asegura que IPSec es el mejor protocolo que se debería implementar en una VPN para mejorar el rendimiento en la transición de videoconferencias se rechaza, este resultado se refleja objetivamente y se puede observar en el (Gráfico 27-4).

4.4.1.4. *Anova de un factor para porcentaje de datagramas I.4 con software libre*

Tabla 20-4: Datos descriptivos prueba del porcentaje de datagramas recibidos

	N° de muestras	Media	Desviación típica	Error típico	Intervalo de confianza para la media al 95%		Mínimo	Máximo
					Límite inferior	Límite superior		
Conexión	30	,8900	,01203	,00220	,8855	,8945	,86	,91
OPENVPN SSL	30	,8917	,01020	,00186	,8879	,8955	,87	,92
OPENSSH	30	,8923	,00568	,00104	,8902	,8945	,88	,90
OPENSWAN IPSEC	30	,8747	,02788	,00509	,8643	,8851	,81	,94
Total	120	,8872	,01764	,00161	,8840	,8904	,81	,94

Realizado por: Javier E. Solano Y. 2016

Tabla 21-4: Prueba ANOVA de un factor del porcentaje de datagramas recibidos

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	,006	3	,002	7,981	,000
Intra-grupos	,031	116	,000		
Total	,037	119			

Realizado por: Javier E. Solano Y. 2016

El resultado de la prueba de Anova de un solo factor con un nivel alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad, para el indicador I.4 porcentaje de datagramas recibidos se obtuvo un grado de significancia de cero coma cero cero (0,00) lo que permite decir que entre los protocolos existen diferencias significativas.

Tabla 22-4: Prueba post hoc de comparaciones múltiples HSD de Tukey para porcentaje de datagramas recibidos

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	OPENVPN SSL	-,00167	,00420	,979	-,0126	,0093
	OPENSSH	-,00233	,00420	,945	-,0133	,0086
	OPENSWAN IPSEC	,01533*	,00420	,002	,0044	,0263
OPENVPN SSL	Conexión	,00167	,00420	,979	-,0093	,0126
	OPENSSH	-,00067	,00420	,999	-,0116	,0103
	OPENSWAN IPSEC	,01700*	,00420	,001	,0061	,0279
OPENSSH	Conexión	,00233	,00420	,945	-,0086	,0133
	OPENVPN SSL	,00067	,00420	,999	-,0103	,0116
	OPENSWAN IPSEC	,01767*	,00420	,000	,0067	,0286
OPENSWAN IPSEC	Conexión	-,01533*	,00420	,002	-,0263	-,0044
	OPENVPN SSL	-,01700*	,00420	,001	-,0279	-,0061
	OPENSSH	-,01767*	,00420	,000	-,0286	-,0067

*. La diferencia de medias es significativa al nivel 0.05.

Realizado por: Javier E. Solano Y. 2016

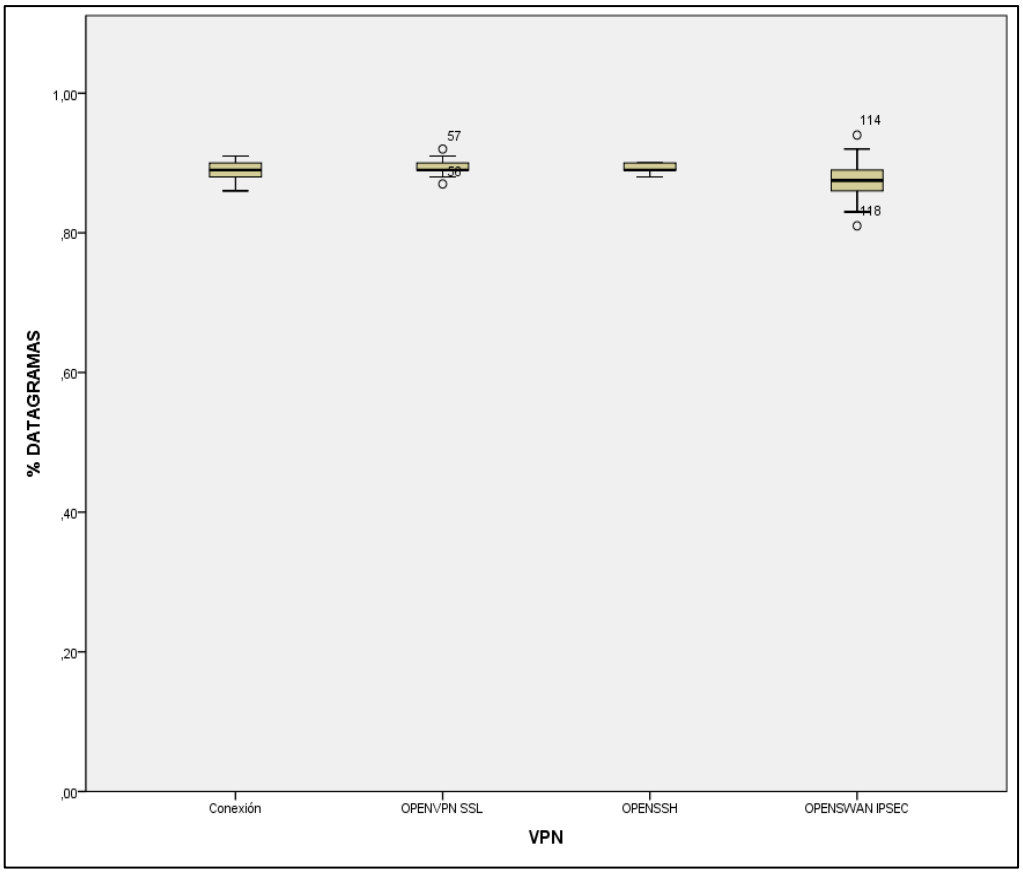


Gráfico 28-4: Representación de caja del indicador I.4 software libre

Realizado por: Javier E. Solano Y. 2016

Con respecto a la comparación realizada entre la prueba testigo (conexión normal para videoconferencia) y los protocolos se observa que no existen diferencias significativas con SSL y SSH mientras que con IPSec existen diferencias significativas.

De los resultados obtenidos en la prueba de HSD de Tukey para la diferencia de medias, para comprobar la hipótesis planteada que asegura que, IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar el rendimiento en la transmisión de videoconferencias, para él porcentaje de datagramas recibidos los niveles de significancia con la prueba de conexión es de cero coma cero dos (0,02) con SSL cero coma cero uno (0,01), con SSH cero coma cero cero cero (0,000), por lo que se acepta la hipótesis del investigador.

4.4.2. *Comprobación de hipótesis para el simulador de equipos GNS3 de cisco*

4.4.2.1. *Anova de un factor para la latencia I.1 con GNS3*

Tabla 23-4: Datos descriptivos prueba latencia.

	N° de muestras	Media	Desviación típica	Error típico	Intervalo de confianza para la media al 95%		Mínimo	Máximo
					Límite inferior	Límite superior		
Conexión	30	145,0197	274,39803	50,09800	42,5578	247,4816	11,34	1438,00
SSL	30	69,1733	25,39590	4,63664	59,6903	78,6563	27,60	122,00
SSH	30	67,9739	22,89610	4,18024	59,4243	76,5234	17,08	119,00
IPSEC	30	16,1907	11,97923	2,18710	11,7175	20,6638	6,85	76,00
Total	120	74,5894	144,21389	13,16487	48,5216	100,6571	6,85	1438,00

Realizado por: Javier E. Solano Y. 2016

Tabla 24-4: Prueba ANOVA de un factor latencia

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	253317,998	3	84439,333	4,409	,006
Intra-grupos	2221601,946	116	19151,741		
Total	2474919,945	119			

Realizado por: Javier E. Solano Y. 2016

Con la utilización del simulador de equipos GNS3 cisco, aplicada la prueba de Anova de un factor con un valor alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad se ha determinado un nivel de significancia de cero coma cero cero seis (0,006), lo que quiere decir que entre los protocolos establecidos para la VPN, con el indicador I.1, coexiste una diferencia significativa.

Tabla 25-4: Prueba post hoc de comparaciones múltiples HSD de Tukey para latencia

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	SSL	75,84633	35,73210	,152	-17,2953	168,9879
	SSH	77,04578	35,73210	,142	-16,0958	170,1874
	IPSEC	128,82900*	35,73210	,003	35,6874	221,9706
SSL	Conexión	-75,84633	35,73210	,152	-168,9879	17,2953
	SSH	1,19944	35,73210	1,000	-91,9422	94,3410
	IPSEC	52,98267	35,73210	,451	-40,1589	146,1243
SSH	Conexión	-77,04578	35,73210	,142	-170,1874	16,0958
	SSL	-1,19944	35,73210	1,000	-94,3410	91,9422
	IPSEC	51,78322	35,73210	,472	-41,3584	144,9248
IPSEC	Conexión	-128,82900*	35,73210	,003	-221,9706	-35,6874
	SSL	-52,98267	35,73210	,451	-146,1243	40,1589
	SSH	-51,78322	35,73210	,472	-144,9248	41,3584

*. La diferencia de medias es significativa al nivel 0.05.

Realizado por: Javier E. Solano Y. 2016

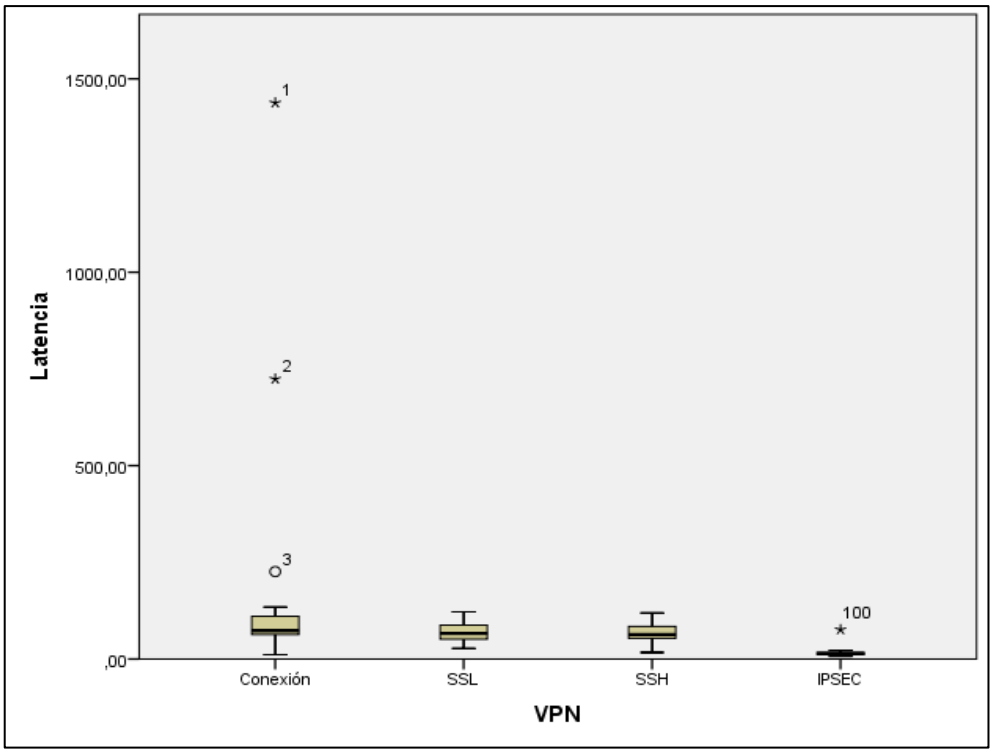


Gráfico 29-4: Representación de caja del indicador I.1 GNS3

Realizado por: Javier E. Solano Y. 2016

Como resultado de la prueba post hoc de HSD de Tukey con respecto a la comparación de la prueba testigo (conexión normal para videoconferencias) con respecto a los tres protocolos con SSL y SSH no existen diferencias, mientras que con IPSec el nivel de significancia es de cero coma cero cero dos (0,002).

Comparando IPSec con los otros protocolos para establecer la valides de la hipótesis con el indicador de rendimiento latencia, utilizando el simulador de equipos GNS3 cisco se asegura que , IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar el rendimiento en la transmisión de videoconferencia, se encuentra que existen diferencias significativas de IPSec con respecto a la conexión normal es de cero coma cero cero dos (0,002) de significancia, con respecto a SSL es de cero coma cero cero uno (0,001) de significancia y con respecto a SSH es de cero coma cero cero cero (0,000) de significancia, aceptándose la hipótesis del investigador con respecto a la latencia con el simulador GNS3 de cisco.

4.4.2.2. *Anova de un factor para el jitter I.2 con GNS3*

Tabla 26-4: Datos descriptivos prueba de jitter

	N° de Muestras	Media	Desviación típica	Error típico	Intervalo de confianza para la media al 95%		Mínimo	Máximo
					Límite inferior	Límite superior		
Conexión	30	14,4120	6,72192	1,22725	11,9020	16,9220	8,27	27,14
SSL	30	51,1787	5,56756	1,01649	49,0997	53,2576	39,02	56,48
SSH	30	14,6270	5,98183	1,09213	12,3933	16,8607	8,37	24,73
IPSEC	30	17,9440	1,93433	,35316	17,2217	18,6663	14,64	22,35
Total	120	24,5404	16,39188	1,49637	21,5775	27,5034	8,27	56,48

Realizado por: Javier E. Solano Y. 2016

Tabla 27-4: Prueba ANOVA de un factor jitter

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	28619,092	3	9539,697	329,791	,000
Intra-grupos	3355,470	116	28,926		
Total	31974,562	119			

Realizado por: Javier E. Solano Y. 2016

Para la prueba de Anova de un factor referente al jitter con el simulador GNS3 Cisco con un valor alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad se ha obtenido un valor de cero coma cero cero (0,0)0 lo que significa que existe una diferencia significativa entre los protocolos para este indicador.

Tabla 28-4: Prueba post hoc de comparaciones múltiples HSD de Tukey para el jitter

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	SSL	-36,76667*	1,38868	,000	-40,3865	-33,1468
	SSH	-,21500	1,38868	,999	-3,8348	3,4048
	IPSEC	-3,53200	1,38868	,059	-7,1518	,0878
SSL	Conexión	36,76667*	1,38868	,000	33,1468	40,3865
	SSH	36,55167*	1,38868	,000	32,9318	40,1715
	IPSEC	33,23467*	1,38868	,000	29,6148	36,8545
SSH	Conexión	,21500	1,38868	,999	-3,4048	3,8348
	SSL	-36,55167*	1,38868	,000	-40,1715	-32,9318
	IPSEC	-3,31700	1,38868	,085	-6,9368	,3028
IPSEC	Conexión	3,53200	1,38868	,059	-,0878	7,1518
	SSL	-33,23467*	1,38868	,000	-36,8545	-29,6148
	SSH	3,31700	1,38868	,085	-,3028	6,9368

Realizado por: Javier E. Solano Y. 2016

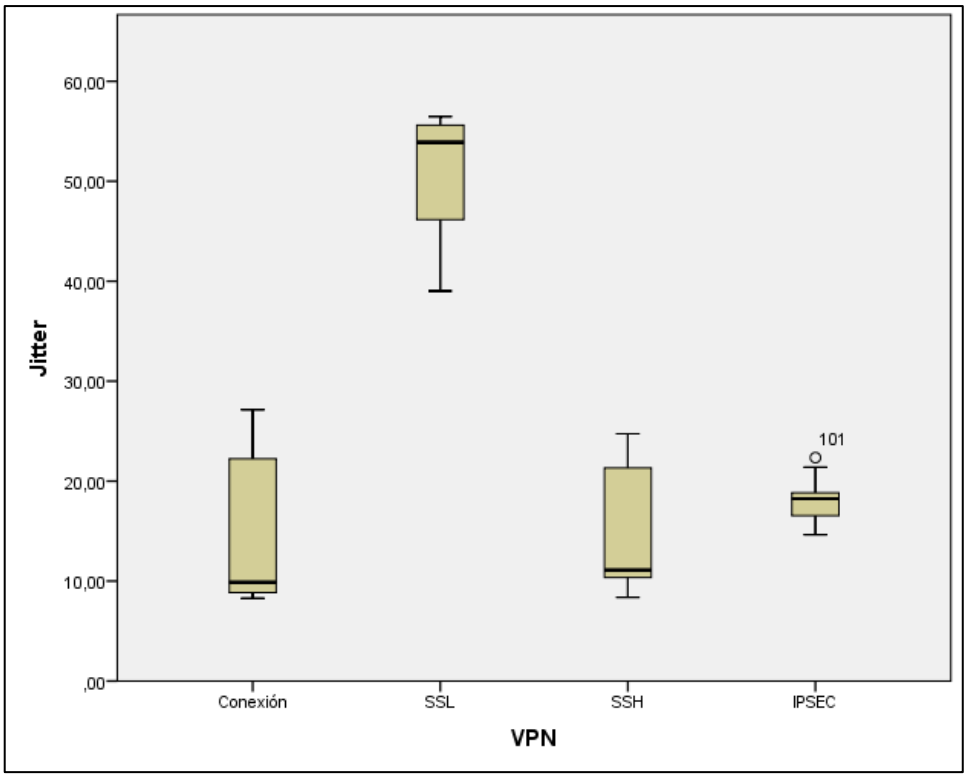


Gráfico 30-4: Representación de caja del indicador I.2 GNS3

Realizado por: Javier E. Solano Y. 2016

Comparando los resultados de la prueba testigo (conexión normal para la videoconferencia) con el simulados GNS3, para jitter con las arquitecturas VPN se ha establecido que no existen diferencias significativas con SSH y con IPSec, pero sí con SSL que es de cero coma cero cero cero (0,000).

La comparación del protocolo IPSec con los otros protocolos VPN utilizando el simulador GNS3 Cisco, para determinar la valides e la hipótesis de que IPSec es el mejor protocolo que se debería implementar en una VPN para mejorar el rendimiento en la transición de videoconferencias, se establece que no existen diferencias significativas con la conexión normal, como tampoco con SSH, se encuentran diferencias de jitter con SSL, rechazándose la hipótesis del investigador. Como se puede observar en la (Tabla 28-4) y el (Gráfico 30-4).

4.4.2.3. *Anova de un factor el ancho de banda I.3con GNS3*

Tabla 29-4: Datos descriptivos prueba de ancho de banda.

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	,115	3	,038	43,801	,000
Intra-grupos	,101	116	,001		
Total	,216	119			

Realizado por: Javier E. Solano Y. 2016

De acuerdo a los resultados obtenidos de la prueba Anova de un factor para el análisis de ancho de banda utilizando el simulador GNS3 de cisco, con un nivel alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad se establece que entre las arquitecturas de conexión VPN existen diferencias significativas, como se puede apreciar en la (Tabla 30-4).

Tabla 30-4: Prueba post hoc de comparaciones múltiples HSD de Tukey para ancho de banda

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	SSL	,08000*	,00762	,000	,0601	,0999
	SSH	,01100	,00762	,475	-,0089	,0309
	IPSEC	,03900*	,00762	,000	,0191	,0589
SSL	Conexión	-,08000*	,00762	,000	-,0999	-,0601
	SSH	-,06900*	,00762	,000	-,0889	-,0491
	IPSEC	-,04100*	,00762	,000	-,0609	-,0211
SSH	Conexión	-,01100	,00762	,475	-,0309	,0089
	SSL	,06900*	,00762	,000	,0491	,0889
	IPSEC	,02800*	,00762	,002	,0081	,0479
IPSEC	Conexión	-,03900*	,00762	,000	-,0589	-,0191
	SSL	,04100*	,00762	,000	,0211	,0609
	SSH	-,02800*	,00762	,002	-,0479	-,0081

*. La diferencia de medias es significativa al nivel 0.05.

Realizado por: Javier E. Solano Y. 2016

Comparando la prueba testigo (conexión normal para videoconferencias) con las arquitecturas VPN para el ancho de banda se establece con SSL e IPSec cero coma cero cero cero (0,000) de nivel de significancia, con SSH, el valor no es significativo.

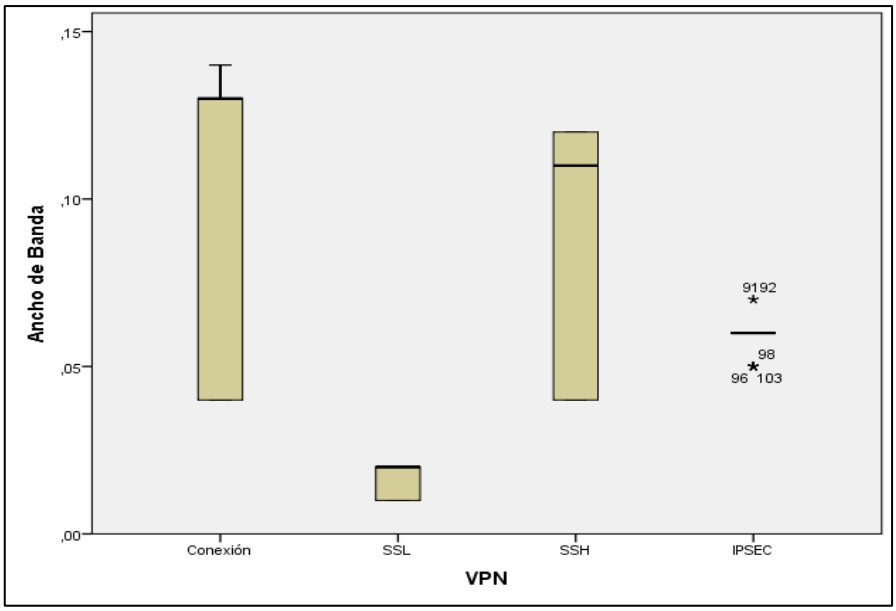


Gráfico 31-4: Representación de caja del indicador I.3 GNS3

Realizado por: Javier E. Solano Y. 2016

Para la comprobación de la hipótesis de que IPSec es el mejor protocolo que se debería implementar en una VPN para mejorar el rendimiento en la transmisión de videoconferencia, la comparación entre los protocolos demuestra que entre IPSec la conexión normal y SSH no existen diferencias significativas, mientras que con el protocolo SSL el nivel de significancia es de cero coma cero cero cero (0,000). Por lo tanto se rechaza la hipótesis del investigador como se puede observar en la (Tabla 30-4) y en el (Gráfico 31-4).

4.2.2.4. *Anova de un factor para el porcentaje de datagramas recibidos I.4 con GNS3*

Tabla 31-4: Datos descriptivos prueba del porcentaje de datagramas recibidos

	N° de Muestras	Media	Desviación típica	Error típico	Intervalo de confianza para la media al 95%		Mínimo	Máximo
					Límite inferior	Límite superior		
Conexión	30	,7740	,49765	,09086	,5882	,9598	,29	2,75
SSL	30	,3343	,37838	,06908	,1930	,4756	,00	1,81
SSH	30	,6763	,24737	,04516	,5840	,7687	,30	,93
IPSEC	30	,8050	,09874	,01803	,7681	,8419	,47	,93
Total	120	,6474	,38439	,03509	,5779	,7169	,00	2,75

Realizado por: Javier E. Solano Y. 2016

Tabla 32-4: Prueba ANOVA de un factor del porcentaje de datagramas recibidos

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	4,191	3	1,397	12,102	,000
Intra-grupos	13,391	116	,115		
Total	17,583	119			

Realizado por: Javier E. Solano Y. 2016

El resultado de la prueba de Anova de un solo factor, con un nivel alfa de cero coma cero cinco (0,05) con tres (3) grados de libertad, para el indicados I.4 del porcentaje de datagramas recibidos con el simulador GSN3 de cisco, se obtuvo un grado de significancia de cero coma cero cero (0,00) interpretando que entre los protocolos existen diferencias significativas.

Tabla 33-4: Prueba post hoc de comparaciones múltiples HSD de Tukey para el porcentaje de datagramas recibidos.

(I) VPN	(J) VPN	Diferencia de medias (I-J)	Error típico	Sig.	Intervalo de confianza al 95%	
					Límite inferior	Límite superior
Conexión	SSL	,43967*	,08773	,000	,2110	,6683
	SSH	,09767	,08773	,682	-,1310	,3263
	IPSEC	-,03100	,08773	,985	-,2597	,1977
SSL	Conexión	-,43967*	,08773	,000	-,6683	-,2110
	SSH	-,34200*	,08773	,001	-,5707	-,1133
	IPSEC	-,47067*	,08773	,000	-,6993	-,2420
SSH	Conexión	-,09767	,08773	,682	-,3263	,1310
	SSL	,34200*	,08773	,001	,1133	,5707
	IPSEC	-,12867	,08773	,461	-,3573	,1000
IPSEC	Conexión	,03100	,08773	,985	-,1977	,2597
	SSL	,47067*	,08773	,000	,2420	,6993
	SSH	,12867	,08773	,461	-,1000	,3573

*. La diferencia de medias es significativa al nivel 0.05.

Realizado por: Javier E. Solano Y. 2016

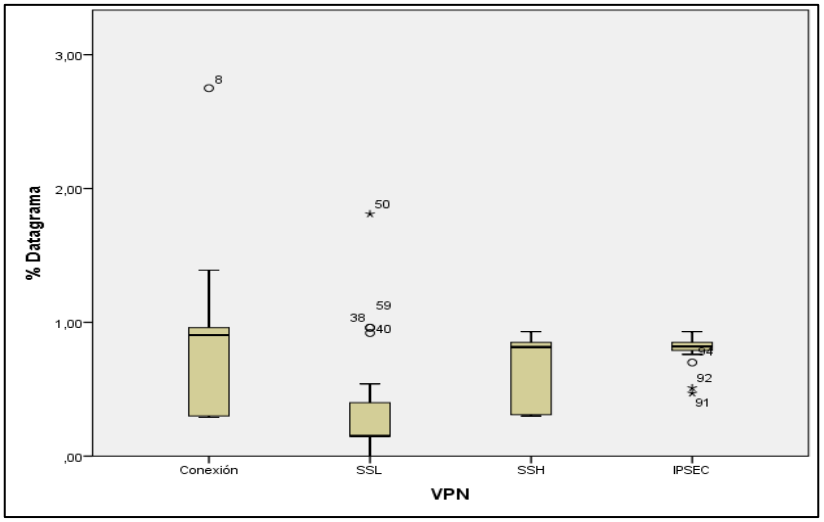


Gráfico 32-4: Representación de caja del indicador I.4 GNS3.

Realizado por: Javier E. Solano Y. 2016

De los resultados obtenidos en la prueba de HSD de Tukey para la comprobación de la hipótesis propuesta por el investigador de que IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar rendimiento en la transmisión de videoconferencia, se ha encontrado que con la comparación de la prueba testigo (conexión normal para videoconferencia) entre las arquitecturas VPN solamente SSL es significativa con cero coma cero cero cero (0,000). Mientras que la comparación de IPSec con la conexión y las otras dos arquitecturas solamente existen diferencias significativas con SSL, rechazándose de esta manera la hipótesis del investigador.

4.4.3. *Cuadro Comparativo de del análisis descriptivo y el análisis de la hipótesis con las arquitecturas para estables diferencias significativas entre las comparaciones múltiples HSD de Tukey de los indicadores*

Tabla 34-4: Prueba post hoc de comparaciones múltiples HSD de Tukey software libre

VPN SOFTWARE LIBRE	I.1 Latencia	I.2 Jitter	I.3 Ancho de banda	I.4 Porcentaje de datagramas recibidos
OpenVPN SSL		0,00		
OpenSSH	0,034	0,00		0,00
OPENSwan IPSec		0,355		0,00

Realizado por: Javier E. Solano Y. 2016

Tabla 35-4: Prueba post hoc de comparaciones múltiples HSD de Tukey GNS3

VPN GNS3	I.1 Latencia	I.2 Jitter	I.3 Ancho de banda	I.4 Porcentaje de datagramas recibidos
SSL				0,00
SSH				
IPSec	0,003	0,00	0,00	

Realizado por: Javier E. Solano Y. 2016

De acuerdo al análisis con los protocolos en la comparación de diferencias significativas de la prueba de Anova de un solo factor con un nivel cero coma cero cinco (0,05) de significancia determinan que la arquitectura adecuada para ser utilizadas son las que están bajo este índice, apoyados en el estudio descriptivo del Capítulo III se puede establecer lo siguiente:

- La (Tabla 34-4), del resumen de los factores que inciden menores a cero coma cero cinco (0,05) de significancia se puede denotar de las pruebas de rendimiento realizadas en las VPN con software libre OpenSSH, tiene un índice de cero coma cero treinta y cuatro (0,034) de latencia, cero coma cero cero (0,00) de jitter, cero coma cero cero (0,00) con respecto a datagramas recibidos, lo que nos permite decir que OpenSSH es la arquitectura para ser implementada en una conexión VPN utilizando software libre para la realización de videoconferencia esto respecto a las pruebas realizadas en los escenario de prueba.

- Como se puede observar en la (Tabla 35-4), los valores de significancia menores de cero coma cero cinco (0,05) en la prueba de Anova de un solo factor con las arquitecturas de conexión VPN con el simulador de redes GNS3 el más adecuado de implementar es: IPSec que tiene un índice de cero coma cero tres (0,03) de latencia, cero coma cero cero (0,00) corresponde al jitter, cero coma cero cero (0,00) para ancho de banda, estos índices nos permiten afirmar lo que este trabajo de investigación plantea en la hipótesis sí; "IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar rendimiento en la transmisión de videoconferencia". Tres índices de rendimiento dan como afirmativo que esta arquitectura es el más adecuado en la transmisión de video conferencia.

CONCLUSIONES

- En las pruebas realizadas con el software libre Iperf para medir el jitter, ancho de banda, porcentaje de datagramas recibidos y la latencia realizado con el comando ping desde en conexiones cliente-servidor , esto en base a la videoconferencia realizada en cada uno de los escenarios uno, dos, tres, cuatro utilizando software libre sobre el sistema operativo Centos y en los escenarios cinco, seis, siete, ocho creados con el simulador de redes GNS3 para equipos cisco, con la obtención de treinta (30) muestras de cada uno de los indicadores se procedió a tabular con valores obtenidos de los servidores ya que el tiempo de respuesta del servidor influirá en el tiempo de transmisión del cliente en el análisis propuesto de la varianza Anova de un solo factor y la prueba post hoc de comparaciones múltiples HSD de Tukey .

- Se puedo determinar que para crear una VPN con software libre el más adecuado es el que pertenece a OPENSSH, porque de acuerdo a las pruebas hechas se obtuvo valores menores al nivel de significancia propuesto que es de cero coma cero cinco (0,05) le corresponden de cero coma cero treinta y cuatro (0,034) de la latencia, cero coma cero cero (0,00) del jitter, cero coma cero cero (0,00) con respecto a datagramas recibidos que de cuatro indicadores en tres tiene menor nivel de significancia. Lo cual permite rechazar la hipótesis planteada de estudio. Esto es corroborado con el análisis descriptivo realizado con las medias de cada uno de las arquitecturas descrita en la (Tabla 5-4) comparaciones realizadas con la media de treinta (30) muestras de datos obtenidas de los escenarios uno, dos, tres, cuatro de los diferentes parámetros de rendimiento propuestos del Capítulo IV.

- Como resultado del estudio también podemos afirmar que para dispositivos Cisco con las pruebas del simulador de redes GNS3 el más adecuado es IPSec con respecto a los niveles de significancia de la prueba de Anova correspondientes a valores de cálculo menores de cero coma cero cinco (0,05) le correspondieron a IPSec cero coma cero tres (0,03) de latencia, cero coma cero cero (0,00) que le corresponde al jitter, cero coma cero cero (0,00) para el ancho de banda con la obtención de estos valores podemos afirmar la hipótesis de estudio planteada que: “IPSec es el mejor protocolo que se debería implementar en una arquitectura VPN para mejorar rendimiento en la Transmisión de Videoconferencia”. ya que en tres indicadores están bajo el nivel de significancia de la prueba realizada. Esto es corroborado con el análisis descriptivo realizado con las medias de cada uno de las arquitecturas descrita en la (Tabla 10-4) comparaciones realizadas con la media de treinta (30) muestras de datos obtenidas de los escenarios cinco, seis, siete, ocho de los diferentes parámetros de rendimiento propuestos del Capítulo IV.

RECOMENDACIONES

- Para los escenarios en la simulación de equipos cisco con GNS3 es necesario identificar el modelo del router con su respectivo IOS esto permitirá realizar las configuraciones, el correcto funcionamiento de las arquitecturas VPN que se desean implementar para la configuración de VPN SSL, SSH, IPSec ya que cada uno de ellos utiliza diferentes versiones, VPN SSL utiliza certificados que deben ser validados desde la interface de red del router para que permite la autenticación.

- Para implementación de las VPN es útil establecer cuáles son las características en el cifrado de claves para la creación de túneles, ya que cada uno de ellos tiene estándares distintos para la generación de credenciales y de llaves para acceder a los túneles con el uso individual de algoritmos de encriptación y autenticación.

- Instalar el GNS3 en una PC robusta en cuanto a la memoria RAM ya que el simulador consume mucho CPU del computador, GNS3 cuenta con herramientas para la optimización del uso del CPU para lo cual se recomienda configurar el Idle de cada equipo a simular para minimizar de manera considerable el consumo de recursos.

- Una alternativa es el uso de software libre para establecer servicios de conexión uso de servicios mediante aplicaciones de software instalables en equipos nada sofisticados permitiendo ahorrar sustancialmente presupuestos es decir no demandan costos altos y cualquier empresa lo pueda implementar, a diferencia del uso de equipos que la mayoría tiene costo un poco alto.

GLOSARIO DE TERMINOS

Ancho de Banda: Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información.

Cliente: Es una aplicación informática o un ordenador que consume un servicio remoto en otro ordenador conocido como servidor, normalmente a través de una red de telecomunicaciones. También se puede definir un cliente es cualquier cosa que se conecta a un servidor que no sea otro servidor.

Criptografía de clave simétrica: Sistema de cifrado en que el emisor y el receptor de un mensaje comparten una sola clave común. Esa clave común se emplea para cifrar y descifrar el mensaje. Las claves simétricas se usan para cifrar la mayor parte de las transmisiones de datos en IPSec. DES constituye un ejemplo de sistema de claves simétricas.

Criptografía por clave pública: Sistema criptográfico basado en dos claves. La clave pública es de dominio general. La clave privada sólo la conoce el destinatario del mensaje. IKE proporciona claves públicas para IPSec.

Datagrama: Un datagrama es un paquete discreto de datos y cabeceras que contiene direcciones, que es la unidad básica de transmisión a través de una red IP, llamado también paquete.

Gateway: Puerta de enlace Es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más computadoras.

GNS3: Es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, **GNS3** está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.
IOS: Archivos binarios comprimidos, que el GNS3 desempaqueta y utiliza para la creación de proyectos.

IP: Protocolo de internet, en dos versiones IPv4; Esta versión admite un espacio de direcciones de 32 bits. IPv6; admite espacio de direcciones de 128 bits.

IPSEC: (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. **IPSec** también incluye protocolos para el establecimiento de claves de cifrado.

IPX: IPX (*Internetwork Packet Exchange*) es un protocolo de Novell que interconecta redes que usan clientes y servidores, protocolo orientado a paquetes y no orientado a conexión (esto es, no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino).

Jitter: El *Jitter* suele considerarse como una señal de ruido no deseada. En general se denomina Jitter a un cambio indeseado y abrupto de la propiedad de una señal en (ms).

LAN: Una **red de área local** o **LAN** (por las siglas en inglés de *Local Área Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

Latencia: Es el tiempo que toma un paquete de data para moverse a través de una conexión de red (ms).

OSI: El **modelo OSI** (Open Systems InterConnect ion) (ISO/IEC 7498-1) es un producto del esfuerzo de Open Systems InterConnect ion en la Organización Internacional de Estándares. Es una prescripción de caracterizar y estandarizar las funciones de un sistema de comunicaciones en términos de abstracción de capas.

RTP: Es la abreviación de Real-time Transport Protocol, por su denominación en Inglés. Es un estándar creado por la IETF para la transmisión confiable de voz y video a través de Internet.
Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "el servidor".

SIP: El protocolo SIP permite el establecimiento de sesiones multimedia entre dos o más usuarios. Para hacerlo se vale del intercambio de mensajes entre las partes que quieren comunicarse.

SSH: (Secure SHell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SSL: Significa "Secure Sockets Layer". **SSL** Definición, Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás.

TCP/IP: (Transmission Control Protocol/Internet Protocol) es el protocolo o lenguaje de comunicaciones básico de Internet. También se usa como protocolo de comunicaciones en redes privadas (tanto intranet como extranet).

UDP: Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo.

Videoconferencia: Sistema de comunicación multimedia que permite, a través de una red de computadoras, que varios participantes puedan verse y hablar en tiempo real, estando a distancia. Se trasmite de forma bidireccional y simultánea, imágenes y sonidos.

VoIP: Proviene del inglés Voice Over Internet Protocol, que significa "voz sobre un protocolo de internet". Básicamente VoIP es un método por el cual tomando señales de audio analógicas del tipo de las que se escuchan cuando uno habla por teléfono se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección IP determinada.
VPN: Una **VPN (Red Privada Virtual)**: Se trata de una red virtual que permite realizar conexiones de forma totalmente privada, ocultando, y con ello también protegiendo, nuestros datos y actividades.

WAN: Es una red de gran cobertura en la cual pueden transmitirse datos a larga distancia, con facilidades de comunicación entre diferentes localidades de un país. En estas redes por lo general se ven implicadas las compañías telefónicas.

WiFi: Es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11.

BIBLIOGRAFÍA

[1.]. **ARRIBAS, A.** (Enero de 2006). *Intranet para la Gestión del Conocimiento y la Comunicación Interna*. Recuperado el 17 de Octubre de 2015, de http://www.razonypalabra.org.mx/anteriores/n48/aarribas.html

[2.] **AYARE, M.** (15 de Abril de 2010). *Conexión a Internet*. Recuperado el 17 de Octubre de 2015, de http://arayemla.blogspot.com/2010/04/conector-vpn.html

[3.] **BERMUDEZ FERNÁNDEZ, J., & CASANOVA VASQUEZ, M.** (2011). *PGP encriptación y cifrado simetrico.* México: semana 13.

[4.] **CEDILLO DURÁN, M., & MOLINA MICHALO, A.** (2006). *Configuaración de una red privada virtual VPN para la transmición de una Pc Cliente (Windows XP), con un servidor Lunux* . Cuenca: Universidad del Azuay.

[5.] **CEVALLOS RODRIGUEZ, M.** (2006). *Diseño e implementación de una red visrtual privada entre las oficinas de INFONET, ubicadas en la ciudad de Quito y Miami.* Quito: ESPE.

[6.] **CISCO.** (31 de Julio de 2013). *Mejora de seguridad de los routers de Cisco*. Recuperado el 17 de Octubre de 2015, de http://www.cisco.com/cisco/web/support/LA/7/74/74465_21.html

[7.] **DAVILA , J., LOPEZ, J., & ROMÁN, R.** (2010). *Introducción de Aplicaciones UDP en Redes Privadas Virtuales*. Recuperado el 4 de 11 de 2015, de Universidad de Malaga: https://www.nics.uma.es/sites/default/files/papers/JorgeDavila2001.pdf

[8.] **DE LUZ, S.** (4 de Noviembre de 2010). *Criptografía : Algoritmos de cifrado de clave simétrica - See more at: http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/#sthash.mekW3tua.dpuf*. Recuperado el 16 de Octubre de 2014, de http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

[9.] **ESPINOZA GARCÍA, R., & MORALE LUNA, G.** (2007). *Una arquitectura de seguridad para IP.* México: CINVESTAV-IPN.

[10.] **ESPINOZA VELEZ, J. V.** (2006). *Estudio de los mecanismos de seguridad de las redes privadas virtuales.* Cuenca: Universidad politécnica Salesiana.

[11.] **GARCÍA COLLIN, R.** (4 de Diciembre de 2012). *implementacion de seguridad en dispositivos ADSL*. Recuperado el 17 de Octubre de 2014, de http://dispositivosadslyseguridad.blogspot.com/

[12.] **GONZÁLEZ, I., GÓMEZ, F., & LÓPEZ , S.** (03 de 2006). *Implementación de SSH sobre un Sistema Auto-Reconfigurables*. Recuperado el 10 de 09 de 2010, de Universidad Autónoma de Madrid: https://repositorio.uam.es/bitstream/handle/10486/667396/implementacion_gonzalez_JCRA_2006.pdf?sequence=1

[13.] **INEM.** (2012). *Ficha de servicios de tecnologías de información.* Quito: Inem.

[14.] **LEMUS BERNAL , C., ESTUPIÑAN CUESTA, E., & GUILLÉN PINTO, E.** (2013). Evaluación del rendimiento de redes ópticas para aplicaciones de telemedicina en ambientes simulados. *Tecnura*, 21 - 40.

[15.] **LÓPEZ JIMENEZ, W.** (9 de Mayo de 2009). *Alcance Libre*. Recuperado el 17 de Octubre de 2014, de VPN en servidor Linux y clientes Windows/Linux con OpenVPN + Shorewall [Parte 1]: http://www.alcancelibre.org/staticpages/index.php/openvpn-clientes-win-linux-shorewall-P1

[16.] **LUJAN MONTES, E.** (2005). *Seguridad el el IP con el protocolo IPSEC para IPV6.* Guatemala: Universidad de San Carlos de Guatemala.

[17.] **MARCELLINO , Á., & MOLLO , D.** (2007). *Video Conferencia*. Comahue: Universidad Nacional del Comahue.

[18.] **MICROSOFT.** (2005). *VPN basadas en Internet*. Recuperado el 17 de Octubre de 2015, de https://msdn.microsoft.com/es-es/library/cc778605%28v=ws.10%29.aspx

[19.] **MONTES DE LOS SANTOS, A., CORONA CARRIÓN, J., & GONZÁLES BELTRAN, J.** (2012). *Propuesta para la implementación de una VPN.* México: Instituto Politécnico Nacional.

[20.] **MORALES SALCEDO, R.** (2008). *Estanbdares de intemporalidad de los Sistemas de Video Conferencias.* Puebla: Universidad de las Américas.

[21.] **MORALES VASQUEZ, M. J.** (2002). *SSL, Secure Sockets Layer y Otros Protocolos Seguros para el comercio electrónico.* Madrid: Universidad politécnica de Madrid.

[22.] **MORENO BRITO, M.** (2008). *Diseño e implementación de un sistema integrado de comunicaciones para la red corporativa Intertrading "Ardilla".* Quito: ESPE.

[23.] **ÑACATO GUALOTUÑA , M. A.** (2007). *Diseño e implementación de una red privada visrtual (VPN, para la empresa HATO Telecomunicaciones.* Quito: Escuela Politécnica Nacional.

[24.] **OÑATE, L.** (2009). *La Metodología PACIE.* FATLA.

[25.] **ORTEGA, C. M.** (2003). *Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace.* Ibarra: Universidad Técnica del Norte.

[26.] **PITA, L.** (15 de Marzo de 2009). *Arquitectura de Red*. Recuperado el 16 de Octubre de 2014, de http://laurapita.blogspot.com/2009/03/arquitectura-de-red.html

[27.] **RIV UAEH.** (2009). *Acerca de la Video Conferencia*. Recuperado el 17 de Octubre de 2015, de http://virtual.uaeh.edu.mx/riv/videoconferencia.php

[28.] **RIVEST, R., SHAMIR, A., & ADLEMAN, L. (**1983). Us Patent No 4,405,859 . Washington: DC: UPatent an Trademark Office.

[29.] **ROMERO TEMERO, M. C.** (2004). *Seguridad en redes y protocolos asociados.* México.

[30.] **RUÍZ GONZÁLES, J. L.** (2002). VPN - Redes Privadas Virtuales. *Redes privadas Visrtuales*, 2.

[31.] **SIERRA RODRÍGUEZ, A.** (2008). *Instalación de un sistema VoIP corporativo basado en Asterisk.* Cartagena: Universidad Técnica de Cartagena.

[32.] **SOSA DELGADO, M., & VELAZQUES SANCHES, D.** (Noviembre de 2000). *Redes Privadas Virtuales, estudio de sus principales algoritmos de encriptación y protocolos e implementación del algoritmo DES*. Recuperado el 8 de 10 de 2015, de http://bibdigital.epn.edu.ec/bitstream/15000/5260/1/T1676.pdf

[33.] **TORRES CARRIÓN, H. (**Julio de 2010). *Diseño de Seguridad Informática en la implementación del Data Center de Loja*. Recuperado el 6 de 9 de 2010, de Universidad de Cuenca: http://dspace.ucuenca.edu.ec/handle/123456789/2535

[34.] **UNIVERSIDAD AUTONOMA DE MEXICO "UNAM".** (2012). *Fundamentos de Criptografia*. Recuperado el 16 de Octubre de 2014, de Principales Algoritmos Simétricos - 3DES o TDES: http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/4-criptografia-simetrica-o-de-clave-secreta/41-introduccion-a-la-criptografia-simetrica/413-principales-algoritmos-simetricos?showall=&start=5

[35.] **VILLACIS MENDOZA, J. L.** (2009). *Analisis, diseño e implementación de una redd inalámbrica en el colegió internacional SEK_Quito, cosiderando aspectos de seguridad perimetral.* Quito: Universidad Internacional SEK.

ANEXOS

Anexo A: Captura del trafico UDP con Iperf del servidor SSH

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[5] 0.00-1.00 sec	64.0 KBytes	0.06 MBytes/sec	1132.235 ms	83/91 (91%)
[5] 1.00-2.00 sec	0.00 Bytes	0.00 MBytes/sec	1132.235 ms	0/0 (nan%)
[5] 2.00-3.00 sec	8.00 KBytes	0.01 MBytes/sec	1169.869 ms	229/230 (1e+02%)
[5] 3.00-4.00 sec	16.0 KBytes	0.02 MBytes/sec	1107.063 ms	0/2 (0%)
[5] 4.00-5.00 sec	8.00 KBytes	0.01 MBytes/sec	1071.074 ms	0/1 (0%)
[5] 5.00-6.00 sec	16.0 KBytes	0.02 MBytes/sec	1016.081 ms	0/2 (0%)
[5] 6.00-7.00 sec	8.00 KBytes	0.01 MBytes/sec	987.732 ms	0/1 (0%)
[5] 7.00-8.00 sec	0.00 Bytes	0.00 MBytes/sec	987.732 ms	0/0 (nan%)
[5] 8.00-9.00 sec	16.0 KBytes	0.02 MBytes/sec	1007.467 ms	47/49 (96%)
[5] 9.00-10.00 sec	8.00 KBytes	0.01 MBytes/sec	977.704 ms	0/1 (0%)
[5] 10.00-11.00 sec	8.00 KBytes	0.01 MBytes/sec	987.886 ms	489/490 (1e+02%)
[5] 11.00-12.00 sec	0.00 Bytes	0.00 MBytes/sec	987.886 ms	0/0 (nan%)
[5] 12.00-13.00 sec	0.00 Bytes	0.00 MBytes/sec	987.886 ms	0/0 (nan%)
[5] 13.00-14.00 sec	0.00 Bytes	0.00 MBytes/sec	987.886 ms	0/0 (nan%)

Anexo B: Captura del trafico UDP con Iperf del servidor SSL

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[3] 0.0- 1.0 sec	0.02 MBytes	0.02 MBytes/sec	39.019 ms	1/ 15 (6.7%)
[3] 1.0- 2.0 sec	0.02 MBytes	0.02 MBytes/sec	52.918 ms	0/ 15 (0%)
[3] 2.0- 3.0 sec	0.02 MBytes	0.02 MBytes/sec	54.170 ms	0/ 16 (0%)
[3] 3.0- 4.0 sec	0.02 MBytes	0.02 MBytes/sec	55.166 ms	0/ 15 (0%)
[3] 4.0- 5.0 sec	0.02 MBytes	0.02 MBytes/sec	55.613 ms	0/ 15 (0%)
[3] 5.0- 6.0 sec	0.02 MBytes	0.02 MBytes/sec	54.916 ms	0/ 15 (0%)
[3] 6.0- 7.0 sec	0.01 MBytes	0.01 MBytes/sec	51.906 ms	30/ 40 (75%)
[3] 7.0- 8.0 sec	0.01 MBytes	0.01 MBytes/sec	46.155 ms	91/ 96 (95%)
[3] 8.0- 9.0 sec	0.00 MBytes	0.00 MBytes/sec	45.257 ms	52/ 54 (96%)
[3] 9.0-10.0 sec	0.00 MBytes	0.00 MBytes/sec	45.429 ms	91/ 92 (99%)
[3] 0.0- 1.0 sec	0.02 MBytes	0.02 MBytes/sec	40.599 ms	0/ 15 (0%)
[3] 1.0- 2.0 sec	0.02 MBytes	0.02 MBytes/sec	53.631 ms	0/ 15 (0%)
[3] 2.0- 3.0 sec	0.02 MBytes	0.02 MBytes/sec	56.482 ms	0/ 14 (0%)
[3] 3.0- 4.0 sec	0.02 MBytes	0.02 MBytes/sec	55.499 ms	0/ 15 (0%)

Anexo C: Captura del trafico UDP con Iperf del servidor IPSec

[3] local 192.168.1.3 port 5001 connected with 192.168.2.3 port 48892
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[3] 0.0- 1.0 sec 0.07 MBytes 0.07 MBytes/sec 14.721 ms 0/ 47 (0%)
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[3] 1.0- 2.0 sec 0.07 MBytes 0.07 MBytes/sec 16.552 ms 4/ 51 (7.8%)
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[3] 2.0- 3.0 sec 0.05 MBytes 0.05 MBytes/sec 14.828 ms 49/ 86 (57%)
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[3] 3.0- 4.0 sec 0.06 MBytes 0.06 MBytes/sec 15.667 ms 29/ 70 (41%)
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[3] 4.0- 5.0 sec 0.06 MBytes 0.06 MBytes/sec 15.944 ms 48/ 88 (55%)
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams