UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRONICA Y TELECOMUNICACIONES

“IMPLEMENTACIÓN DEL PROTOCOLO GETVPN PARA OPTIMIZAR EL PROCESO DE SEGURIDAD MEDIANTE LA ENCRIPTACIÓN DE TRÁFICO EN UNA ENTIDAD FINANCIERA”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

RAMOS ZAPANA, JOHN WILLIAMS

Villa El Salvador
2017

DEDICATORIA

A mis padres

Por todo su apoyo incondicional en todo momento de mi vida, por siempre estar en los momentos felices y difíciles de mi vida, por aquellos consejos, palabras que me motivaron a seguir en pie de lucha cuando sentía que ya todo estaba perdido, por su comprensión, ayuda, amor que siempre me brindan y sobre todo por la confianza depositada en mí, porque hoy en día soy lo que soy gracias a ellos.

A mi esposa e hijos quienes son el motivo fundamental de mi vida, brindándome comprensión y apoyo hasta incluso en los momentos más turbulentos de mi vida, gracias por el apoyo incondicional y la confianza que depositan en mí.

A mis hermanos

Por su incondicional apoyo y motivación a lo largo de toda mi vida, por esos buenos c consejos y palabras de motivación para seguir adelante y sobre todo por siempre estar en los momentos claves de mi vida apoyándonos siempre en todo momento.

AGRADECIMIENTO

A papá Dios

Por darme la vida, por haberme acompañado, guiado y permitirme el haber llegado hasta este momento tan importante de mi formación profesional con salud, fortaleza para poder seguir luchando por mis sueños.

A mis padres

Por enseñarme que todo sacrificio es recompensado, que si uno se propone algo lucha por sus ideales y lo consigue sin importar que tan lejos esté de ello practicando la perseverancia.

Y sobre todo por enseñarme el verdadero significado de Familia

A mis padrinos

Por haber apostado siempre por mí, por estar en las buenas y en las malas, por orientarme en lo largo de toda mi carrera profesional y formar parte de este proyecto.

A mis asesores

Ing. Bernardo Castro Pulcha, Ing. Jeanpierre Soto Salvatierra, Ing. Kervy Ramos Zapana, Ing. Cesar Ramos Mosqueira; por todo su apoyo y asesoramiento en este proyecto de tesis y no solo asesores sino que también por formar parte de mi formación profesional como catedráticos y guías para ser un profesional competitivo.

Son muchas las personas que han formado parte de mi vida profesional a las cuales agradezco por brindarme su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

En la actualidad, la transferencia de datos que realizan los bancos y el intercambio de información confidencial entre el organismo regulador de la banca y los bancos que operan en nuestro país, necesitan de protocolos de seguridad. Los especialistas en redes y comunicaciones de nivel senior's y junior's deben analizar diversas posibilidades que les pueda brindar la seguridad de la transferencia de datos seguros en tiempo real para proteger la integridad de las transacciones que realizan los bancos.

Este es el caso del área de Redes y Comunicaciones de las empresas privadas de Redes, que preocupados en la mejora de la eficiencia en sus áreas de TI, concentran su atención en implementaciones de protocolos, el mismo que ayude a mejorar la seguridad de transferencia de datos.

Existe una problemática en la etapa de implementación del protocolo IPSec, por la complejidad de realizar túneles para cada sede de la empresa, ya que va a encriptar el paquete del router por cada sucursal, pero desde esa perspectiva nace otro problema, que hace que el especialista se adecue a la trasformación del encabezado del paquete del router, pudiendo no respetar políticas de seguridad ni los QoS.

Para resolver dicha problemática se implementó el protocolo GETVPN, el mismo que permitirá ayudar a mantener la seguridad y la encriptación evitando la complejidad de crear tuéneles y poner el riesgo la administración de seguridad en cada sede de la identidad financiera.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

Es necesario que la entidad financiera de nuestro proyecto con la estructura actual requiera un protocolo de seguridad que pueda solucionar los actuales problemas en la red del banco, lo cuales son la complejidad de administrar todos los túneles de todas sus sedes que actualmente se tiene y el problema de que el la tecnología IPSec implementada cambia el encabezado del paquete(reenviado por los routers), ya que nuestro proveedor da el servicio de tipos de calidad de servicio (QoS) pero al cambiarse el header (encabezado) no se puede explotar este servicio ya que no hay manera de clasificar el tráfico de origen y destino original.

Muchos de los especialistas en redes y comunicaciones buscan siempre de suites de protocolos que cumplan con la seguridad en lo que respecta con la transmisión de datos en los dispositivos de redes, ya sea en la parte de redes LAN, WAN o VPNs (Redes Privadas Virtuales). En redes privadas virtuales se utiliza en la actualidad la tecnología de seguridad IPsec, el cual brinda seguridad,

integridad, autenticación y anti-replay al momento de establecer comunicación entre dos puntos (site to site), y como también ya antes mencionado esta tecnología realiza una transformación de encabezado el cual se podría no llegar a respetar las políticas generadas por el proveedor.

1.2 Justificación del proyecto

Visto la problemática mencionada anteriormente es importante implementar el protocolo GETVPN ya que tiene beneficios como optimizar la escalabilidad por lo que esta tecnología no utiliza túneles, la cual proporciona seguridad de extremo a extremo manteniendo la inteligencia de la red como conexiones full-mesh, routing y QoS. Asimismo, el protocolo permitirá preservar la dirección IP de origen y destino en el encabezado del paquete (copia el encabezado original y realiza el encriptado). De esta manera se soluciona la problemática de preservar el encabezado original para poder aplicar políticas de QoS, Se implementara el protocolo en los proyectos realizados por el área de TI.

1.3 Delimitación del Proyecto

- **Delimitación Temporal**

  El trabajo ha sido efectuado entre los días 1 y 30 de enero del 2017 y actualmente está operativo con los beneficios proyectados.

- **Delimitación Espacial**

  Se llevó a cabo en la ciudad de Lima.

- **Delimitación Conceptual**

  GETVPN se basa en un modelo de seguridad de miembros confiables. Los miembros de un grupo de GETVPN pueden comunicarse entre sí utilizando una política común, por lo que no es necesaria la negociación de túneles entre los GMs.

1.4 Formulación del Problema

1.4.1 Problema General

¿De qué manera la implementación del protocolo GETVPN permite mejorar el proceso de seguridad mediante la encriptación de tráfico en una entidad financiera?

1.4.2 Problemas Específicos

- ¿De qué manera la implementación del protocolo GETVPN permite respetar el marcado de tráfico para una mejor QoS y respetar políticas de seguridad?

- ¿De qué manera la implementación del protocolo GETVPN permite no cambiar el encabezado de los paquetes?

- ¿De qué manera la implementación del protocolo GETVPN permite no hacer túneles por destino o sucursal?

1.5 Objetivos

1.5.1 Objetivo General

Implementar el protocolo GETVPN para optimizar el proceso de seguridad mediante la encriptación de tráfico en una entidad financiera.

1.5.2 Objetivos Específicos

- Implementar el protocolo GETVPN para respetar el marcado de tráfico para una mejor QoS y respetar las políticas de seguridad.

- Implementar el protocolo GETVPN para permitir preservar el encabezado original de los paquetes enviados por los router.

- Implementar el protocolo GETVPN para no realizar túneles por cada destino o sucursal implementada.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

- Antecedente 01:

Título: Diseño y evaluación de nivel de seguridad del protocolo GETVPN en una red de datos para un entorno multipunto que utiliza MPLS para su comunicación WAN.

Autor: Aimacaña Valladares, Darwin Ramiro

Esta tesis presenta las aplicaciones y tecnologías actuales como la computación distribuida, voz y video sobre IP, que ahora requiere una comunicación eficiente y segura entre sitios remotos o sucursales de manera instantánea. Para proporcionar un cierto grado de conexión de malla completa (Full Mesh) o incluso una conectividad de malla parcial, las soluciones basadas en túnel IP requieren la provisión de una conexión de mallado complejo, a más de implementación de seguridades tradicionales con IPSEC punto a punto, la cual sufre de problemas de replicación de multidifusión porque esta debe ser realizada antes de la encapsulación del túnel y el cifrado. Con este antecedente se hace necesario buscar un

mecanismo que elimine las conexiones punto a punto, manteniendo los niveles de seguridad y convergencia de las aplicaciones sensibles como son voz y video, es por eso que en este trabajo se realiza un análisis del mecanismo de VPNs multipunto multipunto (Aimacaña Valladares, Darwin Ramiro, 2014).

- Antecedente 02:

Título: Encriptacion GETVPN para el banco nacional de Colombia

Autor: Bonilla Puerto, Carlos Alberto

El presente trabajo de tesis propone la encriptación de la red de comunicaciones del banco nacional de Colombia aplicando tecnologías de calidad de servicio y alta disponibilidad para solucionar los problemas de comunicaciones de la empresa. Para lo cual se realizó el análisis de las tecnologías de calidad de servicio y alta disponibilidad utilizadas en el diseño de los sistemas de comunicaciones, los mismos que constituyen un conjunto de medidas, técnicas y mecanismos tendientes a garantizar la disponibilidad y calidad de los servicios de comunicaciones en la entidad financiera. (Bonilla Puerto, Carlos Alberto, 2010).

- **Antecedente 03:**

Título: GETVPN para protección de canales MPLS en redes utilizadas para el transporte de información de clientes del sector financiero y privada

Autor: Luis Álvaro Velásquez

Es una tecnología VPN túnel inferior o sea que no utiliza túneles la cual proporciona seguridad de extremo a extremo para el tráfico de red en un modo nativo y mantenimiento la inteligencia de la red como conexiones full-mesh, routing, QOS. GETVPN Utiliza la capacidad de la red de núcleo para poder enrutar y replicar los paquetes entre diferentes sitios dentro de la empresa. Por lo tanto, es en gran medida adecuado para una empresa que se encuentre corriendo sobre una MPLS (Luis Álvaro Velásquez, 2013).

- **Antecedente 04:**

Título: Diseño e implementación de solución GETVPN

Autor: Diego Ortiz Rodríguez

El presente trabajo de diseño e implementación propone la solución del problema existente hoy en día, cuando se quiere garantizar seguridades a nivel WAN, es que estas están en marcadas para topología punto a punto (any to any) lo cual hace que se genere inconvenientes para las empresas u organizaciones que requieren soluciones de comunicación eficientes en topologías multipuntos – multipunto. (Diego Ortiz Rodríguez, 2015).

- **Antecedente 05:**

Título: Tecnología GETVPN en el sector financiero

Autor: Enzo Angeles

La seguridad no es un aspecto a descuidar y por ello resulta necesario fortalecer la infraestructura tecnológica adaptándola a las nuevas

tendencias y preparándola para afrontar las amenazas emergentes contra la confidencialidad, integridad y disponibilidad de sus activos de información. Ello implicará construir un nivel de seguridad de red que detecte y bloquee los ataques de software invasivo, el acceso por parte de intrusos, proteja los límites e interiores de la red corporativa con el uso de Firewalls perimetrales y sistemas de monitoreo en base a comportamientos de red (Firewall , Cisco Adaptive Security Appliances -ASA y Cisco Intrusion Prevention System -IPS), asegurar la confidencialidad de la información que viaja entre oficinas del Banco, encriptando esta data desde el origen hasta el destino (Group Encrypted Transport VPN - GETVPN) (Enzo Angeles, 2012).

2.2 Bases Teóricas

2.2.1. Protocolo

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores.

Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

También se define como un conjunto de normas que permite la comunicación entre ordenadores, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse. (Licesio J. Rodríguez., 2013).

2.2.2. VPN

Una VPN o Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local.

En la informática una Red Privada Virtual (RPV) o Virtual Private Network (VPN) supone una tecnología de red que, por razones de costo y comodidad, brinda la posibilidad de conectarse a una red pública generando una extensión a nivel de área local. Por caso, este tipo de redes se utilizan a la hora de conectar dos o más oficinas de una empresa a través de Internet. Esto facilita la conexión y el intercambio a un bajo costo económico, y permite que miembros de un mismo equipo se conecten entre sí desde locaciones remotas.

Las VPN funcionan de manera tal que, si bien se utiliza una red pública como es la de conexión a Internet, los datos son transmitidos por un canal privado, de forma que no peligra la seguridad ni la integridad de la información interna. Los datos son cifrados y descifrados alternativamente, ahorrando dinero y problemas a empresas de distinta escala. A continuación se muestra un cuadro comparativo (tabla 01) de redes con las ventajas de la tecnología VPN.

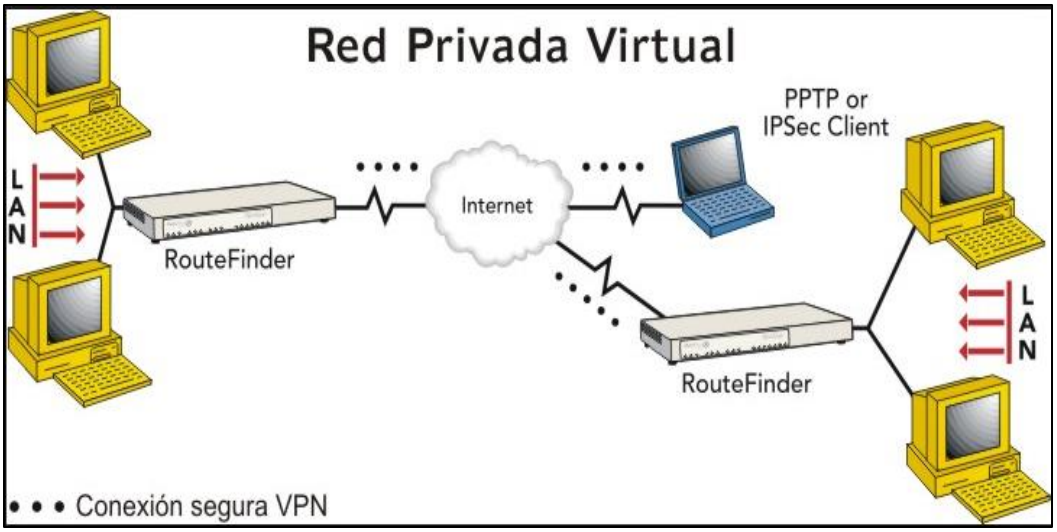
Tabla 01: Cuadro comparativo de redes

LAN	WAN	VPN
*Es interconexión de uno o varios dispositivos. *Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps. *Utiliza medios de transmisión como: el cable coaxial, cables telefónicos, fibra óptica y Wi-Fi. *Operan dentro de área geográfica limitada	Operan dentro de un área geográfica extensa. *Suministra velocidad parcial y continua. *Conecta dispositivos separados por grandes distancias, e incluso a nivel mundial. *División entre líneas de transmisión y elementos de conmutación.	*ofrece conectividad segura y confiable en una infraestructura de red pública compartida. *es la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa. *tiene una buena calidad del servicio.

Fuente: https://es.slideshare.net/tutorial-4-28344060

Si se tiene en cuenta el costo que supondría conectar dos oficinas en dos países distintos como se muestra en la figura 1, las VPN son una excelente alternativa que se vale de una tecnología ya existente de redes interconectadas para crear una red más pequeña y privada. (Roberto Nader Carreon, 2008).

Figura 01: Estructura de la tecnología VPN



Fuente: https://www.incubaweb.com/sabes-una-red-vpn-se-puede-utilizar/

2.2.3. Key Server

Es responsable de la aceptación o rechazo de los miembros dentro de la VPN, la generación/regeneración y la distribución de las claves de cifrado, y la implementación de las políticas de cifrado a todos los miembros de grupos registrados, comúnmente denominados passwords.

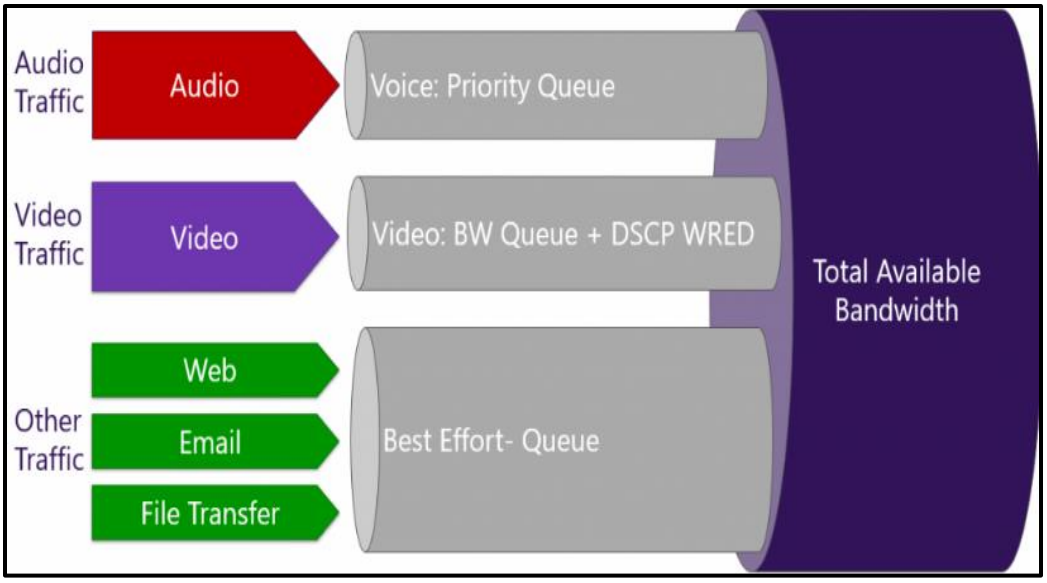
Se requiere un único servidor de claves, pero varios servidores de claves se puede implementar y se recomienda para proporcionar redundancia y equilibrio de carga ya que la función de encriptación de la VPN es totalmente dependiente de la disponibilidad del servidor de claves (Itzcoatl Espinosa, 2014).

2.2.4. QoS

QoS o **Calidad de Servicio** (*Quality of Service*, en inglés) es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente mide la calidad de los servicios que son considerados en varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter, etc.

Calidad de servicio es particularmente importante para el transporte de tráfico con requerimientos especiales. En particular, muchas tecnologías han sido desarrolladas para permitir a las redes de computadoras ser tan útiles como las redes de teléfono para conversaciones de audio, así como el soporte de nuevas aplicaciones con demanda de servicios más estrictos. En la figura 02, se muestra la distribución del tráfico (QoS). (Itzcoatl Espinosa, 2014).

Figura 02: Estructura de calidad de servicio



Fuente: http://conexionzero.com/configuracion-de-calidad-de-servicio-qos-en-skype-for-business/

2.2.5. IPSec

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. En la tabla 02 se aprecia las ventajas que brinda la tecnología.

Tabla 02: Características VPN-IPSec

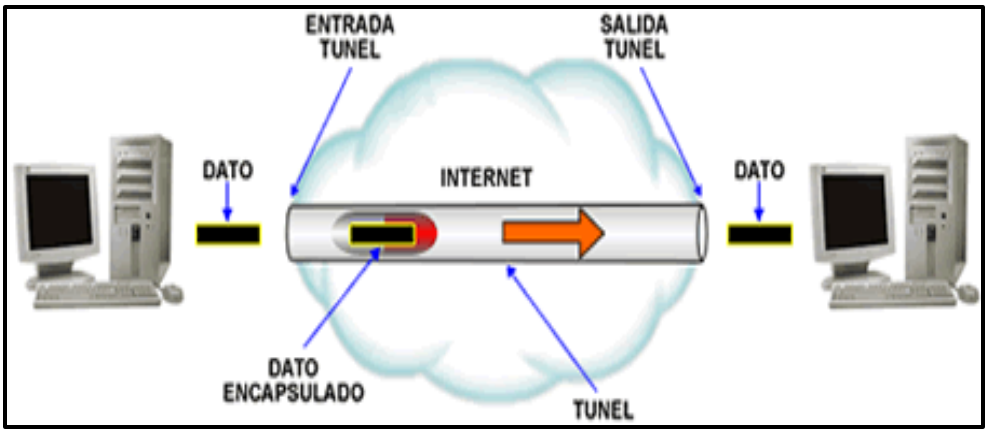
CARACTERISTICAS	VPN-IPSec
Ventajas para administrar	• El cifrado se lo realiza entre sitios
Cuando usar	• Se utiliza cuando se requiere interoperabilidad de múltiples proveedores
Topología	• Topología punto a punto
Ruteo	• No soporta
Multicast	• No soporta
Seguridad	• No dispone de servidor de claves
Túneles	• Si usa
Encriptación	• Soporta
Encabezado original	• No preserva
Alta disponibilidad	• Se genera conmutación de errores

Fuente: http://www.http-peru.com/protocolo_ipsec.php

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores.

Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, como se muestra en la figura 03 el dato solo es encapsulado sin ningún cambio ni transformación, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código. (Steve Friedl, 2012).

Figura 03: Estructura del protocolo IPSec



Fuente: http://www.http-peru.com/protocolo_ipsec.php

2.2.6. GDOI Grupo

El concepto GET-VPN se basa en un modelo de "grupo de confianza" cuyos miembros emplean una metodología de seguridad común. La configuración del grupo GDOI, especificado en el servidor de claves, contiene los parámetros necesarios para establecer y mantener las políticas de cifrado entre miembros del grupo

Después de que las pasarelas VPN se autentican y se proporcionan con las claves de seguridad apropiadas a través de IKE SA, IKE SA expira y GDOI se utiliza para actualizar los GM de una manera más escalable y eficiente (Enlace Blindado Cisco, 2012).

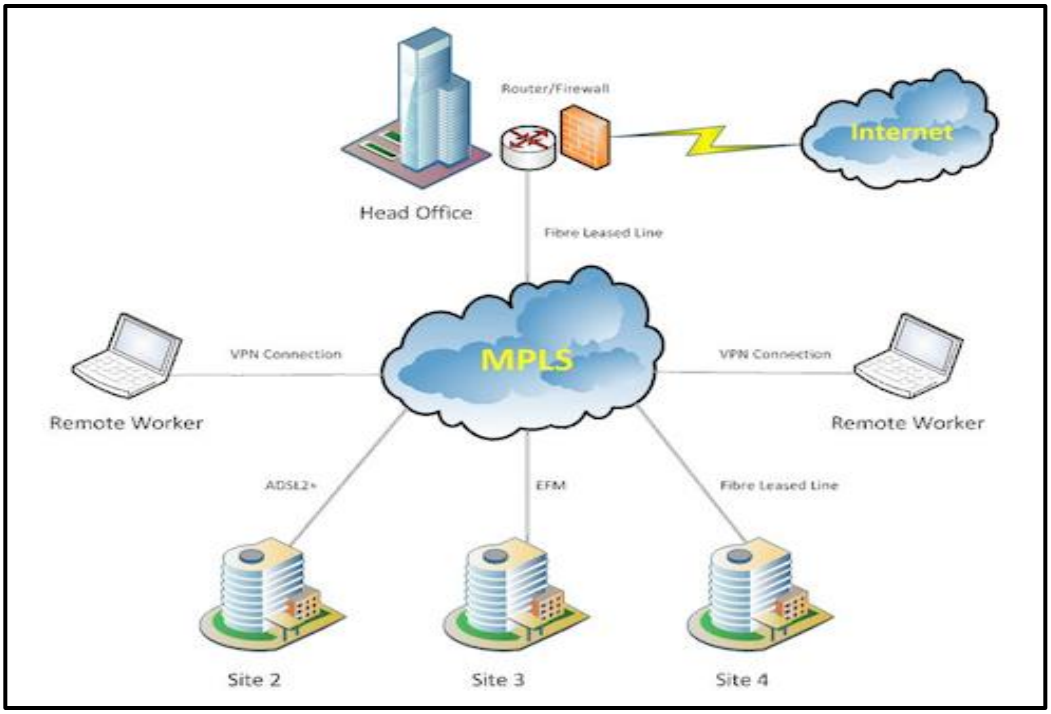
2.2.7. MPLS

MPLS es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. En la figura 04 se muestra la representación de MPLS.

En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router.

La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla (Jose Manuel Huidobro Moya, 2002).

Figura 04: Representación de MPLS para la transmisión de datos



Fuente: https://mastermoviles.gitbooks.io/tecnologias2/content/protocolos_de_comunicacion_en_red.html

2.2.8. GMs (MIEMBRO DE GRUPO)

Un GM es un enrutador IOS responsable de la encriptación y descifrado real, es decir, un dispositivo responsable de manejar el plano de datos GET VPN.

Un GM solo se configura con los parámetros de información KS / Grupo. Las políticas de cifrado se definen centralmente en el KS y se descargan al GM en el momento del registro.

Basándose en estas políticas descargadas, GM decide si el tráfico debe ser cifrado o descifrado y qué claves utilizar. En una red GET

VPN, las políticas GM son dictadas por el KS, pero en algunos casos, un GM puede configurarse para anular localmente algunas de estas políticas. Cualquier política global (incluyendo las entradas de permiso y de denegación) definida en el KS afecta a todos los miembros del grupo si es aplicable a ellos o no y por lo tanto algunas políticas tienen más sentido cuando se definen localmente. Por ejemplo, si un puñado de GM en el grupo está ejecutando un protocolo de enrutamiento diferente, se puede agregar una entrada local a estos GMs para evitar el cifrado del tráfico de protocolo de enrutamiento en lugar de definir la política globalmente en el nivel KS. (Enlace Blindado Cisco, 2012).

2.2.9. Preservación del encabezado del túnel

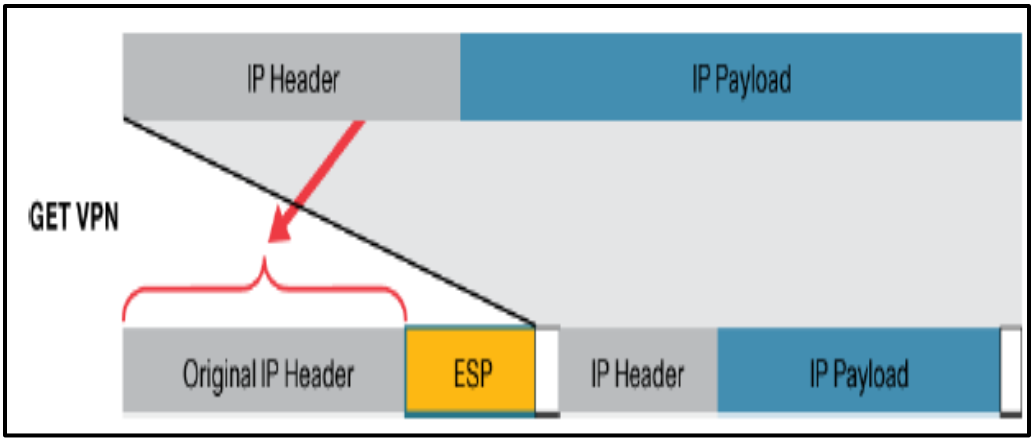
En IPsec tradicional, las direcciones de punto final del túnel se utilizan como nuevo origen de paquetes y destino. El paquete se enruta entonces sobre la infraestructura IP, utilizando la dirección IP de origen de la pasarela de cifrado y la dirección IP de destino de la pasarela de descifrado. En el caso de GET VPN, los paquetes de datos protegidos IPsec encapsulan las direcciones originales del paquete de origen y de destino del host en el encabezado IP externo para "conservar" la dirección IP.

La mayor ventaja de la preservación de encabezado de túnel es la capacidad de enrutar los paquetes cifrados utilizando la infraestructura

de enrutamiento de red subyacente. La alta disponibilidad (HA) proporcionada por la infraestructura VPN IP, VPLS o MPLS (radios dobles, enlaces dobles, etc.) se integra perfectamente con la solución GET VPN. No es necesario proporcionar HA a nivel IPsec (hubs dobles, stateful IPsec HA, etc.).

Debido a que la preservación del encabezado de túnel se combina con SA de grupo, la replicación de multidifusión puede descargarse a la red del proveedor. Como cada GM comparte la misma SA, el enrutador IPsec más cercano a la fuente de multidifusión no necesita replicar paquetes a todos sus pares y ya no está sujeto a problemas de replicación de multidifusión que se ven en las soluciones IPsec tradicionales, tal como se muestra en la figura 05. (Cisco , 2012).

Figura 05: Preservación del encabezado del túnel



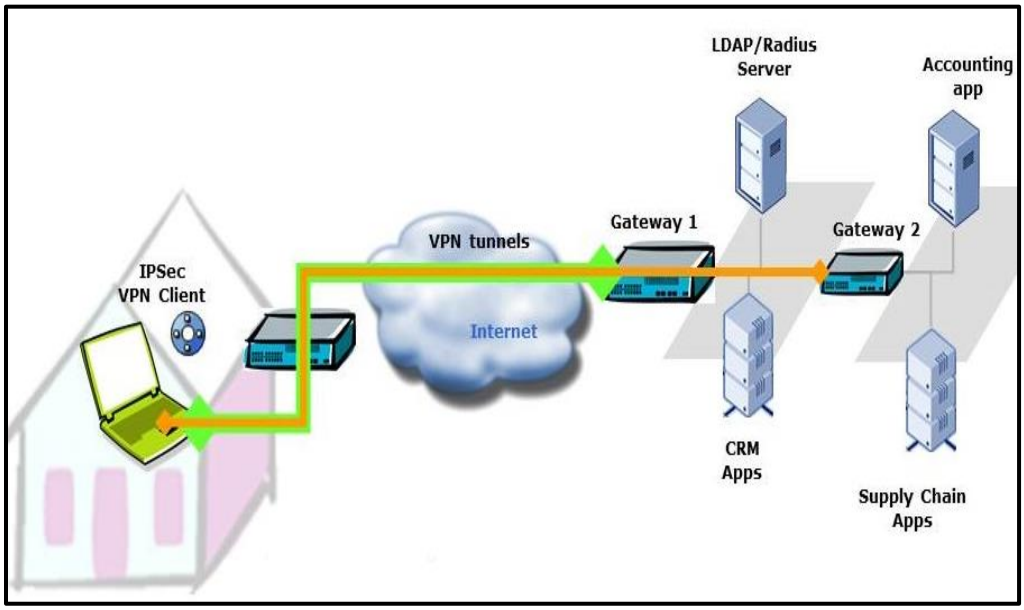
Fuente: Guía de diseño e implementación de VPN (GETVPN) CISCO, 2012

2.2.10. Tunneling o túnel

El tunneling es una tecnología que permite enviar datos en una red mediante otras conexiones de la red, como se muestra en la figura 06. El tunneling funciona encapsulando el protocolo de red dentro de paquetes transportados por la segunda red. También es conocido como encapsulation (encapsulamiento).

Un uso importante del protocolo tunneling es permitir a protocolos extraños correr sobre una red que no soporta ese protocolo en particular, por ejemplo usar IPv6 sobre IPv4 (Leandro Alegsa, 2016).

Figura 06: Estructura de tecnología Tunnels



Fuente: http://www.thegreenbow.com/vpn_faq.html

2.2.11 Anti-Replay basado en el tiempo

En las soluciones IPsec tradicionales, las capacidades anti-replay impiden que un tercero malintencionado capture paquetes IPsec y retransmita esos paquetes posteriormente para lanzar un ataque de denegación de servicio contra los puntos finales IPsec. Estas soluciones IPsec tradicionales utilizan un protocolo de ventana deslizante basado en contador.

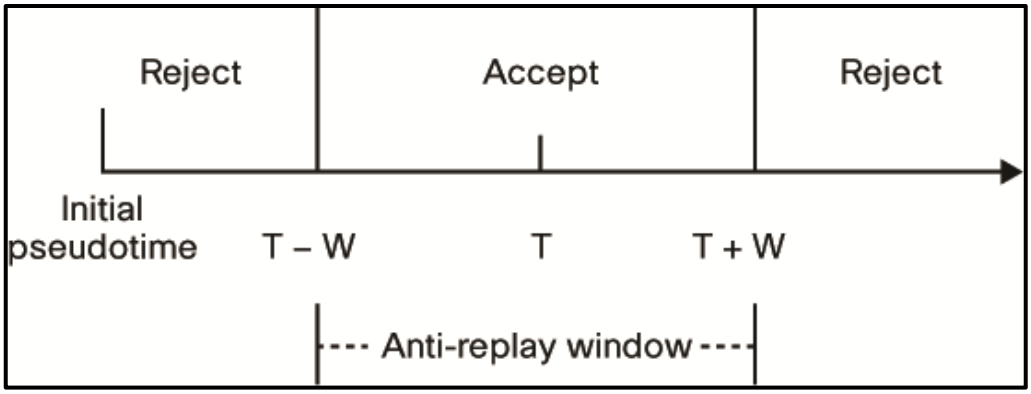
El remitente envía un paquete con un número de secuencia y el receptor utiliza la ventana deslizante para determinar si un paquete es aceptable o ha llegado fuera de secuencia y está fuera de la ventana de paquetes aceptables.

Debido a que usamos el grupo SA en GET VPN, el anti-replay basado en contador es ineficaz. Se requiere un nuevo método para protegerse contra los ataques de repetición. GET VPN utiliza anti-replay basado en tiempo (TBAR), que se basa en un pseudo-reloj de tiempo que se mantiene en el KS. Una ventaja de usar pseudotime para TBAR es que no hay necesidad de sincronizar el tiempo en todos los dispositivos GET VPN usando NTP.

El KS primario es responsable de establecer y mantener el pseudo-tiempo para un grupo. El KS primario también debe mantener pseudotime sincronizado en todos los GMs a través de actualizaciones de rekey, que por defecto se envía cada 7200 segundos. Cada GM incluye su pseudo-tiempo como un sello de tiempo en los paquetes de datos.

Una pasarela de VPN de recepción compara entonces la marca de tiempo del paquete recibido con el reloj de pseudo-hora de referencia de GM que mantiene para el grupo. Si el paquete llega demasiado tarde, se deja caer, se puedes apreciar en la figura 07 el anti-Replay basado en el tiempo.

Figura 07: Anti-Replay basado en el tiempo



Fuente: Guía de diseño e implementación de VPN (GETVPN) CISCO, 2012

2.3 Marco Conceptual

2.3.1. WAN

Es una red de área amplia, utilizan una tecnología de ancho de banda alto no es generalmente rentable para redes de área extensa que cubren áreas geográficas (varias ciudades por ejemplo), El costo de los enlaces físicos de larga distancia y la tecnología utilizada para transportar las señales a través de esas distancias generalmente, ocasionan un menor capacidad de ancho de banda.

2.3.2. LAN

Es una red de área local. Generalmente utiliza una tecnología de ancho de banda alto que es capaz de sostener un gran cantidad de host, en un área geográfica relativamente pequeña (un único edifico, o campus de varios edificios) y su alta densidad de usuarios hacen que esta tecnología sea rentable.

2.3.3. Junior’s

Especialista en redes con conocimientos de nivel intermedio, es el encargado de realizar los cambios, mantenimientos y resolver los problemas de la red.

2.3.4. Senior's

Especialista en redes con conocimientos a nivel avanzado.
El cual tiene la función de administrar los cambios y mejoras de tecnologías en una red.

2.3.5. Autenticación

Definimos la Autenticación como la verificación de la identidad del usuario, generalmente cuando entra en el sistema o red, o accede a una base de datos.

2.3.6. Seguridad

Los servicios de seguridad se consideran desde consultorías y análisis de riesgo hasta la implementación de tecnologías y nos permite el monitoreo de la información de toda la red y los dispositivos que lo conformen

2.3.7. Integridad

La integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

2.3.8. Tráfico

El tráfico es la cantidad de datos enviados y recibidos por los dispositivos de un sitio de red.

2.3.9. Switch

Dispositivo de red que se encarga de conectar uno o varios usuarios finales hacia la red de una empresa

2.3.10. Escalabilidad

Es la propiedad deseable de una red o un proceso, que indica su habilidad para reaccionar y adaptarse sin perder calidad.

2.3.11. Router

Es un dispositivo que proporciona conectividad a nivel de red o nivel 3 en el modelo OSI.

2.3.12. Paquete

Es cada uno de los bloques en que se divide la información para enviar, en el nivel de red.

2.3.13. Encriptación

Es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que sea ilegible.

2.3.14. IP, dirección lógica

Es un protocolo de red para las comunicaciones digitales actuales, Siendo la dirección lógica, el número que identifica a cada dispositivo dentro de una red.

2.3.15. Control de acceso

Sirve para evitar el uso no autorizado a los recursos de la red.

2.3.16. IWAN

El ancho de banda de la WAN para sus sucursales debe ganar en capacidad, simplicidad operativa y con costos más bajos. La WAN debe evolucionar. Solo iWAN de Cisco, ayuda a sus clientes a una transición confiable sin comprometer el rendimiento, la habilidad o la seguridad del usuario final.

2.3.17. ACL

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

2.3.18. Capas

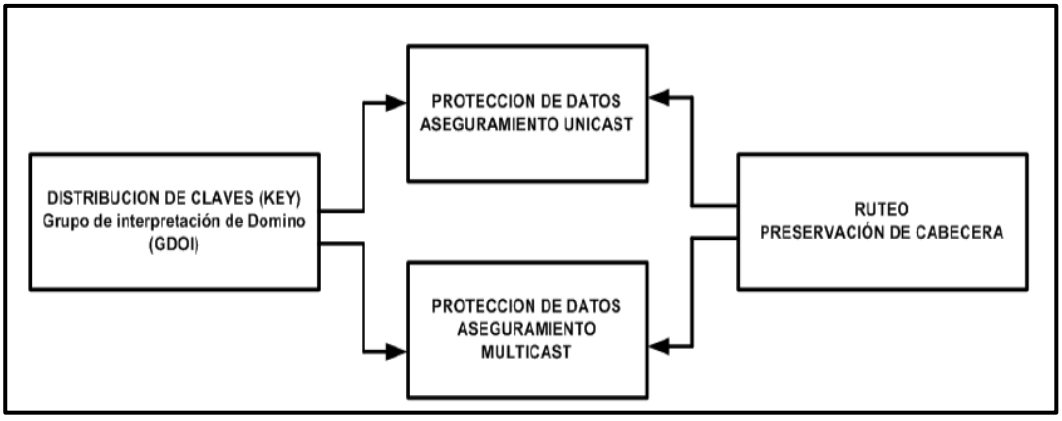
Son módulos que contienen información de sistemas que separan de las lógicas de negocios de la lógica de diseño.

CAPÍTULO III: ANÁLISIS Y DESCRIPCIÓN DEL PROTOCOLO GETVPN

3.1 Descripción del protocolo GETVPN

Se presenta a continuación un diagrama conceptual (figura 08), en la que describe la aplicación del protocolo GETVPN; el cual introduce el concepto de un grupo de confianza para eliminar túneles punto a punto y la superposición de rutas. Todos los miembros del grupo (GMS) comparten una asociación de seguridad común (SA). Esto permite encriptar el tráfico del grupo de miembros (GMS) y este sea cifrado por otro grupo de miembros (GMS).

Figura 08: Diagrama conceptual del protocolo GETVPN



Fuente: Elaboración propia

Cuando se implementa Grupo Encrypted Transport VPN (GETVPN) se asume que existe una infraestructura de red basada VPN la cual está operativa y que simplemente el requerimiento es activar el cifrado por motivos de seguridad en nivel de capa 3.

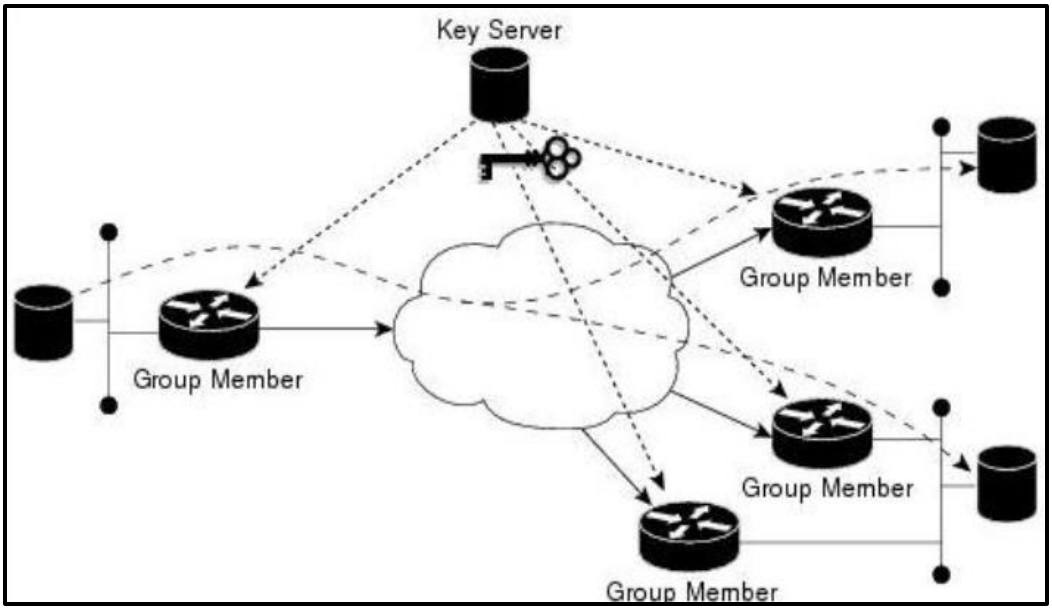
La tecnología GETVPN ofrece en particular a las redes financieras la capacidad de escalar las aplicaciones de voz video y datos con una mayor eficiencia de la red, garantizando una transmisión encriptada eficiente.

3.1.1. Componentes de GETVPN

La tecnología GETVPN es una suite de protocolos, con el cual se logra formar una optimización de seguridad óptima de encriptación en capa 3, como se visualiza en la figura 09, los componentes para el utilizar el protocolo GETVPN, logrando de esta manera.

- Comunicación muchos a muchos (any to any).
- Cifrado de tráfico tanto de unicast como multicast.
- Cifrado de tráfico de voz, datos y video.
- Preservación de cabecera IP.

Figura 09: Topología de componentes GETVPN



Fuente: Enlace blindado Cisco, 2012

3.2 Diseño y aplicación del protocolo GETVPN

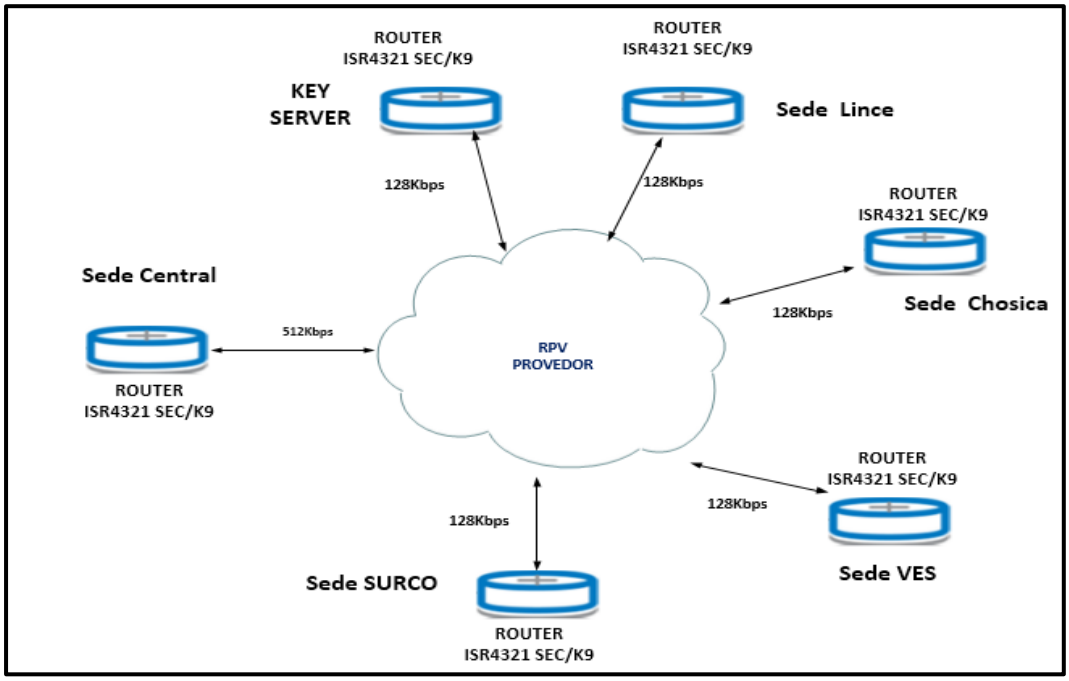
Es necesario efectuar la configuración de este protocolo en los dispositivos como KS, GMS y tener una red VPN bien implementada como desarrollamos a continuación.

3.2.1. Definición de la topología de red

Determinar sobre que topología de red VPN se implementara. Sabiendo que la infraestructura de la entidad cuenta con una sede central y varias sedes remotas como se muestra en la figura 10. En la sede central se encuentran todos los servicios que los trabajadores deben usar como

(correo, intranet, telefonía, archivos, compartidos, etc.) y en las sedes remotas se encuentran los trabajadores de agencias que necesitan ingresar a los recursos compartidos en la sede central.

Figura 10: Topología de red VPN



Fuente: Elaboración propia

a. Router ISR4321 /K9

Para la implementación del protocolo GETVPN, se emplea los equipos ROUTER ISR4321SEC/K9, el cual cuenta con una gama alta y tiene todas las características necesarias para el uso de la configuración de GET, tipos de CPU de acuerdo a la necesidad, para nuestro caso utilizaremos CPU 4core, algunas características se muestran en la tabla 03:

Tabla 03: Características del Router ISR 4321

Caracteristicas CISCO ISR 4321	
Entity	ISR 4321
CPU architecture	4-core CPU
#NIMs	2
#SMs	0
FPGE	2GE 1xCU+1xCU/SFP combo
ISC slot	1 for all ISC cards
USB type A ports	1
Power	1 External AC
Control/services memory	Base 4 GB max 8 GB 1333 MHz DIMMs 2 DIMM slots
Mgmt Ethernet	1 Gbps

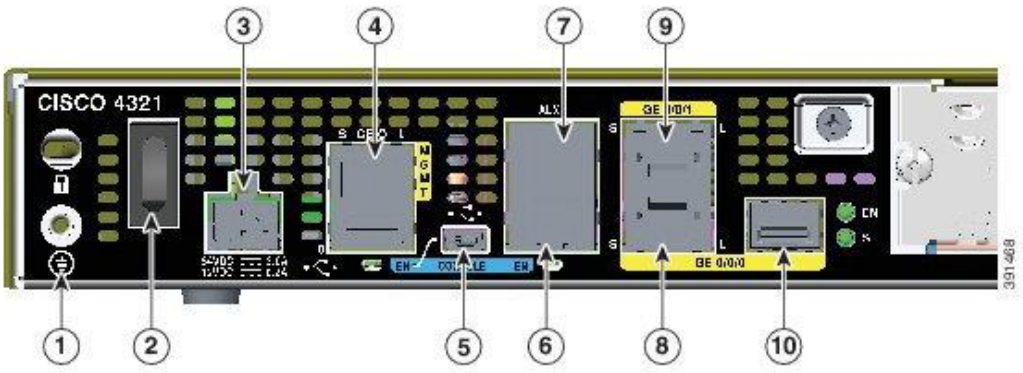
Fuente: Manual del router ISR4321

El enrutador de servicios integrados (ISR) de la familia Cisco 4000 revoluciona las comunicaciones WAN en la sucursal de la empresa. Con increíbles niveles de capacidades integradas de red inteligente y convergencia, se ocupa específicamente de la creciente necesidad de redes de aplicaciones en sitios de empresas distribuidas. Estas ubicaciones tienden a tener recursos de TI magros. Pero a menudo también tienen una creciente necesidad de comunicación directa con los centros de datos privados y las nubes públicas a través de diversos enlaces, incluyendo las VPN de conmutación de etiquetas multiprotocolo (MPLS) e Internet.

Los Cisco ISRs de la serie Cisco 4000 consolidan muchas funciones imprescindibles de TI, incluyendo recursos de red, de computación y de

almacenamiento. Los enrutadores integrados de alto rendimiento ejecutan múltiples servicios IWAN simultáneos sin ralentizar el rendimiento de los datos.

Figura 11: Puertos del panel posterior del router 4321 ISR/k9



1	Grounding	2	Power switch
3	Power input connector	4	GE “MGMT” port (with USB port below)
5	USB Type B mini port	6	Console port
7	Auxiliary port	8	GE 0/0/1 (copper cable) port
9	GE 0/0/0 RJ-45 (copper cable) port	10	GE 0/0/0 SFP (fiber-optic) port

Fuente: http://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation

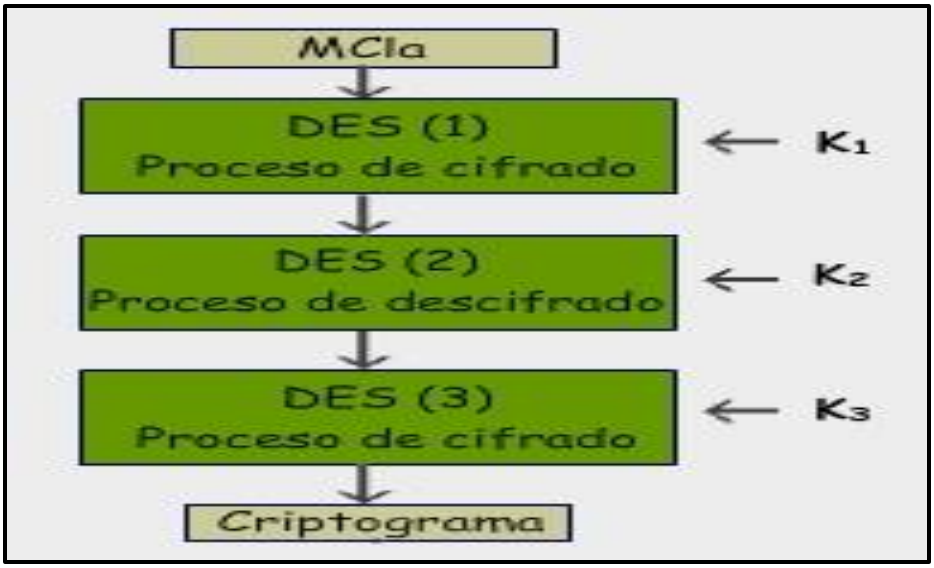
Como se aprecia en la figura 11, Cisco ISR 4321 cuenta con interfaces de red modulares con diversas opciones de conexión para balanceo de carga y resiliencia de red e interfaces modulares con extracción e inserción en línea (OIR) para actualizaciones de módulos sin interrupción de red.

3.2.2. Métodos de optimización

3.2.2.1. Algoritmo 3DES

Algoritmo que realiza un triple cifrado tipo DES, esto lo hace muchísimo más seguro que el cifrado DES simple. 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 12) con lo que se tiene una longitud de clave efectiva de 112 bits. La figura muestra el diagrama que representa al algoritmo 3DES.

Figura 12: Diagrama del algoritmo 3DES



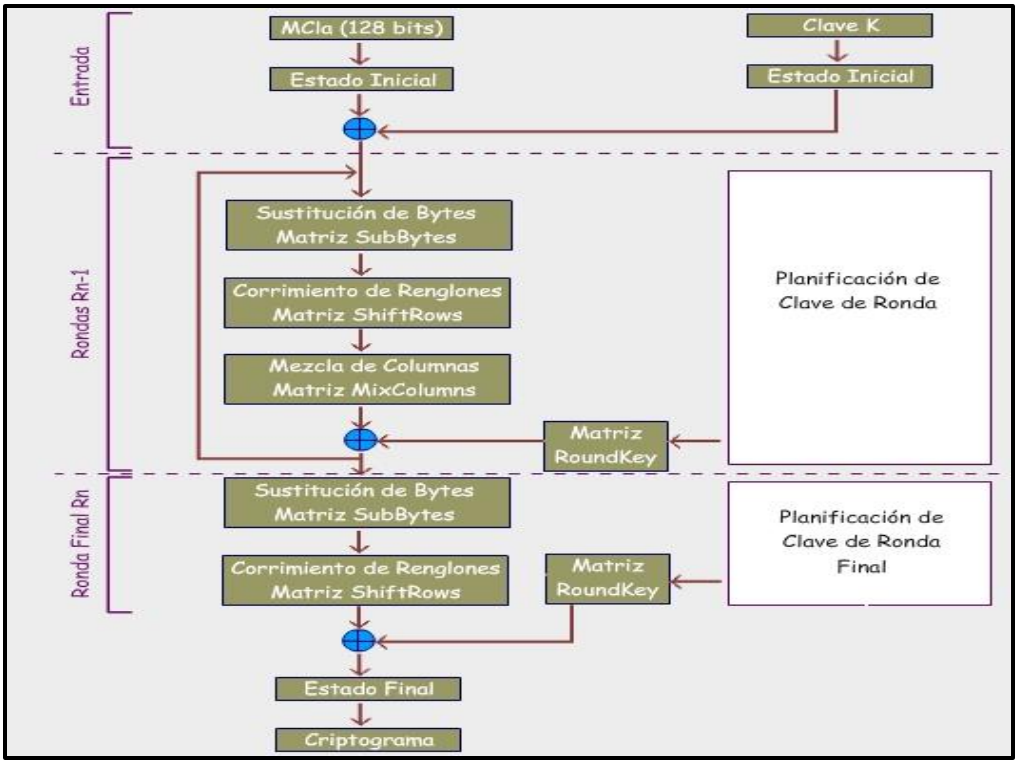
Fuente: http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php

3.2.2.2. Algoritmo AES

El algoritmo de cifrado AES hace uso de matemáticas polinomiales en estructuras de campos finitos, en particular opera en el Campo de Galois $GF(2^8)$ Los campos finitos permiten manejar cada elemento del campo con una cantidad determinada de memoria, además siempre que se realiza una operación se tendrá una operación inversa bien definida, por lo tanto las operaciones son bidireccionales permitiendo de este modo los procesos de cifrado y descifrado. La razón por la que AES opera en el $GF(2^8)$ es que hace posible su implementación en varias plataformas debido a que los coeficientes están en el rango de 0 a 7, considerando así el sistema binario y a un byte como la palabra básica del algoritmo.

AES opera sobre bloques de datos de 128 bits y la clave que utiliza puede ser de 128, 192 o 256 bits. La figura 13 muestra el esquema del cifrado AES.

Figura 13: Diagrama del cifrado AES



Fuente: http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php

Dependiendo del tamaño de la clave que se emplee, AES realiza un número fijo de rondas tal y como se muestra en la tabla 04.

Tabla 04: Numero de rondas AES

	Longitud de clave Nk (palabras de 32 bits)	Longitud de bloque de datos Nb (palabras de 32 bits)	Número de rondas
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Fuente:http://redyseguridad.fi-nam.mx/proyectos/criptografia/criptografia/index.php

Cada una de las rondas se compone de cinco matrices, la primera es la matriz de entrada o inicio de ronda y las cuatro restantes son transformaciones o funciones bien definidas:

1. **Matriz de entrada o inicio de ronda:** para la entrada su contenido corresponde al MCla, para cada una de las rondas es necesario calcular el texto de entrada.
2. **Matriz SubBytes:** sustituye individualmente cada byte del estado por otro de acuerdo a una tabla fija.
3. **Matriz ShiftRows:** toma cada renglón del estado completo y hace un corrimiento cíclico un determinado número de bytes o columnas que depende del renglón del que se trate.
4. **Matriz MixColums:** opera idénticamente con cada columna completa (4 bytes) aplicando una transformación lineal.
5. **Matriz Round Key:** modifica el estado de la clave sumándole módulo 2 (XOR) byte a byte la clave de la ronda correspondiente.

En la última ronda se omite el cálculo de MixColumns.

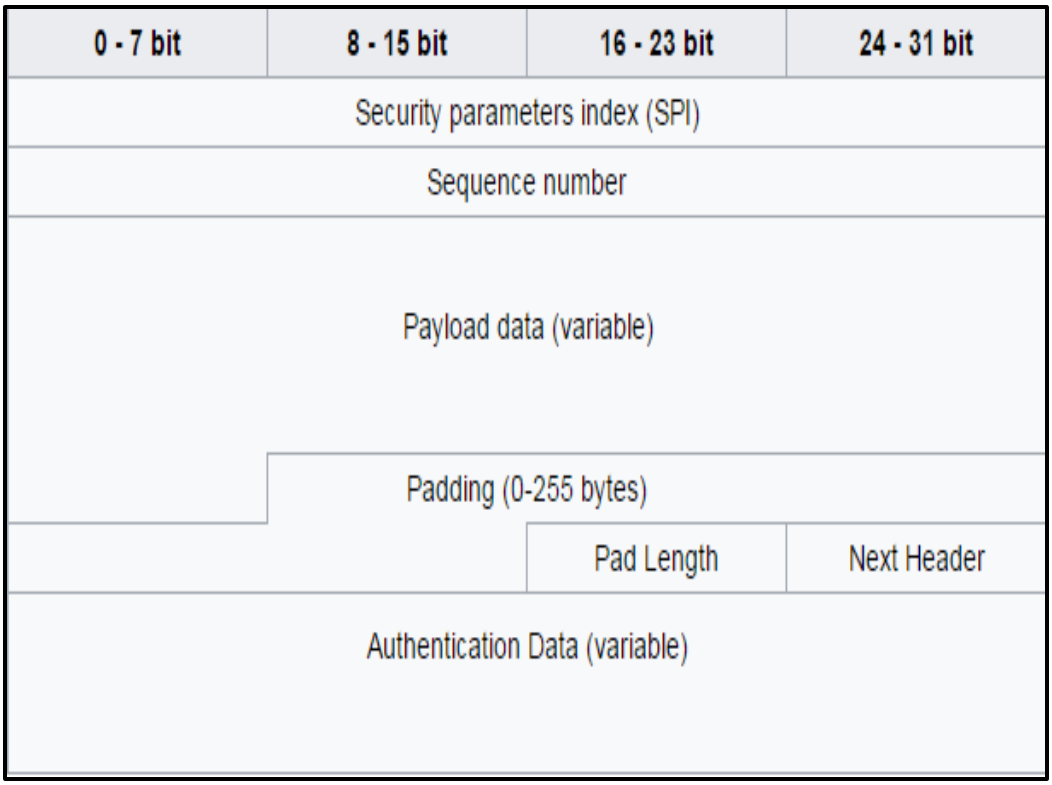
Independientemente del tamaño de K siempre se tienen las siguientes características:

- Matrices de 4x4.
- Cada elemento de la matriz es de dos dígitos hexadecimales.
- MCla siempre será procesado en bloques de 128 bits, manejados en las matrices en hexadecimal.

3.2.2.3. Protocolo ESP

El protocolo ESP proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete (ver figura 14). ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro. Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (AH protocolo de seguridad). ESP opera directamente sobre IP, utilizando el protocolo IP número 50. Un diagrama de paquete ESP:

Figura 14: Diagrama de paquete ESP



Fuente: https://es.wikipedia.org/wiki/IPsec

Significado de los campos:

- **Security parameters index (SPI)**

  Identifica los parámetros de seguridad en combinación con la dirección IP.

- **Sequence number**

  Un número siempre creciente, utilizado para evitar ataques de repetición.

- **Payload data**

  Los datos a transferir.

- **Padding**

  Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.

- **Pad length**

  Tamaño del relleno en bytes.

- **Next header**

  Identifica el protocolo de los datos transferidos.

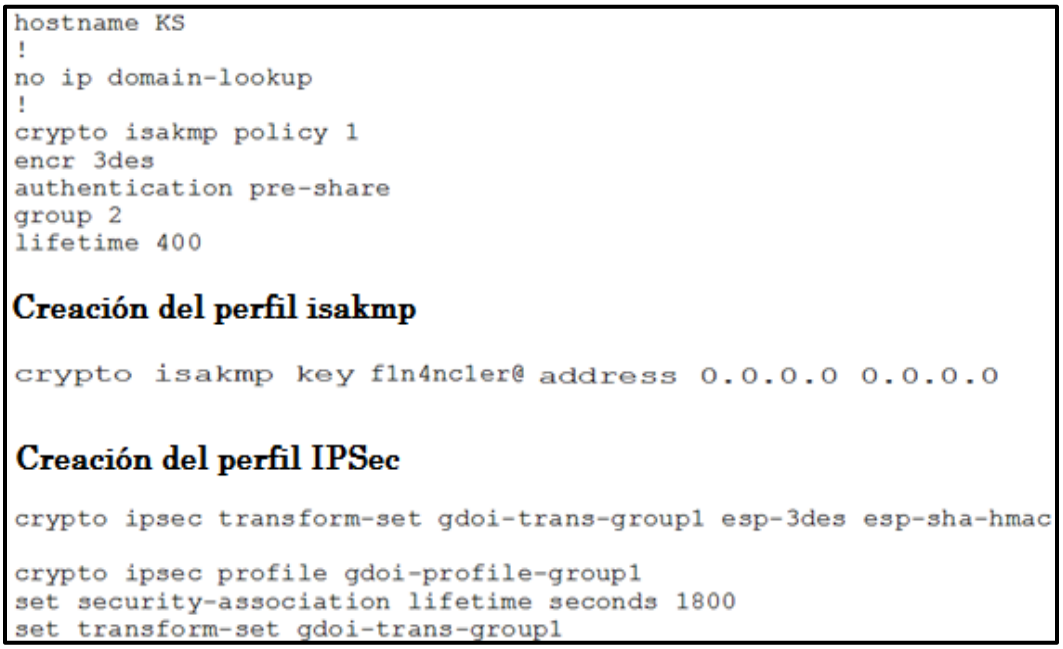
- **Authentication data**

  Contiene los datos utilizados para autenticar el paquete.

3.2.3. Configuración Key Server

Para realizar la configuración del Key Server se debe definir las IP de los GMs y la contraseña que tendrán, como se puede ver en la figura 15. Se recomienda que todos los GMs tenga la misma contraseña ya que los router tiene la funcionalidad de encriptar las contraseña y en un futuro esto podría traer problemas ya que no podemos ver en texto plano la contraseña, también debemos definir el tipo de encriptación que se debe realizar esto es dependiendo de la organización mientras más encriptación se determine en encabezado tendrá un mayor peso.

Figura 15: Configuración Key Server



Fuente: Elaboración propia

También debemos definir las políticas para los GDOI las cuales deben ser definidas correctamente ya que todos los GMs tendrán dicha configuración, tal cual se visualiza en la figura 16.

Figura 16: Configuración GDOI

```
crypto gdoi group group1
identity number 1

server local
 rekey lifetime seconds 89400
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa group1-export-general
 rekey transport unicast

sa ipsec 1
 profile gdoi-profile-group1
 match address ipv4 101
 replay counter window-size 64

address ipv4 10.10.10.2
redundancy
 local priority 10
```

Fuente: Elaboración propia

3.2.3.1. Consideraciones de diseño de KS

a**. ISAKMP**

El KS debe configurarse en el modo de Estándar de Cifrado Avanzado (AES) para el cifrado, utilizando claves de 128 bits (o mejores) porque el modo AES proporciona una seguridad más robusta con una

sobrecarga de cálculo reducida. Se recomienda que la vida útil de las sesiones ISAKMP en el KS sea la vida útil predeterminada de 24 horas. Los KSs necesitan la sesión Internet Key Exchange (IKE) activa para transmitir mensajes COOP (Protocolo Cooperativo) entre sí. Se trata de un proceso de sincronización de bases de datos persistentes, por lo que la sesión IKE siempre es necesaria. No tiene sentido arrancar la sesión IKE porque se restaura inmediatamente.

b. IPsec

Se recomienda el modo AES para la clave de cifrado de tráfico. Dado que el modo AES proporciona una seguridad más robusta con una sobrecarga de cálculo mínima.

c. Clave de cifrado de tráfico

La vida útil de la clave de cifrado de tráfico (TEK) no debe ser inferior a los 3600 segundos predeterminados. La vida útil de TEK nunca debe establecerse por debajo de 900 segundos en implementaciones reales, porque una vida útil TEK corta, crea más rollovers clave que deben sincronizarse entre todos los GM. Si el KS no tiene tiempo suficiente para completar la distribución de claves antes de pre-posicionar la asociación de seguridad con el TEK siguiente, el sistema funciona en un estado inestable.

La vida útil más larga mejora la estabilidad de la red y minimiza el cambio de red. Una vida de TEK de dos horas (7200 segundos) es un buen valor a utilizar.

Si las políticas cambian con frecuencia en el KS (por ejemplo, durante etapas de despliegue temprano), la vida útil de TEK se puede reducir para minimizar el número de SA activos; Sin embargo, establecer el tiempo de vida de TEK demasiado bajo conduce a generación de clave excesiva y superposición de claves. El establecimiento de la vida de TEK a 900 segundos se hace comúnmente en un laboratorio donde la limpieza de toda la red es factible.

d. ACL en la política de cifrado de trafico

Las entradas de permiso en la lista de control de acceso (ACL) para la política de cifrado deben incluir las subredes que deben ser cifradas. El número máximo de líneas en una ACL de tráfico es 100. Tenga en cuenta que cada declaración de permiso en el ACL de KS resulta en una SA en el GM, por lo que el número de entradas de permiso debe limitarse a minimizar la base de datos SA (SADB) en el GM.

Es posible agregar una sola entrada "allow ip any any" en la ACL para cifrar todo el tráfico. Sin embargo, las entradas de denegación explícita

deben configurarse en la ACL para excluir del cifrado el tráfico de control (por ejemplo, los protocolos de enrutamiento). El diseñador de red debe determinar qué tráfico requiere cifrado.

e. Key encryption key lifetime

Key encryption key lifetime debe dejarse en el valor predeterminado de 86400 segundos. Dado que el KEK se utiliza para cifrar los mensajes del plano de control entre el KS y el GM. Cambiar el valor de KEK frecuentemente somete al GM a posibles fallas de rekey y posteriormente requiriendo que el GM registre de nuevo más frecuentemente de lo necesario. Se recomienda que la vida útil de KEK siempre sea al menos el doble de la vida útil de TEK.

f. Rekey retransmit interval

El intervalo de retransmisión rekey debe establecerse como se muestra, ya que para grupos con muchos GMs, puede tomar un tiempo significativo para enviar mensajes unicast rekey. La retransmisión debe comenzar después de un ciclo completo de mensajes de rekey con tiempo suficiente para los reconocimientos.

Los intervalos de rekey más amplios y las retransmisiones aseguran que los TEKs son preposicionados con mucha anticipación a la expiración de TEK, y mitigan el impacto de la partición de red.

g. Authentication polivy para el registro de GM

Los GM pueden autenticarse al KS en el momento del registro usando Pre-Share Keys (PSKs). Los PSK son fáciles de implementar, pero deben gestionarse de forma proactiva. Se recomienda desplegar un PSK basado en peer en lugar de definir una clave predeterminada (la clave definida con una dirección de 0.0.0.0) para todos los dispositivos de la red. Los PSK deben actualizarse regularmente (cada pocos meses)

Un PSK se puede actualizar sobre una base de pares KS-GM sin afectar el plano de datos criptográficos o plano de control porque las claves se aseguran utilizando el KEK. Es importante asegurarse de que un GM puede volver a registrar a cada conjunto ordenado de KS usando el PSK recién asignado.

h. Rekey transport

Unicast y multicast son los dos métodos de transporte para los servicios de rekey GDOI. Unicast rekey se requiere cuando la

infraestructura WAN no admite la multidifusión o cuando el operador desea tener un reconocimiento positivo de la participación de GM en el grupo. Se necesita una nueva clave de multidifusión para escalar redes GET VPN más allá de los límites de las capacidades de reestructura unicast de una plataforma KS.

Para soportar las claves de multidifusión, la infraestructura de la WAN debe soportar la multidifusión, de lo contrario GM se volverá a registrar de forma persistente.

Los mensajes de rekey deben enviarse desde una dirección IP que no esté afiliada a una interfaz física en el KS. Si el KS pierde una interfaz, el plano de control de enrutamiento puede reconvertir y proporcionar mensajes de rekey a través de una interfaz alternativa mientras utiliza la misma dirección IP de origen. Se recomienda una interfaz de loopback como fuente de los mensajes de rekey.

i. TBAR

TBAR debe ser configurado en todas las plataformas y anti-replay basado en contador no debe ser configurado.

Debido a que múltiples fuentes y destinos utilizan el mismo SA, el anti-replay basado en contador no tiene sentido y el TBAR es el único método viable. TBAR es suficiente porque el KS mantiene la sincronización de tiempo para todos los GMs. Este no es el tiempo global; Pero es un reloj de tiempo relativo para ese grupo de seguridad. No se requiere NTP (Network Time Protocol) ni sincronización de tiempo basada en GPS. El KS transmite periódicamente las cadenas de sincronización de tiempo antes de la caducidad de la clave de cifrado de tráfico (TEK).

3.2.4. Configuración GM

Para la configuración de los GM, se debe definir el KS server como la IP y la contraseña, también configuración del GDOI la cual se encarga de definir las políticas para los GMs

Un GM debe ser seleccionado sobre la base de la tasa de transferencia requerida. . Si la mezcla de tráfico comprende principalmente paquetes pequeños (por ejemplo, como en VoIP), los paquetes / segundo rendimiento son más importantes. En la figura 17 se muestra la configuración a realizarse .

Figura 17: Configuración GM

```
hostname GM
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 3600


  crypto isakmp key f1n4nc1er@  address 1.1.1.1
  crypto isakmp key f1n4nc1er@  address 2.2.2.2
  crypto isakmp key f1n4nc1er@  address 3.3.3.3


  Configuración del GDOI

crypto gdoi group group1
 identity number 1
 server address ipv4 10.10.10.2

 Configuración de la interface de encriptación

 crypto map map-group1 10 gdoi
 set group group1
```

Fuente: Elaboración propia

3.2.5. Configuración ACL

Es necesario configurar listas de control de acceso las cuales nos ayudaran a definir qué tráfico se encriptara y que tráfico no, no es recomendable encriptar todo el tráfico, sino el tráfico entre Lan to Lan. En la figura 18 se muestra la configuración recomendada.

Figura 18: Configuración ACL

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Fuente: Elaboración propia

Nota: Uno debe ejercer la precaución extrema al usar "cualquier entrada del permiso" cualquier entrada durante despliegue. Si esta entrada

precede accidentalmente a las entradas de denegación para el control y el tráfico de gestión, y la ACL se descarga a los GM, esto puede romper el tráfico de control / gestión mediante el cifrado de las actualizaciones.

3.2.6. Troubleshooting Tools

Como regla general, estas son las salidas de comandos que debe recopilar para casi todos los problemas de GETVPN.

a. KS

- show crypto gdoi
- show crypto gdoi ks coop
- show crypto gdoi ks members
- show crypto gdoi ks rekey
- show crypto gdoi ks policy

b. GM

- show crypto eli
- show ceypto isakmp sa
- show crypto gdoi
- show crypto gdoi gm
- show crypto gdoi gm rekey

c. Syslog messages

GETVPN proporciona un conjunto extenso de mensajes syslog para eventos significativos de protocolo y condiciones de error, como se aprecia en la tabla 05 y tabla 06. El syslog siempre debe ser el primer lugar para buscar cuando se realiza la solución de problemas GETVPN.

Tabla 05: Mensajes comunes de Syslog de KS

Syslog Messages	Explanation
COOP_CONFIG_MISMATCH	La configuración entre el servidor de claves primarias y el servidor de claves secundarias no coincide.
COOP_KS_ELECTION	El servidor de claves local ha entrado en el proceso de elección en un grupo.
COOP_KS_REACH	Se restablece la accesibilidad entre los servidores de clave cooperativa configurados.
COOP_KS_TRANS_TO_PRI	El servidor de claves local pasó a un rol principal de ser un servidor secundario en un grupo.
COOP_KS_UNAUTH	Un servidor remoto autorizado intentó ponerse en contacto con el servidor de claves local de un grupo, lo que podría considerarse un evento hostil.
COOP_KS_UNREACH	Se pierde la accesibilidad entre los servidores de clave cooperativos configurados, lo que podría considerarse un evento hostil.
KS_GM_REVOKED	Durante el protocolo de rekey, un miembro no autorizado intentó unirse a un grupo, lo que podría considerarse un evento hostil.
KS_SEND_MCAST_REKEY	Envío de la clave de multidifusión.
KS_SEND_UNICAST_REKEY	Enviar una llave unicast.
KS_UNAUTHORIZED	Durante el protocolo de registro de GDOI, un miembro no autorizado intentó unirse a un grupo, lo que podría considerarse un evento hostil.
UNAUTHORIZED_IPADDR	La solicitud de registro se canceló porque el dispositivo solicitante no estaba autorizado para unirse al grupo.

Fuente: Elaboración propia

Tabla 06: Mensajes comunes de Syslog de GM

Syslog Messages	Explanation
GM_CLEAR_REGISTER	El comando clear crypto gdoi ha sido ejecutado por el miembro del grupo local.
GM_CM_ATTACH	Se ha adjuntado un mapa crypto para el miembro del grupo local.
GM_CM_DETACH	Se ha separado un mapa de criptograma para el miembro del grupo local.
GM_RE_REGISTER	IPsec SA creada para un grupo podría haber caducado o borrado. Necesita volver a registrar el servidor de claves.
GM_RECV_REKEY	Rekey recibido.
GM_REGS_COMPL	Registro completo.
GM_REKEY_TRANS_2_MULTI	El miembro del grupo ha hecho la transición de usar un mecanismo unicast rekey a utilizar un mecanismo de multidifusión.
GM_REKEY_TRANS_2_UNI	El miembro del grupo ha hecho la transición desde el uso de un mecanismo de reescritura de multidifusión hasta el uso de un mecanismo de unidifusión.
PSEUDO_TIME_LARGE	Un miembro del grupo ha recibido un pseudo-tiempo con un valor que es en gran medida diferente de su propio pseudo-tiempo.
REPLAY_FAILED	Un miembro del grupo o un servidor de claves ha fallado una comprobación anti-reproducción.

Fuente: Elaboración propia

3.3 Revisión y Consolidación de Resultados

En este apartado se describen los resultados obtenidos luego de la implementación, con el objetivo de evaluar el procedimiento y puesta de la solución de las cuales se extraerán conclusiones y recomendaciones para futuros trabajos similares.

3.3.1 Casos de prueba sobre una infraestructura sin GETVPN

Tomando en cuenta la infraestructura sin la implementación del protocolo GETVPN, se obtuvieron los siguientes datos, los cuales se detallan a continuación (tabla 07):

Tabla 07: Detalle de datos sobre red sin GETVPN

			LATENCIA			
CANTIDAD ARCHIVOS (MB)	TIEMPO	ANCHO DE BANDA (Bits/seg)	MAXIMA	MINIMA	MEDIA	PING RATE (%)
1 MB	00:00:14	30 K	3,04	3,04	3,96	3,92
2 MB	00:00:34	40 K	5,05	5,05	8,88	8,57
3 MB	00:00:39	90 K	6,62	6,62	11,91	11,87
4 MB	00:00:55	120 K	8,28	8,28	15,58	16,54
5 MB	00:01:10	150 K	20,29	11,79	11,79	20,64
6 MB	00:01:18	160 K	22,86	7,22	7,22	23,25
7 MB	00:01:21	200 K	24,71	5,41	5,41	25,12
8 MB	00:01:26	210 K	26,13	5,62	5,62	26,56
9 MB	00:01:53	290 K	35,81	35,32	35,32	36,13
10 MB	00:02:00	300 K	36,17	12,05	12,05	36,84

Fuente: Elaboración propia

3.3.2 Casos de prueba sobre una infraestructura con GETVPN

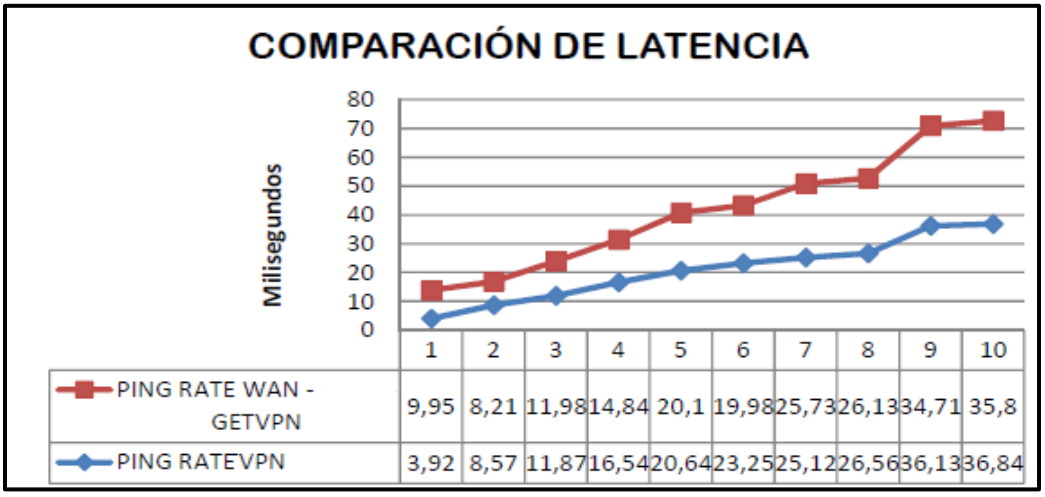
Tomando en cuenta la infraestructura con la implementación del protocolo GETVPN, se obtuvieron los siguientes datos, los cuales se detallan a continuación (tabla 08):

Tabla 08: Detalle de datos sobre red con GETVPN

			LATENCIA			
CANTIDAD ARCHIVOS (MB)	TIEMPO	ANCHO DE BANDA (Bits/seg)	MAXIMA	MINIMA	MEDIA	PING RATE (%)
1 MB	00:00:16	30 K	3,94	2,37	1,1	9,95
2 MB	00:00:30	60 K	8,21	1,05	1,05	8,21
3 MB	00:00:40	90 K	11,97	6,7	6,7	11,98
4 MB	00:00:48	120 K	14,83	3,54	3,54	14,84
5 MB	00:01:06	150 K	20,10	11,19	11,19	20,1
6 MB	00:01:15	160 K	20,24	15,83	15,83	19,93
7 MB	00:01:20	200 K	25,83	4,68	4,68	25,73
8 MB	00:01:24	210 K	26,12	5,63	5,63	26,13
9 MB	00:01:52	300 K	34,71	3,52	3,52	34,71
10 MB	00:01:56	300 K	35,79	6,07	6,07	35,8

Fuente: Elaboración propia

Figura 19: Comparación de latencia



Fuente: Elaboración propia

Como se puede observar en la figura 19 los valores cuando es implementado GETVPN aumentan progresivamente, esto se debe a que se está manejando Calidad de Servicio y Seguridad a nivel de la red WAN.

3.3.3 Encriptación de paquetes

A continuación se presenta detalles de la cantidad de paquetes que son encriptados y descifrados cuando es aplicado el algoritmo de seguridad basado en GETVPN.

Tabla 09: Detalle de paquetes encriptados al transmitir archivos

TRANSFERENCIA DE ARCHIVOS					
			ENRIPTACION GETVPN		
CANTIDAD ARCHIVOS (MB)	TIEMPO	ANCHO DE BANDA (Bits/seg)	ENCAPSULADOS	DESENCAPSULADOS	VERIFICADOS
1 MB	00:00:26	35 K	248	248	248
2 MB	00:00:59	65 K	570	570	570
3 MB	00:01:16	70 K	754	754	754
4 MB	00:01:25	120 K	882	882	882
5 MB	00:01:55	150 K	1192	1192	1192

Fuente: Elaboración propia

En los datos reflejados en la tabla 09 se verifica que la cantidad de paquetes transmitidos que son encriptados, desencriptados y verificados en su totalidad sin desechar ninguno, lo cual indica que el algoritmo de seguridad aplicado en la configuración trabaja sin problemas.

En el caso de transmisión de paquetes de voz y video para evidenciar la funcionalidad de la encriptación, las métricas que fueron consideradas son ancho de banda y el tiempo en el cual el algoritmo es aplicado. En la tabla 10 se verifica que la cantidad de paquetes enviados

como recibidos no varían y de esta manera podemos garantizar que los servicios se mantengan estables.

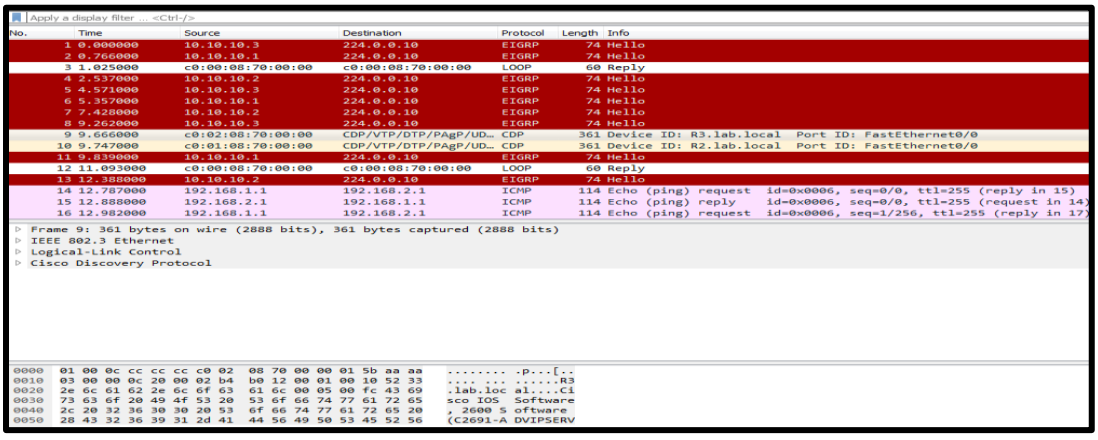
Tabla 10: Detalle de paquete encriptados al transmitir VOZ y VIDEO

TRAFICO DE VOZ Y VIDEO					
			ENRIPTACION GETVPN		
DESCRIPCION	TIEMPO (minutos)	ANCHO DE BANDA (Bits/seg)	ENCAPSULADOS	DESENCAPSULADOS	VERIFICADOS
Voz/Video	1	20 K	415	415	415
Voz/Video	2	30 K	625	625	625
Voz/Video	3	40 K	1878	1878	1878
Voz/Video	4	70 K	2520	2520	2520
Voz/Video	5	80 K	3082	3082	3082

Fuente: Elaboración propia

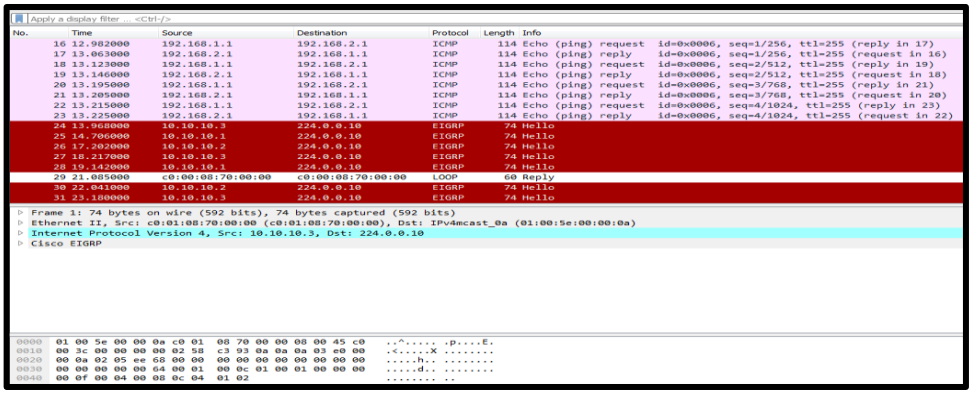
Así mismo para corroborar que los datos estén encriptados se utilizó la herramienta WIRESHARE, el cual es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado equipo de comunicación u ordenador. A continuación se detalla el análisis sobre los paquetes de red (ver figuras 20 al 25) captados desde la herramienta Wireshare:

Figura 20: 1° detalles y análisis sobre paquete de red sin GETVPN



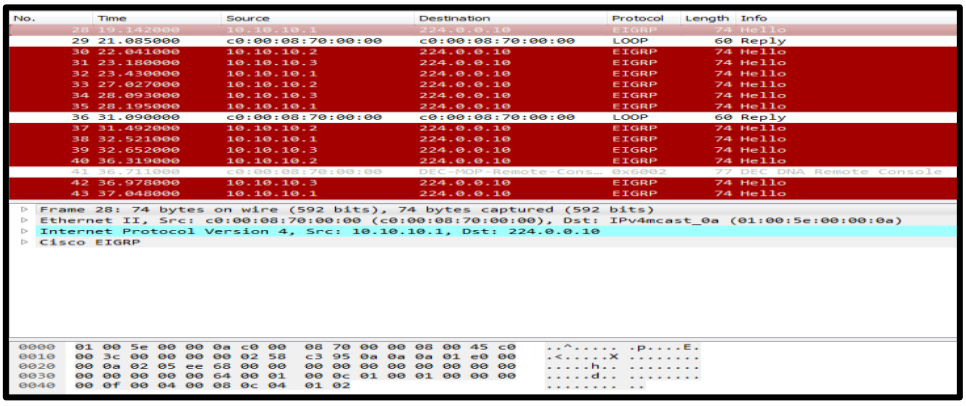
Fuente: Elaboración propia

Figura 21: 2° detalles y análisis sobre paquete de red sin GETVPN



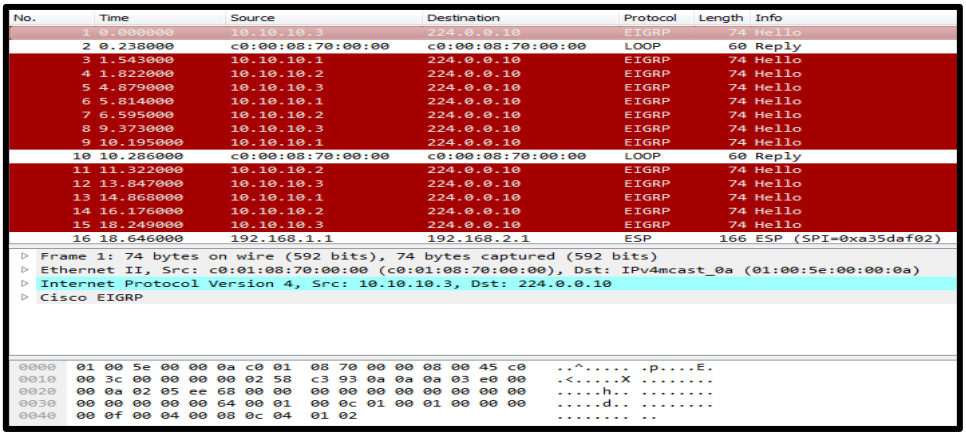
Fuente: Elaboración propia

Figura 22: 3° detalles y análisis sobre paquete de red sin GETVPN



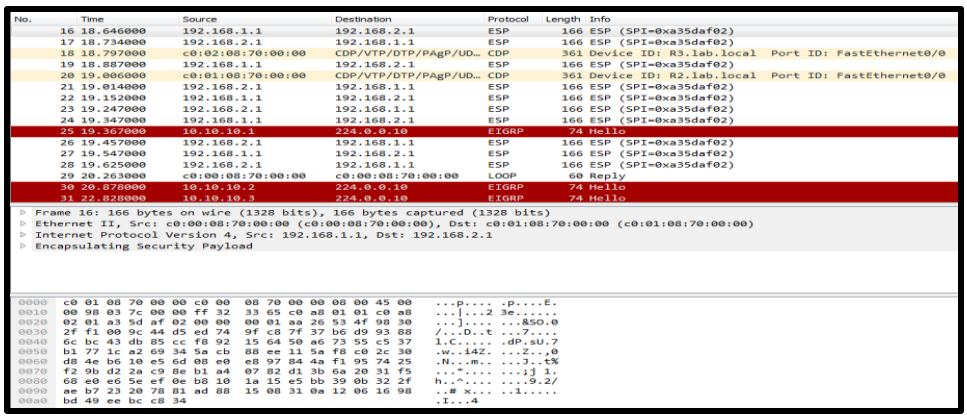
Fuente: Elaboración propia

Figura 23: 1° detalles y análisis sobre paquete de red con GETVPN



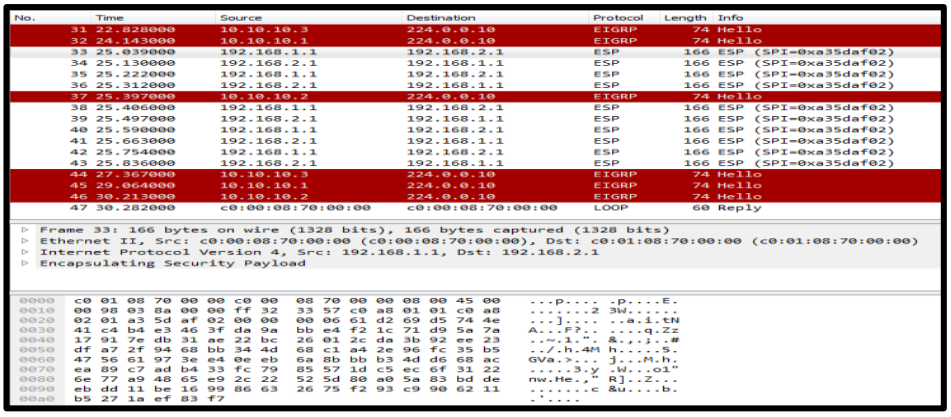
Fuente: Elaboración propia

Figura 24: 2° detalles y análisis sobre paquete de red con GETVPN



Fuente: Elaboración propia

Figura 25: 3° destalles y análisis sobre paquete de red con GETVPN

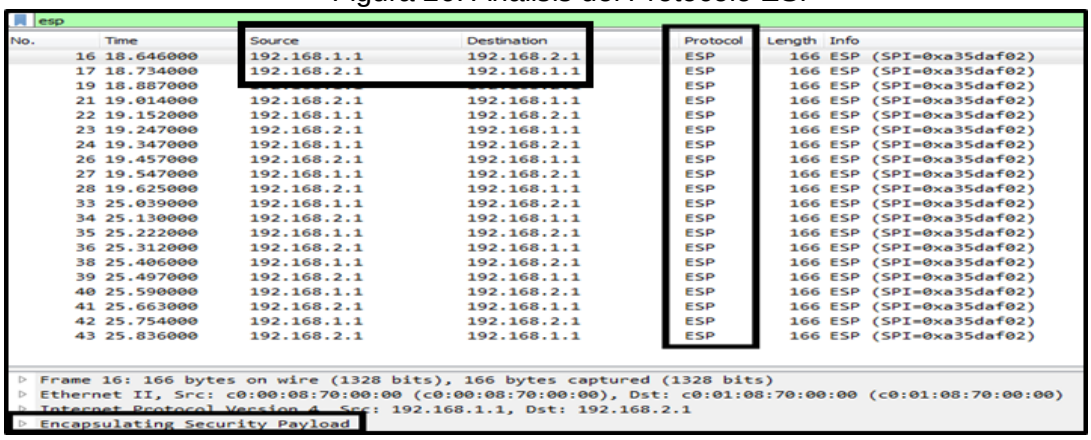


Fuente: Elaboración propia

3.3.4 **Encabezado del paquete IP**

Producto de esta implementación se consiguió superar la problemática que tenía la entidad financiera, ya que se evita que el encabezado del paquete IP no sea modificado como sucedía cuando se tenía implementado solo IPSEC. Como se ve en la figura 26, el protocolo ESP aparece con GETVPN y se visualiza las IP originales.

Figura 26: Análisis del Protocolo ESP

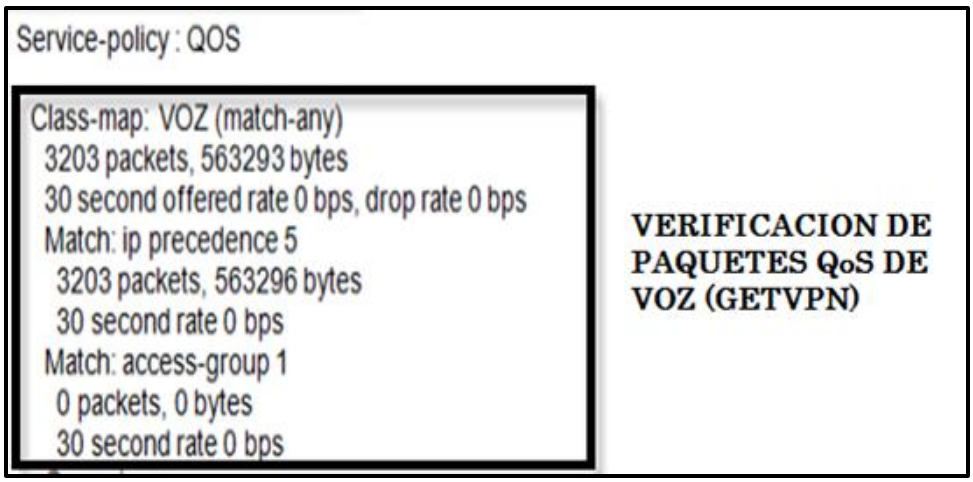


Fuente: Elaboración propia

3.3.5 Marcado de tráfico para QoS

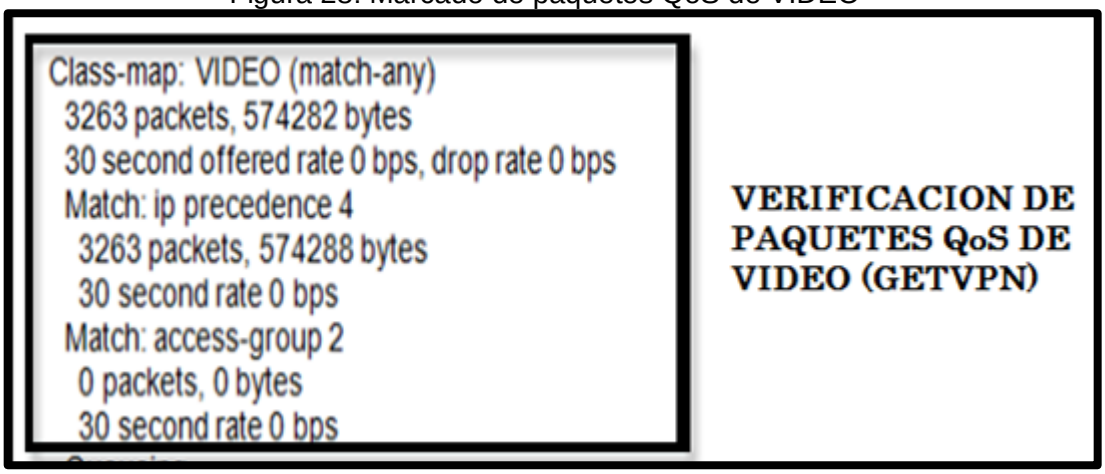
Se logró respetar el marcado de tráfico para QoS (voz, data y video) que el proveedor brinda a la entidad financiera, ya que la calidad de servicio se especifica y se respeta, así mismo se logra una optimización con respecto al ancho de banda. A continuación se muestra el marcado de paquetes (figura 27 y 28).

Figura 27: Marcado de paquetes QoS de VOZ



Fuente: Elaboración propia

Figura 28: Marcado de paquetes QoS de VIDEO



Fuente: Elaboración propia

3.3.6 Tunneling por destino

Implementando el protocolo GETVPN eliminamos el concepto de túneles por sitios, evitando que se tenga que realizar configuración con cada sucursal a implementar, ya que ahora el tráfico realiza encriptación sin necesidad de establecer túneles y por lo tanto se optimiza en tiempo y seguridad la configuración.

Detallando los resultados, llegamos a la siguiente tabla 11 que resumen el detalle de la implementación del protocolo GETVPN.

Tabla 11: Cuadro comparativo de GETVPN y IPSec

CARACTERISTICAS	GETVPN	VPN-IPSec
Ventajas para administrar	• Simplifica la gestión de cifrado a través del uso de grupo de claves • Permite escalabilidad de conectividad • Soporta Calidad de Servicio (QoS), multicast y enrutamiento	• El cifrado se lo realiza entre sitios
Cuando usar	• Soporte un mallado completo utilizando VPNS IPSec • Permite la participación de todos los Router para realizar una red mallada	• Se utiliza cuando se requiere interoperabilidad de múltiples proveedores
Topología	• Se adapta a toda topología, previa revisión del diseño	• Topología punto a punto
Ruteo	• Soporta conectividad punto a punto, punto multipunto, multipunto-multipunto	• No soporta
Multicast	• Soporta	• No soporta
Seguridad	• Seguridad a través de direccionamiento y a través de clases	• No dispone de servidor de claves
Túneles	• No usa	• Si usa
Encriptación	• Soporta	• Soporta
Encabezado original	• Preserva Encabezado IP original	• No preserva
Alta disponibilidad	• Se realiza a traves de ruteo	• Se genera conmutación de errores

Fuente: Elaboración propia

CONCLUSIONES

- Después de analizar la revisión y consolidación de resultados se pudo llegar a determinar que la implementación del protocolo GETVPN solucionó el problema de la modificación del encabezado original en los paquetes, con esta mejorar el encabezado no es modificado o transformado.

- Con el desarrollo de la implantación del protocolo GETVPN se consiguió optimizar la configuración y administración de los túneles VPN, en este caso ya no existe el concepto de túneles, sino se le denomina trafico encriptado.

- Al realizar la implementación del protocolo se obtiene mejor calidad de servicio para los clientes de la entidad financiera, al optimizarse el ancho de banda y así mismo permite a la entidad realizar políticas de QoS para cada servicio.

- Luego de realizar la implementación, los actuales administradores de redes ya no tienen el problema de la administración de túneles por sede ya que ahora solo se deberá definir que tráfico se desea encriptar.

- Con este proyecto se concluye que la implementación del protocolo GETVPN optimiza la seguridad mediante el encriptado ya que el tráfico es distribuido de la mejor manera y priorizado, según acorde a la entidad financiera

RECOMENDACIONES

- Se recomienda la configuración de GETVPN para que los administradores no tengan mucha complejidad en administración y resolver problemas.

- Se recomienda realizar un levantamiento de información de la infraestructura de comunicación existete, antes de implementar GTVPN, así como la topología sobre la cual se implementara la solución.

- Se recomienda al personal que implemente el protocolo GETVPN tener conocimientos de routing y switching, con la finalidad de poder entender las diversas configuraciones que se desarrollaron en los diferentes router en la topología propuesta, así como también de mecanismos de seguridad que pudieran ser implementados en los equipos de comunicación.

- Se recomienda la configuración de GETVPN ya que es un protocolo de seguridad totalmente escalable en redes muy complejas o extensas.

- Para trabajos futuros se recomienda investigar el protocolo de comunicación IPV6, para tener un referente acerca de las novedades y mejoras en seguridad y que estas puedan ser implementadas a nivel VPNs y usuarios.

BIBLIOGRAFÍA

- Bonilla Puerto, Carlos. (2010). Encripcion GET VPN Banco Nacional. Sitio web: http://catalogo.urosario.edu.co/cgi-bin/koha/opac-detail.pl?biblionumber=38697

- Aimacaña Valladares, Darwin. (2014). Diseño y evaluación de nivel de seguridad del protocolo GETVPN en una red de datos para un entorno multipunto que utiliza MPLS para su comunicación WAN. Sitio web: http://repositorio.espe.edu.ec/xmlui/handle/21000/10380?show=full

- Luis Álvaro Velásquez. (2013). GETVPN para protección de canales MPLS en redes utilizadas para el transporte de información de clientes del sector financiero y privada. Sitio web: http://52.0.140.184/typo43/fileadmin/HVIng/15072014448.pdf

- Diego Alejandro, Ortiz Rodríguez. (2015). Diseño e implementación de solución GETVPN. Sitio web: https://co.linkedin.com/in/daor82

- Enzo Angeles. (2012). Tecnología GETVPN en el sector financiero. Sitio web: http://www.tecnologiahechapalabra.com/tecnologia/comunicados/ti/articulo.asp?i=7141

- Steve Friedl, (2012). ¿Qué es tecnología IPSec? Sitio web: http://www.http-peru.com/protocolo_ipsec.php

- Cisco. (2014). Libro configuración y resolución de problemas para GETVPN. Lima, Perú: CCIE seguridad

- Jose Manuel Huidobro Moya, (2002). MPLS. Sitio web: https://mastermoviles.gitbooks.io/tecnologias2/content/protocolos_de_comunicacion_en_red.html

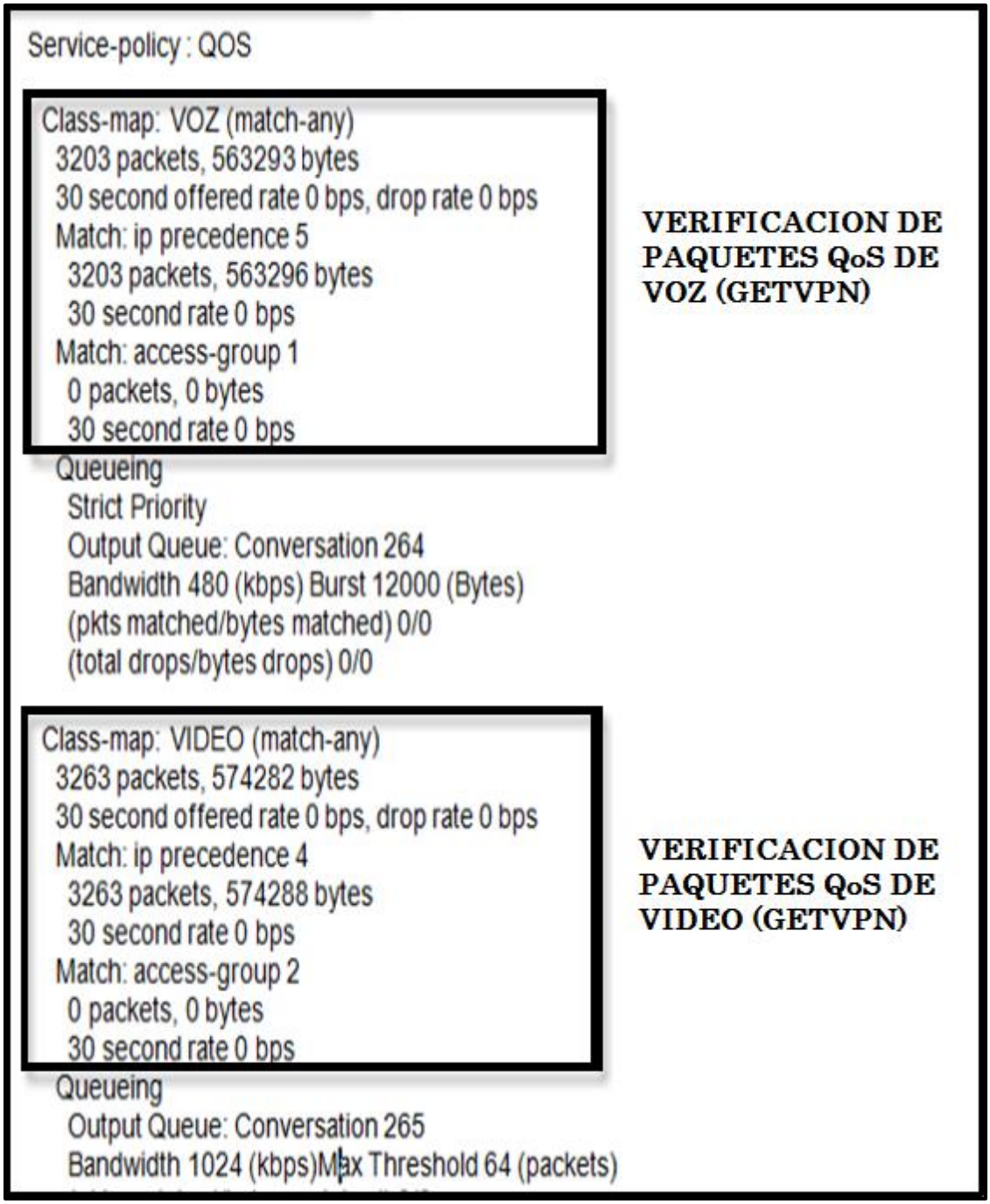
- Roberto Nader Carreon, (2008). VPN. Sitio web: https://www.incubaweb.com/sabes-una-red-vpn-se-puede-utilizar/

- Itzcoatl Espinosa, (2014). Definición QoS. Sitio web: http://conexionzero.com/configuracion-de-calidad-de-servicio-qos-en-skype-for-business/

- Wilfredo flor. (2015). Arquitectura de protocol GETVPN. Sitio web: http://www.redescisco.net/sitio/2014/01/11/cisco-ios-security-getvpn/

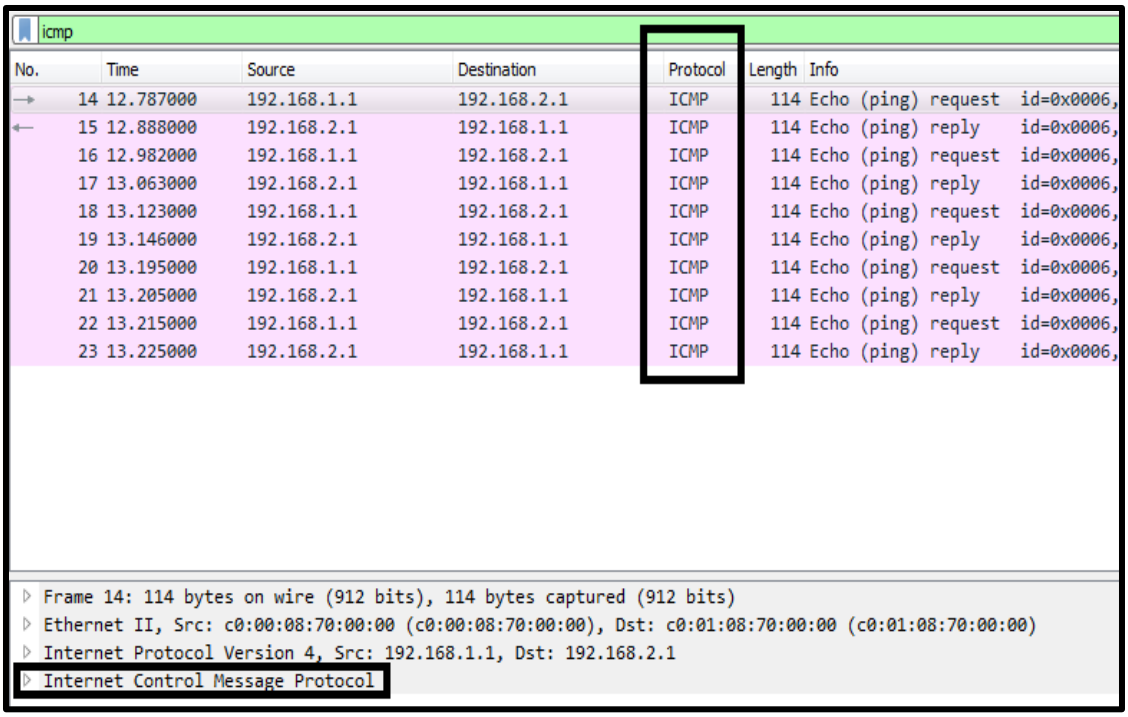
ANEXOS

Marcado de paquetes QoS



Datos referentes al cifrado y descifrado

Filtrado de protocolos sin encriptación



Filtrado de protocolo con encriptación