ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN REDES DE LA INFORMACIÓN Y CONECTIVIDAD

III PROMOCIÓN

TESIS DE GRADO MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

TEMA: “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: ING. AIMACAÑA VALLADARES, DARWIN RAMIRO

DIRECTOR: ING. OLEAS, JUAN CARLOS

SANGOLQUÍ, NOVIEMBRE DEL 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS
MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

CERTIFICADO

ING. JUAN CARLOS OLEAS C.
Director

ING. JOSE LUIS TORRES
Oponente

CERTIFICAN

Que el trabajo titulado **"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"**, realizado por **AIMACAÑA VALLADARES DARWIN RAMIRO,** ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que cumple con lo planteado en el plan de tesis y de acuerdo a los requerimientos del programa de maestría, se recomiendan su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a **AIMACAÑA VALLADARES DARWIN RAMIRO** que lo entregue a Ing. Rodrigo Silva Msc, en su calidad de Coordinador del Programa de Maestría en Redes y Conectividad, tercera Promoción

Sangolquí, Noviembre del 2014

Ing. Juan Carlos Oleas C. Msc
DIRECTOR

Ing. José Luis Torres. Msc.
OPONENTE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

DECLARACIÓN DE RESPONSABILIDAD

AIMACAÑA VALLADARES, DARWIN RAMIRO

DECLARO QUE:

El proyecto de grado denominado **"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",** ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Noviembre del 2014.

_____

AIMACAÑA VALLADARES, DARWIN RAMIRO

UNIVERSIDAD DE LAS FUERZAS ARMADAS

MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

AUTORIZACIÓN

Yo, **AIMACAÑA VALLADARES, DARWIN RAMIRO**

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo **"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"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Noviembre del 2014.

_____

AIMACAÑA VALLADARES, DARWIN RAMIRO

DEDICATORIA

La concepción de este proyecto está dedicada a mi familia en especial a mis abuelos, pilares fundamentales en mi vida. Sin ellos, jamás hubiese podido conseguir lo que hasta ahora he logrado. Su tenacidad y lucha insaciable han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para toda la familia en general. También dedico este proyecto a mi novia y sobrinos, compañeros inseparables de cada jornada. A ellos este proyecto, ya que han hecho posible la culminación del mismo.

Darwin Ramiro Aimacaña Valladares

AGRADECIMIENTO

El presente trabajo de tesis primeramente me gustaría agradecerte a Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño anhelado.

A la UNIVERSIDAD DE LAS FUERZAS ARMADAS por darme la oportunidad de formar parte de la institución y ser un mejor profesional. A mi director de tesis, Ing. Msc. Juan Carlos Oleas Castelo por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito.

También me gustaría agradecer a los ingenieros que formaron parte del proyecto de Maestría MRIC III, porque todos han aportado con un granito de arena a mi formación.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE GRAFICOS

RESUMEN

Las aplicaciones y tecnologías actuales como la computación distribuida, voz y vídeo sobre IP, ahora requieren 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.

INFRAESTRUCTURA, SEGURIDAD, TOPOLOGÍA, MULTIPUNTO, VIRTUAL

ABSTRACT

Applications and technologies such as distributed computing, voice and video over IP, now require an efficient and reliable communication between remote sites or branches instantly. To provide some degree of full mesh connection (full mesh) or even a partial mesh connectivity, the IP tunneling based solutions require the provision of complex mesh connection, a more traditional implementation of securities with PtP IPSEC which suffer from multicast replication problems because this must be done before the tunnel encapsulation and encryption. With this background it is necessary to find a mechanism that eliminates point-to-point, maintaining levels of security and convergence-sensitive applications such as voice and video, that is why in this paper analyzes the mechanism of multipoint VPNs is done multipoint

INFRASTRUCTURE, SAFETY, TOPOLOGY, MULTIPOINT, VIRTUAL

CAPITULO I

1. FUNDAMENTOS DE TECNOLOGÍA MPLS Y SEGURIDAD

La evolución tecnológica de los mercados, la globalización, la integración de la sociedad y las tecnologías de información y comunicación entre otros factores, obliga a que las telecomunicaciones en el Ecuador estén a la par con esta evolución, para lo cual se deberá establecer políticas claras elaborando proyectos y acciones concretas que permitan implementar infraestructuras de comunicación seguras, convergentes y escalables.

Con este antecedente y tomando en cuenta que la información es uno de los activos más importantes con que cuenta toda organización, se hace necesario garantizar y mantener su integridad, así como la seguridad durante todo el proceso de transmisión de datos que se realice a través de un entorno WAN.

Con el presente trabajo se pretende plantear objetivos realizables, medibles y fiables cuando se implemente seguridades a nivel de capa 3, haciendo frente a la evolución tecnológica en materia de telecomunicaciones que obliga a que se introduzca en el país cambios sustanciales tomando en cuenta las regulaciones existentes.

La topología de red actual de muchos a muchos (any to any) ofrece flexibilidad para desviar tráfico sobre la marcha en caso de fallos de los enlaces o congestión en la infraestructura de comunicación que en la actualidad es soportada por la tecnología MPLS (Multiprotocol Label Switching).

1.1 JUSTIFICACIÓN E IMPORTANCIA

La topología MESH introduce una nueva forma de estructurar las redes de comunicación triple-play (voz, datos y vídeo), permitiendo así superar las limitaciones inherentes a escenarios que requieren despliegues rápidos y de alta capacidad.

Con este antecedente las empresas modernas requieren redes de datos malladas multipunto – multipunto, las cuales deben permitir la encriptación de la información sin perder las facilidades que poseen su infraestructura actual como por ejemplo la capacidad de convergencia.

1.2 PLANTEAMIENTO DEL PROBLEMA

Este trabajo está enfocado a las redes de datos convergentes, lo cual permitirá por medio del análisis de riesgo, identificar las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de un entorno WAN.

En Ecuador las empresas tanto públicas como privadas han dado poco o ninguna importancia al tema de encriptación de datos a nivel de capa 3. Al momento el backbone principal de comunicación a nivel nacional se basa principalmente en tecnología MPLS, por tanto es necesario poseer un mecanismo de encriptación de datos eficiente para este tipo de redes, más aún cuando en la actualidad los organismos de control aplican nuevas regulaciones.

Con este antecedente con fecha 26 de abril del 2012 y resolución No.JB-2012-2148 [1] la Superintendencia de Bancos y Seguros entidad que regula el sistema financiero nacional dispuso a las instituciones que componen esta implementar suficientes medidas de seguridad para mitigar el riesgo de fraude mediante el uso de información y comunicaciones.

Adicionalmente la Policía Nacional del Ecuador busca incluir en el proyecto de Código Integral Penal a los delitos informáticos, la propuesta fue presentada el mes de agosto de 2013 a la Comisión de Justicia y Estructura del Estado para su análisis.

Por lo expuesto anteriormente se puede concluir que se hace necesario buscar un mecanismo de seguridad que sea implementado en capa 3, el cual sea dimensionado para un gran número de puntos de acceso, ya que con las soluciones tradicionales de encriptación por VPNs (Red Privada Virtual) es casi imposible controlar un número considerablemente grande de sitios remotos que deben estar conectados entre sí, ya que al realizar esta acción se pueden llegar a la degradación y rendimiento de la red, perjudicando las aplicaciones sensibles a la latencia, tales como VoIP y Video (streaming), por tal motivo con esta investigación se logró identificar un mecanismo de encriptación, el cual ayuda a controlar y mitigar los riesgos que involucra la seguridad en un entorno WAN.

1.3 FORMULACIÓN DEL PROBLEMA A RESOLVER

El problema existente hoy en día, cuando se quiere garantizar seguridades a nivel WAN, es que estas están enmarcadas para topologías 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 multipunto – multipunto, por tanto en este trabajo se plantea investigar las siguientes interrogantes:

a) ¿Es factible la implementación de encriptación multipunto - multipunto en una red MPLS sin perder la funcionalidad de convergencia?

b) ¿Puede ser aplicado este proyecto en redes corporativas en producción?

1.4 HIPÓTESIS.

Es factible la implementación de GETVPN (Group Encrypted Transport) en una red Multipunto aplicando seguridad a nivel de capa 3 utilizando su mismo enrutador? Las variables a considerar en este proyecto son: paquetes encriptados, consumo de ancho de banda, retardos y estabilidad de (QoS).

1.5 OBJETIVO GENERAL

Diseñar y evaluar una red segura sin necesidad de túneles punto a punto y que permita mantener las características de conectividad full mesh que brinda una red MPLS.

1.6 OBJETIVOS ESPECÍFICOS

1. Buscar un mecanismos de encriptación multipunto - multipunto eficiente que se adapte a los requerimientos actuales de comunicación IP/MPLS.
2. Realizar una emulación para validar si la encriptación propuesta funciona.
3. Procesar y analizar los datos obtenidos de la emulación para poder justificar la validez de la hipótesis planteada.
4. Evaluar la gestión de seguridad de GETVPN con respecto a otros protocolos de seguridad en un mismo escenario de implementación.

1.7 SITUACION DE LAS TELECOMUNICACIONES EN EL ECUADOR

De acuerdo al Plan de Desarrollo de las Telecomunicaciones 2007 – 2012 emitido por la Secretaría Nacional de Telecomunicaciones SENATEL, la cual menciona “La evolución tecnológica y de los mercados, la globalización, la integración de la sociedad y las tecnologías de información y comunicación, entre otros factores, obliga a que las telecomunicaciones en el Ecuador estén a la par con la evolución y sus influencias en el medio que nos rodea, estableciendo políticas claras, elaborando planes, proyectos y acciones concretas que permitan fortalecer a los sectores existentes, desarrollar otros y especialmente a las áreas marginadas con el objeto de mejorar la calidad

de vida de nuestros habitantes y garantizar un desarrollo armónico de la sociedad”

Con este antecedente y tomando en cuenta que el Backbone principal de las telecomunicaciones en el ECUADOR a nivel nacional está compuesto por una red de alta capacidad basada en fibra óptica y tecnología MPLS (Multiprotocol Label Switching) ha facilitados el ampliar varios servicios como Voz, Datos y Video los cuales deben tener seguridades criptográficas para garantizar su integridad cuando estos son transportados a nivel WAN.

A continuación se presenta un cuadro en el cual se detalla los diez proveedores más importantes en ecuador y el porcentaje de las tecnologías de comunicación más usadas por estos [2]:

Tabla 1

Tecnologías de Comunicación implementadas en Ecuador

N°	PROVEEDOR	SERVICIO	COBERTURA	TECNOLOGIAS (%)			
				ATM	SATELITAL	CELULAR	MPLS
1	Corporación Nacional De Telecomunicaciones CNT EP	Portador	Nacional	5	5	10	80
2	Ecuador Telecom S.A. / Conecel (Claro)	Portador	Nacional	0	5	50	45
3	Otecel S.A. (Movistar)	Portador	Nacional	5	5	50	40
4	Global Crossing Comunicaciones Ecuador S.A.	Portador	Nacional	0	10	0	90
5	Puntonet S.A.	Portador	Nacional	20	10	0	70
6	Telconet S.A.	Portador	Nacional	0	0	0	100
7	Megadatos S.A.	Portador	Nacional	90	10	0	0
8	Teleholding S.A.	Portador	Nacional	100	0	0	0
9	Etapa Ep.	Portador	Nacional	80	0	0	20

(Fuente SUPERTEL)

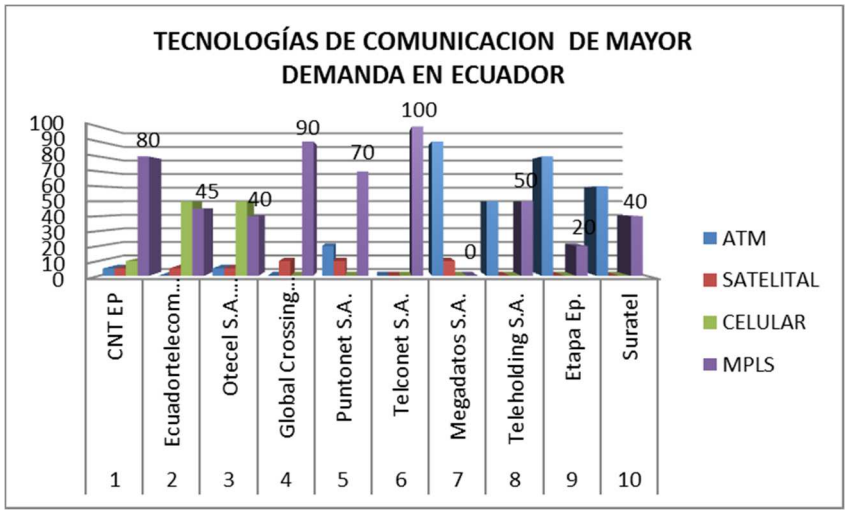


Figura 1. Tecnologías de Comunicación de mayor demanda en Ecuador

1.8 FUNDAMENTOS DE MPLS

MPLS (MultiProtocol Label Switching) es una tecnología que usa etiquetas para hacer decisiones de reenvío de tráfico. Con la tecnología MPLS, el análisis capa 3 del encabezado de un paquete se hace sólo una vez, en el punto donde el paquete entra al dominio MPLS, y por medio de la inspección de las etiquetas se maneja el posterior direccionamiento dentro de la red de MPLS.

Con la secuencia mencionada se obtiene una mayor velocidad al no tener que procesar el encabezado de IP en cada salto (o router) porque las decisiones de reenvío se toman comparando las etiquetas (como en un switch) en lugar utiliza una base de información de ruteo.

Adicionalmente se reduce el overhead (Desperdicio de ancho de banda, causado por la información adicional como control, secuencia, entre otros.) dentro de los routers de núcleo o de core, obtenemos también ingeniería de tráfico (TE), calidad de servicio (QoS), todo tipo de transporte sobre MPLS (Any Transport over MPLS o AToM) y redes privadas virtuales (VPN).

Entre las ventajas más relevantes de MPLS tenemos:

- **Ahorros en costos.** Del estudio realizado por la revista española Networkworld [3] dependiendo de la combinación específica de aplicaciones y de la configuración de red de una empresa, los servicios basados en MPLS pueden reducir los costos entre un 10 y un 25% frente a otros servicios de datos comparables (como Frame Relay y ATM). Y, a medida que se vayan añadiendo a las infraestructuras de networking el tráfico de vídeo y voz, los ahorros de costos empiezan a dispararse alcanzando niveles de hasta un 40%.

- **Soporte de QoS**. Uno de los principales beneficios de los servicios basados en MPLS reside en su capacidad para aplicar calidades de servicio (QoS) mediante la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y vídeo en las redes de datos.

- **Rendimiento mejorado**. Considerando que la infraestructura de comunicación muchos a muchos (any to any) que disponen los servicios MPLS, se logra reducir el número de saltos entre puntos (routers), lo que se traduce directamente en una mejora de los tiempos de respuesta y del rendimiento de las aplicaciones.

- **Recuperación ante desastres**. Los servicios basados en MPLS mejoran la recuperación ante desastres de diversas maneras. Con esta tecnología se podrá conectar los centros de datos (Data Center) y otros emplazamientos clave mediante múltiples conexiones redundantes a la nube MPLS y, a través de ella, a otros sitios de la red. Además, los sitios remotos pueden ser reconectados fácil y rápidamente a las localizaciones de backup en caso de necesidad; a diferencia de lo que ocurre con las redes ATM y Frame Relay, en las cuales se requieren circuitos virtuales de backup permanentes o conmutados. Esta flexibilidad para la recuperación

del negocio es precisamente una de las principales razones por la que muchas empresas están optando por esta tecnología.

- **Preparación para el futuro.** La mayoría de las empresas han llegado a la conclusión de que MPLS representa “el camino del futuro”. La inversión en servicios WAN convencionales, como los citados ATM y Frame Relay, prácticamente se ha paralizado. Según Current Analysis [4] si hoy el 44% de las empresas todavía utilizan Frame Relay y un 25% ATM, estos porcentajes pronto bajarán en favor de las nuevas alternativas como IP VPN o Carrier Ethernet, de las que MPLS constituye hoy uno de sus principales soportes.

1.9 FUNCIONAMIENTO DE MPLS

Una red MPLS básicamente funciona cambiando las etiquetas de un paquete que ya está etiquetado. Cuando un paquete se envía de la computadora A, a la computadora B, mediante una red MPLS, y la secuencia que sigue es la siguiente [5]:

a) Creación y distribución de etiquetas
b) Creación de tablas en cada enrutador
c) Creación de LSPs (Label-switched path)
d) Agregar etiquetas a los paquetes con la información de la tabla.
e) Envío del paquete

Considerando la secuencia anterior se indica que el paquete enviado sale de la computadora para llegar al router que se encuentra en la infraestructura interna, luego el paquete llega hasta un router con características MPLS el cual es denominado Router Extremo de Ingreso (Ingress Label Edge Router). En este punto se analiza el destino del paquete, esto puede varía si el paquete proviene de una red ATM y una red IP. La particularidad de que MPLS difiera de la tecnología de comunicación de redes implementadas es una de las ventajas que posee esta tecnología, ya que este puede empezar a funcionar

sobre redes ya existentes y no es necesario invertir en más hardware, esto se puede hacer sobre el hardware existente con algunas actualizaciones de software.

Una vez que se analiza el destino del paquete, y dependiendo de su destino este se le denomina FEC “L”(etiqueta). No necesariamente el mismo destino tiene la misma FEC, todo depende de cómo se deba tratar ese paquete. Cada FEC tiene un camino específico a seguir por la red MPLS y es independiente en cada router. También cada FEC tiene diferente QoS (Quality of Service) que necesita. El QoS es muy importante ya que nos permite tratar a paquetes que van al mismo destino de diferente manera.

El QoS también nos permite utilizar todos los recursos de la red ya que no necesariamente se van a utilizar las líneas más rápidas, sino se van a tratar de utilizar todos los recursos de una manera óptima.

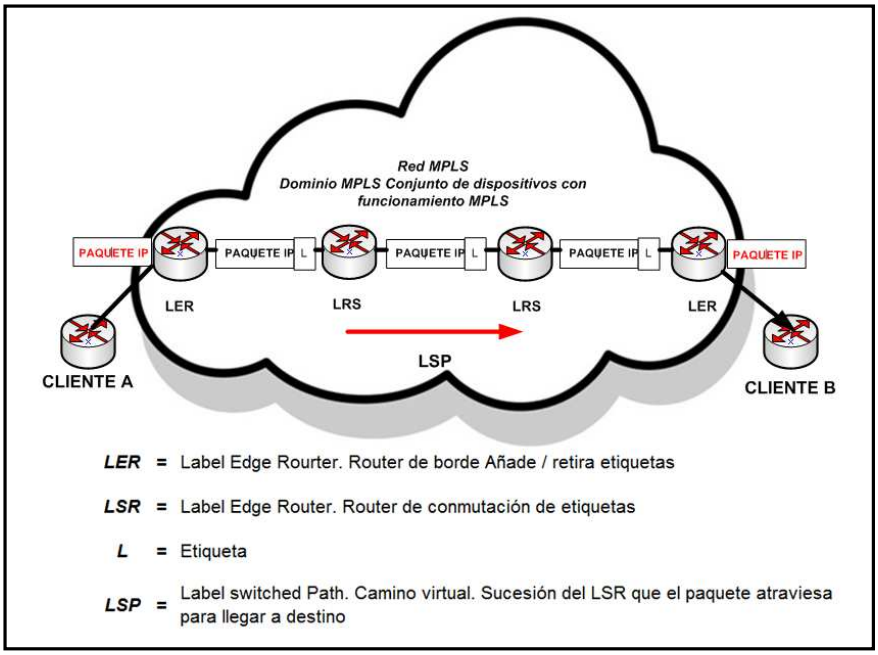


Figura 2. Funcionamiento de MPLS
(fuente: Cisco Press)

Para saber qué etiqueta asignarle al paquete se tiene que comparar con las etiquetas ubicadas en las tablas de enrutamiento que se van dando desde la dirección destino a la dirección fuente por medio de pequeños mensajes entre los routers. Normalmente ese camino es decidido antes de que se mande la información; el camino se forma en las tablas de enrutamiento cuando los dispositivos son conectados a la red.

Una vez que ya se tienen las tablas de enrutamiento al paquete se le asigna una etiqueta la cual va cambiando en cada conmutador o enrutador MPLS al que llega simplemente revisando esa etiqueta.

El paquete sigue su camino hasta que llega al enrutador extremo de egreso (Egress Label Edge Router) en el cual se le quitan todas las etiquetas que tenía y llega a la computadora destino o simplemente sale de la red MPLS.

Uno de los protocolos más usado en sistemas autónomos MPLS es OSPF (Open shortest path first) ya que por ser dinámico distribuye automáticamente la información de ruteo entre los equipos activos que compone una red WAN. Otras características importantes es que permite habilitar tanto enlaces redundantes como balanceo de carga.

Todas estas características son necesarias de tomar en cuenta ya que en la actualidad las redes de datos son de gran tamaño y por esta se transporta son transportadas diversidad de información y aplicaciones.

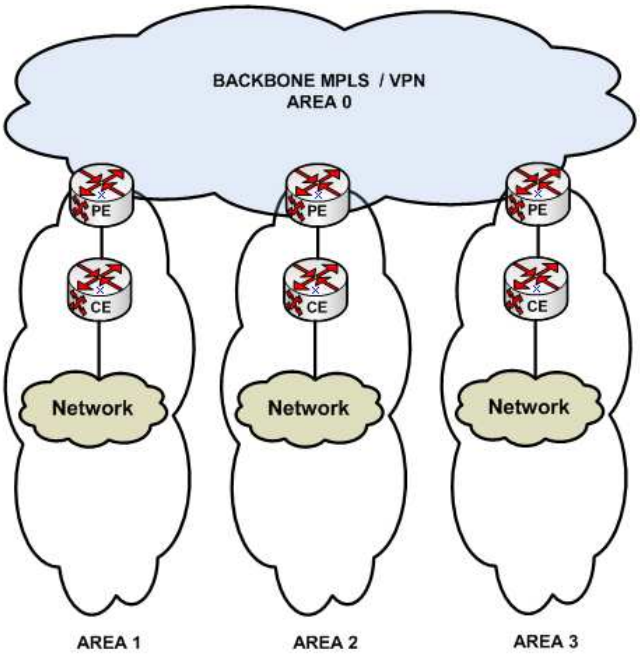


Figura 3 Funcionamiento de MPLS
(Fuente: Cisco Press)

1.9.1 APLICACIONES DE MPLS

Una red de comunicaciones IP y MPLS de extremo a extremo ayuda a las organizaciones a encontrar un equilibrio entre los requerimientos de negocio actuales y los objetivos del futuro. IP/MPLS se ha convertido en la tecnología de elección para el backbone principal de transmisión de datos a nivel nacional tanto para empresas privadas como públicas.

Con este antecedente y tomando en cuenta que los administradores y usuarios de estas redes requieren cada vez un mayor grado seguridad de los datos es necesario considerar los siguientes requerimientos:

1.9.2 MPLS UNICAST IP

Con MPLS el reenvío de paquetes Ips unicast envía los paquetes lógicos basado en etiquetas. Sin embargo, cuando las interfaces escogen la salida para el reenvío de los paquetes, MPLS considera sólo las rutas en la tabla de

enrutamiento unicast, pero todos los demás factores se mantuvieron sin cambios.

Cuando MPLS reenvía un paquete IP unicast, no proporciona ninguna ventaja significativa por sí misma, sin embargo, muchas de las aplicaciones de MPLS más útiles, tales como MPLS VPN e ingeniería de tráfico MPLS (TE), usan el reenvío de IP unicast como una parte de la red MPLS, por tanto se debe considerar lo siguiente:

a) Para el ruteo unicast IP son necesarios dos mecanismos en el plano de control y estos son:
   - IP routing protocol (OSPF, IS-IS, EIGRP,)
   - Label distribution protocol (LDP or TDP)
b) Un protocolo de ruteo transporta información de accesibilidad de redes.
c) El protocolo de distribución de etiquetas asigna etiquetas a redes aprendidas a través de protocolos de enrutamiento.
d) El Forwarding Equivalence Class (FEC) es equivalente a la red de destino almacenada en la tabla de enrutamiento IP.

1.9.3 MPLS MULTICAST IP

La tarea de seleccionar una ruta entre dos nodos de una red es uno de los aspectos más importantes en las redes de computadoras. Esta tarea es llevada a cabo por los algoritmos de enrutamientos, los cuales se encargan de seleccionar la ruta más adecuada.

La construcción del árbol multicast más adecuado, con raíz en el nodo origen y alcanzando cada uno de los nodos destinos a través de un camino es llevada a cabo por el algoritmo de enrutamiento multicast.

El ruteo multicast puede optimizar distintas métricas, además la aplicación para la cual se construye el árbol puede tener diversos requerimientos de QoS como retardo máximo de extremo a extremo limitado,

retardo medio acotado o ancho de banda mínimo requerido para llevar a cabo la transmisión.

Por tanto cuando se implementa una infraestructura MPLS se debe considerar:

- No se necesita un protocolo dedicado para enviar multicast a través de un dominio MPLS.
- Se utiliza “peripheral interface manager” (PIM) versión 2 con extensiones para MPLS para propagar información de enrutamiento y de etiquetas.
- FEC (Forwarding equivalence class) es el equivalente a las direcciones de multicast almacenadas en la tabla de ruteo.

1.10 REDES VIRTUALES PRIVADAS

Una red privada virtual **(**VPN**)** se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada.

El objetivo de las VPNs es el soporte de aplicaciones intranet/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces.

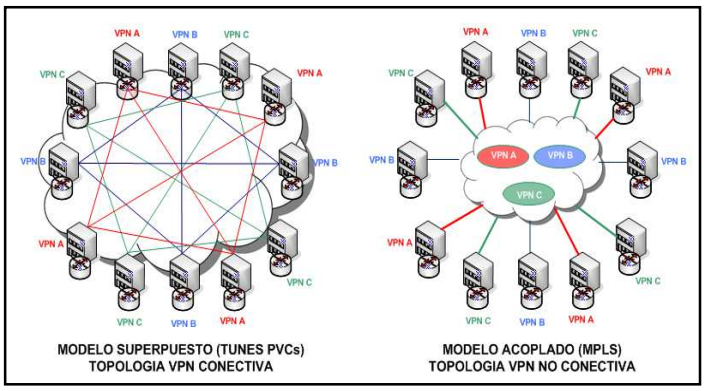


Figura 4. Redes Virtuales Privadas

En la figura anterior se realiza una comparación entre el modelo de túneles (PVCs - Private Virtual Circuits) y el modelo de LSPs (label-switched path) de MPLS. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, basados en LSPs, y no de extremo a extremo a través de la red.

Resumiendo, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionar un modelo "acoplado" o "inteligente", ya que la red MPLS conoce de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).
- Evita la complejidad de los túneles y PVCs.
- Provee de un servicio sencillo: una nueva conexión afecta a un solo enrutador y tiene mayores opciones de crecimiento modular.
- Permite mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda y retardo), lo que es necesario para un servicio completo VPN.

1.11 INGENIERIA DE TRÁFICO

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera de evitar que un subconjunto (enlaces y equipos) de la red se sature mientras otro subconjunto de la misma se encuentra sub utilizado, con esto se mejoraría el rendimiento de la red global.

Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP (Interior Gateway Protocol) correspondiente. En casos de congestión de algunos enlaces, el problema se resolverá añadiendo más capacidad a los

enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP (Interior Gateway Protocol) sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

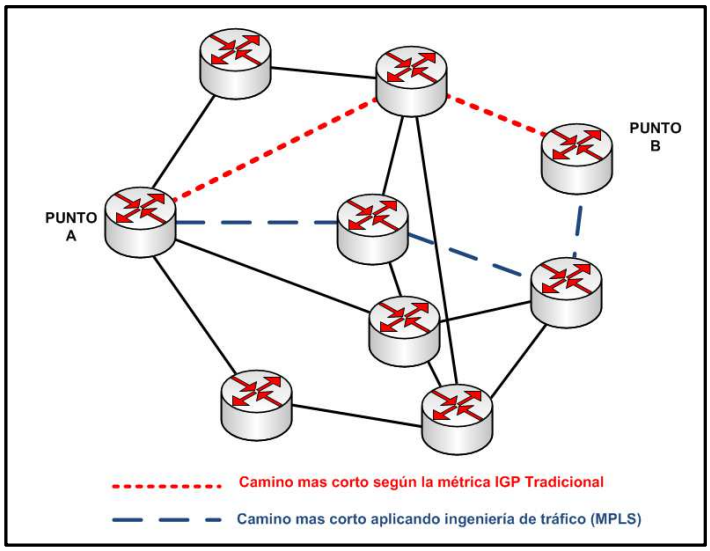


Figura 5. Comparación métrica IGP e Ingeniería de Tráfico

El camino más corto entre A y B según la métrica normal IGP (Interior Gateway Protocol) es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces hagan aconsejable la utilización del camino alternativo indicado con un salto más (o más saltos también). La utilización de MPLS es efectivo para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP (Label Switched Path).
- Permite obtener estadísticas de uso LSP (Label Switched Path), que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer "enrutamiento restringido" (Constraint-based Routing, CBR), de modo que cuando administramos una red, podremos

seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad).

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costos de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

1.11.1 SELECCIÓN DE LA MEJOR RUTA (POLICY ROUTING)

La selección de ruta hace referencia a la selección de un LSP (Label Switched Path) para un FEC (Forwarding Equivalence Class) particular. La arquitectura MPLS soporta dos opciones: ruteo salto-a-salto o ruteo explícito.

Con el ruteo salto-a-salto, cada LSR (Label Switching Router) seleccionada en forma independiente el próximo salto para cada FEC (Forwarding Equivalence Class).

Esta opción proporciona alguna de las ventajas de MPLS, incluida la conmutación rápida mediante etiquetas, la habilidad de emplear pilas de etiquetas, y el tratamiento diferencial de paquetes pertenecientes a diferentes FECs que siguen la misma ruta.

Sin embargo, debido al uso limitado de métricas de desempeño en los protocolos de ruteo más difundidos, el ruteo salto-a-salto no soporta TE (Traffic Engineer) o políticas de ruteo (definición de rutas en base a alguna política relacionada con QoS, seguridad u alguna otra consideración).

Con el ruteo explícito generalmente el LSR ((Label Switching Router) ingress o el LSR (Label Switching Router) egress, especifica algunos o todos los LSRs dentro del LSP para un FEC particular. En el caso de ruteo explícito estricto, un LSR especifica todos los LSRs existentes en el LSP (Label

Switched Path); para el caso de ruteo explícito débil, sólo especifica algunos LSRs.

El ruteo explícito ofrece todos los beneficios de MPLS, incluidas la capacidad de TE (Traffic Engineer) y políticas de ruteo. Las rutas explícitas pueden seleccionarse mediante configuración, esto es, establecidas en forma preliminar, o dinámicamente.

El ruteo explícito dinámico proveerá el mejor soporte para TE (Traffic Engineer); en este caso, el LSR (Label Switching Router) que establece el LSP (Label Switched Path) necesitará información acerca de la topología del dominio MPLS e información QoS acerca de ese dominio.

Una especificación de TE (Traffic Engineer) en MPLS sugiere que la información relacionada con QoS corresponde a una de dos categorías:

- Un conjunto de atributos asociados con un FEC (Forwarding Equivalence Class) o un conjunto de FECs similares que colectivamente especifican sus características de comportamiento.
- Un conjunto de atributos asociados con recursos (nodos, enlaces) que restringen la ubicación relativa de los LSPs (Label-switched path).

Un algoritmo de ruteo que tiene en cuenta los requerimientos de tráfico de los diferentes flujos y los recursos disponibles a lo largo de varios saltos y a través de diferentes nodos se denomina algoritmo de ruteo basado en restricciones. En esencia, una red que utilizar un algoritmo de este tipo está en conocimiento permanente de la utilización vigente, la capacidad existente, y los servicios comprometidos.

Los algoritmos tradicionales, tales como OSPF y Border Gateway Protocol (BGP), no utilizan un suficiente arreglo de métricas de costos en sus algoritmos como para calificar dentro de esta categoría.

Más aún, en el cálculo de una ruta dada, sólo puede utilizarse una única métrica de costo (por ejemplo, número de saltos, retardo). En el caso de MPLS, resulta necesario mejorar un protocolo existente o desplegar uno nuevo. Por ejemplo, se ha definido una versión mejorada de OSPF [6] que provee al menos parte del soporte requerido por MPLS. Ejemplos de métricas que podrían ser utilizadas:

- Tasa de enlace de datos máxima.
- Reservación de capacidad corriente.
- Tasa de pérdida de paquetes.
- Retardo de propagación del enlace.

1.11.2 QoS

En la actualidad, el tráfico de red es muy diverso, cada tipo de tráfico tiene requerimientos específicos en términos de ancho de banda, retraso, latencia y disponibilidad. Con el explosivo crecimiento de Internet, la mayor parte del tráfico de red está basado en el protocolo IP. Contar con un único protocolo de transporte de punta-a-punta es beneficioso, ya que el equipo de redes se simplifica en términos de mantenimiento, con la consecuente disminución de costos operativos.

Ese beneficio, sin embargo, se enfrenta al hecho de que el protocolo IP es un protocolo sin conexión, es decir que los paquetes IP no toman un camino específico al atravesar la red, lo cual genera una Calidad de Servicio impredecible.

La calidad de servicio o QoS (Quality of Service) se podría definirse como garantizar un transporte confiable de los datos a través de las redes, manteniendo los requerimientos necesarios que permitan correr los servicios de forma óptima.

Cada tipo de servicio, como navegación WEB, servicios de voz, datos y video, tienen diferentes requerimientos para su transporte. Para esto las redes

deben ser capaces de identificar y asegurar los distintos tráficos y otorgarles un tratamiento específico que asegure la calidad de su transporte.

1.11.3 NIVELES DE SERVICIO

Los niveles de Calidad de Servicio se refieren a las actuales capacidades de las conexiones que tiene una red determinada por la cual pasa un tráfico específico. Los servicios difieren en cuán estrictos y puntuales pueden ser los niveles de QoS, o sea, que tiene que ser específico para un ancho de banda, jitter o pérdida de paquetes determinado estos son:

- Nivel Best Effort: básicamente estos servicios no ofrecen ninguna garantía. Usualmente utiliza técnicas FIFO (First in First Out o Primero en Entrar Primero en Salir), que no tienen ninguna diferenciación entre los distintos flujos.
- Nivel para Servicios Diferenciados (Diffserv): se basa en la división del tráfico en diferentes clases y en la asignación de prioridades.
- Nivel Garantizado: está destinada para aplicaciones con requerimientos exigentes de tiempo real. Esta calidad asegura un ancho de banda, un límite en el retardo y ninguna pérdida en las colas.

Tabla 2

Protocolos de control utilizado en diversas aplicaciones de MPLS

N°	APLICACION	TABLA FEC (FORWARDING EQUIVALENCE CLASS	PROTOCOLO DE CONTROL USADO PARA CONSTRUIR LA TABLA FEC	PROTOCOLO DE CONTROL USADO PARA EL INTERCAMBIO FEC TO LABEL MAPPING
1	IP Routing	Tabla IP Routing	Cualquier protocolo de ruteo	TDP (Tag Distribution Protocol) o LDP (LABEL Distribution Protocol)
2	Milticast IP Routing	Tabla IP Multicast	PIM (Protocol Independent Multicast)	PIM Version 2

CONTINUA

3	VPN Routing	Per - VPN Routing Table	La mayoría de los protocolos de enrutamiento IP entre los proveedores de servicios y clientes, multiprotocolo BGP (Border Gateway Protocol) dentro de la red de proveedores de servicios	Multiprotocolo BGP (Border Gateway Protocol)
4	Ingeniería de Tráfico	Defínción de túneles MPLS	Definiciones de Interfaces manuales, IS-IS(Intermediate System to Intermediate System) or OSPF (Open Shortest Path First)	RSVP(Repondez sil vous plait / Protocolo de reserva de recursos) or CR-LDP(Constraint-based Routing Label Distribution Protocol)
5	Calidad de Servicio	Tabla IP Routing	Protocolo de Ruteo	Extensiones TDP(Transmission Control Protocol), LDP(Label Distribution Protocol

En este capítulo se han descrito conceptos importantes, que serán utilizados a lo largo del escrito de tesis y cuya comprensión fue esencial para el desarrollo del trabajo. Esta Capitulo es resultado de la investigación de la tecnología de comunicación actual y las protecciones que deben ser consideradas dentro del área de Seguridad. El siguiente capítulo describirá el funcionamiento de la aplicación de servicios de seguridad.

CAPITULO II

2. FUNDAMENTOS DE VPN

La globalización en la actualidad ha despertado un gran interés por los mecanismos de transporte de datos y sus diferentes aplicaciones, entre los que se encuentran las Redes Privadas Virtuales o VPNs (Virtual Private Networks).

Las soluciones MPLS-VPN, además de proporcionar escalabilidad, permiten dividir una gran red en pequeñas redes separadas, lo cual es necesario cuando las empresas tienen varias oficinas remotas, donde la infraestructura tecnológica debe ofrecer redes aisladas a áreas individuales.

Si bien es cierto MPLS es una tecnología innovadora, escalable y eficiente, esta no posee un mecanismo de seguridad en Capa 3, por lo que los proveedores del servicio como ISPs deben implementar soluciones basadas en firewalls para de alguna manera mitigar el tema de encriptación de la información.

En este capítulo se detallará los mecanismos existentes al momento de crear VPNs sobre una infraestructura MPLS. Así mismo al final se evaluará cuál de estos es el más eficiente al momento de implementar VPNS en una red Full Mesh.

2.1 ANTECEDENTES DEL ESTADO DEL ARTE

De la investigación realizada se evidencia que hay varios trabajos respecto a la implementación de VPNs en entornos punto a punto sobre redes MPLS, pero existe poca información respecto al uso de VPNs en entornos multipunto – multipunto conocidos como full mesh.

Al momento en el mercado mundial de las comunicaciones existe una propuesta de encriptación multipunto – multipunto diseñada por la empresa CERTES NETWORKS [7] la cual propone una solución de gestion de

seguridad basada en hardware y software denominada TrustNet Manager [8] compatible con servicios MPLS, lo cual implica instalar nueva infraestructura en cada sitio en donde se requiere un nivel de seguridad óptimo.

Localmente existe poco conocimiento respecto al tema de transporte multipunto – multipunto sobre todo en medios de comunicación MPLS, por tal motivo con esta investigación se buscó un mecanismo idóneo que permita la transmisión de datos en forma segura bajo entornos WAN, y cuyo objetivo principal sea de minimizar el uso de nueva infraestructura.

Tomando en cuenta la documentación existente referente a la implementación de VPNs sobre MPLS la mayoría son basados en documentos de referencia para la comunidad de Internet como por ejemplo el RFC 2547 el cual habla de implementaciones punto a punto sobre cualquier tipo de tecnología WAN, no obstante MPLS no tiene en estos momentos ningún mecanismo para proteger la seguridad en las comunicaciones, por lo que los proveedores de servicios de telecomunicaciones y sus clientes deben utilizar cortafuegos y algún protocolo de encriptación tipo IPsec para garantizar la integridad de sus datos.

Con este antecedente la implementación de VPNs sobre redes MPLS utilizando IPSec es común en entornos punto a punto, pero aún no se profundiza el tema de utilización de Grupo de Cifrado de Transporte (GETVPN) sobre redes MPLS, por tal motivo en esta investigación se dio un enfoque práctico al tema.

2.2 MARCO TEORICO

De la indagación realizada se pudo determinar que existen muchos estudios e implementaciones de seguridades en redes WAN que funcionan bajo la tecnología de MPLS y en entornos punto a punto, de las cuales podemos citar la tesis de Rafael Trujillo “Diseño e Implementación de una VPN en una Empresa Comercializadora utilizando IPSEC” [9]. En este trabajo se

hace un análisis de las redes privadas virtuales implementadas en el protocolo IPSEC.

Otro trabajo que profundiza en el tema de seguridad es el planteado por Victor Limari en su tesis “Protocolos de Seguridad para redes Privadas Virtuales (VPN)” [10], en el cual analiza las diferentes formas que hacen posible la creación de túneles para transmitir información de manera confiable. Así mismo en esta se da énfasis en el protocolo de Seguridad IPSEC, el cual reúne la mayoría de las características que hace que un modelo sea seguro sobre un medio de comunicación masivo como es el Internet.

Como se puede observar los trabajos descritos anteriormente se centran en la implementación de redes virtuales (VPN) punto a punto utilizando IPSEC como protocolo de seguridad. Con las soluciones comunes de implementación de VPNs el procesamiento del equipo CORE de comunicación aumenta considerablemente, lo cual hace que la latencia en la red sea notoria.

2.3 MARCO CONCEPTUAL

En este trabajo se describió el funcionamiento de las redes privadas virtuales tanto en entornos punto a punto como en un entorno multipunto – multipunto basadas en conmutación multiprotocolo.

El objetivo es mostrar su utilidad y servir como referencia a la hora de construir GETVPN [11] (Group Encrypted Transport) basadas en una infraestructura de comunicación mallada MPLS.

GETVPN representa una nueva categoría de VPNs diseñadas para encriptar datos transmitidos en redes de área extendida WAN. Esta solución ayudará a eliminar la necesidad de túneles punto a punto, lo que permitirá que las redes distribuidas de las empresas amplíen sus VPN en varios sitios al mismo tiempo soportando simultáneamente las necesidades de inteligencia

de la red, las cuales son esenciales para garantizar tanto la calidad de la voz y el vídeo.

Debido a que la aplicación principal de GETVPN se ejecuta en redes basadas en conmutación multiprotocolo, la flexibilidad inherente de GETVPN permitirá que las empresas refuercen su seguridad gestionando su propia protección de red sobre el servicio WAN.

2.4 DEFINICION DE VPN (VIRTUAL PRIVATE NETWORK)

Una red privada virtual (VPN) se define en términos generales como una red que permite la conectividad de uno o varios usuarios entre múltiples sitios, los cuales están dentro de una infraestructura de red compartida.

Esto es posible ya que la tecnología ha permitido crear túneles de encriptación a través de la Internet u otra red pública, y de esta manera se puede permitir a los usuarios que forman parte de la red virtual end to end, compartir servicios, aplicaciones de manera segura y confiable.

Como podemos observar en la figura anterior una red VPN es una extensión de una red privada que utiliza enlaces a través de redes públicas, privadas o compartidas (una red pública y compartida más común es Internet).

Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas:

a) Deben ser capaces de transportar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por esta red.
b) La solución debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser interceptado, leído o modificado.

c) Esta debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de modo que un adversario no pueda acceder a los recursos del sistema.

Para emular un enlace punto a punto, los datos son encapsulados o envueltos, con una cabecera que proporciona la información de enrutamiento que le permite atravesar la red pública o compartida para llegar a su destino.

Para emular un enlace privado, los datos enviados son encriptados para tener confidencialidad. Los paquetes que son interceptados en la red pública o compartida son indescifrables.

El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de red privada virtual (VPN).

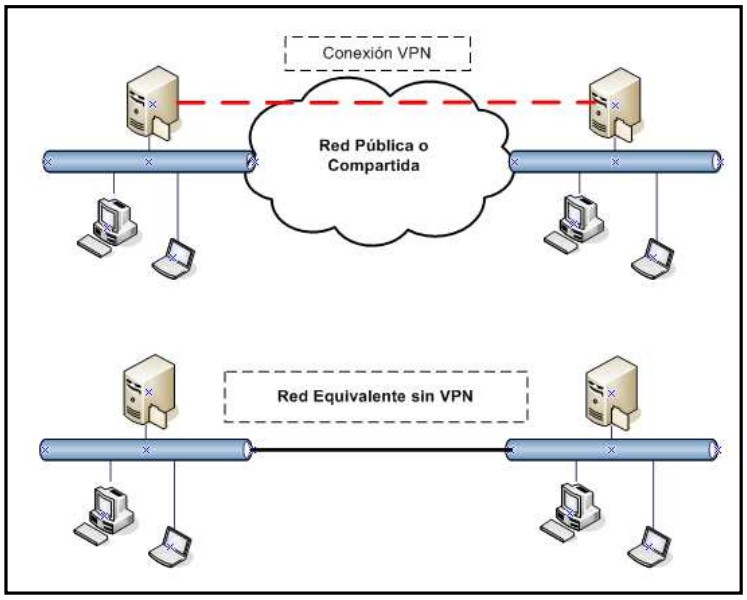


Figura 6. Conexiones entre sitios remotos

En una red privada virtual todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) las cuales se encuentran separadas geográficamente.

2.5 TIPOS DE TOPOLOGIAS VPNS

2.5.1 TOPOLOGIA HUB-AND-SPOKE

La topología que comúnmente es la más usada es una topología hub-and-spoke, donde un número de oficinas remotas (spokes) se conectan a un sitio central (hub), como se muestra en la figura 2.2. Las oficinas remotas por lo general pueden intercambiar datos (no hay restricciones de seguridad explícitas entre oficinas de tráfico), pero la cantidad de datos intercambiados entre ellos es insignificante.

La topología hub-and-spoke se utiliza normalmente en las organizaciones con estructuras jerárquicas pequeñas

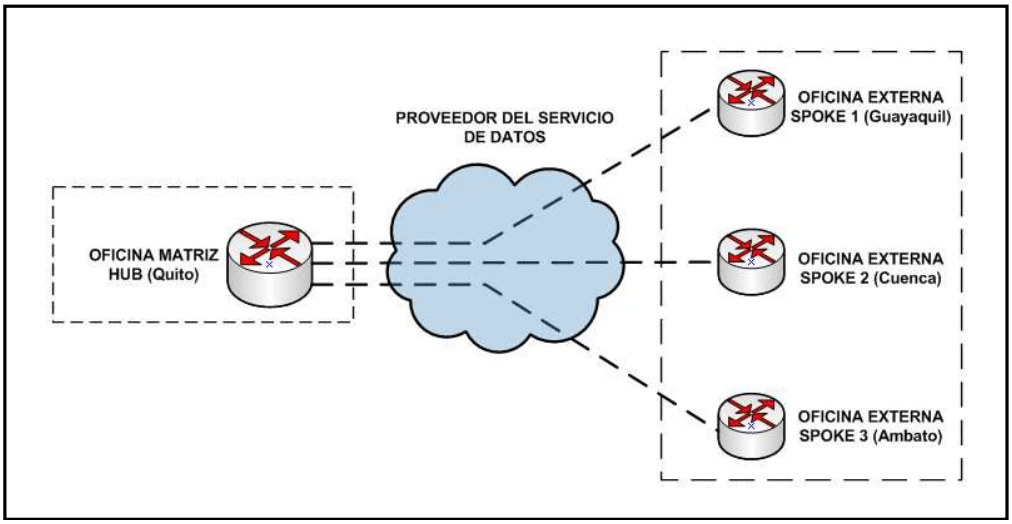


Figura 7. Topología Hub-Spoke

2.5.2 TOPOLOGIA MALLA PARCIAL.

El modelo de malla parcial es aquel en donde los sitios que disponen de una VPN están conectados por circuitos virtuales según la necesidad de tráfico que estos requieran. Si uno o varios puntos remotos no tienen conectividad directa a todos los otros sitios que están inmersos en la solución de comunicación tal como se muestra en la figura 2.3, la topología se llama una malla parcial; si cada sitio tiene una conexión directa con cada otro sitio, la topología se llama una malla completa.

Una malla parcial no suministra el nivel de redundancia de una topología de malla completa pero su implementación es más económica. Las topologías de malla parcial generalmente se usan en las redes periféricas que se conectan a un backbone de malla completa.

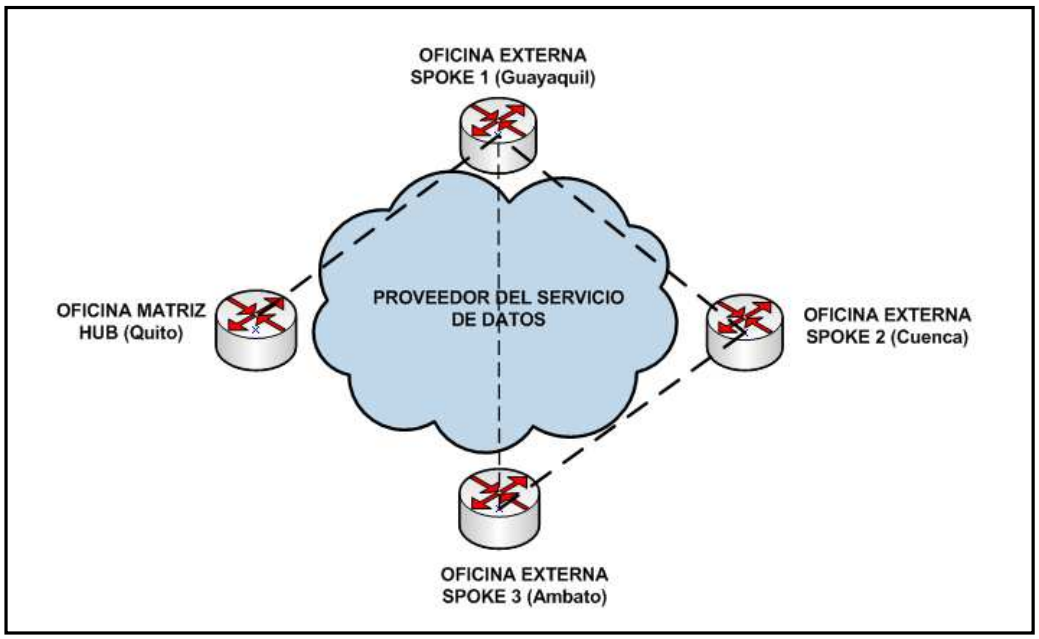


Figura 8. Topología Hub-Spoke

2.5.3 TOPOLOGIA HIBRIDA

Es una topología que utiliza VPNs superpuestas y que combina la topología hub-and-spoke con la topología de malla parcial. Por ejemplo, una gran organización multinacional podría tener redes de acceso en cada país implementado con una topología de hub-and-spoke, mientras que la red central internacional se llevaría a cabo con una topología de malla parcial. La figura 2.4 se muestra un ejemplo de tal organización.

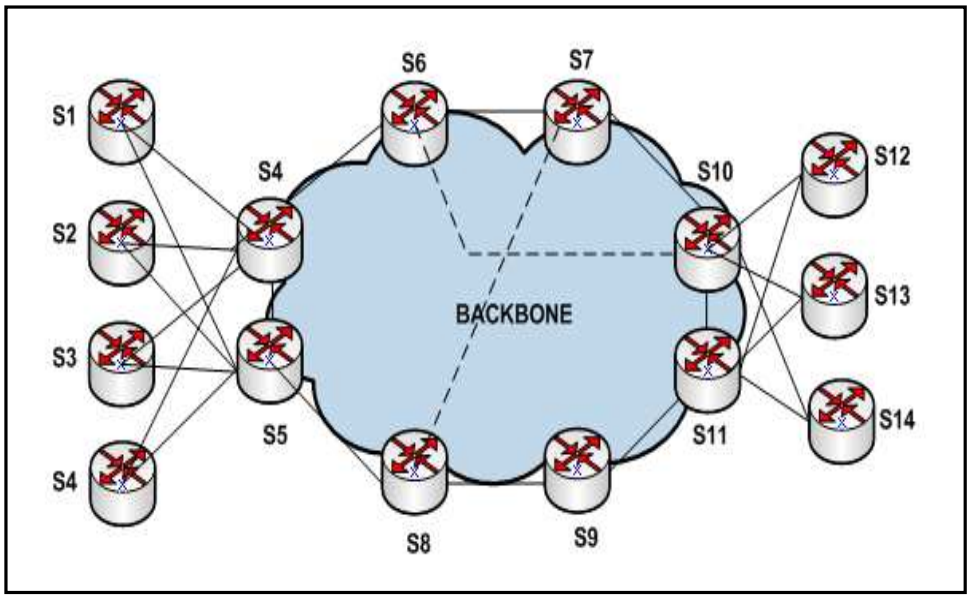


Figura 9. Topología Hibrida

2.6 TIPOS DE VPNS (NIVEL FUNCIONAL)

Entre las implementaciones más comunes se tiene 4 maneras claramente identificadas y son:

Tabla 3

Implementaciones comunes de una VPN

N°	TIPO	DETALLE
1	VPN de Intranet	Creación de conexiones entre las oficinas centrales y las oficinas remotas
2	VPN de Acceso Remoto	Creación de conexiones entre las oficinas centrales y los usuarios móviles remotos
3	VPN de Extranet	Creación de conexiones entre la empresa y sus socios comerciales.
4	VPN Interna	Creación de conexiones dentro de una LAN

2.6.1 VPN DE INTRANET.

Este tipo de implementación está dada por la creación de una conexión entre las oficinas centrales corporativas y las oficinas remotas que se encuentran en el exterior. A comparación con una Intranet típica el acceso viene desde el exterior a la red y no desde el interior. La siguiente figura ilustra una Red privada Virtual de Intranet.

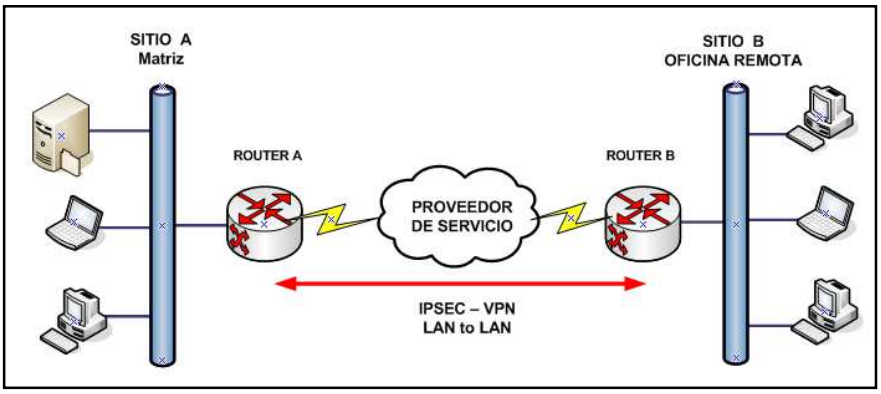


Figura 10. VPN de Intranet

2.6.2 VPN DE ACCESO REMOTO.

Una red privada virtual de acceso remoto se crea entre las oficinas centrales corporativas y los usuarios móviles remotos a través de un ISP. Como se puede observar en la figura 2.6, el usuario móvil levanta una conexión con un ISP y crea un túnel de conexión hacia las oficinas centrales corporativas.

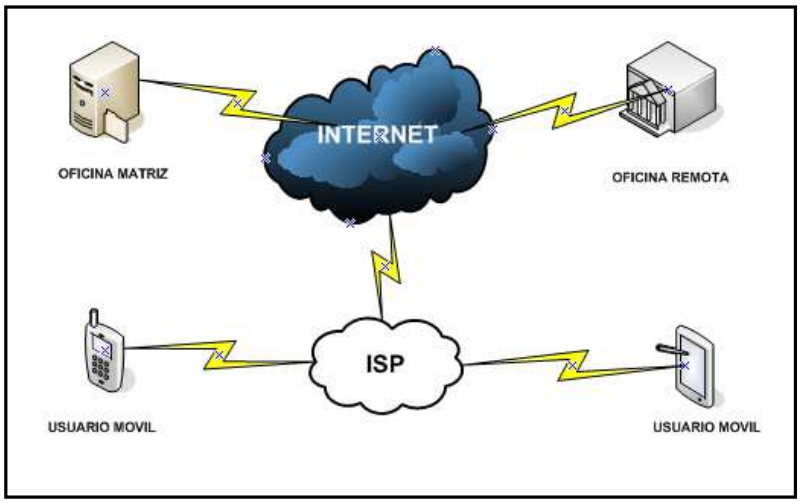


Figura 11. VPN de Acceso Remoto

2.6.3 VPN DE EXTRANET.

Una red privada virtual de Extranet se crea entre la empresa y sus socios comerciales (clientes, proveedores), mediante el protocolo HTTP, que es el común de los navegadores de Web, o mediante otro servicio y protocolo ya establecido entre las dos partes involucradas. Esta implementación tiene mayor impacto en todo lo referente al comercio electrónico brindando seguridad y eficacia para las empresas y sus socios comerciales. La figura 12 se ilustra una red privada virtual de extranet.

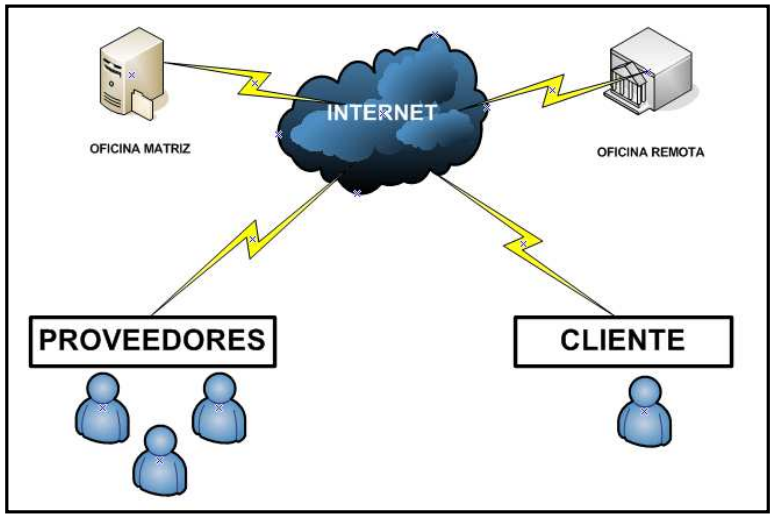


Figura 12. VPN de Extranet

2.6.4 VPN INTERNA.

Una red privada virtual interna, es una implementación que no tiene un uso frecuente en el entorno de las redes. Este tipo de implementación se crea en una LAN, siempre que se considere necesario transferir información con mucha privacidad entre departamentos de una empresa.

Esta red privada virtual interna es necesaria implementarla cuando se cree que se pueden tener ataques informáticos realizados por los mismos empleados de la empresa. La figura 13 ilustra una configuración típica de red privada virtual interna.

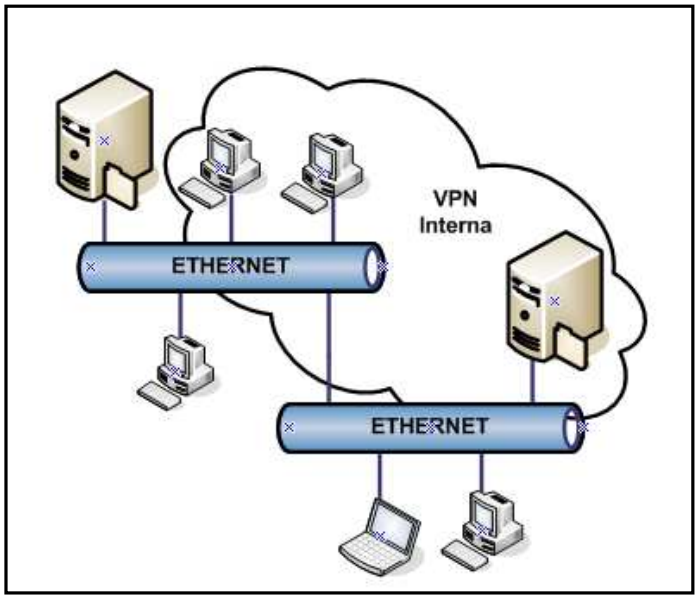


Figura 13. VPN Interna

Protocolos VPN seguras incluyen:

- IPSec: Internet Security Protocol
- Transport Layer Security (TLS)
- Secure Sockets Layer (SSL)
- Datagram Transport Layer Security (DTLS)

- Secure Socket Tunneling Protocol (SSTP)
- Microsoft P-P Encryption (MPPE)
- Secure Shell (SSH)

2.7 TIPOS DE VPNS (NIVEL TECNICO)

2.7.1 VPN DINAMICAS (DMVPN)

Una de las principales preocupaciones y desafíos que existe al momento de la implementación de VPN sitio a sitio usando la topología Hub & Spoke con un gran número de sitios remotos es la escalabilidad que debería tener. Con el hecho de que la implementación de muchos túneles GRE (Generic Routing Encapsulation) sobre IPSec con un protocolo de ruteo dinámico puede ser escalable, hay que tomar en cuenta que con el número de listas de acceso y de túneles punto a punto es difícil la administración cuando existe un gran número de sitios remotos sobre una topología mallada.

Además de los problemas de escalabilidad, la implementación de un gran número de VPN sitio a sitio usando la topología Hub & Spoke con un gran número de comunicaciones spoke to spoke, dará lugar a una sobrecarga alta en el CPU y a la memoria del Router porque todo el tráfico spoke to spoke debe transitar por el hub (router CORE).

Una de las soluciones más escalables a los problemas mencionados de VPN usando la topología Hub & Spoke con un gran número de comunicaciones spoke to spoke es DMVPN (Dynamic Multipoint VPN). Uno de los requisitos principales de las implementaciones de DMVPN es el uso de la topología Hub & Spoke, pero eso no significa que el tráfico spoke to spoke deba atravesar el hub. El hub requiere para el registro de dirección de los spokes usar NHRP (Next Hop Resolution Protocol) el cual es definido en el RFC 2332.

Con DMVPN cualquier flujo de tráfico entre los routers se envía vía un túnel GRE (Generic Routing Encapsulation), pero la característica interesante que

distingue a DMVPN entre otras implementaciones de VPN es que el túnel GRE (Generic Routing Encapsulation) sobre DMVPN es un túnel multipunto.

Con esto el hub y los spokes requerirán un túnel cada uno para alcanzar una conectividad DMVPN completamente mallada, por tanto las ventajas de esta tecnología son:

- Simplificar la porción de la configuración del router hub eliminando la necesidad de configurar crypto maps en las interfaces de túnel, y ACL de cada spoke.

- Los routers spoke pueden obtener sus direcciones IP dinámicamente, por ejemplo un router de borde de Internet conectado con un enlace ADSL puede obtener su IP automáticamente del ISP y entonces el túnel se registrará con el hub usando NHRP (Next Hop Resolution Protocol).

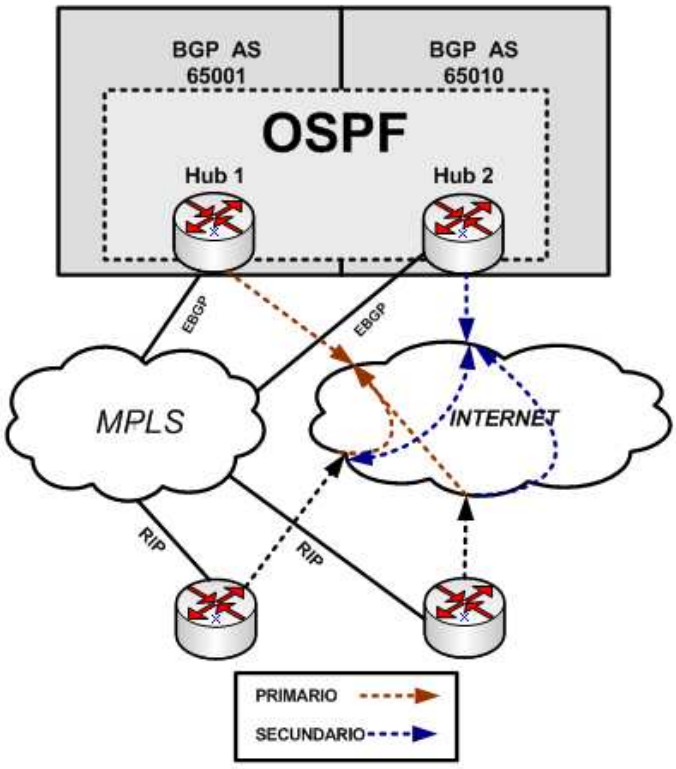


Figura 14. Funcionamiento de DMVPN (Dynamic Multipoint VPN)

Por lo indicado anteriormente se puede concluir que DMVPN es muy flexible, dinámico y seguro que puede adaptarse a diversos tipo de implementaciones, también podemos controlar nuestro tráfico y selección de trayecto usando los ajustes simples del protocolo dinámico de ruteo.

2.7.1.1 TOPOLOGIAS DE DMVPN

En un diseño DMVPN, se puede implementar dos tipos de topologías tales como:

a) Dual hub-dual DMVPN cloud.

Una topología Dual hub-dual DMVPN cloud es un conjunto de routers que se configura ya sea con una interfaz multipunto GRE (Mgre) o punto a punto (p2p), interfaz GRE (o una combinación de los dos) que comparten la misma dirección de subred. La alta disponibilidad se proporciona a través de la utilización de un segundo router (HUB), que puede ser en la misma subred DMVPN como el router principal.

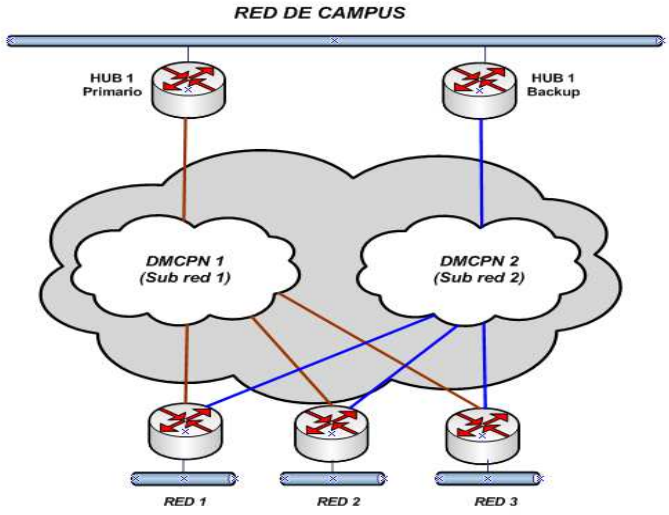


Figura 15. Topología Dual hub-dual DMVPN cloud

b) Dual hub-single DMVPN cloud

La topología Dual hub-single DMVPN cloud generalmente no se recomienda porque se basa en mecanismos que se aplicarían fuera del

túnel. En contraste, cabeceras utilizando subredes DMVPN dual (doble nube DMVPN topología) se basan en los protocolos de enrutamiento los cuales son ejecutados dentro del túnel para determinar la selección de la ruta.

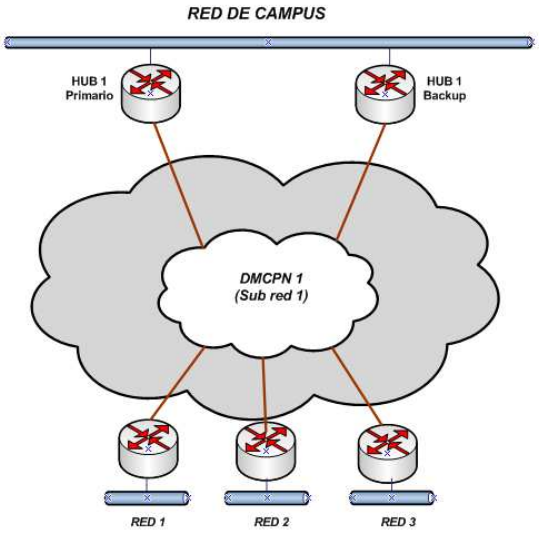


Figura 16. Dual hub-single DMVPN cloud

2.7.2 ENCAPSULACION DE PAQUETES GRE

La implementación del protocolo GRE (Generic Routing Encapsulation) este protocolo es viable para ser aplicada en infraestructuras pequeñas, ya que por el tipo y cantidad de información utiliza menos recursos. Funciona como un protocolo de túnel que a su vez cubre una mezcla de protocolos de capa de red.

Esto representa que para cada punto final del túnel no se retiene ninguna información sobre el estado o la disponibilidad del túnel remoto.

De acuerdo a las especificaciones basadas en los RFCs (Request For Comments) 1701 Y 1702, los paquetes GRE encierra paquetes de carga útil que tienen los detalles de la ruta de origen así como los paquetes procesados y encapsulados por el protocolo de entrega.

En general, este protocolo se ejecuta a través de redes basadas en IP. De acuerdo con RFC 1918, esto les ayuda a llevar los paquetes IP con direcciones privadas mediante paquetes de entrega con direcciones IP públicas en Internet. Los protocolos de entrega y la carga útil se adaptan bien mientras que las direcciones de carga útil no se ajustan con los de la red de entrega.

El transporte de tráfico de la VPN se puede hacer tanto con túneles IP /GRE incluso en redes que no han implementado MPLS. Como resultado, la etiqueta exterior será IP / GRE en lugar de la etiqueta MPLS.

2.7.2.1 VPN GRE.

Esta tecnología proporciona un mecanismo para hacer un túnel con paquetes de conmutación de protocolo (MPLS) sobre una red que no sea MPLS.

Lo más destacado en este mecanismo es que la etiqueta exterior puede estar sustituida por la cabecera de encapsulación IP o GRE. Esto puede lograrse sin interrumpir su funcionamiento inicial, por la razón de que el paquete de MPLS se encapsula en los encabezados de IP /GRE.

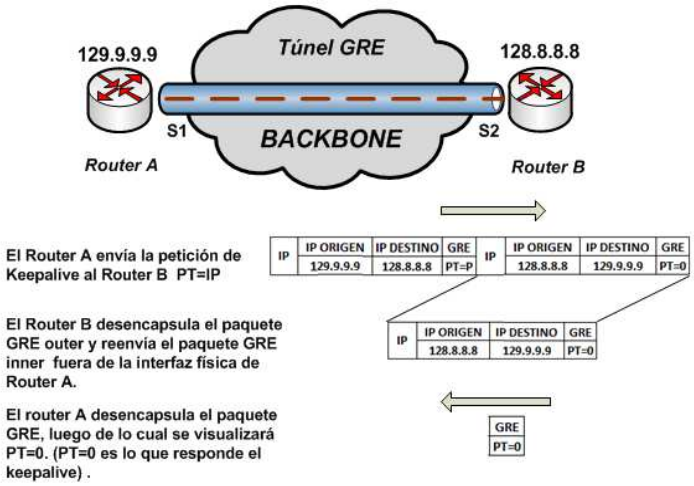


Figura 17. Esquema de funcionamiento de túnel GRE
(Fuente Cisco Press)

2.7.2.2 BENEFICIOS GRE.

La implementación de GRE ofrece las siguientes ventajas:

a) Implementación en empresas en las cuales su backbone es MPLS
b) Funciones de router de borde.
c) Las soluciones de implementaciones de GRE no son dependientes de los proveedores de servicio.
d) Fácil de agregar función de cifrado para redes basadas en IP en la nube MPLS utilizando GRE.

2.7.3 REDES PRIVADAS VIRTUALES - EASY VPN

La implementación de Easy – VPN, es una solución ideal para oficinas remotas con escaso soporte de TI o para las grandes instalaciones de equipos CPE (Customer Premises Equipment) de clientes en los que es poco práctico para configurar varios dispositivos remotos de forma individual.

Esta característica hace que la configuración de Easy VPN sea considerada para minimizar el soporte de TI y aumentar la productividad reduciendo los costos.

- La función Easy VPN permite a los routers que actúen como dispositivos de cabecera de sitio a sitio y de acceso remoto VPN. La característica de esta solución hace que las políticas de seguridad definidas en el sitio central para el dispositivo remoto se mantengan, por lo que cuenta con políticas en todo momento en su sitio remoto antes de que se establezca una conexión. Esta flexibilidad permite a los trabajadores móviles y remotos acceder a los datos y aplicaciones críticas en su intranet corporativa.

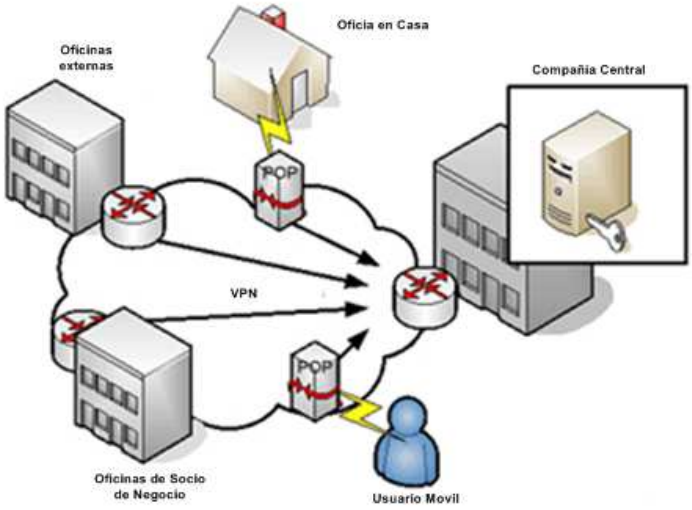


Figura 18. Configuración típica de Easy VPN

2.7.4 REDES PRIVADAS VIRTUALES MOVILES (mVPN)

Una red privada virtual móvil (VPN móvil o mVPN) proporciona conectividad a los dispositivos móviles que acceden a las aplicaciones de software y recursos de red en las redes domésticas a través de otras redes cableadas o inalámbricas. VPN móvil son ampliamente utilizados en situaciones en las que los trabajadores tienen que mantener las sesiones abiertas en todo momento.

Una Red Privada Virtual Móvil (mVPN) tiene las siguientes características:

- **Compatibilidad de aplicaciones**: Las aplicaciones de software que se ejecutan en un entorno LAN también son ejecutadas en mVPN sin necesidad de ninguna modificación
- **Roaming:** La conexión se mantiene intacta como cambiar redes manejan inicios de sesión automáticamente.
- **Persistencia:** Las solicitudes no resueltas están activos y disponibles incluso cuando se interrumpe la conexión inalámbrica.
- **Seguridad:** Autenticación de usuarios y dispositivos se aplica junto con el cifrado de los datos de tráfico de datos de acuerdo con las normas de seguridad, como FIPS 140-2.

- **Autenticación:** Dos factores o factores múltiples autenticaciones se aplican utilizando combinaciones de contraseña, certificado de clave pública y la biometría.
- **Aceleración:** La compresión de datos y la optimización del enlace mejora el rendimiento a través de redes inalámbricas. mVPNs se utilizan en la atención domiciliaria, hospitales, seguridad pública, servicios públicos y la gestión de servicios de campo.

2.7.5 GETVPN (GROUP ENCRYPTED TRANSPORT VPN)

Las aplicaciones y tecnologías actuales tales como la computación distribuida, voz y vídeo sobre IP, ahora requieren una comunicación eficiente y segura entre sitios remotos o sucursales de manera instantánea. Debido a estos requisitos, la topología tradicional hub-and-spoke ya no es suficiente, por tanto las empresas deben implementar una topología todos con todos (any-to-any) la cual debe trabajar bajo el modelo de redes privadas virtuales IP (VPN).

Considerando que los servicio IP/VPN son implementados sobre infraestructuras de BACKBONE MPLS (Multiprotocol Label Switching), el tráfico que por esta se transmita debe tener niveles de seguridad eficientes los cuales garanticen la integridad de los datos.

Esto es necesario ya que en la actualidad con los avances tecnológicos, también se ha incrementado los métodos de vulnerar las seguridades que se disponen. Con este antecedente y tomando en cuenta las nuevas regulaciones, es necesario implementar mecanismos que nos ayuden a encriptar los datos a nivel WAN.

Para proporcionar un cierto grado de conexión de malla completa (Full Mesh) o incluso una conectividad de malla parcial, las soluciones basadas en túneles actualmente tienen conexiones complejas. Esta particularidad

demanda mayor procesador y memoria en los equipos de comunicación y esto hace que la administración sea compleja.

Una solución a estos inconvenientes es la implementación de DMVPN (Dynamic Multipoint VPN). Sin embargo, DMVPN requiere la superposición de una infraestructura de enrutamiento secundaria a través de encaminamiento de túneles según el requerimiento. La topología de enrutamiento de capa también reduce la escalabilidad inherente de la IP VPN topología de red subyacente.

La soluciones tradicionales con IPSEC punto a punto sufren de problemas de replicación de multidifusión porque esta debe ser realizada antes de la encapsulación del túnel y el cifrado.

La replicación Multicast no se puede realizar en la red de los proveedores de servicios porque los encapsulamientos multicast se muestran en la red central como datos Unicast.

Grupo Encrypted Transport VPN (GETVPN) 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 (GM).

GETVPN utiliza el mecanismo GDOI (Dominio del grupo de Interpretación) para seguridad, el cual es definido en el RFC 3547 para IPSEC fase 1, fase 2.

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.

2.7.5.1 BENEFICIOS GETVPN

GETVPN proporciona los siguientes beneficios:

a) Conectividad instantánea de gran escala any to any para lo cual utiliza un grupo de seguridad IPSEC.
b) Toma ventaja de la infraestructura subyacente IP VPN de enrutamiento y no requiere un plano de control de encaminamiento de superposición
c) Se integra perfectamente con las infraestructuras de multicast sin los problemas de replicación de multicast, el cual se observa típicamente en soluciones tradicionales basadas en túneles IPsec.
d) Conserva la IP de origen y destino durante el cifrado IPsec y el proceso de encapsulación. Por lo tanto GETVPN se integra muy bien con las características tales como calidad de servicio e ingeniería de tráfico.

2.7.5.2 ARQUITECTURA DE GETVPN

GETVPN abarca Rekeying Multicast, lo cual es una manera de habilitar el cifrado de paquetes "nativos" multicast y unicast Rekeying través de una WAN privada. Rekeying Multicast y GETVPN se basa en un grupo GDOI (Group Domain of Interpretation) como se define en Internet Engineering Task Force (IETF), RFC 3547, además, hay similitudes en IPsec en la zona de cabecera de la preservación y SA de búsqueda.

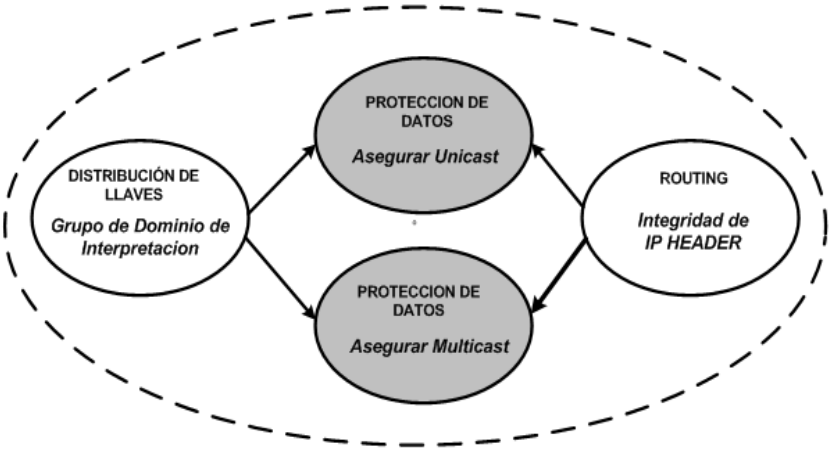


Figura 19. Diagrama de Relación de conceptos de GETVPN

La tecnología GETVPN (Group Encrypted Transport VPN) es basada en estándares y se integra fácilmente con enrutamiento y seguridad juntos en la estructura de red.

Los miembros del grupo son manejados a través de un estándar de IETF (Internet Engineering Task Force), el cual es detallado en el RFC-6407 para el Grupo de Dominio de Interpretación (GDOI).

2.7.5.3 GDOI (GROUP DOMAIN OF INTERPRETATION)

El protocolo de llaves de gestión de grupo (GDOI) se utiliza para proporcionar un conjunto de claves criptográficas y políticas para un grupo de dispositivos. En una red GETVPN, GDOI se utiliza para distribuir las claves IPsec comunes a un grupo de gateways VPN (router) de la infraestructura que debe comunicarse de forma segura. Estas claves se actualizan periódicamente en todos los gateways VPN mediante un proceso llamado "cambio de claves."

Todos los gateways VPN participantes deben autenticarse en el dispositivo que proporciona claves mediante IKE (Internet Key Exchange). Así mismo todos los métodos de autenticación IKE (claves pre-compartidas PSK) y la infraestructura de clave pública (PKI) son compatibles con la autenticación inicial. Después de que los gateways VPN se autentican, el protocolo GDOI es implementado para actualizar a los GMs (miembros del grupo) de una manera más escalable y eficiente.

GDOI introduce dos claves de cifrado diferentes que son:

a) Una clave asegura para el plano de control GETVPN;
b) Una Clave para cifrar el tráfico de los datos

La clave que se utiliza para fijar el plano de control se conoce comúnmente como la clave de cifrado de claves (KEK) y la clave utilizada para cifrar el tráfico de datos se conoce como clave de cifrado de tráfico (TEK).

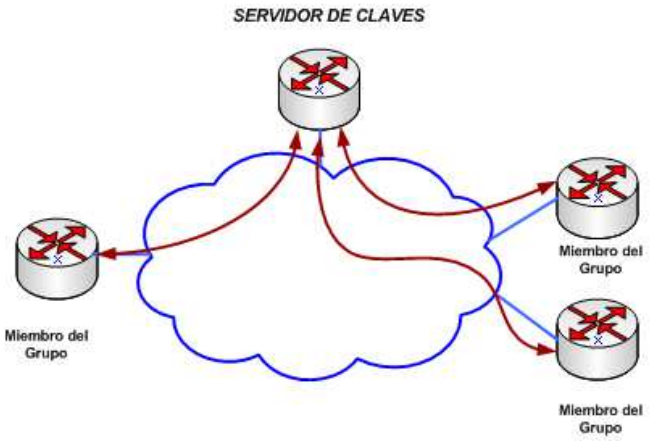


Figura 20. Distribución de Política con GDOI

El protocolo GDOI se utiliza entre el servidor de claves y un miembro del grupo para distribuir la política de seguridad (IPsec SA) y las claves dentro del grupo. El servidor de claves es responsable de crear y mantener el IPsec SA.

Los miembros del grupo autenticados pueden entonces comunicarse entre sí (dentro del mismo grupo) mediante el uso de la SA IPsec recibida desde el servidor de clave.

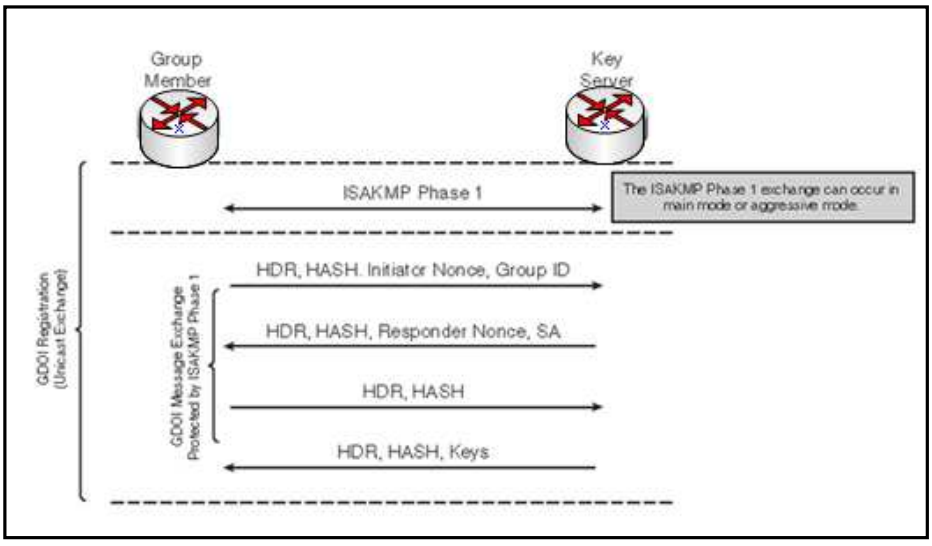


Figura 21. Protección de registro GDOI

2.7.5.4 PRESERVACION DE TUNEL HEADER

En IPsec tradicional, las direcciones de extremo del túnel se utilizan como un nuevo paquete de origen y destino. El paquete se enruta a través de la infraestructura IP, utilizando la dirección de origen del router de encriptación y la dirección del router de destino.

En el caso de GETVPN, IPsec protege los paquetes de datos encapsulados de la dirección tanto de origen como del destino.

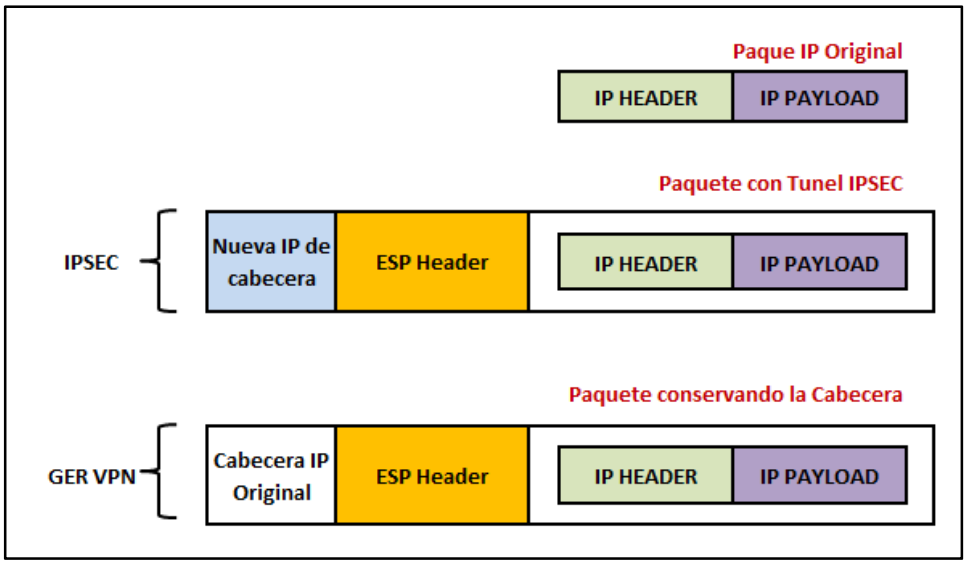


Figura 22. Túnel Header

La mayor ventaja de la preservación de la cabecera del túnel es la capacidad para enrutar paquetes cifrados utilizando la infraestructura de enrutamiento de red subyacente. La alta disponibilidad de derivación (HA) proporcionada por una infraestructura VPN MPLS (dual spoke, dual links, y así sucesivamente) es su integración perfectamente con la solución GETVPN, con esto no hay necesidad de proporcionar HA en el nivel de IPsec (dual hubs estado de IPsec HA, y así sucesivamente).

Considerando que la cabecera del túnel es preservada, y esta se combina con el grupo de las SA, la replicación de multicast es más eficiente dentro de un backbone de comunicación. Así mismo debido a que cada GM comparte

la misma SA, el enrutador IPsec más cercano a la fuente de multicast no requiere reenviar paquetes a todos los demás miembros del grupo, ya no está sujeto a los problemas de replicación de multicast que existe en soluciones tradicionales de IPsec.

2.7.5.5 KS (KEY SERVER)

Un servidor de claves (KS) es responsable de crear y mantener el plano de control GETVPN. Las responsabilidades del servidor de claves incluye el mantenimiento de la política y creación de claves, así como la subsistencia de estas para todo el grupo. Cuando un miembro del grupo se registra en el servidor de claves, descarga esta política y las claves respectivas para el GM.

El servidor SK también realiza la regeneración de claves para todo el grupo antes que las credenciales existentes expiren. El servidor de claves tiene dos responsabilidades importantes y estas son:

a) Atender a las solicitudes de registro de mantenimiento
b) Regeneración de claves de origen.

Un miembro del grupo puede registrarse en cualquier momento y recibir la política y claves actuales. Cuando un miembro del grupo se registra con el servidor de claves, este verifica la identificación (ID) del miembro del grupo está intentando unirse. Si este ID es un identificador de grupo válido, el servidor envía la clave de la política de asociación segura (SA) al miembro del grupo.

Existe dos tipos de llaves (KEYS) que el servidor de claves puede proporcionar y son:

- ✓ **La clave de cifrado de clave (KEK - Key Encryption Key).** esta encripta el mensaje de cambio de claves.

- ✓ **La clave de cifrado del tráfico (TEK - Traffic Encryption Key)**. Esta realiza la función de IPSEC -SA (asociaciones seguras) con los miembros del grupo que en ese momento se encuentren.

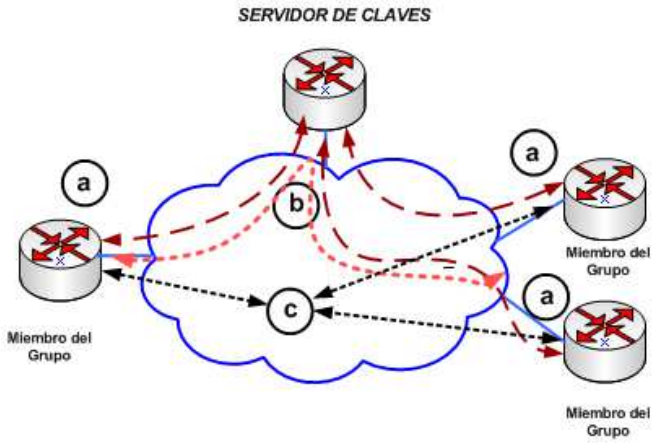


Figura 23. Funcionalidad del Servidor de Claves

La topología muestra los flujos de protocolo que son necesarios para los miembros del grupo puedan participar dentro de este, y su funcionamiento es el siguiente:

a) Los miembros del grupo se registran con el servidor de claves. El servidor de claves autentica y autoriza a los miembros del grupo y descarga la directiva IPsec y las claves necesarias para que puedan cifrar y descifrar los paquetes de multicast IP.
b) Según sea necesario, el servidor de claves envía pushes que no es más que un mensaje de cambio de claves de los miembros del grupo. El mensaje de cambio de claves contiene una nueva política y claves IPsec para utilizar cuando las claves IPsec antiguas caduquen. Los mensajes de cambio de claves se envían antes de la fecha de caducidad para asegurar que las claves de grupo válido siempre están disponibles
c) Los miembros del grupo son autenticados por el servidor de claves, por lo que en ese momento ya pueden comunicarse con otros miembros

del grupo que también se encuentren autenticados y en el mismo grupo.

2.7.5.6 GMs (MIEMBROS DEL GRUPO)

Un miembro de Grupo (GM) es el router responsable de la encriptación y desencriptación de los paquetes, es decir un dispositivo encargado de manejar el plano de datos VPN. Un Miembro del Grupo (GM) sólo es configurado una vez con los parámetros IKE y la información de KS / Grupo en la Fase uno (1).

Así mismo las políticas de cifrado se definen centralmente en el KS y descargan al miembro del grupo (GM) en el momento de la inscripción. En base a estas políticas el miembro del grupo (GM) decide las necesidades del tráfico para cifrar o descifrar y qué llaves utilizará. En una red GETVPN, las políticas del miembro del grupo (GM) son dictadas por el servidor KS pero en algunos casos, un miembro del grupo (GM) se pueden configurar para anular localmente algunas de estas políticas.

Cualquier política global (incluyendo tanto permiso y negar entradas) definido en el servidor KS afecta a todos los miembros del grupo, por lo tanto algunas políticas tienen más sentido cuando se define a nivel local.

2.7.5.7 GRUPO SA (ASOCIACIONES SEGURAS)

A diferencia de las soluciones tradicionales de cifrado IPsec, GETVPN utiliza el concepto de grupo de asociación segura (SA). Todos los miembros en el grupo de GETVPN pueden comunicarse entre sí usando una política de cifrado común y una SA compartida. Con una política de cifrado común y una asociación segura (SA) compartida, no hay necesidad de negociar IPsec entre GMs; esto reduce la carga de recursos en los equipos routers IPsec.

2.7.5.8 REKEY PROCESS

Como se mencionó anteriormente, el servidor KS no sólo es responsable de la creación de las políticas y las claves de cifrado, sino también para las llaves refrescantes y distribuirlos a los miembros del grupo (GMs). El proceso de envío de claves nuevas tiene que realizarse cuando las claves existentes están a punto de expirar, esto se conoce como el proceso de cambio de claves. GETVPN es compatible con dos tipos de mensajes de cambio de claves: unicast y multicast.

Si un miembro del grupo (GM) no recibe información REKEY del servidor (KS) (por ejemplo, el KS está inactivo o la conectividad de red fue suspendida), el miembro del grupo (GM) intenta volverse a registrar.

La acción de asociación de los miembros del grupo debe ser completada en 30 segundos antes que las credenciales de IPsec caduquen. Esta ventana de 30 segundos proporciona un período de gracia para que el tráfico cifrado generado anteriormente con la TEK (traffic encryption key) se mantenga antes de que se suprima. Si el registro es exitoso, el miembro del grupo (GM) recibe nuevas asociaciones en el marco del proceso de reinscripción.

Si el registro no tiene éxito (el KS asignado no está disponible), el miembro del grupo (GM) intenta tres veces más, a intervalos de 10 segundos, para establecer una conexión con el servidor (KS).

El proceso se repite a través de cada miembro del grupo y el servidor KS hasta que todos se han integrado.

2.7.5.9 UNICAST REKEY

En el proceso de cambio de claves unicast, el KS genera un mensaje de cambio de claves y envía varias copias del mensaje, una copia a cada GM. Al recibir el mensaje de cambio de claves, un miembro del grupo (GM) envía un mensaje de ACK al servidor de claves (KS).

Este mecanismo ACK no sólo asegura la lista de los miembros del grupo concurrentes sobre el servidor de claves (KS), también asegura que el cambio de claves sólo se envíe una vez a los miembros del grupo.

Un servidor de claves (KS) puede ser configurado para retransmitir un paquete de cambio de claves para superar defectos transitorios en la red. Si un miembro del grupo (GM) no reconoce en tres ocasiones consecutivas las claves enviadas (retransmisiones se consideran parte de la regeneración de claves), el servidor de claves (KS) elimina el mensaje a partir de su base de datos del miembro del grupo activo y deja de enviar mensajes de regeneración de claves a este.

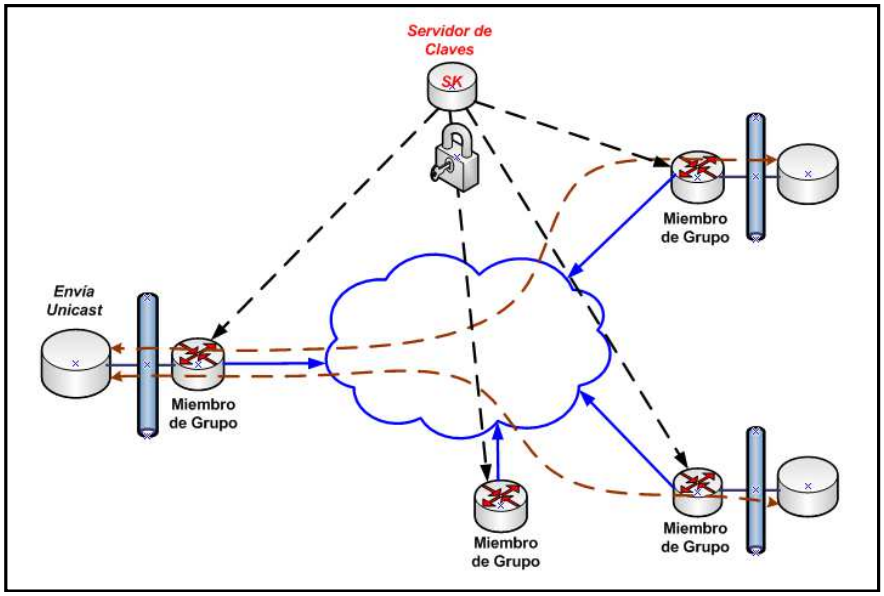


Figura 24. Unicast Re Key

2.7.5.10 MULTICAST REKEY

En el proceso de cambio de claves multicast, un servidor de claves (KS) genera un mensaje de cambio de claves y envía una copia del mensaje a una dirección de grupo de multicast que está predefinida en la configuración.

Cada miembro del grupo (GM) se une al grupo multicast en el tiempo de registro, por lo que cada miembro del grupo (GM) recibe una copia del mensaje de cambio de claves.

A diferencia del cambio de claves unicast, multicast rekey no tiene un mecanismo de ACK. El servidor de claves (KS) no mantiene una lista de los miembros de grupos (GMs) activos.

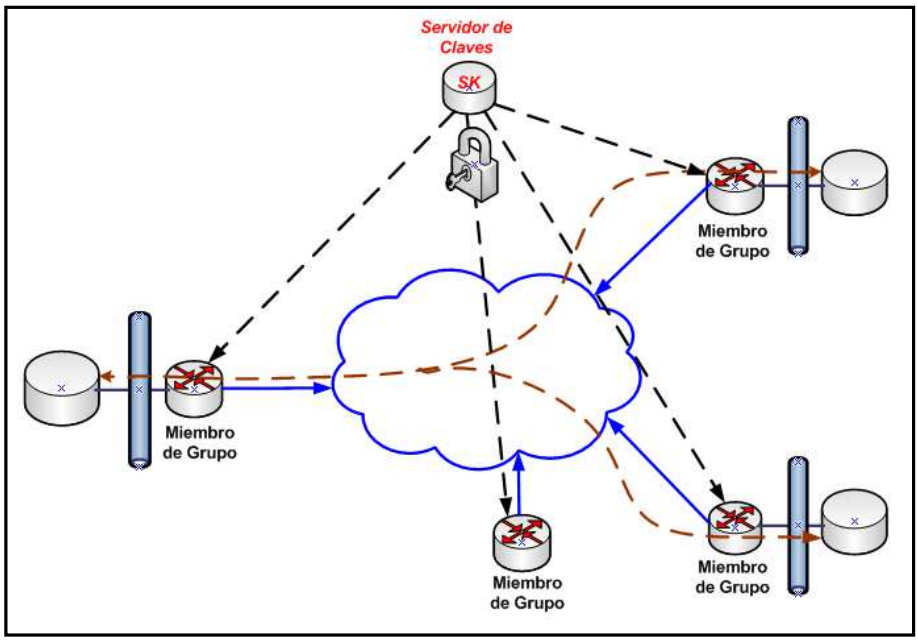


Figura 25. Multicast Re Key

2.8 APLICACIONES DE GETVPN

2.8.1 PRIVATE WAN (IP/MPLS) ENCRYPTION

El aumento de los riesgos de seguridad de red y cumplimientos regulatorios han llevado a la necesidad de implementar mecanismos de seguridad a nivel WAN, por tanto las empresas que utilizan infraestructuras de comunicación MPLS necesitan implementar GETVPN para garantizar la privacidad de datos, manteniendo una conexión todos con todos (any-to-any).

2.8.2 PRIVATE SECURE CLOUD COMPUTING

La tendencia hacia la virtualización del centro de datos y cloud computing da lugar a tener en cuenta los riesgos que se generan al utilizar este tipo de servicios, por tanto se hace indispensable buscar e implementar mecanismos de seguridad como encriptación de paquetes, los cuales se debe aplicar para garantizar y proteger los datos que en su momento están en tránsito sobre toda infraestructura de comunicación.

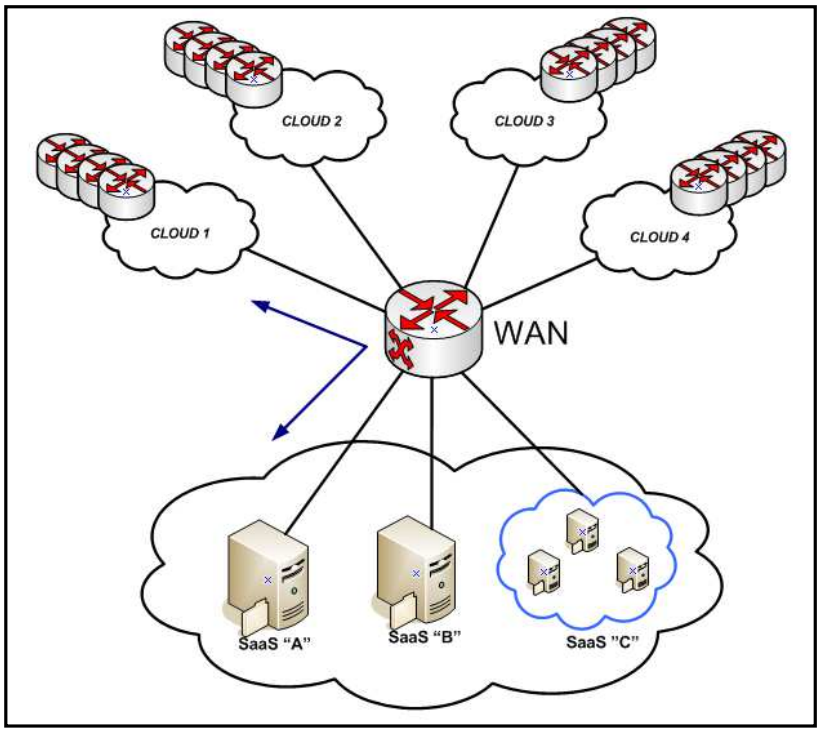


Figura 26. Private Secure Cloud Computing

2.8.3 ADMINISTRACION SEGURA

GETVPN ha sido diseñado para añadir cifrado sin problemas en redes MPLS. En la actualidad los proveedores de servicios pueden ofrecer servicios de valor adicional de encriptación MPLS, manteniendo la inteligencia de red que es fundamental para la transmisión de voz y vídeo, incluyendo calidad de servicio (QoS), ruta de acceso natural, y multicast.

2.9 CONSIDERACIONES DE DISEÑO CRÍTICOS

Tabla 4

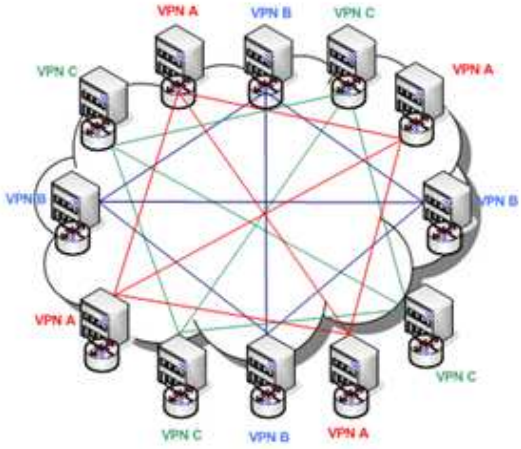
Consideraciones de diseño

No	REQUERIMIENTOS	CONSIDERACIONES
1	Encriptación Estándar	• DES (Data Encryption Standard) • 3DES (T Data Encryption Standard) • AES (Advanced Encryption Standard)
2	Tipo de Autenticación IKE	• Pre-shared Keys (PSK), • X.509 – Certificados Digitales (PKI)
3	Requisitos adicionales de seguridad para empresas	• Grupos de Autenticación • Autenticación de Usuarios
4	Requerimientos de QoS	• LLQ (Low Latency Queuing) • Conformación de trafico • Nivel de interfaces • Túnel per-VPN
5	Aplicaciones Multicast IP	• Encriptación Multicast Nativa
6	Requerimientos de Any to Any	• Se requiere tráfico todos con todos (any-to-any)
7	Direccionamiento de los Routers remotos	• Direccionamiento Estático o Dinámico
8	Escalabilidad	• Full mesh
9	Ancho de banda y rendimiento	• DS3 (velocidad de conexión) • multi DS3 (velocidad de conexión) • OC3 (portadora óptica) • OC12 (portadora óptica) • OC48 (portadora óptica)
10	Diversidad de Trafico	• Pps, • Bps • Tamaño de paquetes

2.10 DIFERENCIAS ENTRE VPN IPSEC Y GETVPN

Tabla 5.

Diferencias de conectividad de protocolos

Punto a Punto IPSEC	Multipunto a Multupunto GETVPN
	
IPSec se superposeciona cuando realiza Ip routing	GETVPN no se superpocesiona, maneja ruteo nativo
Topología Full mesh no es escalable N^2 túneles para N sitios	Posee escalabilidad todos contra todos (any to any)
Utiliza dos capas para gestionar y solucionar problemas.	Utiliza una sola capa para estas dos funciones
Posee QoS limitado	Posee QoS avanzado
Posee una ineficiente replicación de Multicast	Posee una eficiente replicación de Multicast
Tiene menor capacidad de mallado	Capacidad de mallado Full Mesh
No soporta Multicast	Tiene la capacidad de Multicast

En este Capítulo se ha descrito los principales fundamentos y tipos de seguridades implementadas mediante Redes Privadas Virtuales(VPNs) así como las características de funcionamiento. Entre los aspectos más importantes presentados en este capítulo se pueden nombrar la arquitectura de cada solución VPN y sus servicios autenticación y cifrado, el mantenimiento de la cabecera del paquete cuando se implementa el nuevo concepto de VPN denominado GETVPN y se concluye realizando una comparación ente una VPN punto a punto y una VPN multipunto - multipunto así como los parámetros a considerar para el diseño de una VPN segura.

CAPITULO III

3. DISEÑO DE UNA RED SEGURA

Este capítulo está enfocado a las consideraciones que se deben tomar en cuenta al momento de diseñar un red de datos segura, para lo cual se identificará las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de una infraestructura de red WAN corporativa, y de esta manera podremos entender y definir políticas, procedimientos y estándares que deben ser tomados en cuenta a nivel de capa 3 (Capa Acceso).

De la investigación realizada y tal como se detalla en el Capítulo I se concluye que el backbone principal de comunicación a nivel nacional se basa principalmente en tecnología MPLS, por tanto es necesario poseer un mecanismo de encriptación de datos eficiente para este tipo de redes, más aún cuando en la actualidad los organismos de control están aplicando nuevas regulaciones [2].

Con estos antecedentes el servicio de Red privada virtual IP (VPN IP) ha sido expresamente diseñada con el objetivo de proporcionar un mecanismo fiable, escalable, eficaz y seguro para la conexión entre sitios remotos independientemente del lugar donde se encuentren tanto en ambientes punto a punto como multipunto - multipunto.

3.1 VARIABLES CONSIDERADAS PARA EL DISEÑO PROPUESTO

Considerando que en el presente trabajo se profundizo en la investigación de las hipótesis planteadas anteriormente, se utilizó el método HIPOTETICO DEDUCTIVO, ya que con este se abarcó varios pasos esenciales como la observación de los requerimientos actuales de comunicación, consecuencias que conlleva la implementación de una posible solución y por último se concluirá con la verificación de las preguntas descritas en la formulación del problema mencionado en el Capítulo I mediante la experiencia que se obtengan de la emulación.

El desarrollo del proyecto se basó por las técnicas propias de la ingeniería informática y de telecomunicaciones, como son:

a) **Estudio del problema existente**. Iniciamos investigando por varios medios como libros e Internet, los antecedentes del estado actual de las redes de comunicaciones y de las tecnologías que están surgiendo, con el objetivo de identificar inconvenientes puntuales en el tema de seguridad en redes malladas a los cuales deberemos dar una solución óptima.

b) **Estudio de viabilidad**: En este apartado se analizó si existe una solución viable para el problema o problemas identificados en el punto anterior. Para este análisis se tomó en cuenta las tecnologías existentes y el costo que estas representan.

c) **Diseño de la solución (Experimentación)**: En esta parte se profundizó en el problema existente, para lo cual se realizó una emulación y el escenario planteado contempla un sitio matriz y tres sucursales que estarán interconectadas a través de una red MPLS, la cual en un inicio no contempla ningún tipo de seguridad. Con el escenario definido se determinó las variables a medir las cuales son latencia entre sitios (suma de retardos temporales los cuales se producen por la demora en la propagación y transmisión de paquetes dentro de la red), tasa de transferencia (velocidad con la cual podemos transferir información y se mide en bits/seg), QoS (Calidad de Servicio) dividido en tres clases: voz, video, datos y finalmente se analizara las seguridades implementadas en el escenario propuesto.

Una vez validada la conectividad entre los sitios se procedió a encriptar la comunicación con cada uno de los protocolos propuestos con el fin de volver a medir las variables y determinar la variación y funcionalidad de la infraestructura de red, verificando que se respete el QoS. Con los resultados

obtenidos se analizará las diversas variables definidas en la hipótesis y de esta manera validar la solución que se dará a la hipótesis planteada.

d) **Análisis, Evaluación y Validación de resultados:** El análisis**,** evaluación y validación se lo realizará por medio de estadísticas obtenidas como resultado de la emulación propuesta para este proyecto y cuyas variables a considerar serán ancho de banda, paquetes encriptados, niveles de encriptación, retardos entre otros, los mismos que serán comparados entre un escenario con IPSEC y otro con GETVPN.

e) **Documentación**: Para que el proyecto cumpla con el objetivo, se documentará todas las fases que involucre esta investigación.

3.2 DISEÑO DE REDES CORPORATIVA

El funcionamiento, éxito y seguridad de una red depende de una implementación por capas, las cuales deben basarse en modelos jerárquicos para aprovechar las ventajas de modularidad a medida en que la red crece.

Para el caso de una red poseer de un backbone de comunicación es necesario ya que nos permite asignar tareas específicas a los dispositivos de conmutación y enrutamiento y de esta manera tener la diferenciación entre el acceso, borde y núcleo lo cual servirá para operar y mantener una red multiservicio.

Dentro de las características que debe poseer una red se debe tomar en cuenta:

- **Disponibilidad.** Es la cantidad de tiempo que está trabajando el sistema en la red, para determinar el porcentaje de disponibilidad.

- **Fiabilidad**. Es tiempo utilizado para reparar todas las fallas o caídas de la red en un tiempo determinado.

- **Desempeño**. El desempeño es necesario en redes de computadoras conectadas entre sí en donde son muy comunes las interacciones complejas lo que conduce a un desempeño pobre y la mayor parte de las veces no se sabe porque es ocasionado. La principal medida del desempeño es el Retraso.

- **Retardo.** Es el tiempo de espera de una estación para enviar un paquete listo antes de que se le permita accesar.

- **Seguridad**. Se debe implementar métodos de seguridad que reglamenten el acceso a la infraestructura de red de la institución u organización solo del personal autorizado.

- **Análisis Costo Beneficio**. Para este análisis se debe considerar los siguientes parámetros:

    - Equipos de comunicación
    - Medios de comunicación
    - Cantidad de información a transmitir
    - instalación(fácil, difícil)
    - seguridad(alta, baja)
    - Costo de mantenimiento(alto, medio, bajo)
    - Presupuesto (estimación alto, bajo)

3.3 DISEÑO DE UNA RED WAN

Cuando se habla de diseño a nivel WAN no es más que la integración de dos oficinas externas separadas geográficamente. Cuando una estación final local desea comunicarse con una estación final remota (es decir, una estación final ubicada en un sitio diferente), la información se debe enviar a través de uno o más enlaces WAN. Los routers dentro de las WAN son puntos de

conexión en una red, y estos determinan la ruta más adecuada a través de la red para enviar la información.

Como la infraestructura WAN a menudo se arrienda a un proveedor de servicio, el diseño WAN debe optimizar el costo y eficiencia del ancho de banda. Por ejemplo, todas las tecnologías y funciones utilizadas en las WAN son desarrolladas para cumplir con los siguientes requisitos de diseño:

- Optimizar el ancho de banda de WAN
- Minimizar el costo
- Maximizar el servicio efectivo a los usuarios finales
- Seguridad sobre toda la infraestructura de comunicación.

Con los antecedentes mencionado anteriormente y tomado en cuenta los requerimientos actuales de servicios, las redes tradicionales de medios compartidos WAN se están sobrecargando debido a:

- El uso de las redes ha aumentado a medida que aumenta el uso por parte de las empresas de aplicaciones cliente/servidor y multimedia las cuales se orientan al aumento de la productividad.
- La velocidad de los cambios en los requisitos de las aplicaciones ya que hoy en día la tendencia es Cloud Computing.
- Cada vez más, las aplicaciones requieren calidad de servicio (QoS) diferenciado.
- El crecimiento de las redes internas y externas corporativas ha creado una mayor demanda de ancho de banda.

Con estos antecedentes para el diseño de una red WAN se debe utilizar nuevas tecnologías, las cuales garanticen niveles de seguridad adaptadas a los requerimientos actuales.

3.4 REDES DE DATOS SEGURAS

La infraestructura de una red de datos, es la parte más importante de toda la gestión como administradores, dado que si nuestra estructura de medio de transporte (carrier) es débil o no lo conocemos, conlleva a no tener un nivel alto de confiabilidad y confidencialidad de los datos que enviamos a través de este medio.

El avance tecnológico y del conocimiento de servicios en línea ha tenido como consecuencia que hoy en día las empresas o negocios se enfrenten a múltiples intrusos o usuarios mal intencionados que intentan vulnerar sus sistemas de información y comunicación.

Los desafíos asociados a la seguridad de la información evolucionan muy rápidamente, de forma tal que la tecnología por sí sola no es suficiente y que las políticas de seguridad deben ser acorde con las actividades del negocio.

La seguridad de la información, de igual forma a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada, para ello se deben evaluar y cuantificar que información es imprescindible proteger, y en función de estos análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables.

3.5 OBJETIVO DE LA SEGURIDAD

El objetivo de la seguridad en una red de datos es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software, a través de implementación de sistemas de seguridad adecuados.

Otro objetivo importante es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias

para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

3.6 SERVICIOS DE SEGURIDAD

Los servicios de seguridad se consideran desde consultorías y análisis de riesgo hasta la implementación de tecnologías de seguridad específicas que permiten monitorear de forma permanente la seguridad de la información y de los dispositivos, detectando ataques y tomando acciones para corregir problemas o para evitar que los intentos de ataques puedan afectar gravemente los activos de información

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

3.6.1 CONFIDENCIALIDAD

La confidencialidad hace referencia a la necesidad de ocultar o mantener secreto determinada información o recursos.
El objetivo de la confidencialidad es prevenir la divulgación no autorizada de la información.

3.6.2 AUTENTICACIÓN

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

3.6.3 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.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.

3.6.4 CONTROL DE ACCESO

Sirve para evitar el uso no autorizado a los recursos de la red, por tanto solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

3.6.5 NO REPUDIO

Evita que cualquier entidad que envió o recibió información alegue, que no lo hizo, para lo cual se debe considerar:

3.6.5.1 PRUEBA DE ORIGEN

El receptor del mensaje adquiere una prueba, demostrable ante terceros, del origen de los datos recibidos.

3.6.5.2 PRUEBA DE ENVIÓ

El receptor o el emisor del mensaje adquieren una prueba demostrable de la fecha y hora del envío.

3.6.5.3 PRUEBA DE ENTREGA

El emisor del mensaje adquiere una prueba, demostrable ante terceros, de que los datos han sido entregados al receptor adecuado.

3.7 ARQUITECTURA ORIENTADA A LA SEGURIDAD

3.7.1 ACTIVIDAD DE DISEÑO

En esta sección lo que se pretende es diseñar una arquitectura de seguridad eficaz que sirva de referencia para mitigar problemas de seguridad a nivel de capa 3, por tanto esta debe ser capaz de ser implementada en cualquier infraestructura de red.

Los equipos perimetrales en las redes WAN actuales no poseen un sistema de seguridad adecuado y acorde a los retos actuales, por tanto una arquitectura se debe construir bajo un entorno seguro, flexible, escalable, interoperable, dinámico y abierto, por tanto, siguiendo estas metas podremos

cubrir la mayoría de requisitos planteados en nuestros objetivos, para lo cual se utilizará estándares que puedan coexistir con la gran mayoría de aplicaciones, ofreciendo protocolos de seguridad para las comunicaciones y permitiendo múltiples implementaciones dentro de la misma arquitectura y que sean capaces de cooperar entre ellas.

3.7.2 DEFINICIÓN DE CAPAS DE SERVICIOS DE SEGURIDAD

Considerando que la mayoría de arquitecturas de redes de datos se definen mediante capas o niveles, a continuación se propone una arquitectura de servicios de seguridad para entornos WAN.

El objetivo de esta arquitectura es que esta pueda interoperar con el resto de capas adyacentes para ofrecer o beneficiarse de los servicios.

A continuación se muestra una propuesta de 8 capas en las cuales podemos enmarcar los servicios y mecanismos de seguridad necesarios:

Figura 27. Capas de Servicio de Seguridad

Del cuadro propuesto anteriormente y tomando en cuenta los objetivos de este trabajo la capa en la que se pondrá mayor énfasis es Seguridad de la Comunicación, ya que son a menudo asociados con los términos de

confidencialidad, integridad, autenticación y no repudio de los datos transmitidos. Estos servicios de seguridad son a su vez implementados por varios mecanismos que suelen ser de naturaleza criptográficos.

La confidencialidad de los datos que se transmiten en una red WAN puede realizarme mediante el mecanismo de cifrado entre los elementos que lo componen el medio de comunicación lo cual puede ser end-to-end o punto multipunto.

Los tipos de autenticación disponibles dependen del protocolo de seguridad utilizado. El ejemplo más tangible es en Internet ya que este puede utilizar el protocolo SSL (Secure Sockets Layer) el cual permite cifrar con cuatro opciones de autenticación diferentes como son:

1) Autenticación del servidor.
2) Autenticación del cliente.
3) Autenticación tanto del servidor como el cliente
4) Ninguna autenticación y solo proporcionando confidencialidad.

3.8 COMUNICACIONES SEGURAS

El surgimiento de nuevas tecnología referentes a redes de comunicación y en particular de Internet, ha abierto nuevas posibilidades para el intercambio de información, y al mismo tiempo, son cada vez mayores las amenazas a la seguridad de la información que se transmite a nivel WAN.

Con este antecedente es necesario entonces, implementar diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos, para lo cual se debe utilizar la tecnología criptográfica para mitigar la inseguridad existente.

A partir de la capa física a la capa de aplicación del modelo de referencia OSI, la criptografía es el primero de muchos pasos necesarios para proporcionar soluciones de comunicación seguras.

3.8.1 SISTEMA CRIPTOGRAFICO

Un sistema criptográfico es una estructura que consiste en la aplicación de la criptografía para proporcionar comunicaciones seguras, la cual está compuesta por un conjunto de protocolos, procedimientos y algoritmos necesarios para implementar un sistema de codificación y decodificación utilizando la tecnología de la criptografía.

Con un sistema criptográfico, la confidencialidad y la integridad de la información se logra utilizando diversos métodos tales como técnicas de cifrado y el descifrado, funciones hash, firmas digitales y técnicas de gestión de claves.

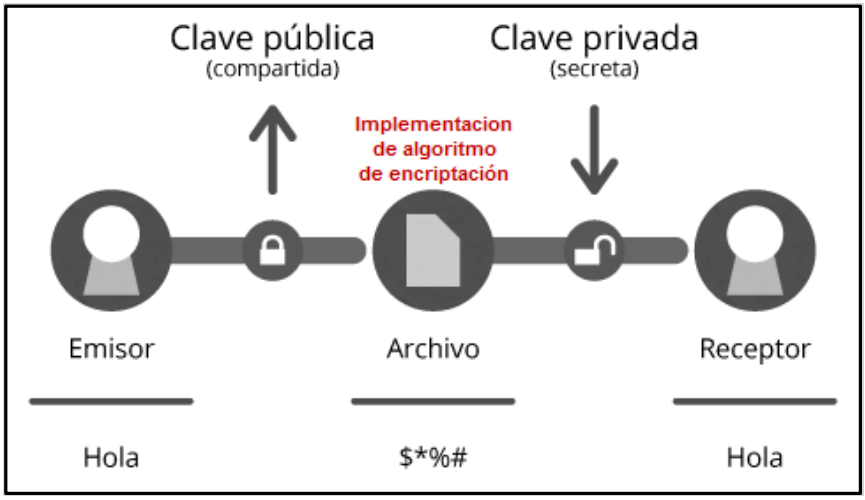


Figura 28. Proceso Criptográfico

3.8.2 ALGORITMOS CRIPTOGRAFICOS

En general, hay tres tipos de algoritmos criptográficos:

a) Criptografía Simétrica: Utilizan la misma clave para el proceso de cifrar y descifrar un documento.
b) Criptografía Asimétrica: Utiliza un par de dos claves, una clave para el cifrado y la otra para el proceso de descifrado.

c) Función Hash: También llamada algoritmo Hash el cual utiliza una función matemática de una manera de producir un valor hash único, el cual es algorítmicamente aleatorio para identificar los datos uno de otros.

La criptografía de clave simétrica se utiliza típicamente para el cifrado de los datos que proporcionan la confidencialidad, mientras que la criptografía de clave asimétrica se utiliza principalmente en el intercambio de claves y el no repudio, proporcionando de este modo la confidencialidad y la autenticación.

El algoritmo de hash (noncryptic), no proporciona confidencialidad, pero proporciona la integridad del mensaje y la identidad de los puntos involucrados durante el transporte por canales de comunicación inseguros.

3.9 TECNOLOGIAS PARA UNA COMUNICACIÓN SEGURA

La seguridad e integridad de los datos que viajan a través de una infraestructura de comunicación WAN es un requerimiento importante a considerar al momento de evaluar que tecnología o medio de comunicación debemos implementar el cual garantice mitigar los riesgos que conlleva no aplicar algún mecanismo de seguridad.

La tecnología WAN ha sido concebida fundamentalmente con el objetivo de trasmitir información sin importar su ubicación física de una manera ágil más no segura, lo cual ha provocado la existencia de vulnerabilidades y fallas de seguridad importantes.

3.10 INTRODUCCION A LAS VPN

Las VPN son cada vez más importantes para las empresas y los proveedores de servicios. IPSec específicamente es una de las tecnologías más populares para implementar VPNs basadas en IP.

Así mismo una VPN utiliza tanto los métodos criptográficos y no criptográficos para crear una comunicación segura a través de medios o canales que no garanticen seguridades adecuadas.

3.11 SEGURIDADES VPN SOBRE UNA RED WAN.

Dentro de los beneficios para la implementación de VPNs a nivel WAN utilizando una infraestructura arrendada a través de un proveedor de servicio es el ahorro en el costo de implementación, pero así mismo existen riesgos que deben ser tomados en cuenta como:

a) Seguridad de los datos

   En el modelo de VPN, los datos de la empresa están siendo transportados a través de una red pública, lo que significa que otros usuarios de la red pública potencialmente pueden acceder a datos de una empresa que ocupa el mismo medio y por lo tanto representan un riesgo para la seguridad.

b) Ancho de Banda dedicado entre los sitios

   El segundo riesgo en el modelo de VPN es la falta de disponibilidad de ancho de banda dedicado entre los sitios, ya que en el modelo de VPN para conectar los sitios utiliza una conexión virtual, a más que los enlaces físicos en la red pública son compartidas por muchos sitios y muchas diferentes VPNs.

c) Ancho de banda entre los sitios no está garantizado a menos que la VPN permite alguna forma de esquemas de reserva de ancho de banda de control y admisión de conexión.

3.12 TECNOLOGIAS VPN

Considerando que una VPN no es más que una conexión lógica entre varias redes, estas pueden ser implementadas tanto en capa 2 como en capa 3 del modelo OSI.

3.12.1 VPNs EN CAPA 2

El encapsulamiento a nivel 2 ofrece ciertas ventajas ya que permite transferencias sobre protocolos no-IP. Teóricamente, las tecnologías implementadas en la capa de Enlace pueden "tunelizar" cualquier tipo de paquetes y en la mayoría de los casos lo que se hace es establecer un dispositivo virtual PPP5 (Point to Point Protocol) con el cual se establece la conexión con el otro lado del túnel.

A continuación se presenta algunos ejemplos de este tipo de tecnología

a) PPTP: Point to Point Tunneling Protocol. Desarrollado por Microsoft, es una extensión de PPP. Su principal desventaja es que solo puede establecer un túnel por vez entre pares.

b) L2F: Layer 2 Forwarding. Desarrollado por la empresa Cisco principalmente, ofrece mejores posibilidades que PPTP principalmente en el uso de conexiones simultáneas.

c) L2TP: Layer 2 Tunneling Protocol. Usado por Cisco y otros fabricantes, se ha convertido en estándar de la industria y combina las ventajas de PPTP y L2F y elimina sus desventajas. Sin embargo su desventaja es que no ofrece mecanismos de seguridad

d) L2Sec: Layer 2 Security Protocol. Desarrollado para proveer una solución con seguridad, utiliza para ello SSL/TLS aunque impone una sobrecarga bastante grande en la comunicación para lograrlo.

3.12.1 VPNs EN CAPA 3

La implementación de VPNs sobre capa 3 o de red es identificar y facilitar la comunicación entre nodos que no tiene el mismo direccionamiento de red y por lo tanto se requiere de un ruteo previo.

En la actualidad existe soluciones de VPNs basadas en IP para capa 3, entre las cuales podemos citar GRE, IPSEC, MPLS, VPN Site to Site.

Con estos antecedentes y tomando en cuenta el BACKBONE en el cual se basa esta tesis, se podrá énfasis en las tecnología IPsec VPN y MPLS VPN.

Tabla 6
Comparación entre VPN L3 y VPN L2

VPNs de Capa 3 (L3VPN)	VPNs de Capa 2 (L2VPN)
Provee el reenvio de paquetes (por ejemplo IP)	Provee el redireccionamiento de frame - base (por ejemplo, VLAN, DLCI, VPI / VCI).
El proveedor de servicio envía paquetes de datos a los clientes, basados en información de capa 3 , (por ejemplo IP)	El proveedor de servicio envía paquetes de datos a los clientes, basados en información de capa 2. Soporta Multiprotocolo , (por ejemplo IP)
Se requiere la participación de SP para realizar el enrutamiento.	No se involucra el SP. Utiliza túneles, circuitos, LSP, Mac address
Su implementación soporta MPLS / VPN BGP (RFC 2547), MPLS VPN sobre IP, GRE, virtual router.	Su implementación puede realizarse en tecnologías existentes

3.13 MPLS VPNS

Como indica su nombre, una red MPLS puede transportar múltiples protocolos distintos y de forma simultánea entre ellos.

Una de las principales ventajas de las MPLS VPN sobre otras tecnologías VPN es que ofrece la flexibilidad para configurar topologías VPN entre sitios, lo cual permite ofrecer soluciones seguras y de calidad, fáciles de desplegar, mantener y notablemente más económicas que las soluciones tradicionales.

Para poder entender mejor su flexibilidad y desempeño citaremos el siguiente escenario:

Si tres sitios remotos de una empresa deben estar conectados uno al otro (any to any) bajo una configuración en malla completa utilizando ATM, Frame Relay, GRE, IPSec u otras tecnologías, cada sitio requiere dos circuitos virtuales a todos los demás sitios.

Si a esta solución queremos incrementar un nuevo sitio manteniendo el mallado completo se requiere la existencia de tres circuitos virtuales que corresponderían a los tres primeros sitios que estaban conectados al inicio, lo cual involucra la modificación en las configuraciones en todos los sitios.

Cuando se implementa este requerimiento sobre una infraestructura MPLS, si los tres sitios iniciales están conectados a través de una VPN de MPLS, la adición del cuarto sitio no afecta a la configuración inicial solo se tendrá que configurar los accesos en el último sitio incrementado.

De esta forma, MPLS para VPN/IP reduce considerablemente la complejidad y los problemas técnicos que se producen al aumentar o reducir el número de sedes corporativas que participen en una VPN/IP, reduciendo los costos asociados y los plazos de puesta en marcha.

Igual que a una red IP, a una VPN/IP sobre MPLS se puede acceder con la más amplia variedad de tecnologías como son ADSL, dial-up (RTC, RDSI, móviles), líneas punto a punto, túneles IPSEC o L2TP, etc.

Con estos antecedentes se puede decir que una VPN/IP sobre MPLS es como disponer de una red propia y privada con todas las prestaciones, la flexibilidad y la sencillez que la caracterizan y que han llevado a su desbordante éxito global.

Así mismo en el documento RFC 2547 se define un esquema para ofrecer un servicio de VPN utilizando MPLS, el cual se consideró para este trabajo.

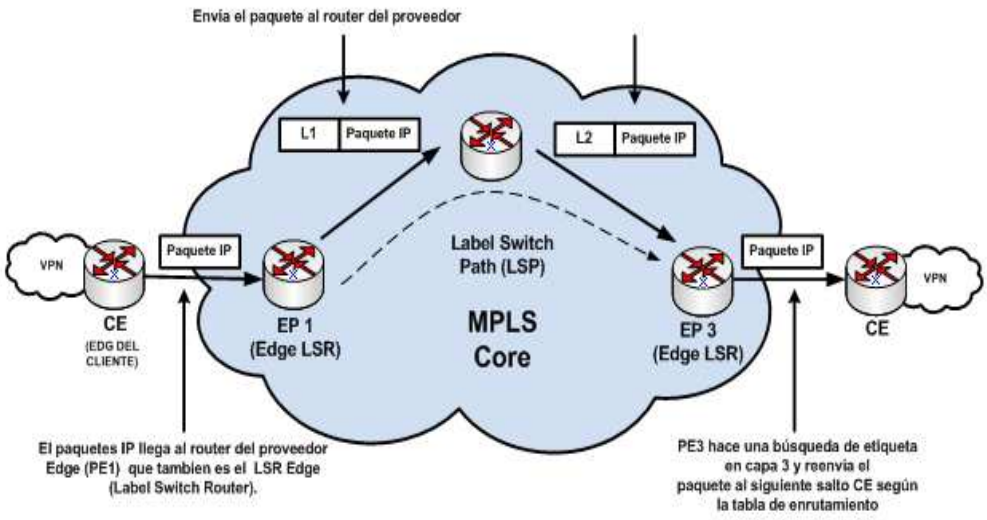


Figura 29. Diagrama MPLS
(Fuente Cisco Press)

3.13.1 ELEMENTOS DE MPLS VPN

a) Virtual Routing: Diferentes instancias o tablas de routing conocidas como VRF(VPN Routing and Forwaring) en los PE (Provider Edge).
b) VRFs con el mismo identificador o nombre pueden intercambiar sus tablas de rutas.

c) Propagación de información de VRF con MP-iBGP dentro de la Red MPLS.
d) Asociación de un interface físico o lógico a un VRF.
e) Vinculo de VRFs con VLAN 802.1Q
f) A la Red MPLS no le afecta el direccionamiento de varios proveedores externos.

3.13.2 MPLS VPN / IPsec VPN

MPLS VPN y VPN IPsec son tecnologías complementarias, ambos tienen sus ventajas, aunque en diferentes implementaciones como:

- MPLS/VPN crea una ruta de datos privados a través de la red central proporcionando rutas de datos más seguro y más rápido sin carga de red.
- MPLS VPN no proporciona funciones de confidencialidad de datos o criptografía, esto significa que los datos podrían ser interceptados durante la transmisión sin conocimiento tanto del emisor como del receptor.

Con este antecedente MPLS/VPN no cumple con los requisitos de confidencialidad y no repudio que puede ser requerido por algunos de los estándares de la industria (por ejemplo, HIPAA (Health Insurance Portability and Accountability).

La solución IPsec VPN a nivel de red se puede implementar como una superposición sobre la red MPLS.

Tabla 7

Comparación VPN MPLS y IPSec VPN

PARAMETRO	MPLS VPN	IPSec VPN
Colocación	Implementado en red de CORE (reside en la red de proveedores de servicios	Implementado en local loop, edge (borde) y fuera de la red (reside en la red del cliente)
Escalabilidad	Altamente escalable, ya no se requiere conexiones sitio a sitio poya a decenas de miles de conexiones VPN a través de la misma red.	La escalabilidad se convierte en un desafío cuando esta es aplicada a gran escala. Las soluciones VPN IPsec requieren una cuidadosa planificación y coordinación para la asignación, gestión y distribución de claves.
Aprovisionamiento	Para permitir una conexión MPLS VPN se requiere de un solo aprovisionamiento de equipamiento (routers) tanto a nivel de edge del cliente (CE) como de edge del proveedor (PE)	IPSec VPN utiliza el aprovisionamiento de una red central IP ofreciendo servicios con reducción de gastos de operación centralizada a través de la misma infraestructura.
Despliegue	Se requiere de una red MPLS con capacidad de infraestructura tanto el CORE como en EDGE del proveedor	No depende del proveedor y puede ser desplegado en cualquier red existente.
Autenticación	Las conexiones se autentican a través de membrecía de VPN lógicas, basado en puerto lógico y el descriptor de ruta única. Acceso no autorizado es negado	Las conexiones se autentican a través de certificados digitales o claves previamente compartidas. Los paquetes que no se ajusten a la política de seguridad se eliminan.

CONTINUA

Confidencialidad	Los circuitos lógicos punto-a-punto se separan, proporcionando una sensación de seguridad y privacidad de los datos.	Set de cifrado estándar y mecanismos de túnel se utilizan en la Capa de red IP para proteger los datos.
Calidad de Servicio QoS y SLA	Proporciona QoS y SLAs con capacidades de ingeniería de tráfico robusto.	No trata directamente la QoS y SLAs.
Cliente VPN	MPLS VPN es un servicio basado en la red, por lo que los usuarios finales no requerir software de cliente VPN para comunicarse con redes remotas.	Para una conexión remota de un usuario es necesario utilizar un cliente VPN (software). Cuando se implementa este protocolo en infraestructuras sitio a sitio no se hace necesario el cliente ya que esta es habilitada entre equipos activos de comunicación (routes)

3.14 IMPLEMENTACIONES DE SEGURIDAD VPN A NIVEL WAN

En la actualidad la implementación de VPNs es una manera de compartir un medio de comunicación entre varios usuarios, para lo cual los mecanismos para realizar estas conexiones son:

- IPsec (IP Security)
- GRE Generic Routing Encapsulation)
- DMVPN (Dynamic Multipoint Vpn)
- Easy VPN (Vpn Básica)
- GETVPN (Group Encrypted Transport Vpn)

El objetivo de este capítulo es detallar de manera general los pasos que se deben considerar al implementar cada tecnología detallada anteriormente, así como también profundizar en dos de estas para poder hacer una comparación de los beneficios técnicos que se lograría con cada una de estas.

3.14.1 IPSEC VPN

Para mitigar los riesgos inherentes al momento de utilizar una infraestructura de red pública para la transmisión de datos en la actualidad se implementa el protocolo IPSec el cual actúan en la capa de red (capa 3). Otros protocolos de seguridad de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capa 4 del modelo OSI) hacia arriba.

Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger también protocolos de la capa 4, incluyendo TCP y UDP. Una ventaja importante de IPsec frente a SSL y otros métodos que operan en capas superiores, es que para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

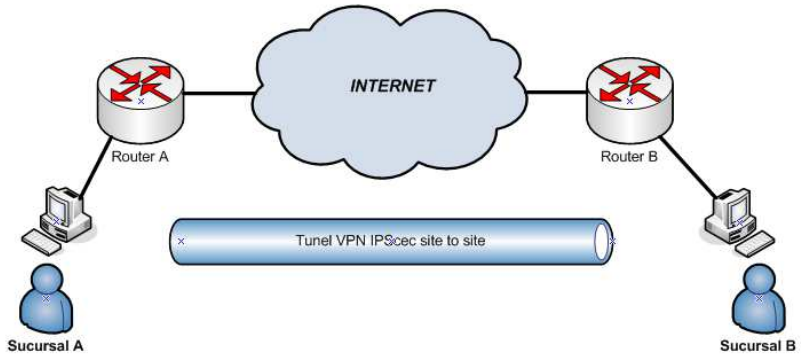


Figura 30. Diagrama de conectividad IPSec

IPsec tiene dos métodos para la propagación de los datos a través de una red:

3.14.1.1 EL MODO DE TÚNEL:

Protege los datos cuando se dispone de escenarios como de red a red o de sitio a sitio, así mismo este método encapsula y protege todo el paquete IP, la carga útil incluida el encabezado IP original y una nueva cabecera IP. Además, se añade la cabecera de IPsec.

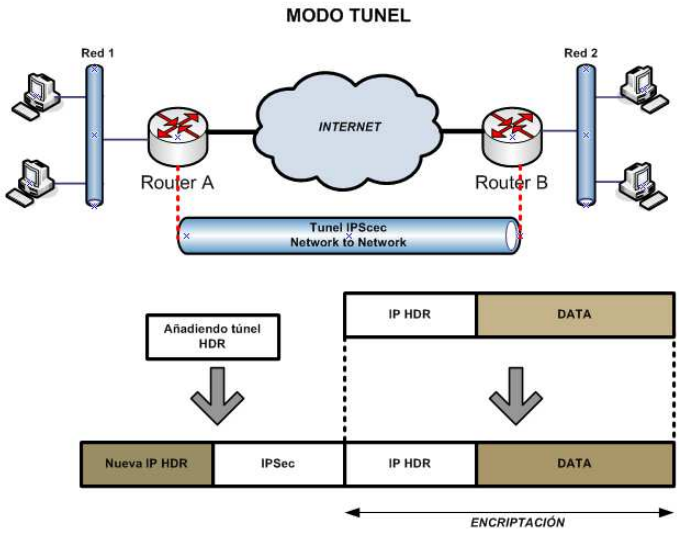


Figura 31.Conexión utilizando Modo Túnel

3.14.1.2 MODO DE TRANSPORTE:

Protege los datos cuando se tiene los escenarios host-to-host o de extremo a extremo. El modo de transporte se utiliza para escenarios de peer-to-peer, es decir, cifrar el tráfico entre pares de IPsec.

El modo de transporte es comúnmente implementado en los equipos finales y de esta manera se logra proteger los sockets individuales, así mismo también puede ser utilizado por sistemas intermedios para proteger la tunelarización del tráfico.

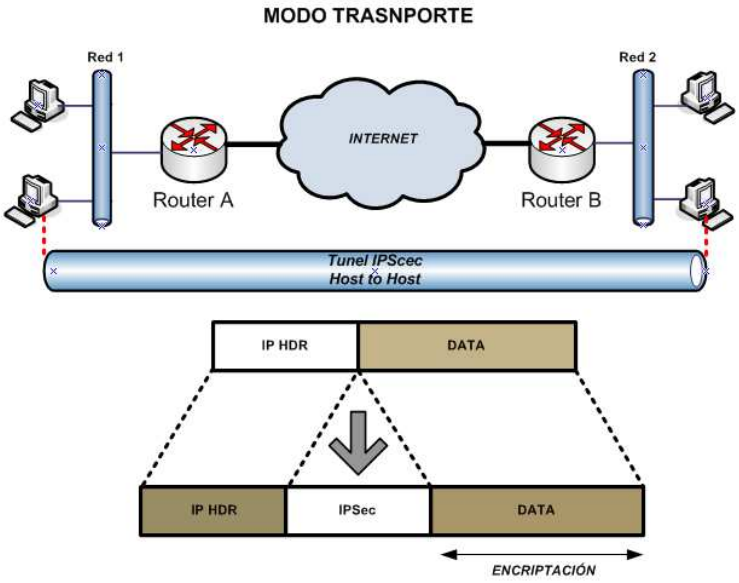


Figura 32. Conexión utilizando Modo Transporte

3.15 IMPLEMENTACION DE IPSEC VPN

IPsec proporciona confidencialidad, integridad, autenticación y servicios de anti-replay, así mismo IPsec VPN es la única manera de implementar VPNs seguras. Las soluciones IPsec VPN se pueden dividir en dos categorías principales:

a) Site-to-Site IPsec VPN
   - Full Mesh
   - Hub-and-Spoke
   - DMVPN
   - Static VTI
   - GETVPN

b) Acceso Remoto IPsec VPN
   - Easy VPN
   - Dynamic VTI

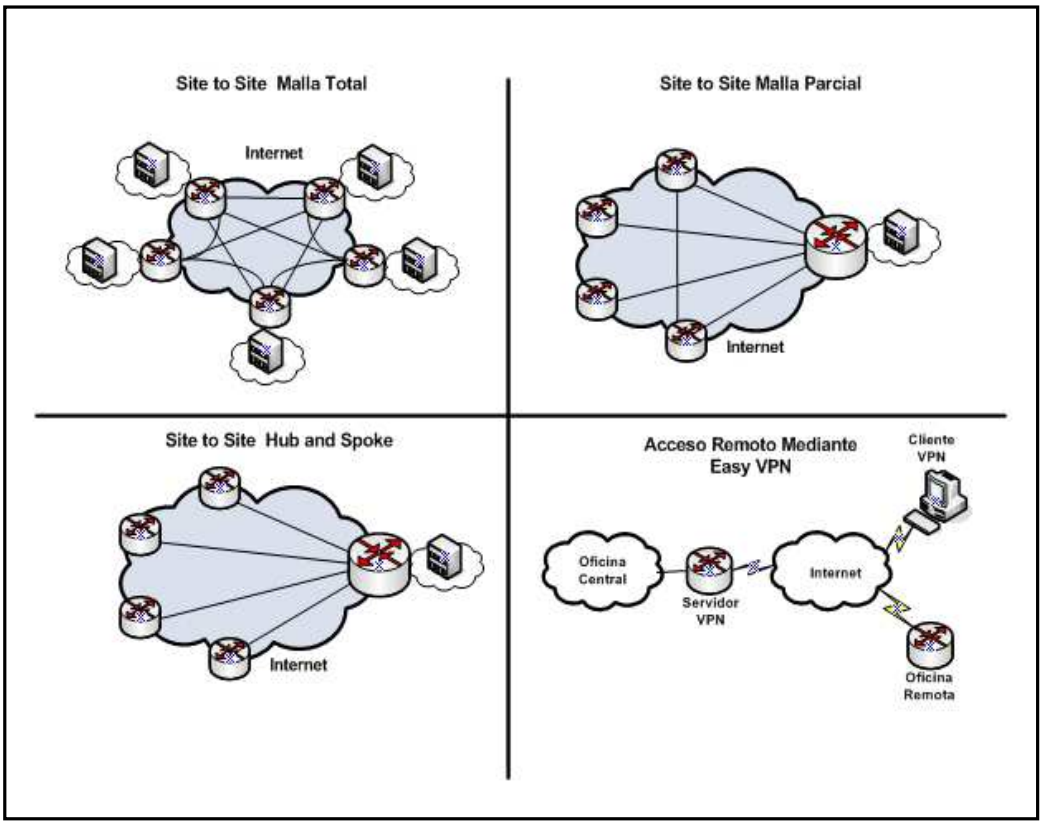


Figura 33. Escenarios de implementación de VPN IPSec

3.15.1 PASOS PARA IMPLEMENTAR IPSEC

Una implementación de IPsec funciona como un Security Gateway (SG), proporcionando protección al tráfico IP. La protección ofrecida se basa en requerimientos definidos en el establecimiento de una "Base de Datos de Políticas de Seguridad" (SPD) y mantenidas por un usuario o administrador del sistema o por una aplicación funcionando dentro de las restricciones ya establecidas.

IPsec utiliza dos protocolos para proporcionar seguridad al tráfico: la Cabecera de Autentificación (AH) y la Carga de Seguridad Encapsulada (ESP).

- La Cabecera de Autentificación (AH): Proporciona integridad sin conexión, autentificación del origen de datos, y un servicio opcional de protección antireplay.

- La Carga de Seguridad Encapsulada (ESP): Puede proporcionar confidencialidad (encriptacion), y confidencialidad limitada de flujo de tráfico. También puede proporcionar integridad sin conexión, autentificación del origen de datos, y un servicio de protección antireplay.

- AH y ESP son instrumentos para el control de acceso, basados en la distribución de claves criptográficas y en el manejo de flujo de tráfico concerniente a estos protocolos de seguridad.

Tabla 8.

Pasos para configurar IPSec

Paso 1	Preparando configuración IPSec	a) Determinar IKE (Internet Key Exchange) y política IPSec. b) Verificar que se establezca la conectividad con el router peer (miembro)
Paso 2	Configuración de parámetros IKE (Internet Key Exchange)	a) Garantizar que el modo de configuración este habilitado. b) Habilitar IKE/ISAKMP en el router c) Crear la política IKE para que se pueda utilizar las claves previamente compartidas • Establezca la prioridad de la política e ingresar al modo config-ISAKMP. • Establezca la autenticación de utilizar claves previamente compartidas • Establecer cifrado IKE. • Establecer un grupo Diffie-Hellman • Establecer el algoritmo hash • Establecer la asociación con el servidor IKE

CONTINUA

		• Salir del modo de configuración config-isakmp • Configurar la clave pre compartida y dirección peer (miembro) • Salir del modo de configuración • Examinar el conjunto de políticas de cifrado
Paso 3	Configurando Parámetros IPSec	a) Verificar que el modo de configuración está habilitada. b) Verificar que las opciones de cifrado IPSec estén disponibles. c) Verificar que el conjunto de opciones de transformación están disponibles. d) Definir un conjunto de transformación. e) Configure el modo túnel. f) salir del modo de configuración g) Verificar la configuración h) Configurar la encriptación de las listas de acceso i) Verificar si el modo de configuración está habilitado. j) Configurar ACLs k) Configurar crypto maps l) Configurar el nombre, número y tipo de intercambio de claves del mapa a ser usado. m) Especificar el conjunto de transformación definido anteriormente n) Asignación de los peers VPN utilizando el nombre del host o la dirección IP de los peer o) Salir del modo de configuración crypto map p) Aplicar crypto map en la interfaz q) Acceder al modo de configuración de la interfaz CONTINUA

		r) Asignación de crypto maps a la interfaz
Paso 4	Verificar y probar la configuración IPSec	a) Verifique las políticas IKE de configuración b) Verificar la configuración del conjunto de transformación c) Verifique la configuración de crypto maps d) Verifique el estado actual de IPSec
Paso 5	Afinamiento de cripto ACL	a) Ajustar las configuraciones de cripto ACL que se utiliza para determinar el tráfico interesante

3.16 IMPLEMENTACION DE GRE

VPN GRE es implementado cuando se trabaja con protocolos no enrutables como NetBios o con protocolos enrutables diferentes de IP a través de una red IP. Se puede constituir un túnel GRE para trabajar con IPX o AppleTalk sobre una red IP.

Actualmente el uso de GRE, se ha vuelto uno de los principales mecanismos de transición para la implementación de redes IPv6. Es decir es posible conectar dos islas IPv6 a través de tunnel Ipv4.

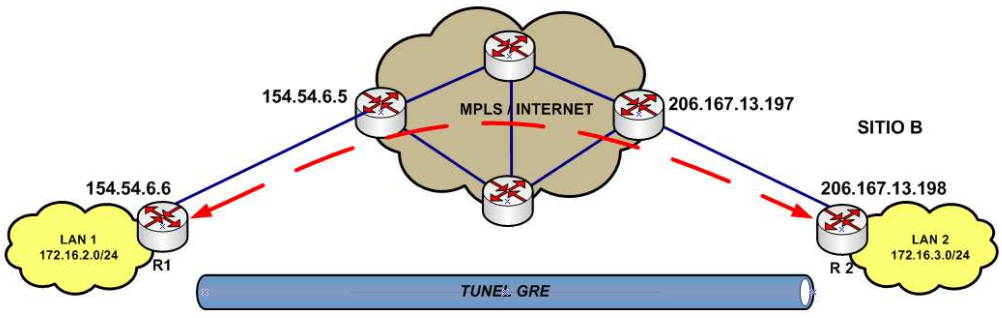


Figura 34. Escenarios de implementación de VPN GRE

3.16.1 FUNCIONAMIENTO DE TUNEL GRE (Genereric Routing Encapsulation)

- GRE toma un paquete ya existente, con su encabezado de capa de red, y le agrega un segundo encabezado de capa de red, lo que implica que el paquete que se envía a través del túnel es de mayor longitud por lo que puede ocurrir que esté excediendo la longitud permitida en la interfaz física. Esto provoca el descarte de ese paquete. Para solucionar este inconveniente se debe aplicar el comando ip tcp adjust-mss 1436 sobre la interfaz del túnel para asegurarse de que no se supere el MTU permitido sobre el enlace.

- El enlace sobre el túnel GRE no requiere ninguna información de estado, por lo que puede ocurrir que un extremo del túnel se encuentre en estado de down y el otro continúe presentándose como up. Para evitar esta situación se debe habilitar keepalive en cada extremo del túnel. De este modo cada extremo enviará mensajes de keepalive sobre el túnel y si un extremo no recibe los mensajes enviados por el otro entonces pasará al estado de down.

Tabla 9

Pasos para configurar GRE

Paso 1	Creamos una interfaz virtual	- Le asignaremos una ip privada - Además le diremos que el origen del túnel es nuestra ip publica (la del router 1) y el destino la ip pública del otro router (el router 2) -Lo configuraremos con la orden keepalive para que la interface virtual este activa - Y añadiremos una descripción a la interfaz para identificarla fácilmente **CONTINUA**

Paso 2	Añadiremos las rutas al router,	Se configura a través de que ip tiene que acceder a la red privada del equipo (router)
Paso 3	Configuración de accesos	Añadir una access list a la interfaz física del router para permitir el tráfico hacia la red destino

3.17 IMPLEMENTACIÓN DMVPN

La implementación de Dinamic Multiponit VPN (DNVPN) permite a los usuarios de disponer de una gran escalabilidad, utilizando un menor número de tunes IPSEC, para lo cual combina encapsulamiento de tunes GRE.

Dinamic Multiponit VPN (DMVPN) permite a las redes que utilizan IPSec VPN una mejor escala de diseños hub-to-spoke y spoke to spoke, optimizando así el rendimiento y reduciendo la latencia de las comunicaciones entre los sitios.

Entre los beneficios de DMVPN podemos nombrar los siguientes:

- Capacidad para construir hub to spoke y spoke to spoke IPSec
- Optimizar el rendimiento de la red
- Reducción de latencia para aplicaciones que se utilizan en tiempo real

3.17.1 COMPONENTES PARA IMPLEMENTAR UNA SOLUCION DMVPN

Una solución DMVPN es una combinación de varios protocolos y los principales componentes funcionales incluyen los siguientes.

a) **Protocolo Generic Routing Encapsulation (GRE).** Está diseñado para encapsulamiento de paquetes IP unicast, muticast y broadcast. GRE utiliza el protocolo IP número 47.
b) **Resolución de Protocolo Next Hop (NHRP):** Es utilizado para mejorar la eficiencia de encaminamiento del tráfico sobre NBMA (non-broadcast multiple access network).

c) **Protocolo Dinámico de Ruteo:** Se utiliza para anunciar las redes privadas dentro de las redes DMVPN. Los protocolos soportados son RIP, EIGRP, OSPF, ODR y BGP.
d) **Protocolos de cifrado IPsec basadas en estándares:** Son protocolos utilizados para proteger los túneles al implementar una solución DMVPN.

Las siguientes reglas deben ser consideradas para la implementación:

a) Cada SPOKE (router) debe tener un túnel IPSEC permanente con el HUB, no a otros SPOKES dentro de la red.
b) Cada uno de los SPOKES necesita enviar un paquete a un destino (privado) de subred o a otro SPOKE.
c) Después que el SPOKE original aprende la dirección del PEER, el objetivo del SPOKE es iniciar el túnel IPSEC.
d) El túnel SPOKE –TO-SPOKE se construye sobre la interfaz multipunto GRE (Mgre)
e) Los enlaces SPOKE-TO-SPKE son establecidos por demanda cuando existe tráfico entre los SPOKES. A partir de esto los paquetes enviados son capaces de pasar por alto el HUB y usa el túnel SPOKE-TO-SPOKE

3.17.1.1 FUNCIONAMIENTO DE DMVPN

a) Inicialmente cada spoke debe establecer un túnel IPSec permanente con el hub. En esta etapa los spokes no establecen túneles con otros spokes dentro de la red. La dirección del hub debe ser estática y a su vez debe ser conocida por los spokes.
b) Cada spoke registra su dirección como un cliente del servidor NHRP. El servidor NHRP mantiene una base de datos NHRP de las direcciones de la interfaz pública para cada radio.
c) Cuando un spoke requiere que los paquetes se envíen a una sub red de destino (privado) a otro spoke, este consulta el servidor NHRP las

direcciones reales (outsite) de otros spokes de destino de esta manera se puede construir tunes directos.

d) El servidor NHRP busca la base de datos de PNDH y de esta manera encuentra el destino correspondiente al spoke y a su vez su dirección real de destino. El uso de NHRP (Next Hop Resolution Protocol) evita la necesidad de protocolos de enrutamiento dinámico para descubrir la ruta hacia el spoke correcto (las adyacencias de enrutamiento dinámico se establece solo desde un spoke to hub).

e) Después de que el spoke original aprende la dirección de sus pares, se inicia un túnel IPSec dinámico al destino del spoke

f) Con la integración de la interfaz multipunto GRE (Mgre), NHRP e IPSec, se establece un túnel dinámico spoke to spoke a través de la red DMVPN.

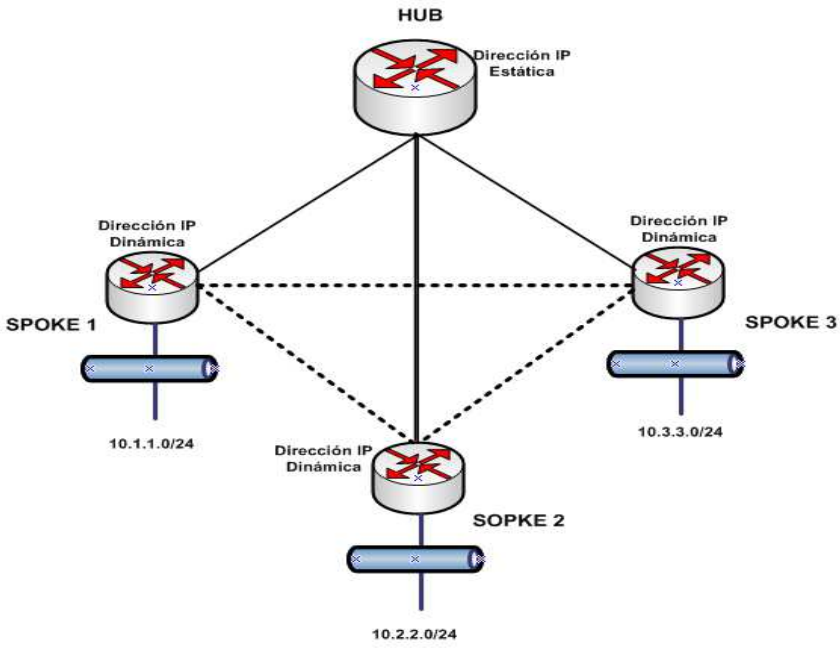


Figura 35. Escenarios de implementación de DMVPN Site to Site

3.17.2 PASOS DE CONFIGURACION: DE DMVPN

Para simplificar la configuración de DMVPN hemos dividido el proceso en 4 pasos, los cuales son secuenciales y debe mantener su orden.

1. Configurar el HUB DMVPNC
2. Configurar los SOPOKES DMVPN
3. Proteger los túneles mGRE con ipsecurity
4. Configurar el enrutamiento de los túneles DMVPN mGRE

Tabla 10

Pasos para configurar DMVPN

Paso 1.	Configuración del equipo HUB (ROUTER)	1.1 Configurar las interfaces LAN y WAN del router 1.2 Creamos la interfaz de túnel mGRE en las interfaces Ethernet 1.3 Levantamos el servidor NHS (Nex Hop Server)
Paso 2.	Configuración del equipo SPOKE (ROUTER)	2.1 Configurar las interfaces LAN y WAN del router 2.2 Construir el túnel 2.3 Configuramos el salto del tráfico al servidor NHS
Paso 3	Proteger los túneles mGRE con ip security	3.1 Encriptar el túnel GRE utilizando IPsec 3.2 Verificar si está operativo las encriptaciones implementadas.
Paso 4.	Configurar el enrutamiento de los túneles DMVPN mGRE	4.1 Permitir enrutamiento en la red DMVPN (Dinámico o por protocolo)

3.18 IMPLEMENTACIONDE EASY VPN

También conocido como EZVPN es un marco unificado utilizado para desplegar soluciones de VPN de punto-a-punto de acceso remoto simplificado para los usuarios remotos, oficinas remotas y teletrabajadores.

Easy VPN ofrece gestión centralizada de VPN, la distribución dinámica de políticas, y el aprovisionamiento sin esfuerzo, lo que reduce la implementación y el aumento de la escalabilidad y la flexibilidad.

Easy VPN puede ser desplegado en una de las siguientes maneras:

a) Software Easy VPN Client Es unas aplicación VPN la cual puede ser utilizada por usuarios móviles para poder realizar conexiones remotas directas hacia el servidor VPN principal.

b) Hardware Easy VPN Client: Con esta solución se realiza conexiones VPNs site to site para establecer una conexión entre dos dispositivos con lo cual se emularía un escario LAN to LAN. Con esto no se requiere una conexión VPN individual por cada usuario.(El tráfico fluye cifrado entre los pares VPN)

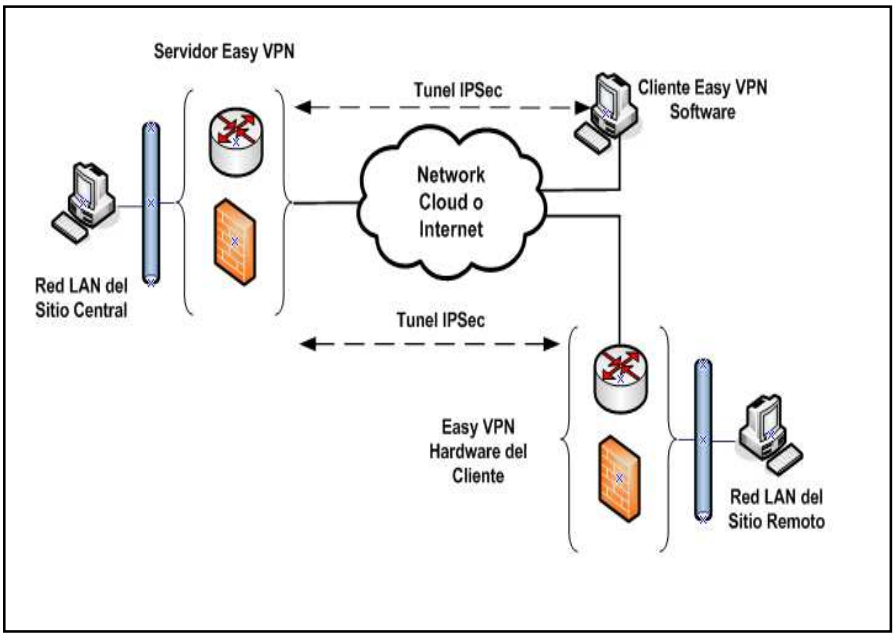


Figura 36. Escenarios de implementación de EASY VPN

Existen dos componentes para la implementación de Easy VPN

a) Servidor para soluciones Easy VPN: Este equipo actúa como un dispositivo de cabecera VPN, con lo cual se emula un escenario de VPN de sitio a sitio falso, donde los dispositivos en los sitios remotos están utilizando la función de cliente remoto de Easy VPN .

b) Cliente Easy VPN (también denominado Easy VPN remoto): VPN Remote Client permite que un dispositivo remoto pueda recibir políticas de seguridad del servidor VPN cuando este estable el túnel. El cliente remoto Easy VPN es fácil de instalar, con una configuración mínima requerida en el sitio del cliente remoto.

El cliente remoto Easy VPN tiene los siguientes tres modos de funcionamiento:

a) Modo Cliente (también conocido como modo PAT):
b) Modo de extensión de la red
c) Extensión de la red Plus + Mode

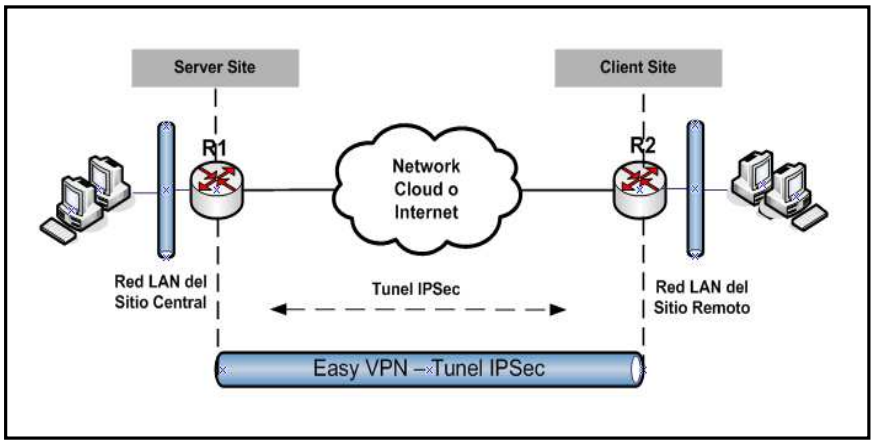


Figura 37. Hardware básico para la implementación de EASY VPN

3.19 IMPLEMENTACION DE GETVPN (GROUP ENCRYPTED TRANSPORT)

Considerando que en la actualidad existen redes malladas de gran escala y estas requieren asegurar la integridad de los datos (voz, datos y video) sin perder características de calidad de servicio y al mismo tiempo pueda garantizar que la infraestructura de red no se degrade, es necesario que se considerar la implementación de un mecanismo de seguridad en capa 3, el cual debe ser independiente a las que en la actualidad son implementadas a nivel perimetral de cada cliente.

En respuesta a esta necesidad, una solución de cifrado es la implementación de la tecnología GETVPN (Group Encrypted Transport) la cual usa un túnel VPN-less (sin túnel) enfocado a redes malladas.

La tecnología GETVPN ofrece a las redes empresariales la capacidad de escalar las aplicaciones de voz, vídeo y datos con una mayor eficiencia de la red, garantizando una conectividad encriptada en un entorno full mesh.

Figura 38. Diagrama conceptual de GETVPN

3.19.1 COMPONENTES DE IMPLEMENTACION GETVPN

La tecnología de solución GETVPN es una combinación de varios protocolos, con los cuales se logra formar una solución de seguridad óptima de encriptación en capa 3, logrando de esta manera:

- Túnel – less muchos a muchos (any to any)
- Cifrado de trafico tanto de unicast como multicast
- Cifrado de tráfico de voz, datos y video
- Preservación de cabecera IP

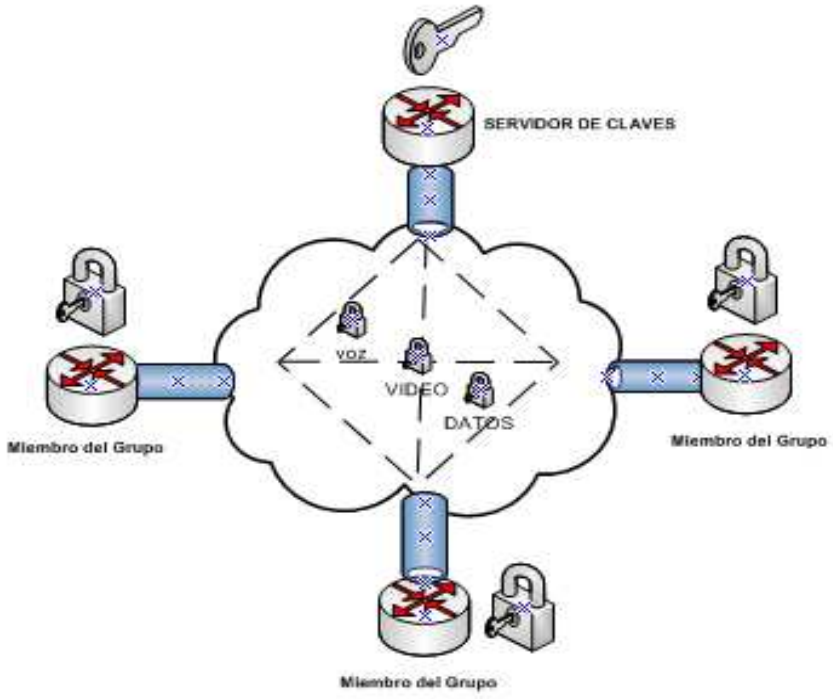


Figura 39. Componentes de GETVPN

3.19.2 PASOS PARA IMPLEMENTACION DE GETVPN

Para la implementación de GETVPN podemos nombrar cinco pasos fundamentales, los cuales se detallan a continuación:

Tabla 11

Pasos para configurar GETVPN

Pasos	Nombre	Descripción
Paso 1	Definición de Topología de Red y Equipamiento	Determinar sobre qué tipo de topología de Red se va a implementar la solución, luego de lo cual se deberá monitorear el tráfico total e identificar cual de este tráfico interesante debe ser protegido como parte de una política de seguridad.
Paso 2	Configuración de servidor de llaves (KS)	a) Configurar la política IKE (Internet Key Exchange). b) Configuración de IPsec. c) Configuración de GDOI. d) Configurar de ACL (listas de acceso) para filtrar tráfico específico.
Paso 3	Configuración de Miembros de Grupo (GM)	a) Fase 1 de IKE (Internet Key Exchange). b) Configuración de GDOI (Group Domain of Interpretation) c) Configuración de Crypto Map. d) Habilitación de GETVPN.
Paso 4	Cooperación de servidor KS	a) Exportar e Importar RSAKEY. b) Configuración de redundancia de KS.
Paso 5	Verificación	a) Envío de tráfico. b) Verificar si se está encriptando el tráfico. c) Verificar si se está manteniendo los niveles de Calidad de Servicio (QoS)

3.20 DISEÑO Y EMULACION DE LA SOLUCION PROPUESTA

Con los antecedentes mencionados anteriormente, podemos indicar que para integrar a la red corporativa a varias oficinas remotas que se encuentran geográficamente distantes, es necesario poseer una línea dedicada de comunicación, la cual por su costo de implementación es recomendable la renta del servicio a un proveedor local.

Los ataques por red y las pérdidas de información ocasionan un gran trastorno y afectan al correcto funcionamiento y progreso de toda empresa, es por eso que estas implementan sistemas de seguridad a nivel perimetral y de esta manera mitigar algún ataque que pueda existir en la infraestructura corporativa.

La solución que se plantea en este proyecto está orientada a la emulación e implementación de un sistema de seguridad a nivel de capa 3 y de esta manera proporcionar un nivel de seguridad adicional a los que posea cada cliente que conforme la solución:

A continuación se presenta el diagrama general en el cual se va a realizar la experimentación y evaluación de los protocolos descritos en el capítulo anterior.

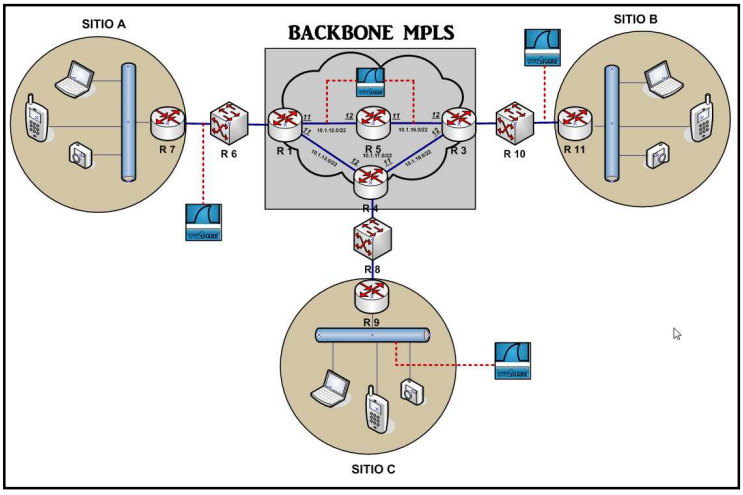


Figura 40. Propuesta de solución

3.21 COMPONENTES LA SOLUCION

Tomando en cuenta que este proyecto está planteado para que su implementación pueda realizarse bajo la infraestructura de comunicación actual y a su vez reutilizando los equipos activos de la red de la parte del usuario final se consideró los siguientes componentes:

a) Backbone (Infraestructura MPLS – Proveedor de Servicio)
b) Equipamiento activo de borde (infraestructura de Cliente)
c) Virtualización de máquinas para la instalación de aplicativos de monitoreo (CACTI)y simulación de servidor de comunicación (Central telefónica ELASTIX)

Los componentes descritos anteriormente formarán parte de la infraestructura básica sobre la cual se empezará la implementación y validación de los objetivos planteados al inicio del proyecto, por tanto se emulará dos escenarios y sobre estos se generarán pruebas con las tecnologías VPN GRE y GETVPN que fueron descritas en el numeral 3.13 de este capítulo.

La idea principal de conexión es interconectar tres sitios que se encuentran geográficamente distantes, los cuales poseen un enlace dedicado de punto a punto.

En la actualidad el Banckbone MPLS a nivel nacional está compuesto por equipos activos de gran performance como:

a) Equipo Cisco 7600 – 7200 para el CORE del Backbone
b) Equipos Cisco 3700 / 2900 / 1800 para red MPLS y Metro Ethernet
c) Equipos Cisco 1800 / 800 para puntos remotos (cliente)

Con este antecedente y considerando que en esta investigación no se contempla el dar énfasis en el Backbone MPLS ya que es una infraestructura

que estaría implementada y que está bajo la responsabilidad de un Proveedor de Servicio, para este proyecto se emulo con el software especializado GNS3 una infraestructura de Backbone MPLS con el siguiente equipamiento:

a) Equipo Cisco 3745 para el CORE del Backbone
b) Equipos Cisco 3725 / 3745 / 2900 / 1800 para red MPLS y Metro Ethernet.
c) Equipos Cisco 3725 / 1800 para puntos remotos (cliente)

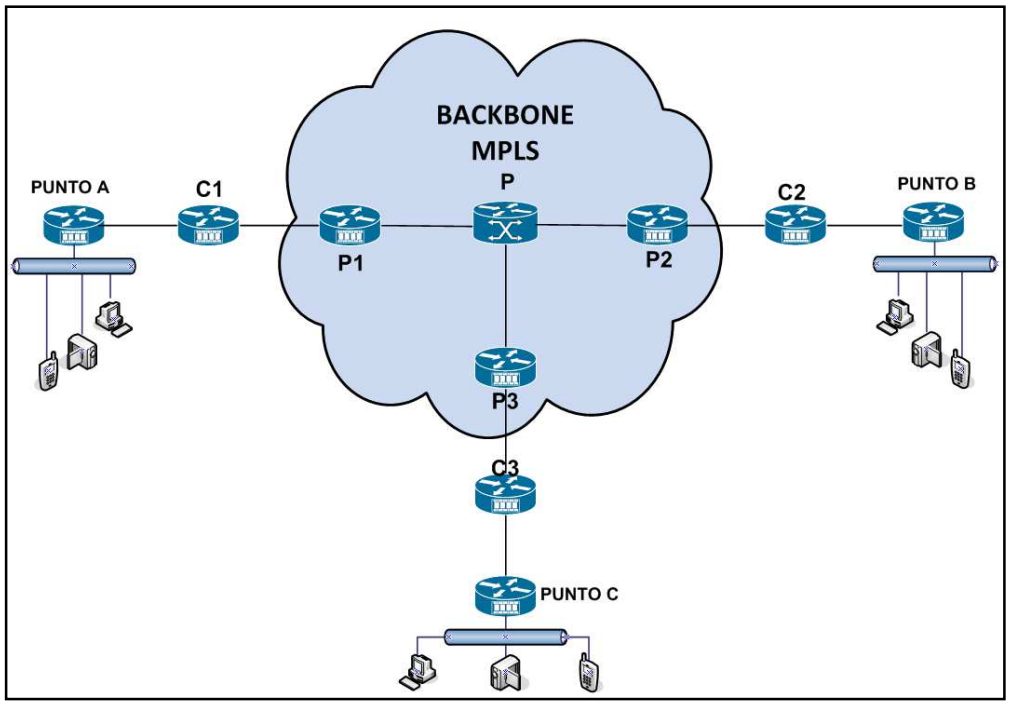


Figura 41. Propuesta de solución con GNS3

En este escenario se utilizó varios equipos activos (routers) de una performance idónea como es Cisco 3740 los cuales serán los agregadores de rutas MPLS para todas las conexiones que están dentro del Backbone, así mismo se utilizó otros dos routers Cisco Catalyst 3725 agregadores en el siguiente nivel (METRO ETHERNET) para unir todas las conexiones de todos los puntos que integran la solución. Esta infraestructura es responsabilidad del proveedor de servicios (SP).

En cada uno de los sitios esta implementado routers Cisco Catalys 3725 los cuales permitieran integrarse a la infraestructura del proveedor de servicio.

Tanto los routers Cisco 3745 como los Catalyst 3725 se encargan de recoger todo el tráfico que lleva de todos los sitios, encontrándose en una jerarquía de primer nivel y al mismo tiempo, estos transfieren a un segundo nivel donde se concentran todas las rutas y que son los otros equipos y son el paso previo antes de conexión con los PEs (Provider Edge) del ISP.

Los agregadores de rutas trabajan, como su propio nombre lo indica, agregando el tráfico que llega de los distintos nodos de acceso de los agregadores de primer nivel y enviándolos hacia otros equipos superiores.

Así mismo estos realizan tareas de conmutación desde los diferentes servicios configurados en los distintos escenarios utilizando VLANS.

Los PEs (Provider Edge) son los equipos en el extremo del IPS y que proporcionan la entrada a la red del trafico IP/MPLS

3.22 EMULACION DE BACKBONE MPLS

A continuación se detalla el procedimiento que se generó para la implementación del Backbone MPLS en esta investigación

PASO 1 Diseño de Backbone

PASO 2 Asignación de direccionamiento

PASO 3 Conexión lógica de los equipos

PASO 4 Verificación de conectividad

PASO 5 Enrutamiento OSPF

PASO 6 Configuración de MPLS

PASO 7 Configuración MP-BGP

PASO 8 Configuración de Vrfs (Enrutamiento Virtual y Reenvío)

PASO 9 Enrutamiento entre los PE (Provider Edge) y CE (Customer Edge) utilizando EIGRP

PASO 10 Redistribución de EIGRP a BGP Y viceversa de BGP a EIRGP en todos los PE

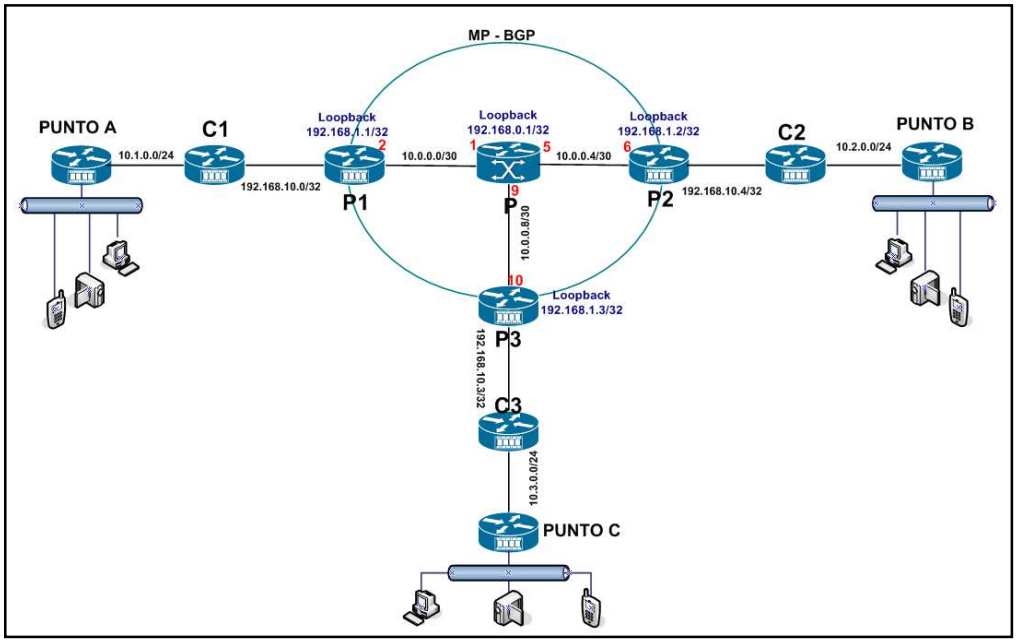


Figura 42. Direccionamiento de Backbone MPLS

3.23 INTEGRACION PROVIDE SERVICE Y CUSTOMER SERVICE

En esta integración de la red es donde se implementó seguridades a nivel de capa 3, ya que es el segmento en el cual fluye el tráfico específico sin control alguno y por tanto de mayor criticidad en el desarrollo del negocio. Este enlace tiene la capacidad de 2 MB.

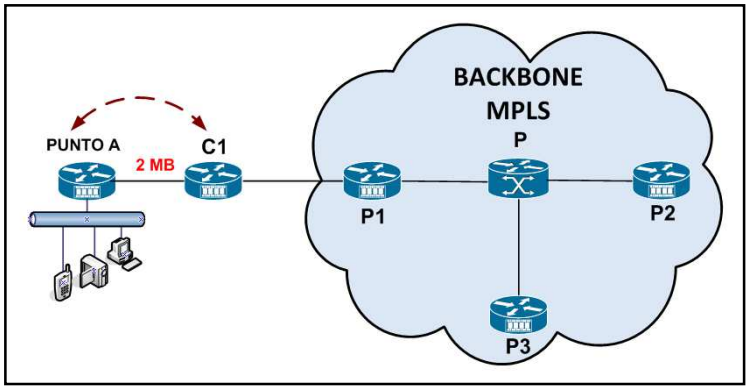


Figura 43. Diagrama de integración Cliente – Proveedor

Una vez implementado el Backbone MPLS y verificada la conectividad entre todos los puntos, se procedió a la evaluación de dos de las cinco tecnologías descritas en este proyecto las cuales son:

a) Implementación de VPN GRE
b) Implementación de GETVPN

3.24 ANALISIS DE RESULTADOS

Para poder determinar si la implementación de redes virtuales seguras en entornos multipunto es viable en redes con infraestructura MPLS, se efectúo un estudio comparativo entre dos tipos de VPNs en donde se determinó cualitativa y cuantitativamente los indicadores de las variables involucradas en este estudio.

En este apartado se va a detallar el análisis comparativo entre dos escenarios, en los cuales las variables que se midieron fueron Latencia, Taza de Transferencia, Calidad de Servicio y Niveles de Seguridades al momento de la transmisión de la Información.

3.24.1 ANALISIS DE DATOS SOBRE INFRAESTRCUTURA MPLS

Para poder validar los resultados se tomaron datos iniciales sobre una infraestructura de comunicación WAN la cual se muestra en la siguiente gráfica.

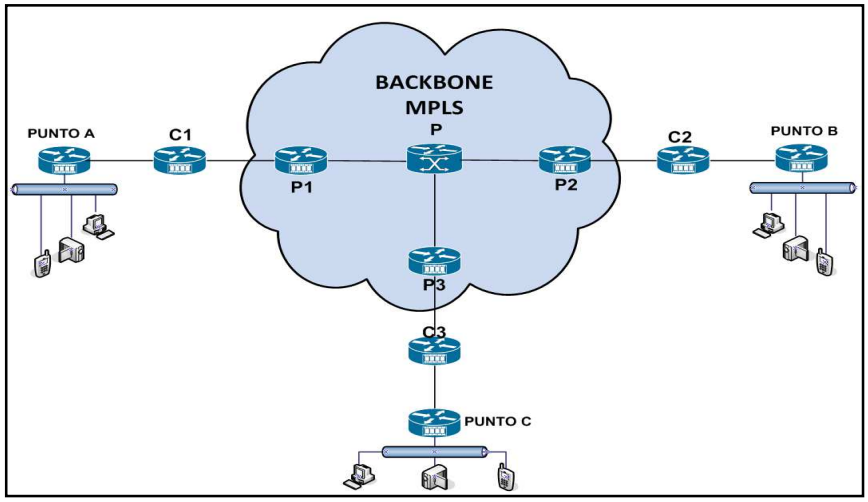


Figura 44. Topología de Red MPLS para pruebas

Tomando en cuenta la Topología anterior se generaron datos, los cuales servirán como base para la comparación de los tipos de VPNs planteadas en este estudio.

Los datos resultantes de la emulación de la red WAN /IP MPLS se detallan a continuación:

Tabla 12

Detalle de Datos sobre red MPLS

N°	CANTIDAD ARCHIVOS (MB)	TIEMPO	ANCHO DE BANDA (Bits/Seg)	LATENCIA (ms)			
				MAXIMA	MINIMA	MEDIA	PING RATE (%)
1	1 MB	0:00:14	30 K	3,04	3,04	3,96	3,92
2	2 MB	0:00:34	40 K	5,05	5,05	8,88	8,57
3	3 MB	0:00:39	90 K	6,62	6,62	11,91	11,87
4	4 MB	0:00:55	120K	8,28	8,28	15,58	16,54

CONTINUA

5	5 MB	0:01:10	150k	20,29	11,79	11,79	20,64
6	6 MB	0:01:18	160k	22,86	7,22	7,22	23,25
7	7 MB	0:01:21	200k	24,71	5,41	5,41	25,12
8	8 MB	0:01:26	210K	26,13	5,62	5,62	26,56
9	9 MB	0:01:53	290K	35,81	35,32	35,32	36,13
10	10 MB	0:02:00	300K	36,17	12,05	12,05	36,84

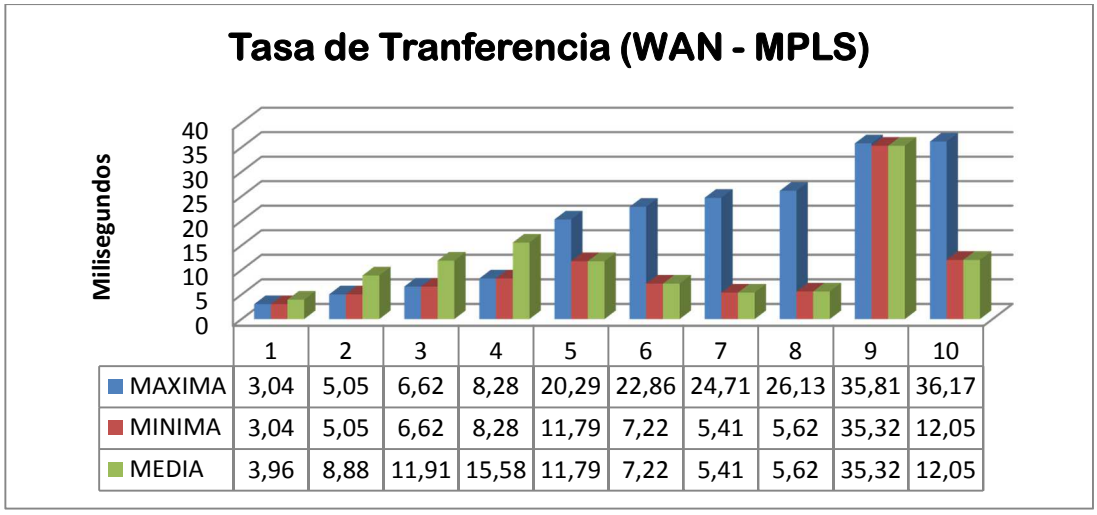


Figura 45. Tasa de Transferencia de Archivos sobre MPLS

Los datos plasmados en al grafica anterior servirán como referente de para comparar y validar el efecto que causa al implementar mecanismos de seguridad sobre una infraestructura WAN que está en producción, así como verificar si los servicios que por esta cursa no sufran degradaciones significativas verificables.

3.24.2 ANALISIS DE DATOS IMPLEMENTADO GETVPN

Para poder validad las hipótesis planteadas se realizó la emulación de una infraestructura de comunicación implementado el mecanismo de seguridad GETVPN y cuya topología es la siguiente:

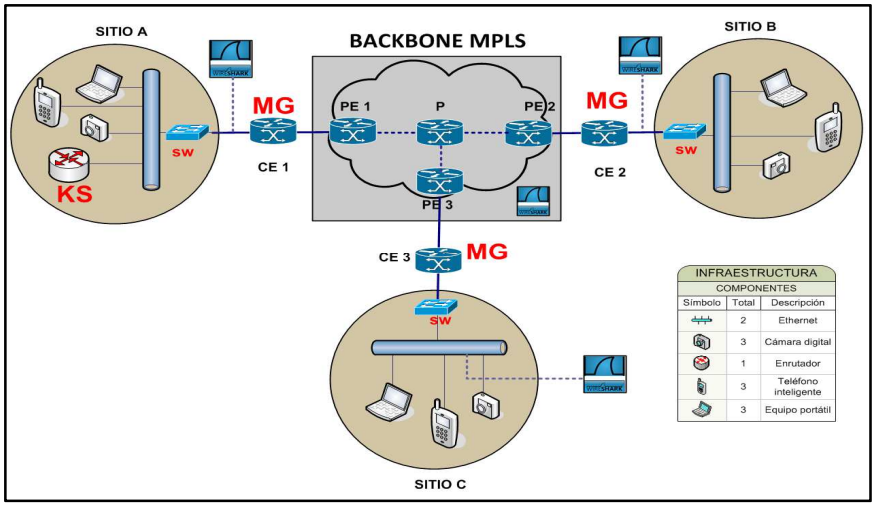


Figura 46. Topología GETVPN

Considerando la topología propuesta para GETVPN, y tomando en cuenta la tabla detallada del apartado 3.24.1 referente al Análisis de Datos sobre Infraestructura MPLS, se realizaron pruebas de conectividad y rendimiento de la infraestructura WAN, de las cuales los resultados son los siguientes:

Tabla 13

Detalle de Datos Implementado GETVPN

N°	CANTIDAD ARCHIVOS MB	DURACIÓN DE TIEMPO AL TRANSMITIR GETVPN	AB (Bits por Segundo)	LATENCIA (ms)			
				MAXIMA	MINIMA	MEDIA	PING RATE (%)
1	1 MB	0:00:16	30 K	3,94	2,37	1,1	9,95
2	2 MB	0:00:30	65 K	8,21	1,05	1,05	8,21
3	3 MB	0:00:40	90 K	11,97	6,7	6,7	11,98
4	4 MB	0:00:48	120K	14,83	3,54	3,54	14,84
5	5 MB	0:01:06	150k	20,10	11,19	11,19	20,1
6	6 MB	0:01:15	160k	20,24	15,83	15,83	19.98
7	7 MB	0:01:20	200k	25,73	4,68	4,68	25,73
8	8 MB	0:01:24	210K	26,12	5,63	5,63	26,13
9	9 MB	0:01:52	300K	34,71	3,52	3,52	34,71
10	10 MB	0:01:56	300K	35,79	6,07	6,07	35,8

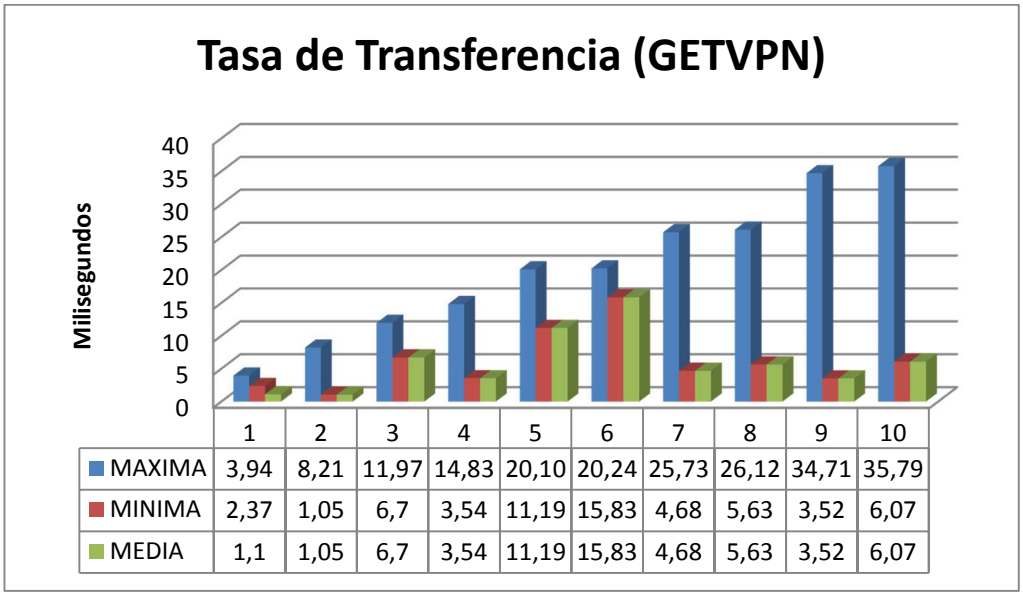


Figura 47. Tasa de Transferencia GETVPN

En la siguiente gráfica se muestra la comparación de la latencia cuando es implementado la encriptación GETVPN sobre WAN / MPLS

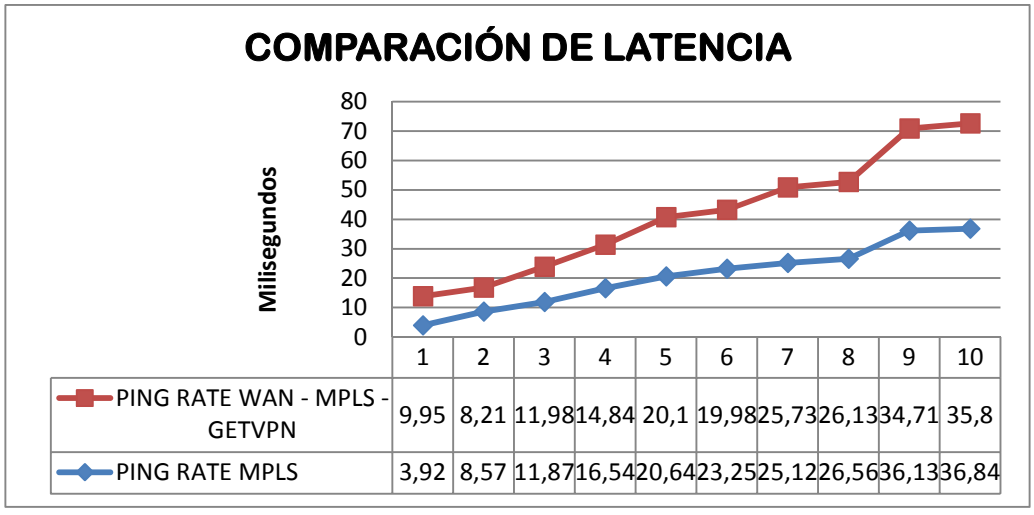


Figura 48. Comparación de Latencia

Como se puede observar en la Figura: 49 los valores cuando es implementado GETVPN aumentan paulatinamente, esto se debe a que se está manejando Calidad de Servicio y Seguridad a nivel de capa 3.

QoS (Paquetes / segundo)	
PRE POLICY	PAQUETES DROPEADOS
4,1	0,9
8,21	1,04
11,98	6,96
14,84	3,53
20,1	11,17
19,98	15,82
25,73	4,67
26,13	5,62
34,71	3,52
35,8	6,06

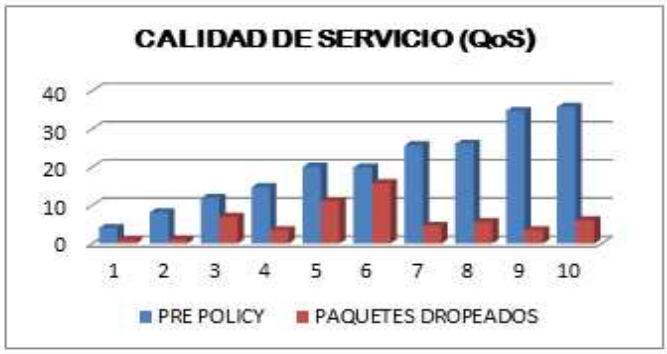


Figura 49. Políticas de QoS sobre GETVPN

A continuación se presenta el cuadro de valores en el cual se detalla la cantidad de paquetes que son encriptados y desencriptados cuando es aplicado el algoritmo de seguridad basado en GETVPN.

Tabla 14

Detalle de paquetes encriptados al transmitir archivos

TRANSFERENCIA DE ARCHIVOS						
N°	CANTIDAD ARCHIVOS MB	DURACIÓN DE TIEMPO AL TRANSMITIR	AB (Bits por Segundo)	ENCRIPTACION GETVPN		
				ENCAPSULADOS	DESENCAPSULADOS	VERIFICADOS
1	1 MB	0:00:26	35 K	248	248	248
2	2 MB	0:00:59	65 K	588	588	588
3	3 MB	0:01:16	70 K	754	754	754
4	4 MB	0:01:25	120K	882	882	882
5	5 MB	0:01:55	150k	1192	1192	1192

De los datos reflejados en la tabla 14 se verifica que la cantidad de paquetes transmitidos son encriptación, desencriptados y verificados en su

totalidad sin desechar ninguno, lo cual indica que el algoritmo de seguridad aplicado en la emulación 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 15 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 15

Detalle de paquetes encriptados al transmitir VOZ y VIDEO

TRAFICO DE VOZ Y VIDEO						
N	DESCRIPCION	DURACION (Minutos)	AB (Bits por Segundo)	ENCRIPTACION GETVPN		
				ENCAPSULADOS	DESENCAPSULADOS	VERIFICADOS
1	Voz / Video	1	20 K	415	415	415
2	Voz / Video	2	30 K	625	625	625
3	Voz / Video	3	40 K	1878	1878	1878
4	Voz / Video	4	70 K	2520	2520	2520
5	Voz / Video	5	80 K	3082	3082	3082

En la figura 50 se puede evidenciar la aplicación de políticas de QoS generadas en este proyecto.

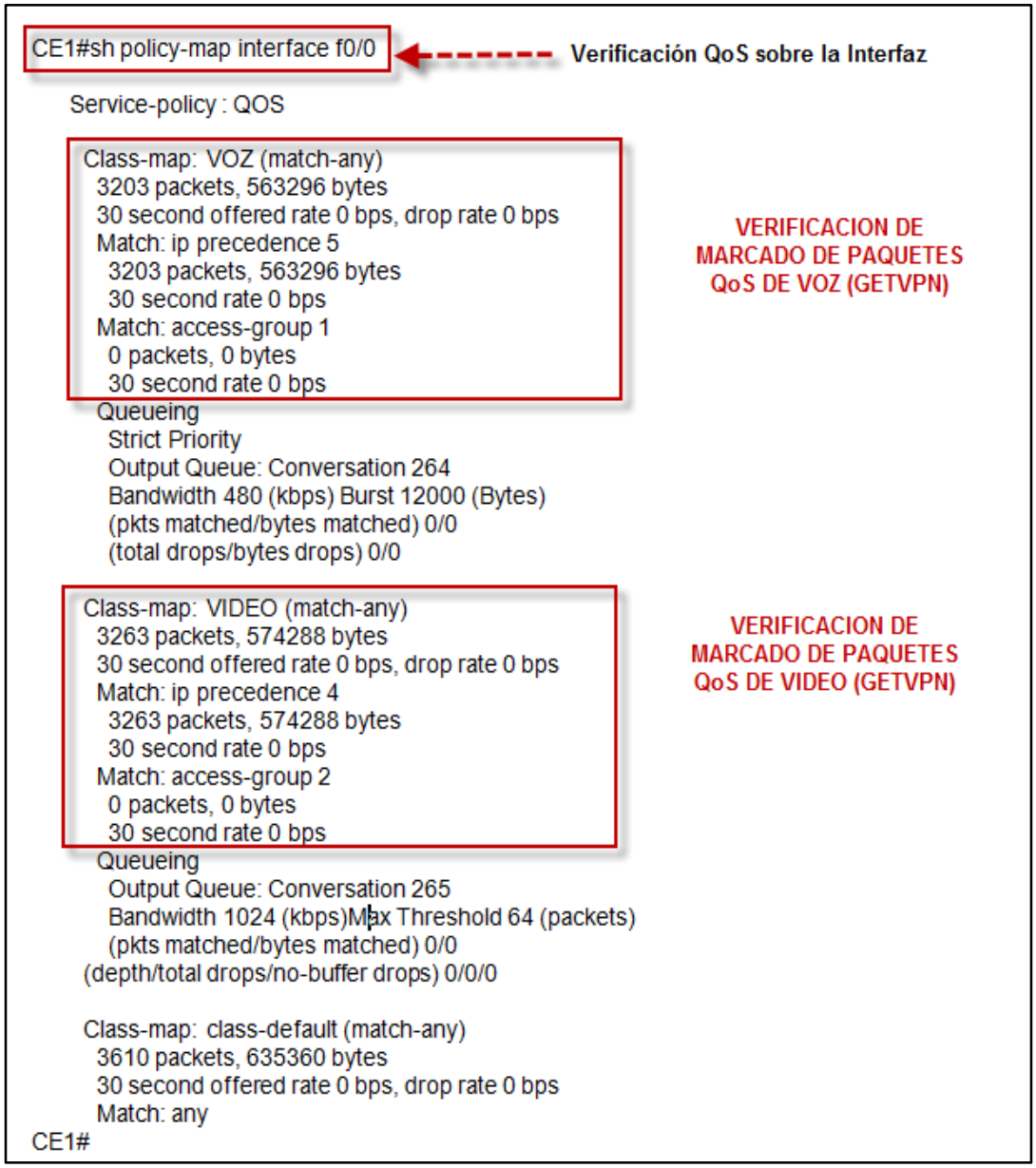


Figura 50. Marcado de paquete QoS

Así mismo en la figura 51 se verifica los datos referentes al cifrado y decifrado los mismos que son obtenidos mediante el comando show crypto ipsec sa.

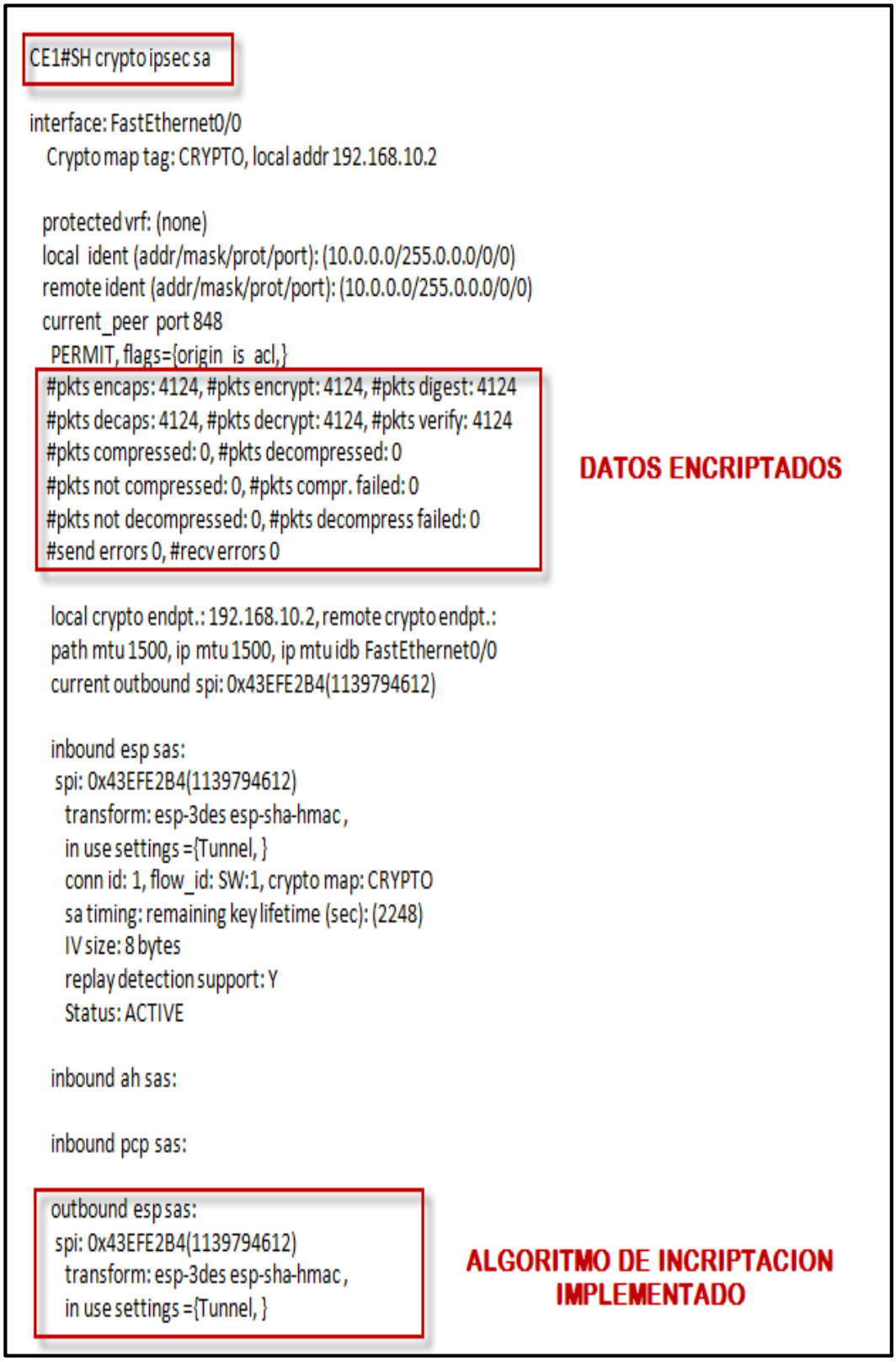


Figura 51. Detalle de comando de verificación de seguridades

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.

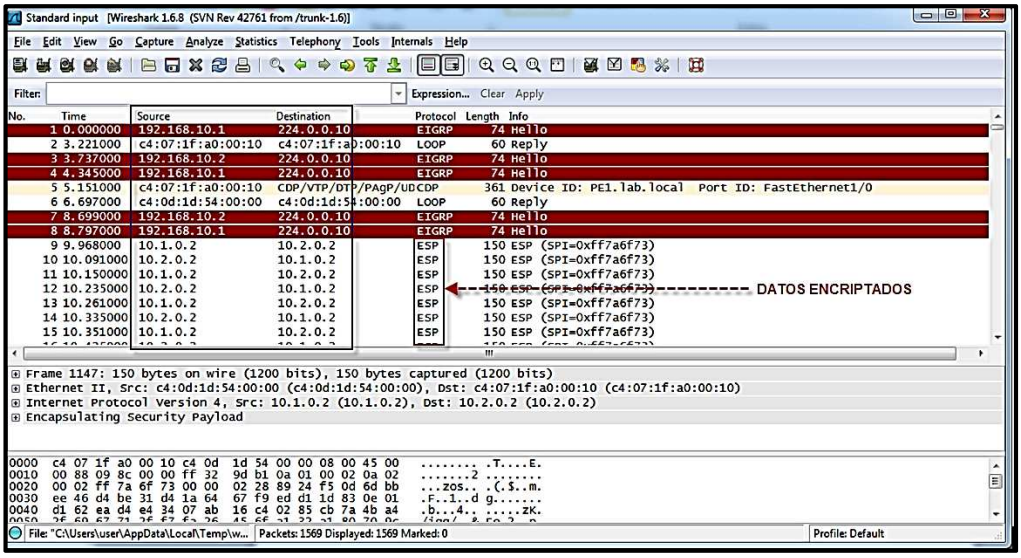


Figura 52. Verificación de Encriptación

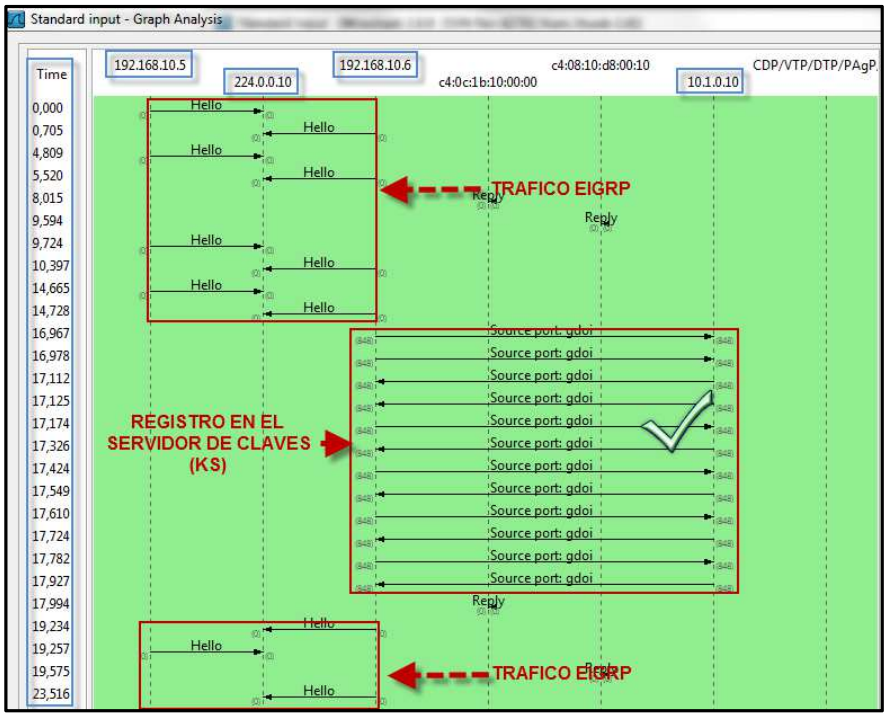


Figura 53. Registro de Miembro de Grupo en KS

3.24.3 ANALISIS DE DATOS IMPLEMENTADO VPN GRE

Otro escenario con el cual se validó seguridades a nivel de capa 3 es utilizando VPNs GRE, para lo cual la topología propuesta es:

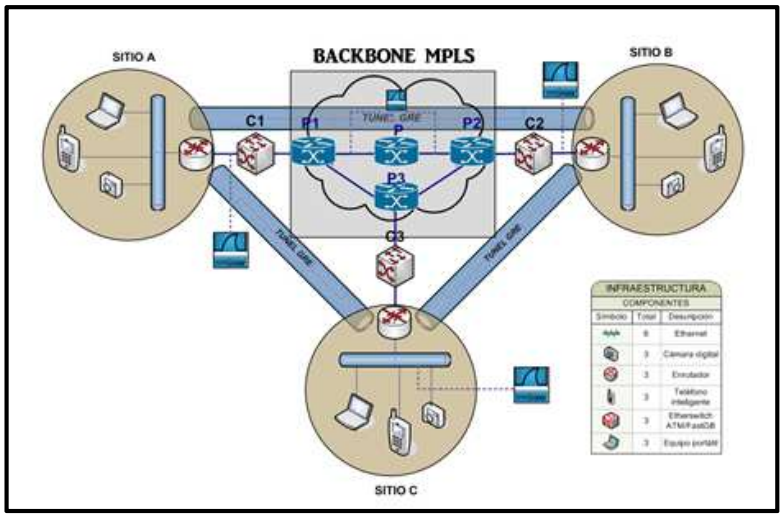


Figura 54. Propuesta de solución implementando VPN GRE

Las pruebas realizadas bajo este escenario fueron las mismas planteadas para GETVPN y cuyos valores resultantes de esta emulación se detallan a continuación:

Tabla 16

Detalle de paquetes encriptados al transmitir archivos

TRANSFERENCIA DE ARCHIVOS

N°	CANTIDAD ARCHIVOS MB	DURACIÓN DE TIEMPO AL TRANSMITIR	AB (Bits por Segundo)	ENCRIPTACION VPN GRE		
				ENCAPSULADOS	DESENCAPSULADOS	VERIFICADOS
1	1 MB	0:00:26	35 K	477	477	477
2	2 MB	0:00:59	65 K	653	653	653
3	3 MB	0:01:16	70 K	807	806	806
4	4 MB	0:01:25	120K	948	948	948
5	5 MB	0:01:55	150K	999	999	999

De igual manera que en el anterior escenario en la tabla 16 se verifica que la cantidad de paquetes transferidos no sufren variación al momento de que estos son pasados mediante túneles GRE, lo mismo sucede en el caso de transmisión de voz y Video lo cual se detalla en la tabla 17.

Tabla 17

Detalle de paquetes encriptados al transmitir VOZ y VIDEO

N°	DESCRIPCION	DURACION (Minutos)	AB (Bits por Segundo)	ENCRIPTACION GRE		
				ENCAPSULADOS	DESENCAPSULADOS	VERIFICADOS
1	Voz / Video	1	20 K	430	430	430
2	Voz / Video	2	30 K	631	631	631
3	Voz / Video	3	40 K	1935	1935	1935
4	Voz / Video	4	70 K	2588	2588	2588
5	Voz / Video	5	80 K	3245	3245	3245

A diferencia de GETVPN, para poder verificar la encriptación del tráfico de Voz, Datos y Video sobre un túnel GRE, esta se la debe realizar sobre el túnel o los túneles de los cuales se requiere obtener la información. Esto conlleva a que si en nuestra infraestructura tenemos configurado un sin número de túneles, cada uno tiene su identificativo al que debemos hacer referencia para verificar el número de paquetes marcados con QoS, lo cual hace que la administración sea más compleja.

El comando aplicado es sh policy-map interface tunnel 0

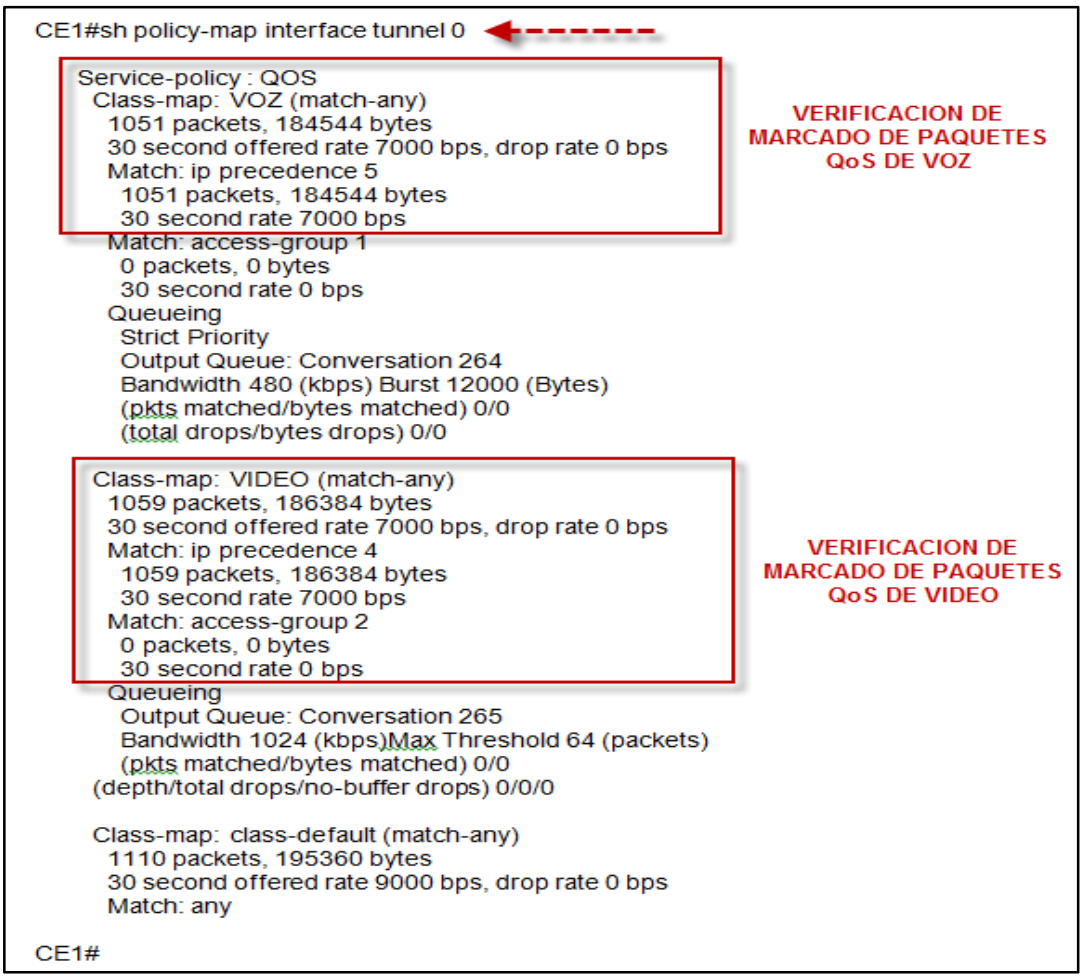


Figura 55. Verificación de paquetes marcados QoS

3.25 COMPARACION DE RESULTADOS ENTRE ESCENARIOS

Para poder determinar si los mecanismos de seguridad planteados en este estudio permiten mantener los niveles de servicios de red combinados con entornos de gestión de administración seguras se realizó un estudio comparativo de encriptaciones a nivel de capa 3 entre GETVPN y VPN GRE donde se evaluó cualitativa y cuantitativamente los indicadores de las variables dependientes como son paquetes encriptados, consumo de ancho de banda, retardos y estabilidad de (QoS).

Tabla 18

Comparación de Resultados VPN GRE y GETVPN

				DATOS AL TRANSFERIR ARCHIVOS					
N°	CANTIDAD ARCHIVOS MB	DURACIÓN DE TIEMPO AL TRANSMITIR	AB (Bits por Segundo)	ENCRIPTACION GRE			ENCRIPTACION GETVPN		
				ENCAPSULAOS	DESENCAPSULADOS	VERIFICADOS	ENCAPSULAOS	DESENCAPSULADOS	VERIFICADOS
1	1 MB	0:00:26	35 K	477	477	477	249	248	248
2	2 MB	0:00:59	65 K	653	653	653	588	588	588
3	3 MB	0:01:16	70 K	807	806	806	754	754	754
4	4 MB	0:01:25	120K	948	948	948	882	882	882
5	5 MB	0:01:55	150k	999	999	999	1192	1192	1192

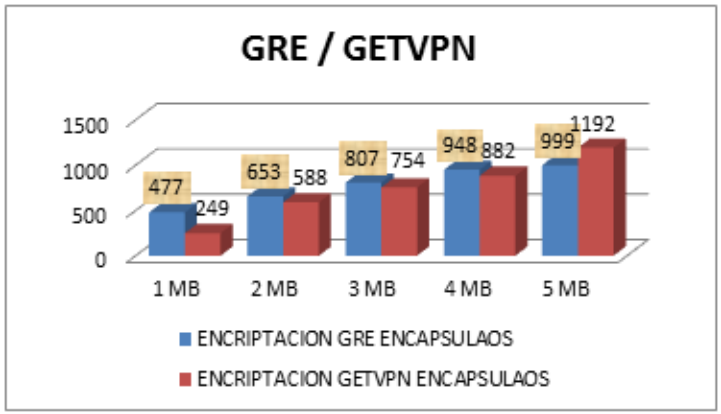
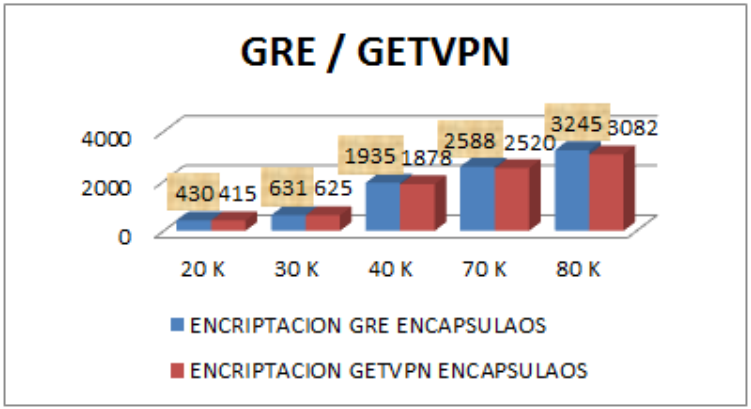


Tabla 19

Comparación de resultados VPN GRE y GETVPN Generando tráfico de Voz y Video

				DATOS DE TRAFICO DE VOZ Y VIDEO					
N°	DESCRIPCION	DURACION (Minutos)	AB (Bits por Segundo)	ENCRIPTACION GRE			ENCRIPTACION GETVPN		
				ENCAPSULAOS	DESENCAPSULADOS	VERIFICADOS	ENCAPSULAOS	DESENCAPSULADOS	VERIFICADOS
1	Voz / Video	1	20 K	430	430	430	415	415	415
2	Voz / Video	2	30 K	631	631	631	625	625	625
3	Voz / Video	3	40 K	1935	1935	1935	1878	1878	1878
4	Voz / Video	4	70 K	2588	2588	2588	2520	2520	2520
5	Voz / Video	5	80 K	3245	3245	3245	3082	3082	3082



A continuación podemos observar el rendimiento a nivel de seguridad de seguridad luego de la implementación de los mecanismos de encriptación a nivel de capa 3.

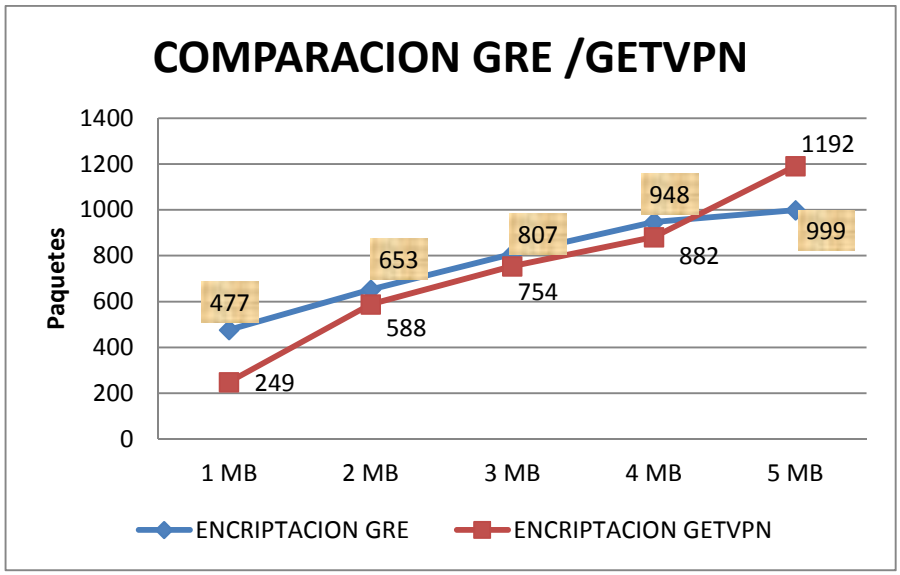


Figura 56. Comparación de Resultados de Paquetes Encriptados

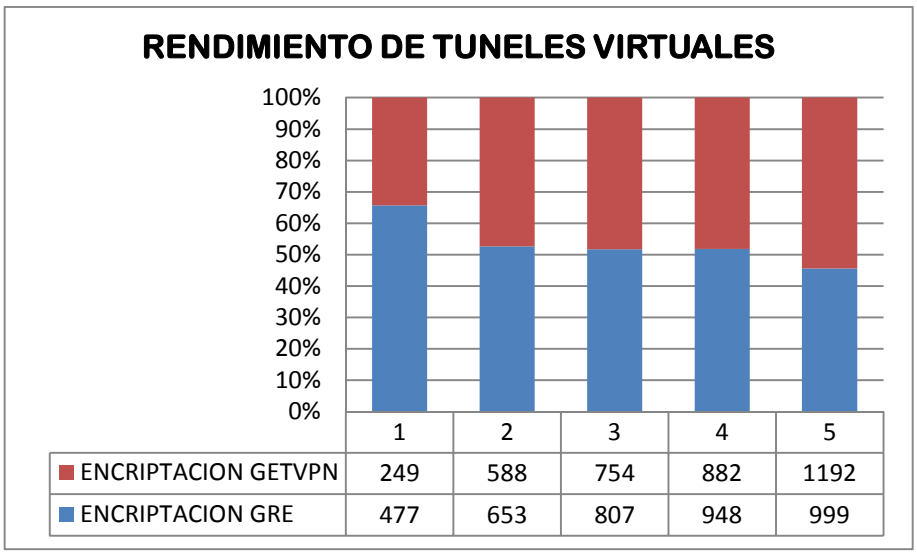


Figura 57. Rendimiento de Tunes Virtuales

Tabla 20.

Características de Tecnología de VPNs Site to Site

N°	CARACTERISTICA	GETVPN	VPN GRE	VPN - IPSec
1	Ventajas para administrar	• Integración de cifrado en IP y Multipunto a nivel de conmutación WAN (etiquetas MPLS) • Simplifica la gestión de cifrado a través del uso de grupo de claves, en lugar del uso de claves pares para enlaces punto a punto. • Permite escalabilidad de conectividad uno a uno entre sitios. • Soporta Calidad de servicio (QoS), multicas y enrutamiento.	• Permite el tráfico de multidifusión y enrutamiento a través de VPNs IPSec • Soporta QoS	• El cifrado se lo realiza entre sitios • Soporta QoS
2	Cuando usar	• Añade cifrado para MPLS preservando la conectividad any to any, así como todas las funciones de red. • Soporte un Mallado completo utilizando VPNS IPSec • Permite la participación de todos los Routers para realizar una red mallada. •	• Se usa cuando el enrutamiento debe ser apoyado a través de la implementación de VPNs	• Se utiliza cuando se requiere interoperabilidad de múltiples proveedores
3	Topología	• Se adapta a toda topología previa revisión del diseño.	• Depende de la topología en la que se requiere implementar (limitación de mallado)	• Topología Punto a punto
4	Ruteo	• Soporta conectividad punto a punto, punto multipunto, multipunto – multipunto	• Soporta	• No soporta
5	QoS	• Soporta	• Soporta	• Soporta
6	Multicast	• Soporte nativo en cada punto	• So al implementar el túnel	• No soporta
7	Seguridad	• Seguridad a nivel de direccionamiento y a través de servidor de claves	• No dispone servidor de claves	• No dispone de servidor de claves
8	Alta disponibilidad	• Se lo realiza a través de ruteo	• Se lo realiza a través de ruteo	• Se generan conmutación de errores.

De las pruebas realizadas se puede concluir que cuando se implementa VPNS GRE sobre Ipsec todo el tráfico entre sitios se encapsula en un solo paquete IP antes de ser cifrado. Esto sucede porque el paquete está compuesto de una cabecera IP, seguido por una cabecera GRE, así como también por una pila de etiquetas MPLS lo cual se especifica en el RFC3032.

Cuando un paquete es recibido por el receptor, este desencapsula el paquete mediante la eliminación de la cabecera IP y la cabecera GRE y lo procesa como cualquier otro paquete MPLS. Este procesamiento hace que exista mayor latencia y consumo de ancho de banda del canal de comunicación.

Lo contrario sucede al implementar GETVPN, ya que combina el protocolo de manipulación de dominio GDOI con encriptación IPsec para proporcionar a los usuarios un método eficiente para proteger el tráfico IP multicast o unicast.

GET VPN permite aplicar el cifrado de extremo a extremo de modo nativo y elimina la necesidad de configurar túneles punto a punto, con esto se mantiene una topología de red de mallado completo y la capacidad de la red de CORE para enrutar y replicar paquetes entre diferentes sitios preservando la fuente original y la información de las direcciones IPs de destino, así como el encabezado del paquete cifrado logrando un enrutamiento que la trasmisión de datos sea más rápida, eficiente y segura.

3.26 ESTUDIO DE FACTIBILIDAD DE IMPLEMENTACION

Tomando en cuenta los tipos de conexiones más usadas para realizar túneles VPNs, y para sustentar la investigación realizada, la solución viable y escalable que se recomienda implementar para eliminar los túneles punto a punto, es la utilización de la tecnología de conectividad multipunto, con la cual se garantiza escalabilidad, funcionalidad, administración y sobre todo seguridad.

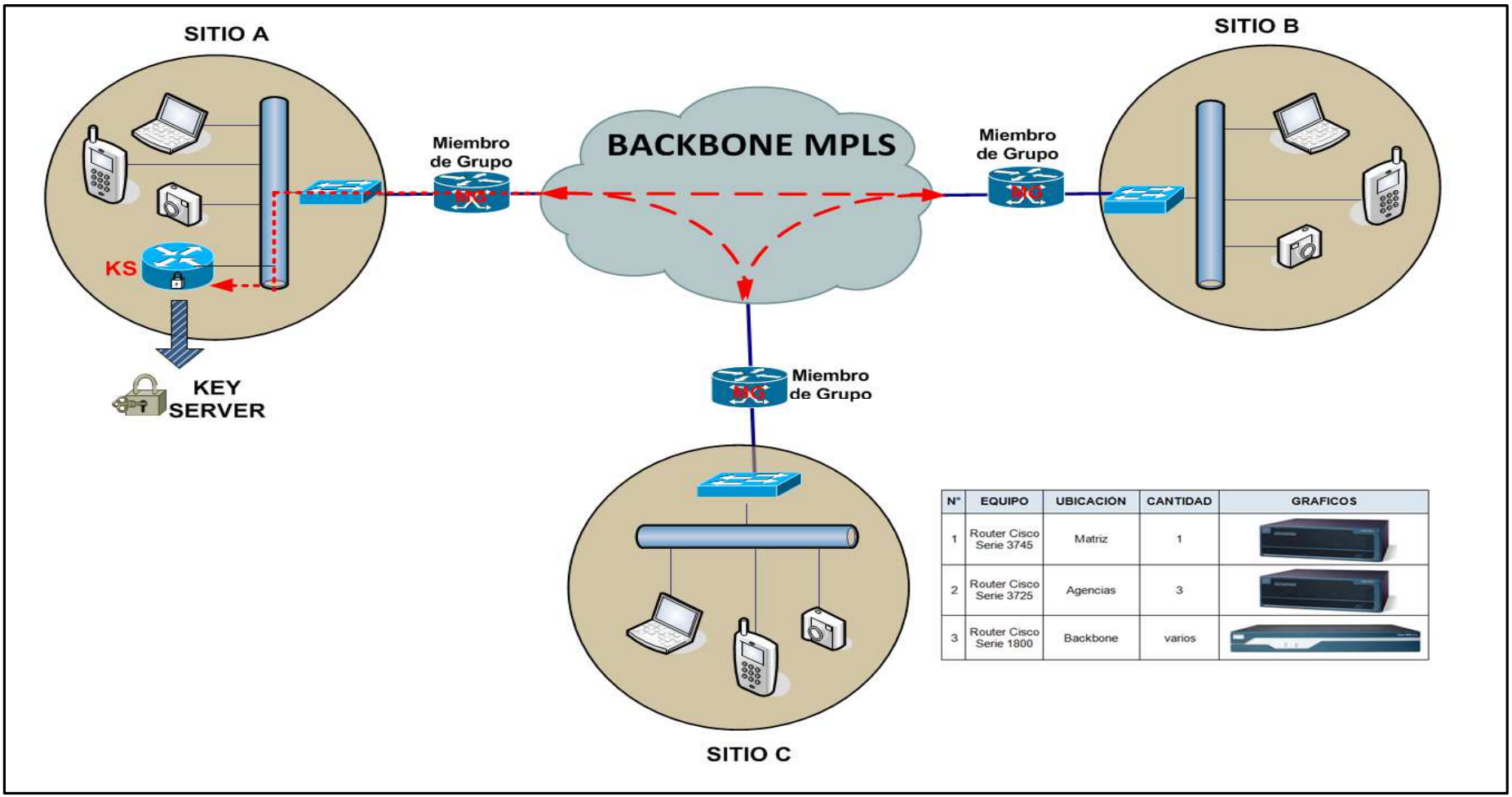
La tecnología planteada puede ser implementada sobre cualquier infraestructura de comunicación WAN que ya esté en producción, minimizando los efectos de migración que pueden darse, así como reutilizando el equipamiento activo y en algunos casos puntuales el remplazo de estos para garantizar la continuidad de la operatividad de la red.

Con estos antecedentes y tomando en cuenta la topología propuesta en el presente capitulo, los equipos a utilizarse serían:

Tabla 21

Equipos a ser utilizados en la solución

N°	EQUIPO	UBICACIÓN	CANTIDAD	VERSION DE IOS
1	Router Cisco Serie 3745	Matriz	1	c3745-advipservicesk9-mz124-15
2	Router Cisco Serie 3725	Agencias	3	c3725-advipservicesk9-mz124-15



N°	EQUIPO	UBICACIÓN	CANTIDAD	GRAFICOS
1	Router Cisco Serie 3745	Matriz	1	
2	Router Cisco Serie 3725	Agencias	3	
3	Router Cisco Serie 1800	Backbone	varios	

Figura 58. Topología Propuesta.

3.27 SELECCIÓN DE TECNOLOGIA VPN

A continuación se detalla las características del equipamiento utilizado en la emulación realizada.

Tabla 22

Especificaciones Técnicas de Equipamiento

Características		
1	Conectividad Integrada Lan/Wan	Más Nm Y Ranuras Hdsm Disponible Para Agregar Servicios En El Futuro • Combinación De Los Objetivos Y Wic Junto Con Nms / Hdsms Da Mayor Flexibilidad Para Crear Nuevas Configuraciones Como Los Requisitos De Cambio
2	Configuración De Seguridad y Vpns	Dispone De Características De Prevención De Intrusos (Ips). Asi Mismo El Sistema Operativo Permite La Creación De Vpns Con Características De Cifrado. (c3745-advipservicesk9-mz124-15)
3	Cisco IOS Software	Permite Soluciones Extremo A Extremo Con Soporte Completo Para Qos Basados En IOS De Cisco, Gestión De Ancho De Banda Y Los Mecanismos De Seguridad
4	Procesador	350-Mhz Pmc-Sierra Rm7000a Risc Processor
5	Sdram	128–256 Mb
6	Nvram	152 Kb
7	Boot Rom	704 Kb
8	Protocolo De Interconexión De Datos	Ethernet, Fast Ethernet
9	Administración	1 Puerto De Consola / 1 Puerto Auxiliar
10	Algoritmo De Cifrado	Des, Triple Des, Aes
11	Normas Que Debe Cumplir	Cispr 22 Class A, En 60950, Ul 1950, Vcci Class A Ite, Iec 60950, Csa 22.2 No. 950, En55022 Class A, Fcc Part 68, Jate, Fcc Part 15, Ices-003 Class A, Cs-03, As/Nzs 3548
12	Memoria Ram	256 Mb - Sdram, 256 Mb (Instalados) / 256 Mb (Máx.) - Sdram, 128 Mb (Instalados) / 256 Mb (Máx.), 256 Mb (Instalados) / 256 Mb (Máx.)
13	Memoria Flash	32 Mb (Instalados) / 128 Mb (Máx.)
14	Velocidad De Transferencia De Datos	100 Mbps
15	Velocidad De Conexión	T-3/E-3

3.28 ANALISIS GENERAL DE COSTOS

Considerando que la funcionalidad de la propuesta realizada radica en la infraestructura de comunicación existente en cada extremo de la topología, se realizó un análisis de costos orientado al incremento de un equipo que vendrá a ser el servidor de claves (KS) y actualización de sistema operativo IOS de los equipos existentes, y de esta manera poder viabilizar la implementación de la solución propuesta en este estudio.

Los valores que se presentan a continuación son estimaciones realizadas considerando la topología presentada en la figura 3.32, estos pudieran variar dependiendo de la magnitud de la infraestructura en la cual se quiera implementar.

Para este proyecto no se consideró los costos de ampliación de memoria de los equipos routers u otros elementos que involucren su implementación a nivel de backbone, ya que estos dependerán de la topología interna que este maneje.

Tabla 23

Costos Referenciales de implementación

N°	EQUIPO	UBICACIÓN	CANTIDAD	COSTO	OBSERVACION
1	Router Cisco Serie 3745	Matriz	1	6000	Reemplazo por equipo existente
2	Router Cisco Serie 3725	Agencias	3	0	Equipo existente, solo actualización de IOS
3	Soporte Técnico		1	1000	implementación (configuración)

Uno de los factores que se tomó en cuenta en este proyecto es el tiempo de implementación, que al igual que los costos, este dependerá de la magnitud, seguridad y alcance que se requería brindar a la infraestructura de comunicación.

CONCLUSIONES:

- Luego de terminado el proyecto, se puede concluir que se cumplieron con los objetivos e hipótesis propuestas para el mismo. Se llegó a diseñar una alternativa de implementación de VPNs, la cual servirá como referencia técnica por cumplir con características de confiabilidad, conectividad multipunto, seguridad y escalabilidad.

- Se analizó que la tecnología GETVPN es una alternativa totalmente viable para ser implementada sobre una infraestructura WAN / MPLS multipunto, logrando mantener los niveles de Calidad de Servicios y Convergencia.

- Los resultados obtenidos demuestran que los protocolos IPSec y MPLS son muy estables al momento de intercambio de información, manteniendo su integridad, confidencialidad, autenticidad y calidad de servicio, proporcionando una buena alternativa de solución a todas las empresas que requieran implementar seguridades en CAPA 3.

- Es importante efectuar la debida verificación de IPSec y MPLS, cuando se configura estos protocolos sobre la infraestructura de comunicación, así como realizar las pruebas de intercambio de información entre los sitios donde se requiera el servicio.

- De las soluciones evaluadas se puede concluir que la implementación de GETVPN es la más idónea por poseer características óptimas de configuración, implementación y administración, lo cual hace que esta tecnología debe ser considerada por los administradores de red para la migración en un corto o mediano plazo.

- La Calidad de Servicio en la topología GETVPN es más eficiente en comparación a VPN GRE, puesto que los recursos de red son distribuidos de mejor manera priorizando solo el tráfico marcado con lo cual también se optimiza los recursos de los equipos de comunicación

- Considerando que la encriptación en GETVPN se la realiza en forma nativa por cada miembro del grupo, hace que el protocolo se seguridad IPSEC sea más eficiente ya que este solo es generado y administrado en el servidor de claves, el cual solo verifica que se respete las políticas configuradas para todo el grupo, lo contrario sucede al implementar VPN GRE ya que el IPSEC debe ser configurado en cada túnel habilitado.

RECOMENDACIONES

- Cuando se requiera implementar seguridades a nivel de capa 3 se recomienda a la hora de escoger una solución ya sea basada en hardware o software se analice aspectos como: número de usuarios, ancho de banda y calidad de servicio.

- Se recomienda cuantificar el ancho de banda para cada sitio, para logra soportar todo el tráfico de red que por este fluya.

- Se debe evitar la utilización de algoritmos de encriptación sencillos ya que son más fáciles de descifrar.

- Debido a la gran cantidad de topologías de red, y estructuras internas de cada empresa se recomienda que se busque documentación del fabricante antes de realizar cualquier implementación.

- Antes de implementar GETVPN es recomendable realizar un levantamiento de información de la infraestructura de comunicación existente, así como de la topología sobre la cual se implementaría la solución. Con esto podremos tener una visión general y considerar las limitantes que se tendrían cuando se realice los trabajos.

- Se debe tener en consideración las políticas de seguridad y confidencialidad que se manejan en las empresas

- El personal que implemente la solución deberá tener conocimientos de routing y switching, así como también de mecanismos de seguridad que pudieran ser implementados en los equipos de comunicación.

TRABAJOS FUTUROS

A continuación se exponen algunos trabajos que podrían complementar el tema abordado en el presente proyecto:

- Investigar a profundidad los algoritmos de cifrado existentes y de esta manera entender su funcionamiento para buscar las mejores alternativas de integración con IPSEC.

- Investigar el protocolo de comunicación IPV6, para tener un referente acerca de las novedades y mejoras de seguridad y que estas puedan ser implementadas a nivel de Backbone y usuarios.

BIBLIOGRAFIA

[1] Superintendencia de Bancos y Seguros. (26 de 04 de 2012). *Resoluciones Superintendencia de Bancos.* Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

[2] Superintendencia de Telecomunicacones. (01 de 06 de 2013). *http://www.supertel.gob.ec/*.

[3]Revista NETWORK. (2012). *http://www.networkworld.es/home*.

[4]Current Analysis. (s.f.). *http://www.currentanalysis.com/*.

[5] Cisco System. (2006). *Cisco MPLS Fundamentals.* Indianapolis USA: Cisco Press.

[6] Cisco System. (2003). *Cisco Self-Study: Implementing Cisco IPv6 Networks (IPV6).* Indianapolis USA: Cisco Press.

[7] CERTES NERWORK. (2012). *CERTESNERWORK Proveedor de Soluciones de Seguridad*. Obtenido de http://www.certesnetworks.com/

[8] CERTES NETWOKS. (2013). *Certes TrustNet Manager*. Obtenido de http://www.certesnetworks.com/products/trustnet.html

[9] Rafael, M. T. (2006). *Diseño e Implementacion de una VPN en una Empresa Comercializadora utilizando IPSEC.* Quito: EPN. Obtenido de http://www.google.com.ec/url?sa=t&rct=j&q=dise%C3%B1o%20e%20implementaci%C3%B3n%20de%20una%20vpn%20en%20una%20empresa%20comercializadora%20utilizando%20ipsec&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fbibdigital.epn.edu.ec%2Fbitstream%2F15000%

[10] Ramirez, V. H. (2004). *Protocolos de Seguridad para Redes Privadas Virtuales (VPN).* Valdivia: UAC.

[11] Cisco System. (2008). *Network Security Technologies and Solutions.* Indianapolis, IN 46240 USA: Cisco Press.

[12]Hardjono Thomas, L. R. (2003). *Multicast and Group Security.* Norwood europe M.A: ARTHECH HAUSE INC.

[13] S. Deering, R. H. (1998). *Internet Protocol, Version 6 (IPv6)*

Specification. New York USA: IETF.

[14] Saldana, E. (29 de Noviembre de 2011). *Cisco Support Community*. Obtenido de https://supportforums.cisco.com/docs/DOC-20873

[15] Northcutt, S. (2003). *Inside Network Perimeter Security.* Estados Unidos: New Riders.

[16] S. Deering, R. H. (1998). *Internet Protocol, Version 6 (IPv6) Specification.* New York USA: IETF.

[17]John William Evans, C. F. (2010). *Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice.* San Francisco: MORGAN KAUPMANN.

[18] Khan, M. A. (2009). *Building Service-Aware Networks: The Next-Generation WAN/MAN.* Indianapolis USA: Pearson Education.

[19] Saldana, E. (29 de Noviembre de 2011). *Cisco Support Community*. Obtenido de https://supportforums.cisco.com/docs/DOC-20873

[20] Riodriguez, M. A. (1 de Mayo de 2002). *NetworkWord*. Obtenido de http://www.networkworld.es/MPLS:-Ventajas-para-las-empresas/seccion-/articulo-134391

[21] IETF Tools. (14 de 11 de 2013). *IETF-related tools, standalone or hosted on tools.ietf.org*. Obtenido de http://tools.ietf.org/html/draft-rosen-mpls-in-ip-or-gre-00