PROPUESTA DE DESARROLLO E IMPLEMENTACIÓN PRÁCTICA DE LABORATORIO GET VPN PARA LA EMPRESA CLARO COLOMBIA S.A.

JOSÉ FERNANDO SÁNCHEZ ESCOBAR

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2015

PROPUESTA DE DESARROLLO E IMPLEMENTACIÓN PRÁCTICA DE LABORATORIO GET VPN PARA LA EMPRESA CLARO COLOMBIA S.A.

Presentado Por:

JOSÉ FERNANDO SÁNCHEZ ESCOBAR
2115159

Proyecto de Pasantía para optar el Título de Ingeniero de Telecomunicaciones

Dirigido por:

ING. IVAN EDUARDO DIAZ PARDO

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2015

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma Ingeniero
Iván Eduardo Díaz Pardo
Tutor Asignado

_____
Firma del jurado

Bogotá 6 Mayo de 2015

RESUMEN

Esta monografía presenta el desarrollo e implementación práctica de un laboratorio GET VPN, para el uso del personal del NOC corporativo de la compañía CLARO COLOMBIA S.A., haciendo uso de guías, manuales, parámetros y procedimientos de configuración relacionados, dentro de la operación del NOC.

Group Encrypted Transport, (GET VPN), permite cifrar tráfico generado entre dispositivos como switches y routers. Es posible crear diferentes grupos de estos dispositivos, con el fin de proteger los datos que entre ellos se transporta.

El presente trabajo, implementa una topología sencilla y propia de muchos de los clientes de CLARO, haciendo uso de dispositivos proporcionados por la misma empresa, y que se encuentran en el laboratorio de la sede Ortezal, sin afectar el desempeño normal de la red de CLARO. Actualmente, muy pocos ingenieros tienen conocimiento en este tema, por lo que para ellos, puede ser de gran ayuda para su aprendizaje, además de estudiar comandos y troubleshooting de una solución como esta.

Palabras Claves

Cifrado, conectividad, configuración, GET VPN, Group Member, IPSec, Key Server, Troubleshooting.

ABSTRACT

This monograph presents the development and practical implementation of a laboratory GET VPN, for the use of corporate NOC staff of the company CLARO COLOMBIA S.A., using guides, manuals, parameters and procedures related configuration, within the operation of the NOC.

Group Encryption Transport (GET VPN), allows encrypting traffic generated between devices such as switches and routers. It is possible to create different groups of these devices, in order to protect the data that are transported between them.

This paper implemts a simple topology and similar of many CLARO's customers, doing use of devices supplied by the same company, without affecting normal network CLARO performance. Currently, very few engineers are knowledgeable in this subject, so this document can be helpful for learning of them, besides studying commands and troubleshooting of a solution like this.

Keywords

Connectivity, configuration, Encryption, GET VPN, Group Member, IPSec, Key Server, Troubleshooting.

TABLA DE CONTENIDOS

TABLA DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1
Introducción a la Investigación

Este capítulo contiene el planteamiento del problema, los objetivos y justificación de la propuesta de desarrollo e implementación práctica de laboratorio GET VPN para la empresa CLARO COLOMBIA S.A.

INTRODUCCIÓN

Desde tiempos remotos, el hombre sintió la necesidad de comunicar sus pensamientos e interactuar con otros para su propia supervivencia. En un principio, bastaba con comunicarse de manera presencial con otros, por medio de la voz. Pero, con el pasar del tiempo y la interacción con personas que habitaban otras poblaciones, se hizo necesario idear otras formas de comunicación que permitieran entablar conversaciones sin necesidad de usar la voz. Fue allí, cuando la comunicación escrita se desarrolló. De esta manera, era posible enviar mensajes a otras personas que se encontraban distantes del emisor. Las condiciones necesarias para recibir el mensaje, consistían simplemente en que se asegurara la entrega del mensaje al receptor, y que este tuviera las facultades para leerlo.

En un principio, debido a que la educación era una habilidad que únicamente podían desarrollar las personas adineradas, era posible proteger el contenido del mensaje, de personas que no debían saber de su contenido. Pero, con el tiempo y el progreso de la humanidad, muchas personas sabían leer por lo que transmitir un mensaje escrito no era del todo fiable. Es allí, cuando por primera vez se detecta la necesidad de cifrar un mensaje para que únicamente el transmisor y el receptor del mismo puedan leerlo. Se generan todo tipo de algoritmos para cifrar los mensajes y garantizar su recepción de manera segura.

Es así como, con el avance de la tecnología el mundo de las comunicaciones avanza a pasos agigantados creando distintas maneras de enviar mensajes y la forma como son recibidos. En todos los ámbitos de la sociedad, van surgiendo diferentes necesidades relacionadas con la forma como requieren comunicarse con los demás. Se crean compañías dedicadas a diferentes actividades económicas y estas van requiriendo poco a poco mayor comunicación entre sus áreas internas y con otras compañías.

El sector de la tecnología, permite a las compañías modernizar su infraestructura y garantizar su comunicación. Pero, tal y como surgió desde tiempos remotos se ha hecho

imprescindible realizar esta comunicación de manera segura, garantizando que la transacción de información sea privada y esté lejos del alcance de personas inescrupulosas.

De esta manera, este trabajo profundiza en el tema de cifrado y protección de la información que es compartida a través de los dispositivos de red más utilizados actualmente por todas las compañías, por medio de una serie de configuraciones que permite a la marca CISCO, ofrecer GET VPN como alternativa para la creación de grupos en los que se asignan estos dispositivos de red, para garantizar una comunicación cifrada entre los mismos.

1.1 PLANTEAMIENTO DEL PROBLEMA

CLARO, es una compañía multinacional, subsidiaria de América Móvil, el proveedor líder de servicios de telecomunicaciones en América Latina con operaciones en 18 países del continente americano y del Caribe. Se caracteriza por incorporar personal joven para el desarrollo de sus actividades, y de esta manera garantizar un crecimiento profesional para aquellos jóvenes sin experiencia laboral.

Como proyecto a desarrollar en el NOC Corporativo, existe la necesidad de profundizar en el conocimiento de GET VPN, puesto que actualmente este tipo de solución está siendo implementada en clientes corporativos que manejan temas transaccionales (entidades bancarias, empresas aseguradoras, almacenes de cadena, entre otros) y requieren seguridad en el manejo de la información, además de que los ingenieros que realizan soporte a este tipo de empresas en esta área, no tienen el conocimiento para realizarlo adecuadamente.

Para que el cifrado de información transmitida entre los dispositivos de red funcione adecuadamente, se requiere de una buena configuración de los mismos y de un amplio conocimiento en el tema GET VPN por parte de los ingenieros del NOC, encargados de prestar soporte.

Dentro del NOC corporativo existe un proceso de capacitación del personal, el cual pretende brindar a los ingenieros que prestan soporte todas las herramientas necesarias para cumplir con sus funciones y actividades dentro del cargo. Con el fin de complementar estas capacitaciones, y de satisfacer la necesidad que requiere el NOC Corporativo con respecto al tema GET VPN, se plantea el desarrollo e implementación práctica de un laboratorio GET VPN.

De acuerdo a lo descrito anteriormente, este trabajo pretende dejar como resultado además de la parte de investigación, una guía práctica donde se evidencie el proceso de configuración GET VPN realizado sobre equipos reales similares a los de un cliente, y que quedaran en el laboratorio Ortezal para su uso y capacitación del personal.

1.2 JUSTIFICACIÓN

El NOC corporativo y CLARO S.A. buscan garantizar y mejorar la calidad de los servicios ofrecidos. Con el transcurrir del tiempo y los avances que se van teniendo respecto a tecnología, las empresas requieren mejorar su infraestructura tecnológica y adquirir nuevos servicios que les permitan suplir sus necesidades. Para brindar nuevos servicios a los clientes, CLARO debe hacer una inversión, no solo a nivel de infraestructura en su red, sino de capacitación del personal que presta soporte.

CLARO S.A al tener una gran cantidad de clientes corporativos debe estar en la capacidad de brindar en sus servicios un alto nivel de disponibilidad y seguridad, ya que muchos de sus clientes como entidades bancarias, aseguradoras, entre otros, manejan temas transaccionales. Actualmente, una solución que brinda CLARO S.A. a los clientes que requieren más seguridad en su red y en el manejo de la información se llama GET VPN, esto permite además de una alta disponibilidad en el servicio, cifrar información y evitar intrusos que quieran acceder a la red.

Sabiendo la necesidad que tiene el NOC corporativo de tener sus ingenieros capacitados en el tema GET VPN, se plantea el desarrollo e implementación práctica de un laboratorio GET VPN, permitiendo a los ingenieros del NOC fortalecer su conocimiento técnico en esta área, ya que podrán aprender comandos, configuraciones y troubleshooting[1], dándoles una capacidad de ser más eficientes a la hora de solucionar fallas relacionadas con ese tipo de configuraciones. Los clientes apreciarán un soporte más eficiente y confiable por parte de los Ingenieros, los tiempos de solución de fallas de este tipo disminuirán y la calidad del servicio mejoraría.

La realización de este trabajo es un referente para futuros laboratorios que deseen implementar en el NOC corporativo, y que ayuden a capacitar los ingenieros de forma teórico - práctica en nuevas temáticas; además de ser útil para otros operadores que prestan servicio de telecomunicaciones, y requieren fortalecer el tema GET VPN.

[1] **troubleshooting: Serie de pasos que permiten identificar una falla rápidamente.

1.3 HIPÓTESIS Y OBJETIVOS

Por medio de la realización de un laboratorio, es posible estudiar diferentes alternativas para dar solución a problemas que se presentan diariamente en muchas áreas de la Ingeniería. Para el caso de una compañía de Telecomunicaciones como CLARO, la cual debe ser líder en el uso de técnicas más eficientes y seguras para el manejo de la información de sus clientes, se hace imperativo profundizar en el conocimiento de GET VPN. El laboratorio que se plantea, permitirá a los ingenieros del NOC Corporativo, aclarar sus inquietudes respecto a las configuraciones de GET VPN, permitiendo así dar solución a diversos tipos de fallas que se presentan relacionadas con este tema y que afectan a los clientes de CLARO.

Pregunta Problema:

¿Qué tipo de laboratorio sobre GET VPN se puede implementar en el NOC corporativo de CLARO S.A. para facilitar el aprendizaje y capacitación de los ingenieros que brindan soporte a empresas que tienen instalado este tipo de servicio?

1.3.1 Objetivo General

Desarrollo e implementación de un laboratorio GET VPN en la empresa CLARO Soluciones Fijas que permita profundizar el conocimiento técnico actual de los ingenieros del NOC para mejorar el soporte a clientes que utilicen el servicio.

1.3.2 Objetivos Específicos

- Seleccionar los equipos necesarios para la implementación de un laboratorio GET VPN.
- Realizar el estudio de redes MPLS y configuración CISCO (GET VPN) que permitan realizar pruebas básicas de su implementación en dispositivos de red.
- Realizar configuraciones sobre los equipos de laboratorio (switch – router) que permitan mediante análisis y pruebas, comprobar el funcionamiento de la red GET VPN.
- Hacer pruebas de configuración que permitan verificar el cifrado de información.
- Desarrollar una guía práctica que ayude a los ingenieros del NOC corporativo a la familiarización con la solución GET VPN.
- Presentar ante la empresa CLARO la documentación obtenida por medio del desarrollo del laboratorio GET VPN, con el fin de ser evaluada.

1.4 CRONOGRAMA

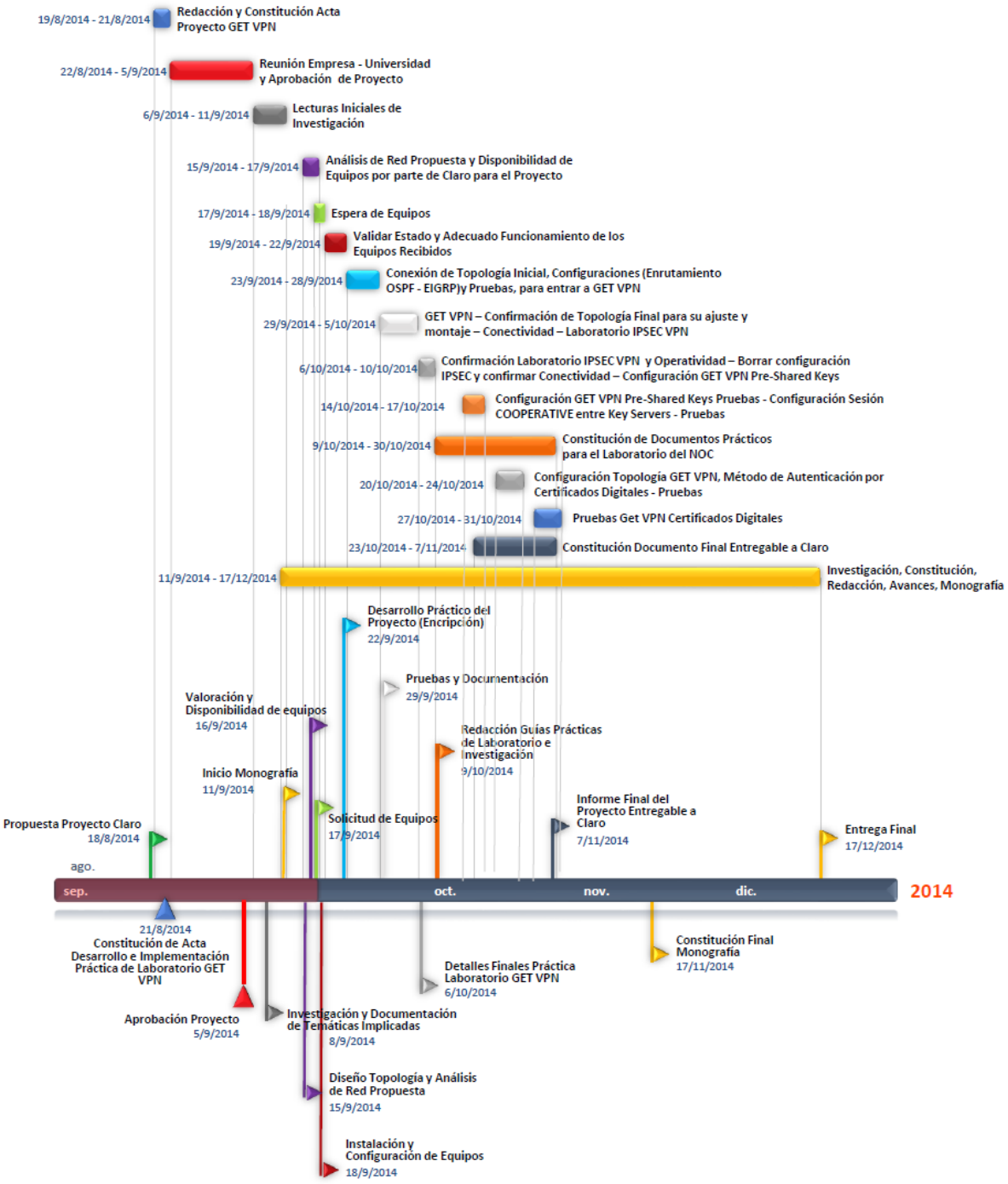

Figura 1 Cronograma Actividades

CAPÍTULO 2

Marco Teórico

El capítulo que se desarrolla a continuación tiene conceptos y fundamentos teóricos que soportan la propuesta de desarrollo e implementación práctica de laboratorio GET VPN para la empresa CLARO COLOMBIA S.A.

2.1 CLARO

Empresa multinacional destacada a nivel mundial en el sector de las Telecomunicaciones, provee servicios de telefonía fija y celular, banda ancha e internet, televisión, entre otros. Claro es una compañía "subsidiaria de América Móvil, el proveedor líder de servicios de telecomunicaciones en América Latina con operaciones en 18 países del continente americano y del Caribe."

Figura 2 Claro Colombia SA
Tomado de http://www.claro.com/paises/

Además Claro como indica en su portal web posee "Un excelente conocimiento de la región... Una sólida estructura de capital... Eficiencia que se sustenta en nuestra vasta experiencia operacional... Esto nos ha permitido consolidar nuestra posición como la empresa líder en el sector de telecomunicaciones móviles de América Latina y la cuarta más grande del mundo en términos de suscriptores proporcionales" [2]

Cabe resaltar que Claro Colombia S.A. en el año 2012, es el resultado de la fusión de dos empresas muy importantes del sector de las telecomunicaciones en Colombia, Comcel (Comunicación Celular S.A.) y Telmex Colombia S.A.

[2] Tomado de: http://www.claro.com

2.2 GET VPN

Group Encrypted Transport VPN (GET VPN) es una tecnología implementada en redes privadas o MPLS (*Multiprotocol Label Switching)*, que no requiere la negociación de túneles punto a punto para establecer un camino adecuado y lograr el cifrado de datos. Establece un nuevo concepto, por medio de la creación de grupos de confianza.[3]

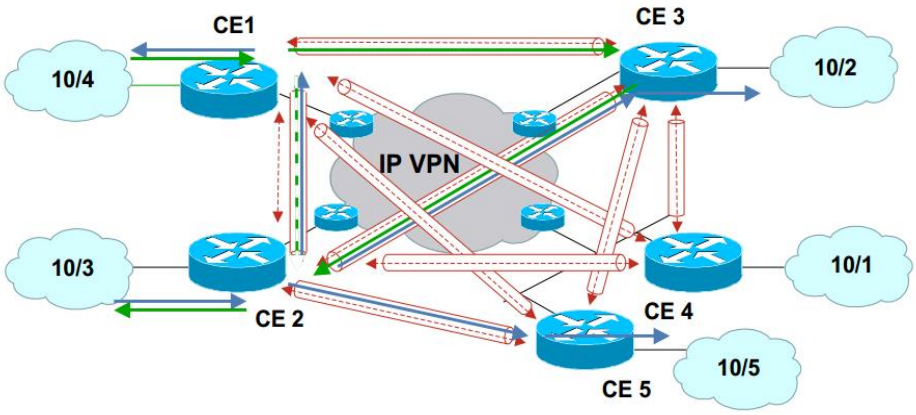

Figura 3 Ipsec túneles punto a punto
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

2.2.1 Estructura y Topología GET VPN

La tecnología GET VPN está basada en estándares patentados por Cisco. Aprovecha tecnologías existentes previamente como IKE (*Internet Key Exchange*), IPsec (*Internet Protocol security*) y multicast que ya existen. Una solución GET VPN se fundamenta en una estructura básica, configurada por bloques; por lo cual requiere de cada una de sus partes para que cumpla con su funcionalidad.

Estos son los bloques principales que hacen parte de la estructura y *topología GET VPN: GDOI (RFC 6407), Key servers (KSs), Cooperative (COOP) KSs, GMs, IP tunnel header preservation, Group security association, Rekey mechanism, Time-based anti-replay (TBAR).*

[3]http://www.cisco.com/c/en/us/products/security/group-encrypted-transport-vpn/index.html

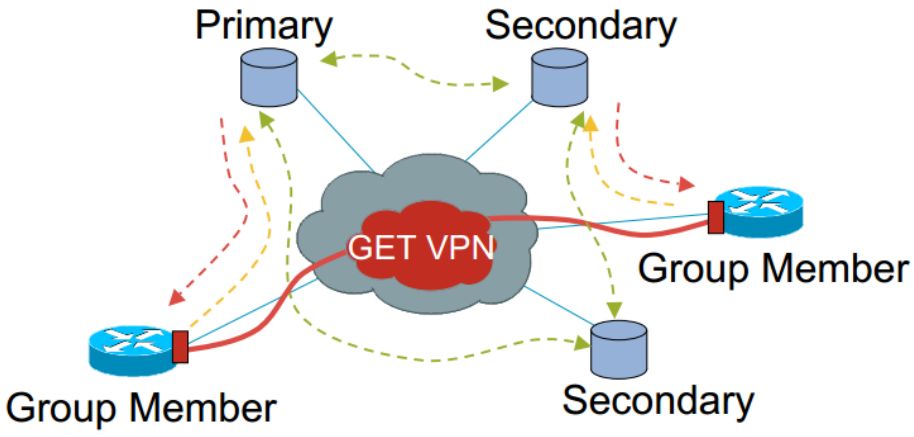

Figura 4 Topología básica tecnología GET VPN
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

2.2.2 Modo de Operación GET VPN

2.2.2.1 GDOI (Group Domain of Interpretation)

Dominio de Interpretación (GDOI) es un protocolo que maneja las llaves del grupo y está basado en la RFC 3547. Es empleado para distribuir y mantener las llaves del Grupo.

Este protocolo se encuentra protegido por la fase 1, *Internet Key Exchange (IKE)*, lo que quiere decir, que todos los participantes en el grupo, deben autenticarse en el dispositivo que está generando las llaves *IKE*. Dos de los métodos de autenticación más comunes son llaves pre compartidas *(PSK - Pre-Shared Key)* y llaves públicas *(PKI - Public Key Infrastructure).* Cuando la llave proporcionada ha expirado *(IKE)*, *GDOI* actualiza los miembros del grupo *(GMS)*.

GDOI tiene la capacidad de generar dos llaves de cifrado diferentes. Una llave es la encargada de asegurar el plano de control *GET VPN*, llamada *KEK*; y la otra se encarga de cifrar el tráfico de los datos, llamada *TEK*.[4]

[4]http://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_version_1_0_External.pdf

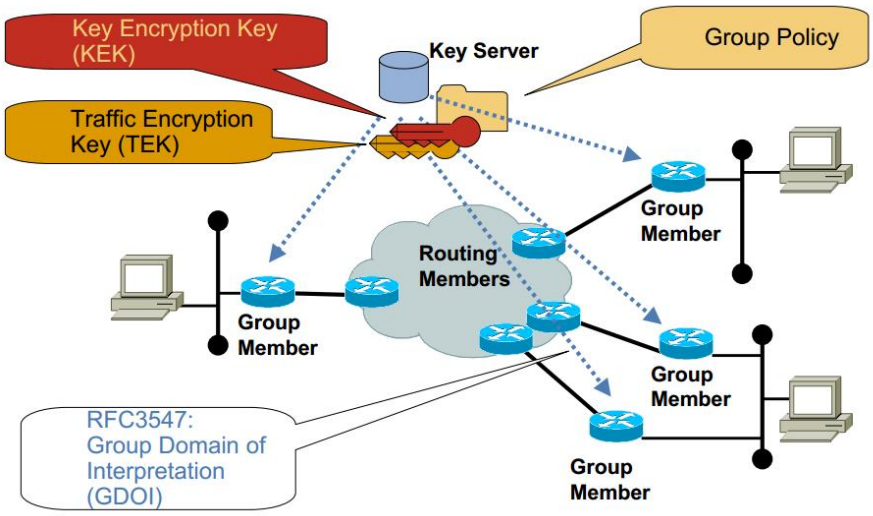

Figura 5 GDOI llaves de cifrado
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

GDOI introduce dos llaves de cifrado diferentes. Una de las llaves asegura el plano de control GET VPN; la otra llave asegura el tráfico de datos. La llave se utiliza para fijar el plano de control se llama comúnmente la clave de cifrado de claves (*KEK - Key Encryption Key*), y la clave utilizada para cifrar el tráfico de datos se conoce como clave de cifrado de tráfico (*TEK - Traffic Encryption Key*).

2.2.2.2 Key Servers (KSs)

Un servidor de llaves, es un dispositivo IOS que tiene como finalidad crear y mantener el plano de control GET VPN. En él, son definidas todas las políticas de cifrado: tráfico interesante, protocolos, asociaciones de seguridad, cifrados temporales, entre otros.

Después de haber definido las políticas de cifrado, estas son transmitidas a todos los GMs en el momento en que realiza la autenticación *figura 6 -A*. Esta autenticación de GMs se realiza mediante la fase 1 (IKE) por PSK o PKI, permitiendo descargar las políticas de cifrado y las llaves requeridas para el funcionamiento GET VPN *figura 6 -B*. El Key Server debe renovar llaves y distribuirlas de nuevo a las GMs *figura 6 -C*.

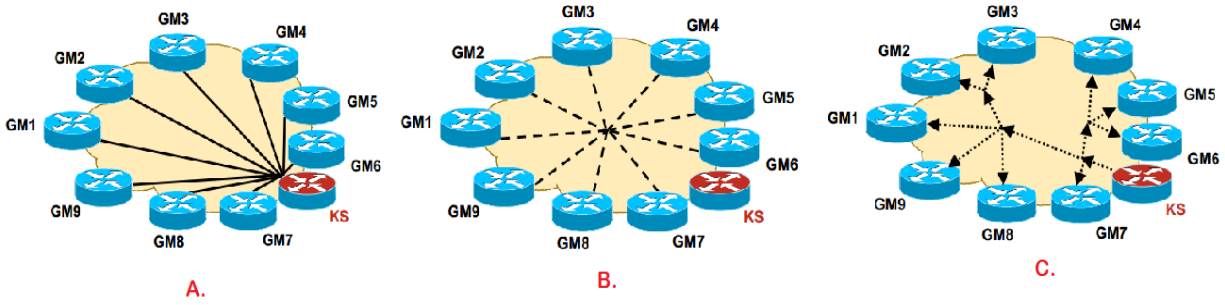

Figura 6 Registro de Group Members con Key Server
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

Debe aclararse que un dispositivo que está funcionando como Key Server, no podrá ser configurado como GM.

2.2.2.3 Group Members (GMs)

Un Group Member, es un dispositivo IOS responsable de manejar el plano de datos GET VPN, con la capacidad de cifrar y descifrar el tráfico que está pasando por él en tiempo real.

Un GM es configurado con la fase 1 IKE, las políticas de cifrado son descargadas directamente desde el Key Server a la hora del GM autenticarse contra el KS como se mencionó anteriormente.

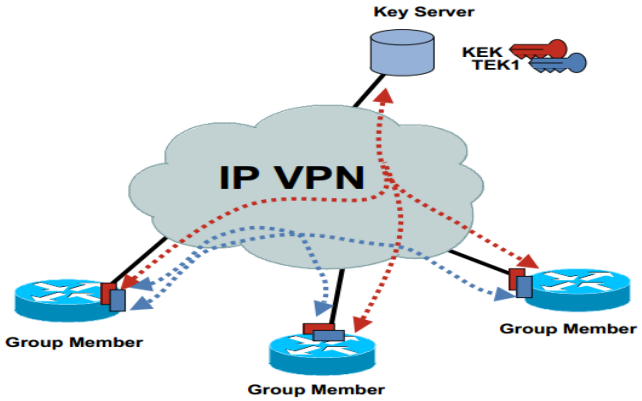

Figura 7 Autenticación Group Members
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

Al descargarse las políticas de cifrado desde el Key Server, el GM ya está en la capacidad de decidir qué trafico debe cifrar y cuál no.

2.2.2.4 Group Security Association – Group S A

GET VPN al hacer uso del concepto Grupo SA, se diferencia del tipo de cifrado IPsec. Mediante el Grupo S A, todos los miembros que pertenecen al grupo GET VPN, pueden y deben tener comunicación entre sí por medio de una política de cifrado común y una asociación de seguridad (S A), lo que permite evitar IPsec entre los GMs, reduciendo la carga de los recursos de los routers que actúan como GMS.[5]

2.2.2.5 Rekey Mechanism

El mecanismo de Rekey se lleva a cabo en el Key Server, pues este dispositivo debe actualizar las llaves generadas y distribuirlas nuevamente a los GMs. Rekey es el proceso de regenerar las llaves, y distribuirlas nuevamente, antes de que las llaves existentes expiren.

Hay dos tipos de mensajes que indican cambio de llaves, el unicast y el multicast.

Unicast Rekey: Es el proceso de regenerar una llave cuando el Key Server envía un mensaje de cambio de llave, envía copias del mensaje a cada GM. Los GMs regresan un mensaje de ACK (*Acknowledgement*) al Key Server indicando que el mensaje de cambio de llaves fue recibido y también indican al KS que aún se encuentran en el grupo, para no ser eliminados.

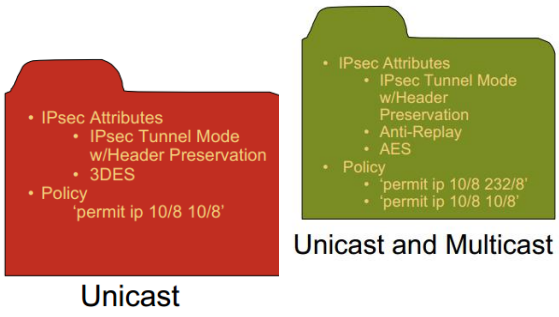

Figura 8 Métodos de Cifrado
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

[5] http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

Multicast Rekey: es el proceso de regenerar una llave mediante multidifusión, el Key Server genera un mensaje de cambio de llaves, la copia del mensaje es enviada a una dirección de grupo multidifusión ya predefinida en la configuración del KS. Cada Group Member se une al grupo multidifusión a la hora de la autenticación y es allí donde cada GM recibe el mensaje de cambio de llave. [6]

2.2.2.6 COOP KSs

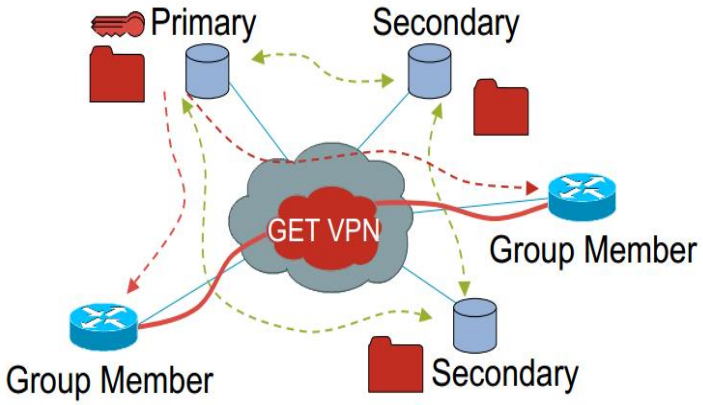

Figura 9 Sesión CooperativeFigura
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

El Key Server es el dispositivo de mayor importancia en la estructura y topología GET VPN, pues es el equipo que mantiene todo el plano de control. Si este equipo presenta una falla, la solución GET VPN deja de existir, por lo que siempre se recomienda instalar una redundancia de Key Servers de modo que, si un Key Server deja de funcionar, sea reemplazado por el de respaldo. A esta redundancia de Key Servers, se le llama sesión COOPERATIVE - COOP.

[6]http://www.cisco.com/c/en/us/products/collateral/security/group-encrypted-transport-vpn/deployment_guide_c07_554713.html

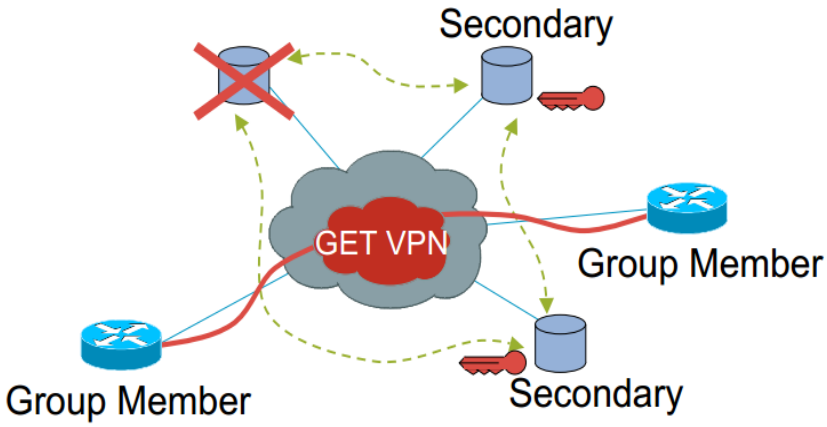

Figura 10 Key Server backup en ausencis del Key Server Principal
Tomado de: Advanced IPSec with GET VPN.
http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

Al tener más de un Key Server en la topología GET VPN, deben ser configurados en cada Group Member su prioridad y orden, con el fin de que cada Group Member sepa ante quién debe autenticarse primero, y en caso de que se presente una falla en el primer Key Server, pueda autenticarse contra el Key Server de Respaldo.

2.2.2.7 Time Based Anti-Replay

El Time Based Anti- Replay es un método para proteger los equipos de ataques de repetición. Estos pueden ser generados por algoritmos o por personas inescrupulosas que quieran causarle un daño a la red, y acceder directamente a los datos que se encuentran allí.

GET VPN hace uso de anti–repetición (denegación de servicio) respecto al tiempo (TBAR), esta se basa en un reloj de pseudo que se encuentra siempre en el KS. El Key Server principal será el único responsable de establecer y mantener el tiempo de pseudo para un grupo. Cada que el KS distribuye las llaves nuevamente a los GM, se mantienen los pseudotiempos sincronizados, esto se hace por defecto cada 7200 segundos.

2.2.3 Dispositivos

Los siguientes dispositivos fueron utilizados para la elaboración del laboratorio:

ROUTER CISCO 1905

Figura 11 Router CIsco 1905
Tomado de: http://www.cisco.com/c/dam/en/us/products/routers/1905-serial-integrated-services-router-isr/data_sheet_c78-598372.pdf

Tabla 1 Beneficios y descripciónes C1905

BENEFICIOS	DESCRIPCIÓN
Integración de Servicios	El Router Cisco 1905 ofrece niveles incrementados de integración de servicios como datos, seguridad, conexión inalámbrica y servicios de movilidad, permitiendo eficiencias más altas y ahorro de costos.
Servicios por demanda	Una imagen del Sistema Operativo IOS simple y universal es instalada en cada Cisco ISR G2. Esta imagen contiende toda la tecnología del Software Cisco, el cual puede ser activado con una licencia, permitiendo descargar características avanzadas sin necesidad de descargar una nueva imagen de Sistema Operativo. Adicionalmente, este modelo tiene incluida una memoria más grande que soporta las nuevas funcionalidades.
Alto desempeño con Servicios Integrados	El Router Cisco 1905 permite realizar despliegues de alta velocidad en ambientes WAN con servicios concurrentes que manejan más de 10Mbps.

Tabla 2 Características Arquitectónicas y Beneficios C1905

CARACTERÍSTICA ARQUITECTÓNICA	BENEFICIOS
Plataforma Modular	Este modelo es una plataforma modular, con una interfaz serial integrada y una interfaz WAN de alta velocidad para proveer conectividad y servicios para redes con requerimientos de sucursales.
Procesadores	El Router 1905 es impulsado por procesadores multinúcleo de alto rendimiento que soporta crecientes demandas de redes con sucursales que tienen altos requerimientos de tráfico WAN.
Seguridad Embebida IP / Capas de Seguridad (IPSec/SSL) VPN aceleración de Hardware	El Hardware de aceleración de cifrado se ha mejorado para proporcionar una mayor capacidad de ampliación, lo que combinado con una licencia opcional del Sistema Operativo IOS de Seguridad, permite los servicios de seguridad y enlace VPN (IPSec y SSL).

Tabla 3 Características y descripciones C1905

CARACTERÍSTICA	DESCRIPCIÓN
Protocolos	IPv4, IPv6, rutas estáticas, Open Shortest Path First (OSPF), IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific

	Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPsec, generic routing encapsulation (GRE), Bidirectional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, Layer 2 Tunneling Protocol Version 3 (L2TPv3), 802.1ag, 802.3ah, and Layer 2 and Layer 3 VPN.
Encapsulaciones	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Manejo de Tráfico	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-B Based Application Recognition (NBAR).

	Cisco 1905 Integrated Services Router
Services and Slot Density	
Embedded hardware-based cryptography acceleration (IPsec + SSL)	Yes
RJ-45 onboard LAN 10/100/1000 ports	2
Serial port	Slot 0 (integrated HWIC-1T)
EHWIC slot	1
Memory (DDR2 DRAM): Default/maximum	256 MB/512 MB (license upgradable)
USB Flash memory: Default/maximum	256 MB/256 MB (internal)
External USB flash-memory slots (Type A)	1
USB console port (mini-Type B) (up to 115.2 kbps)	1
Serial console port (up to 115.2 kbps)	1
Serial auxiliary port (up to 115.2 kbps)	1
Integrated power supply	AC
Power-supply options	PoE (external)
Redundant power-supply support	No
Power Specifications	
AC input voltage	100-240V ~
AC input frequency	47-63 Hz
AC input current range AC power supply (maximum) (amps)	1.5-0.6
AC input surge current	<50A
Typical power (no modules)	25W
Maximum power capacity with AC power supply	60W
Maximum power capacity with PoE power supply (platform only)	70W
Maximum PoE device power capacity with PoE power supply	80W
Physical Specifications	
Dimensions (H x W x D)	1.75 x 13.5 x 11.5 in. (4.45 x 34.29 x 29.21 cm)
Rack height	1 rack unit (1RU)
Rack-mount 19 in. (48.3 cm) EIA	Optional
Wall-mount (refer to installation guide for approved orientation)	Yes
Weight: With AC power supply (no modules)	8 lb (3.175 kg)
Weight: With PoE power supply (no modules)	12.8 lb
Maximum weight: Fully configured	14 lb
Airflow	Back to side
Environmental Specifications	
Operating Condition	
Temperature: 5906 ft (1800m) maximum altitude	32-104°F (0-40°C)
Temperature: 9843 ft (3000m) maximum altitude	32-77°F (0-25°C)
Altitude	10000 ft (3000m)
Humidity	10 to 85 percent relative humidity (RH)
Acoustic: Sound pressure (typical/maximum)	32.9/58.3 dBA
Acoustic: Sound power (typical/maximum)	41.9/67.2 dBA

Figura 12 Especificaciones Técnicas Router C1905
Tomado de: file:///C:/Users/Jos%C3%A9/Downloads/data_sheet_c78-598372.pdf

SWITCH CISCO 2960

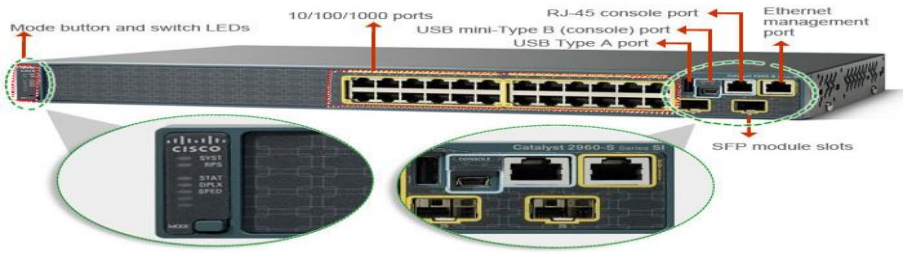

Figura 13 Switch Cisco 2960
Tomado de: http://www.router-switch.com/ws-c2960s-24ts-s-p-1518.html

Tabla 4 Desempeño y Modelos LAN base SW 2960

DESEMPEÑO Y ESCALABILIDAD	MODELOS LAN BASE
Ancho de banda de reenvío	88Gbps
Ancho de banda de conmutación	176 Gbps
Máximo de VLANs activas	255
Disponibilidad de IDs para VLAN	4000
MTU	9198 Bytes
Jumbo frame – Ethernet frame	9216 Bytes

Tabla 5 Conectores e interfaces SW 2960

CONECTORES E INTERFACES	
Ethernet Interfaces	10BASE-T ports: RJ-45 connectors, 2-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling 100BASE-TX ports: RJ-45 connectors, 2-pair Category 5 UTP cabling 1000BASE-T ports: RJ-45 connectors, 4-pair Category 5 UTP cabling 1000BASE-T SFP-based ports: RJ-45 connectors, 4-pair Category 5 UTP cabling

Tabla 6 Categoria y especificaciones SW 2960

CATEGORÍA	ESPECIFICACIÓN
Estándar	● IEEE 802.1D Spanning Tree Protocol ● IEEE 802.1p CoS Prioritization ● IEEE 802.1Q VLAN ● IEEE 802.1s ● IEEE 802.1w ● IEEE 802.1X ● IEEE 802.1ab (LLDP) ● IEEE 802.3ad ● IEEE 802.3af and IEEE 802.3at ● IEEE 802.3ah (100BASE-X single/multimode fiber only) ● IEEE 802.3x full duplex on 10BASE-T, 100BASETX, and 1000BASE-T ports

2.2.4 Valor Comercial De Dispositivos

De acuerdo a la topología básica que compone una red GET VPN y a los servicios actualmente ofrecidos sobre algunos de los clientes de CLARO, se solicitó adquirir una cantidad de equipos con ciertas características para realizar el laboratorio GET VPN de forma práctica.

El precio de los equipos que componen el proyecto, fue consultado para conocer el costo total del proyecto, con el fin de ser estudiado y aprobado por el área beneficiada (NOC Corporativo) y almacén de la compañía, encargados de suministrar equipos para los proyectos. El costo total del proyecto presentado en la *TABLA 7* es un valor aproximado, ya que éste puede depender del precio del dólar, y del lugar donde sean comprados los equipos.

Tabla 7 Precio de equipos proyecto GET VPN

CANTIDAD	REFERENCIA	VALOR
4	CISCO 1905 – SEC/k9	$7.200.000
1	C2960-24TT-L	$1.855.800
	TOTAL	$9.055.800

CAPÍTULO 3
Desarrollo de la Investigación

El siguiente capítulo da a conocer el proceso realizado durante la práctica desarrollada en la empresa CLARO COLOMBIA S.A. para llevar a cabo la propuesta de desarrollo e implementación práctica de laboratorio GET VPN.

3. METODOLOGÍA

El NOC Corporativo de la empresa Claro Colombia S.A es un área de vital importancia para la compañía, debido a que allí se presta un servicio técnico de alto nivel para la solución de fallas e incidentes que ocurren en la red y afectan a los clientes. Por esta razón, el personal que trabaja en esta área, a pesar de que cuenta con la formación técnica para la solución de las fallas presentadas, constantemente debe capacitarse en nuevas y diferentes tecnologías.

Es así como, con la necesidad de tener una constante capacitación de los ingenieros, surge el desarrollo del proyecto propuesto para la compañía CLARO.

El proyecto consistió en desarrollar una guía práctica sobre el tema GET VPN, con el fin de que los ingenieros pertenecientes al NOC Corporativo, pudieran aprender cómo configurar una solución de este tipo, y cómo realizar el troubleshooting, teniendo presente que el material a desarrollar fuese sencillo de entender.

Teniendo clara la propuesta de investigación y el proyecto a desarrollar, se dio inicio al mismo.

La metodología del proceso de investigación y desarrollo del proyecto, siempre fue apoyada por parte de los ingenieros del NOC, desde su inicio hasta el resultado final.

3.1 Diseño de topología

La topología adecuada para elaborar el proyecto, debe cumplir con los elementos principales que hacen parte de una solución GET VPN, además de ser similar a la topología instalada para las compañías de los clientes de CLARO, con el fin de realizar una simulación y un laboratorio que represente la situación actual.

La topología propuesta, plantea la estructura básica de una solución GET VPN, siendo la más utilizada en la red de CLARO para los clientes que adquieren este servicio. Esta fue aprobada por los ingenieros del NOC Corporativo.

El diseño está compuesto por cuatro routers y un switch. Dos router cumplirán la función de Key Servers, y los otros dos simularán los Group Members. El switch permitirá acceder a la topología GET VPN por medio de la red MPLS de CLARO.

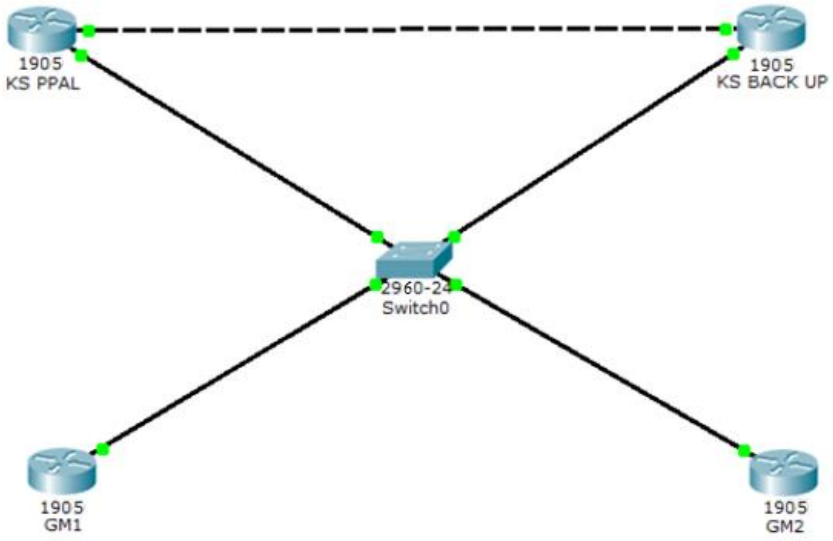

Figura 14 Topología propuesta GET VPN

3.2 DISPONIBILIDAD DE EQUIPOS

De acuerdo al diseño de la topología propuesta, y teniendo en cuenta el uso de equipos que soporten la tecnología GET VPN, se propone el uso de las siguientes referencias de la marca CISCO:

Tabla 8 Referencias de equipos utilizados en el Laboratorio GETVPN

CANTIDAD	***DESCRIPCIÓN***	***REFERENCIA***
4	Router que soporta IOS de cifrado	CISCO 1905 – SEC/k9
1	Switch Capa 2	C2960-24TT-L

La solicitud realizada al almacén de la compañía, fue aprobada y justificada por el Líder del NOC Corporativo, teniendo en cuenta que son equipos requeridos continuamente por su laboratorio y para el beneficio del área, y permiten realizar pruebas sobre la Solución GET VPN, entre otras.

Figura 15 Prueba de equipos recibidos

3.3 CONFIGURACIONES PREVIAS

Antes de realizar cualquier conexión y configurar la topología GET VPN, fue necesario elaborar algunas prácticas y laboratorios previos con el fin de reforzar conocimientos en la configuración de la marca CISCO.

Los temas a reforzar con estos laboratorios previos fueron: subnetting, conectividad de topologías cableadas, TFTP, enrutamientos OSPF, EIGRP y tecnologías IPSEC VPN. Estas configuraciones y laboratorios previos, se encuentran en el ANEXO A para mayor información.

3.4 GESTION REMOTA DE LOS EQUIPOS

La topología final y aprobada para la solución GET VPN, fue conectada e instalada en el rack del laboratorio Ortezal.

Figura 16 Conexiones Routers 1905 Topología Final GET VPN

La instalación de los equipos en el rack, permite tener los equipos conectados a la red MPLS de Claro. Esto facilita su gestión y administración a través de todos los computadores conectados en la red y que tienen instalada la herramienta putty.

Figura 17 Rack Laboratorio Ortezal

Así mismo, tener los equipos instalados en el laboratorio, permite a los ingenieros del NOC Corporativo acceder a ellos remotamente desde sus puestos de trabajo, realizar configuraciones que deseen simular, practicar y estudiar sobre el tema GET VPN.

Los procedimientos y comandos para acceder a los equipos remotamente se encuentran explicados en el ANEXO B.

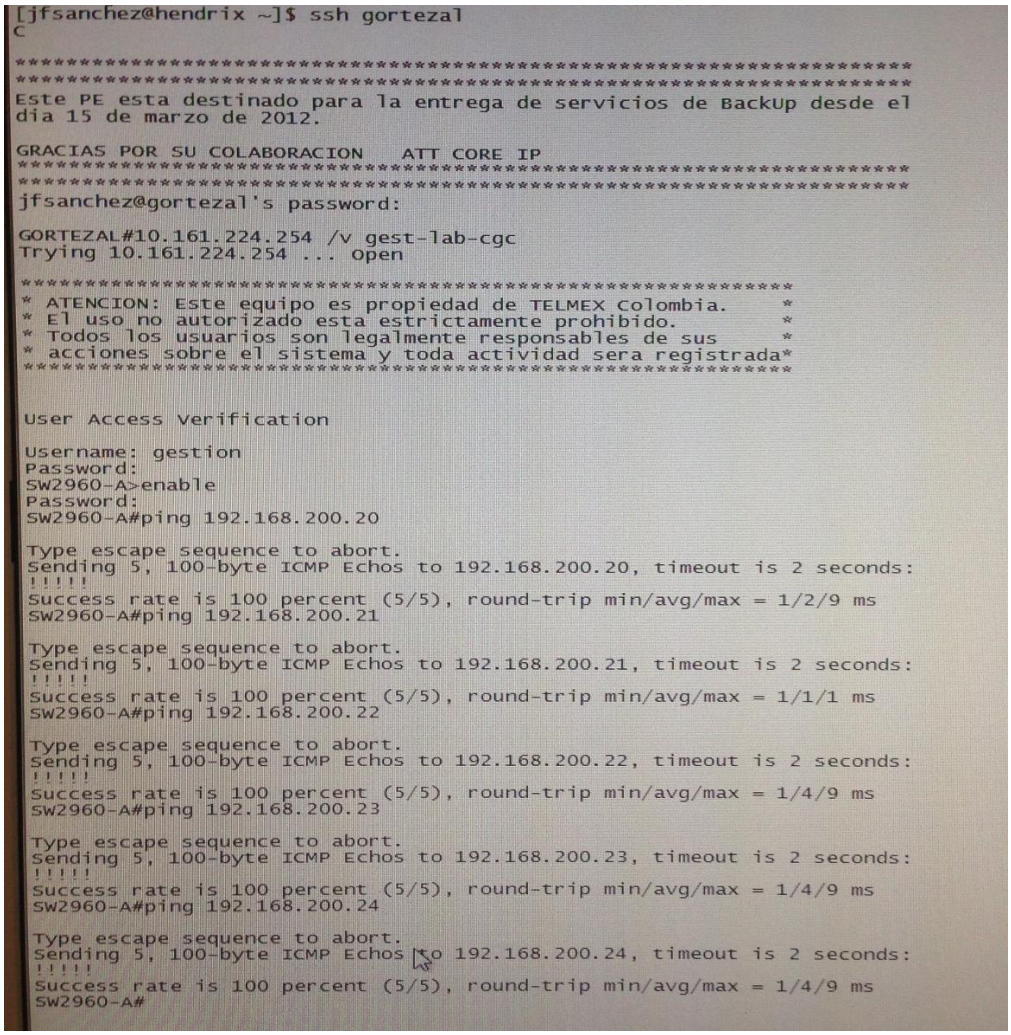

Figura 18 Acceso a los equipos desde puesto de trabajo Ing. NOC Corporativo

3.5 CONFIGURACIÓN GET VPN

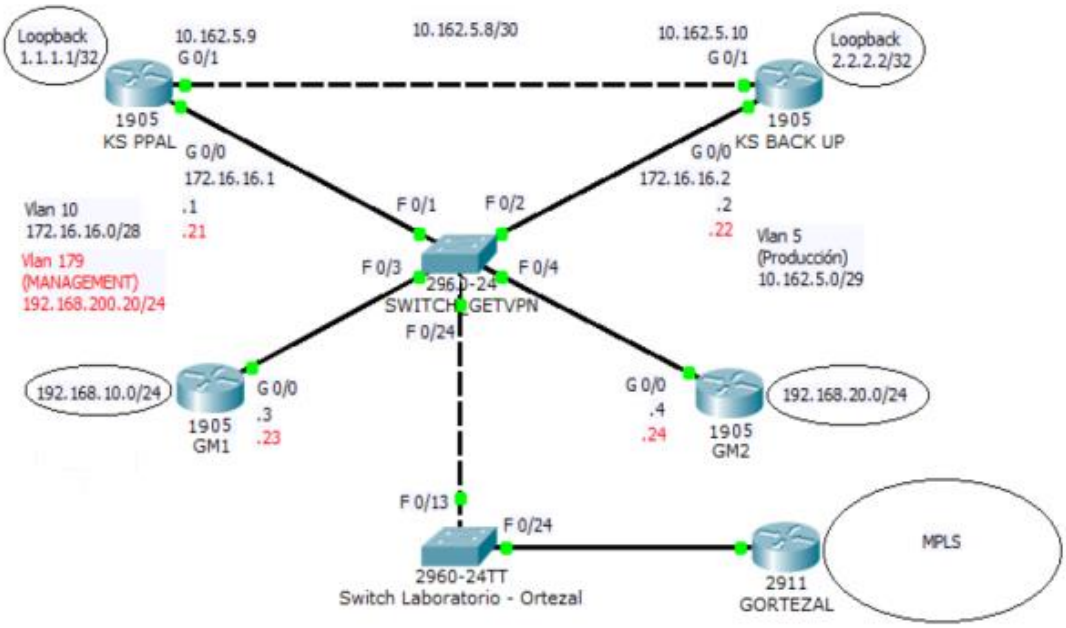

Figura 19 Topología y Direccionamiento final GET VPN

La *Figura 19* muestra la topología instalada y cableada en el rack del laboratorio de la sede Ortezal. También contiene toda la asignación de Ips empleada en los equipos para conformar el Laboratorio GET VPN.

El direccionamiento empleado sobre cada uno de los equipos es estático. El enrutamiento usado en la red es OSPF, método en el cual cada router conoce a los routers cercanos y las direcciones que posee cada router de los cercanos. Además de esto cada router sabe a qué distancia (medida en routers) está cada router. Así, cuando tiene que enviar un paquete lo envía por la ruta por la que tenga que dar menos saltos y si un router desaparece o deja de funcionar, es posible encontrar otra ruta alternativa.

La topología GET VPN presentada, está compuesta de la siguiente manera:

- Dos Key Server, uno principal y un Backup.
- Dos Group Member, donde cada uno representa un equipo instalado en una sede diferente del mismo cliente.

- Un switch que permite la comunicación entre los equipos, y simula la red MPLS de Claro por la cual pasaría todo el tráfico del cliente.

La alta disponibilidad es una de las características principales que caracteriza la topología GET VPN simulada. Desde su estructura de red contiene dos Key Servers, uno principal y otro Backup, los cuales trabajan sincronizados. Si llegara a dejar de funcionar el Key Server Principal en algún momento por cualquier circunstancia, el Key Server Backup inmediatamente está en la capacidad de respaldar el trabajo del KS Principal y a hacerse cargo de la red. Adicionalmente a los Key Servers que componen la topología, el enrutamiento OSPF empleado en la configuración de los equipos, también hace posible la alta disponibilidad como se explicó anteriormente.

La idea principal de este laboratorio es poder simular un cifrado de tráfico entre los dos Group Member, mediante el uso de llaves pre-compartidas y certificados digitales. O dicho de otra manera, se pretende simular el envío de tráfico de datos desde una sede a otra, pertenecientes a una misma compañía. Esta información es de alta seguridad y debe ir cifrada para evitar que personal ajeno a la red, obtenga acceso a dicha información.

Los comandos utilizados, procedimientos a seguir para configurar una solución GET VPN, las verificaciones de cada uno de estos procedimientos, resultados obtenidos y troubleshooting realizados, se encuentran en el ANEXO B.

3.6 VERIFICACIÓN DE CIFRADO LABORATORIO GET VPN

Después de realizadas las configuraciones necesarias sobre los equipos que componen la topología GET VPN, por medio de comandos de verificación fue posible confirmar el funcionamiento del laboratorio y el cifrado de los datos transmitidos.

Usando el comando **show crypto gdoi ks members | inc Mem** se verifica tanto en el Key Server Principal como en el Key Server Backup, que los GMs se encuentran autenticados con cada Key Server. De color verde se resalta la Ip correspondiente al Group Member 1 (10.162.5.3) y de color azul se resalta la Ip correspondiente al Group Member 2 (10.162.5.4).

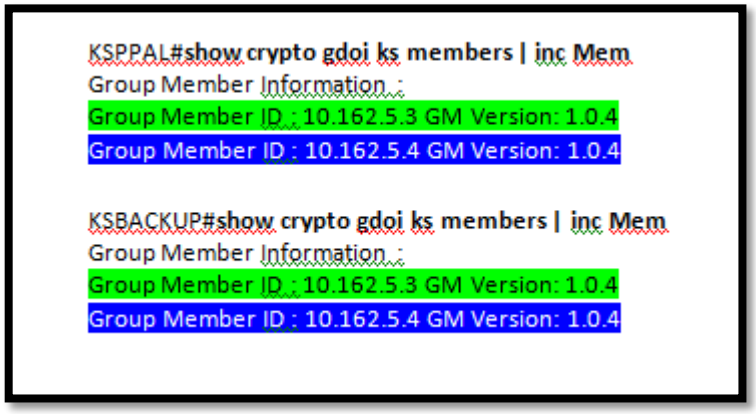

Figura 20 Confirmación de autenticación de los GMs contra los KSs

Teniendo la información de los GMs autenticados ante los Key Servers, utilizando el comando **sh crypto isakmp sa de**, se verifica la entrega de certificados digitales realizada por el Key Server Principal a todos los miembros del grupo. El Group Member 1 (10.162.5.3), el Group Member 2 (10.162.5.4) y el Key Server Backup (2.2.2.2) mediante los certificados digitales recibidos, tienen los permisos necesarios para descargar la lista de acceso proporcionada por el Key Server Principal, y cumplir sus respectivas funciones dentro de la topología GET VPN.

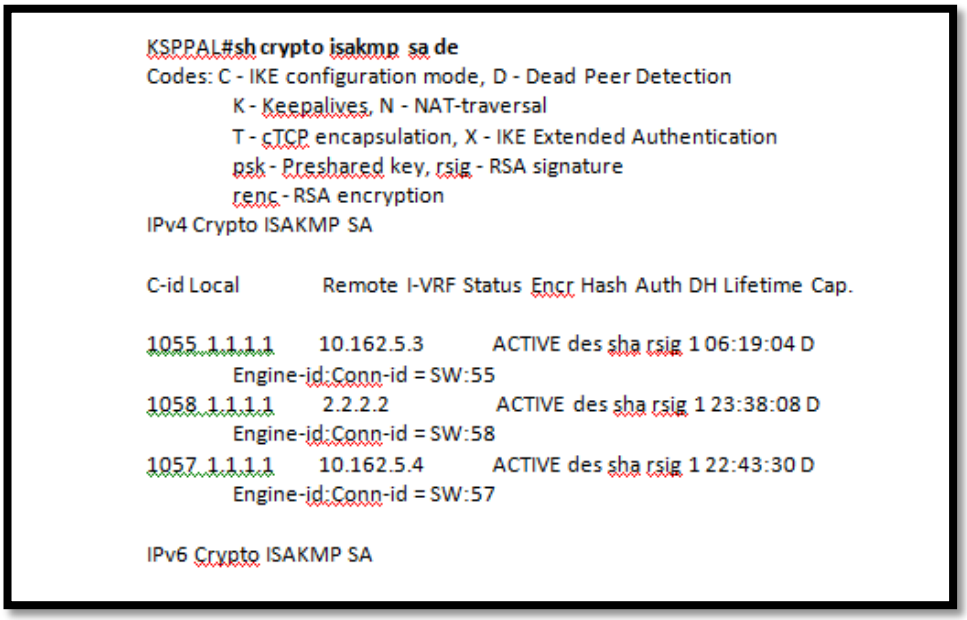

Figura 21 Entrega de certificados digitales de parte del KS Principal a los GMs

Cada miembro del grupo, al tener la lista de acceso conoce los protocolos, direcciones Ips y tipo de tráfico que se debe permitir o denegar en la red determinada por la topología GET VPN.

Para verificar el cifrado de los datos, y el correcto funcionamiento de la solución GET VPN simulada por medio del laboratorio, se realiza una prueba LAN to LAN. Esta consiste en hacer ping desde el Group Member 1 al Group Member 2, a través de las redes LAN que se encuentran simuladas en cada uno de ellos por medio de las loopback respectivamente (192.168.10.0 y 192.168.20.0).

El ping sostenido de 100 paquetes enviados mostrado a continuación, se realiza desde la loopback (192.168.10.1) en el Group Memeber 1 (10.162.5.3), a la loopback (192.168.20.1) en el Group Member 2 (10.162.5.4).

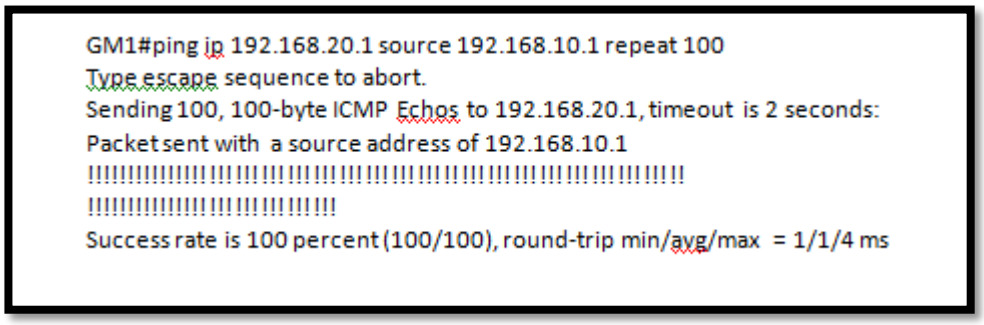

Figura 22 Prueba LAN to LAN – Funcionamiento Solución GET VPN

Al ser enviados 100 paquetes desde el Group Member 1 al Group Member 2, usando el comando **show crypto ipsec sa** en el Group Member 1, permite observar cuantos paquetes fueron cifrados desde la Ip de origen (color verde) a la Ip de destino (color azul). Ver *Figura 23*.

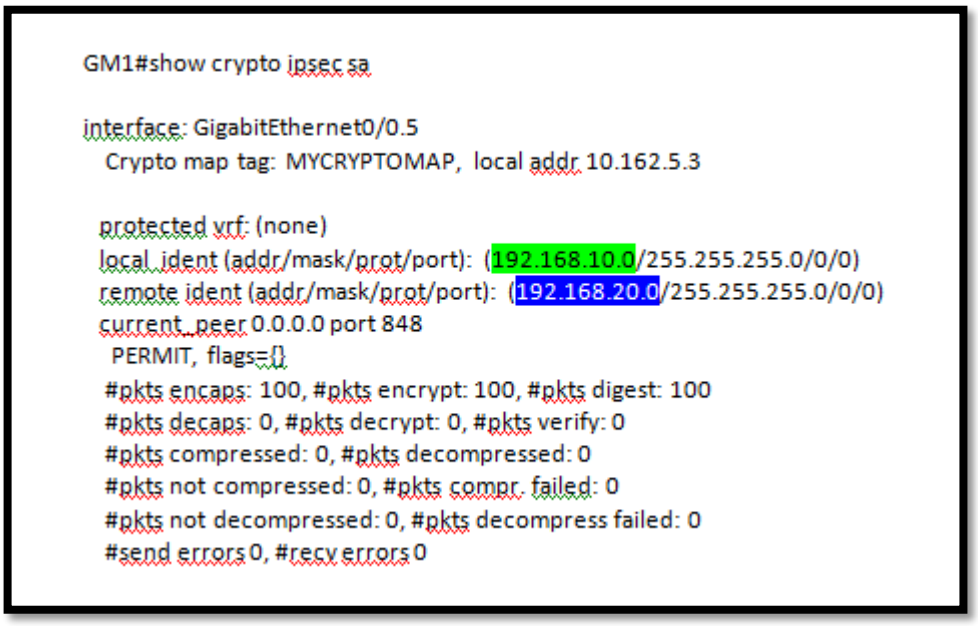

Figura 23 Verificación de cifrado de datos entre los GMs

El resultado obtenido de la prueba anteriormente mostrado, determina el correcto funcionamiento del Laboratorio GET VPN simulado y de sus componentes, obteniendo el cifrado de tráfico entre los GMs.

Un mayor número de comandos, y un procedimiento más detallado de los resultados obtenidos de las pruebas realizadas al laboratorio GET VPN se encuentran en el ANEXO B.

CAPÍTULO 4
Análisis de Resultados

El capítulo presenta el análisis de los resultados obtenidos al desarrollar el laboratorio GET VPN para la empresa Claro Colombia S.A.

Los equipos adquiridos para el laboratorio de la sede Ortezal de la empresa CLARO, que componen la topología de la solución GET VPN, aprobaron las pruebas iniciales propuestas para determinar su correcto funcionamiento. Fue necesario evaluar sus características, para verificar si era viable la realización del laboratorio GET VPN.

Al determinar y concluir que los equipos adquiridos cumplían con los requisitos necesarios para trabajar en una red GET VPN, se procedió al montaje, instalación y configuración de los mismos.

Al finalizar la configuración de los equipos adquiridos, se hizo una presentación del trabajo realizado a las personas encargadas del área relacionada con el proyecto, para determinar el correcto funcionamiento del laboratorio GET VPN y verificar que éste cumpliera las expectativas requeridas para ser implementado dentro de las capacitaciones de los ingenieros.

El laboratorio fue implementado desde el momento de su presentación y entrega a los ingenieros del NOC, encontrándose aún activo en la red. Para el grupo de ingenieros que realizó este laboratorio como práctica, consideró que el laboratorio era sencillo y fácil de realizar, además de tener la ventaja de poder practicar sobre equipos reales y no sobre software que realiza simulaciones, permitiéndoles entender a cabalidad el tema explicado teóricamente en su capacitación. Se demostró que el trabajo solicitado fue exitoso ya que concluye el correcto cifrado de datos, y el correcto funcionamiento de la simulación GET VPN. Ver *Figura 24.*


De: Tobon Salgado, Juan Ignacio (Col)
Para: Sanchez Escobar, Jose Fernando (Ext-Col)
CC: Verdugo Parra, Juan Gabriel - (Col)
Asunto: RE: Soporte documentos GET VPN José Sánchez

Buenos días,

A quien interese:

Por parte del área de Gestión de Red Corporativo recibimos satisfactoriamente el proyecto GET-VPN en el que trabajó Jose Fernando.

Actualmente lo estamos usando dentro del proceso de recapacitación del personal.

Cordialmente,

Claro

Ingeniero Líder Gestión Red Datos
Tobon Salgado, Juan Ignacio (Col)

Telmex Colombia S.A.
Ext 83714
juan.tobon@claro.com.co

Conmutador: Bogotá: 7480000 - 7500300, Cali: 4880000, Medellín: 6041000, B/quilla: 3870000

Figura 24 Soporte entrega de proyecto GET VPN a CLARO

CONCLUSIONES

La práctica realizada en el NOC Corporativo de la empresa CLARO COLOMBIA S.A., permitió desarrollar actividades relacionadas con el área de las Telecomunicaciones, pues allí se realiza gestión, administración y cambios de configuración sobre equipos activos que componen toda la red de CLARO.

GET VPN es una solución que CLARO ofrece a sus clientes con el fin de garantizar que el tráfico de información que viaja a través de su red se transporte de manera segura y confiable, por lo que con la implementación del laboratorio se espera prevenir fallas presentadas en la red de CLARO que impactan de forma negativa a sus clientes, y mejorar el servicio al cliente mediante la capacitación del personal técnico encargado de esta área.

El desarrollo práctico del laboratorio GET VPN, permitió a los ingenieros del NOC Corporativo tener acceso a equipos desde su conexión hasta su configuración remota, permitiéndole al personal practicar sobre equipos reales y no sobre software que realiza simulaciones. Los equipos adquiridos se comportan como los equipos de los clientes, permitiendo realizar pruebas y verificar su comportamiento de forma real. Además de verificarse que el cifrado de la información se lleva a cabalidad.

La guía y documentos presentados a CLARO cumplieron con las expectativas del proyecto, pues allí se aprecia todo el trabajo realizado concluyendo el cifrado de datos y el correcto funcionamiento de una solución GET VPN; además de ser aprobado por el área encargada y utilizado para el proceso de capacitación del personal técnico.

Referencias

Andelić, A., Koprivica, M., & Božilović, B. (2011). Eksperimentalna analiza performansi VPN konekcije izmedu strongSwan klijenta i Cisco IOS IPsec gateway-a. 2011 19th Telecommunications Forum, TELFOR 2011 - Proceedings of Papers, 162–165. http://doi.org/10.1109/TELFOR.2011.6143517

Bahie-Eldin, M. a., & Omar, a. a. (1998). Complexity measure of encryption keys used for securing computer networks. Proceedings 14th Annual Computer Security Applications Conference (Cat. No.98EX217), 250–255. http://doi.org/10.1109/CSAC.1998.738645

Chou, L. Der, & Hong, M. Y. (2006). Design and implementation of two-level VPN service provisioning systems over MPLS networks. Proceedings of ISCN'06: 7th International Symosium on Computer Networks, 2006, 42–48. http://doi.org/10.1109/ISCN.2006.1662506

Confidential, C. (2006). Cisco Group Encrypted Transport VPN – Technical Overview Agenda Problem Statement Solution: Group Encrypted Transport Technology Components Feature Overview Provisioning and Management, (December).

Confidential, C. (2006). Tunnel-less VPN with Cisco Group Encrypted Transport (GET), (December), 1–17.

Cotter, R., & Medhi, D. (2009). Survivable design of reconfigurable MPLS VPN networks. Proceedings of the 2009 7th International Workshop on the Design of Reliable Communication Networks, DRCN 2009, c, 78–85. http://doi.org/10.1109/DRCN.2009.5340021

Detienne, F. (2009). Advanced IPsec with. Transition, 1–44.

Eljack, S. M., & Abdelkarim, S. B. (2013). Effect of the Interior Gateway Routing Protocols in the Multiprotocol Label Switching Networks.

Group Encrypted T ra ns port V P N PetrRůžička, CSE peru zick@cisco.com VPN Methods Summary. (n.d.), 1–36.

Hota, C. H. C., Jha, S. K. J. S. K., & Raghurama, G. (2004). Distributed dynamic resource management in IPVPNs to guarantee quality of service. Proceedings. 2004 12th IEEE International Conference on Networks (ICON 2004) (IEEE Cat. No.04EX955), 1, 414–419. http://doi.org/10.1109/ICON.2004.1409186

Ishimura, K., Tamura, T., Mizuno, S., Sato, H., & Motono, T. (2010). Dynamic IP-VPN architecture with secure IPsec tunnels. Information and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium on.

Jiang, Z., & Xie, Y. (2011). Study and implement of VPN penetrating NAT based on IPSec protocol. Proceedings 2011 International Conference on Transportation, Mechanical, and Electrical Engineering, TMEE 2011, 404–407. http://doi.org/10.1109/TMEE.2011.6199228

Manager, P., & Group, S. T. (2006). Tunnel-less VPN's with Group Encrypted Transport (GET) VPN Siva Natarajan Presenter : Donovan Williams, Product Manager, Security Technology Group Agenda Problem Statement Solution Benefits Main Use Cases Higher Level View: How does it who.

Meng, Z., Li, W., & Gao, Z. (2010). Context-based deep packet inspection of IKE phase one exchange in IPSec VPN. CICC-ITOE 2010 - 2010 International Conference on Innovative Computing and Communication, 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering, 3–6. http://doi.org/10.1109/CICC-ITOE.2010.8

Ming-Hui, L., & Jing-Bo, X. (2008). Research and simulation on VPN networking based on MPLS. 2008 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2008, 1–4. http://doi.org/10.1109/WiCom.2008.997

Morris, T. H., & Nair, V. S. S. (2009). Encryption key protection: For private computing on public platforms. 7th Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2009. http://doi.org/10.1109/PERCOM.2009.4912897

Nguyen, K. V. (2006). Simplifying peer-to-peer device authentication using identity-based cryptography. International Conference on Networking and Services 2006, ICNS'06, 00(c). http://doi.org/10.1109/ICNS.2006.101

Okayama, K., Yamai, N., Ishibashi, H., Abe, K., & Matsuura, T. (2007). An efficient management method of access policies for hierarchical virtual private networks. Proceedings of the 2007 2nd International Conference on Communication System Software and Middleware and Workshops, COMSWARE 2007. http://doi.org/10.1109/COMSWA.2007.382593

Overview, P., & Architecture, P. (2009). Cisco Group Encrypted Transport VPN: Tunnel-less VPN Delivering Encryption and Authentication for the WAN, (Figure 1), 1–8.

Shen, Y., Zhang, Q. F., Ping, L. Di, Wang, Y. F., & Li, W. J. (2012). A multi-tunnel VPN concurrent system for new generation network based on user space. Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012, 1334–1341. http://doi.org/10.1109/TrustCom.2012.41

Song, M., & Yun-he, Z. (2009). One new research about ipsec communication based on HTTP tunnel. Proceedings - 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications, ISPA 2009, 253–257. http://doi.org/10.1109/ISPA.2009.44

Systems, C., & Republic, C. (2007). Group Encrypted Transport VPN PetrRůžička 3 Key Distribution: Group Domain of Interpretation, 115–120

Tanveer, A., Ali, A., Paracha, M. A., & Raja, F. R. (2015). Performance Analysis of AES-Finalists along with SHS in IPSEC VPN over 1 Gbps Link, 323–332.

Wang, S., & Lv, H. (2011). A distributed object-based IPSec multi-tunnels concurrent architecture. 2011 International Conference on Computational Problem-Solving, ICCP 2011, 471–476. http://doi.org/10.1109/ICCPS.2011.6089933

Xia, J. B., Li, M. H., & Wan, L. J. (2008). Research on MPLS VPN networking application based on OPNET. 2008 International Symposium on Information Science and Engineering, ISISE 2008, 1, 404–408. http://doi.org/10.1109/ISISE.2008.129

Anexo A
AVANCE LABORATORIO GET VPN NOC CORPORATIVO

El anexo contiene los detalles iniciales de la elaboración del proyecto GET VPN, instalación de quipos, configuraciones iniciales, pruebas de conectividad y gestión remota.

Anexo B
GUÍA LABORATORIO GET VPN NOC CORPORATIVO

El anexo adjunto, presenta el desarrollo de configuraciones para llevar a cabo el laboratorio GET VPN, procedimiento, comandos, y pruebas de verificación. Contiene toda la información que sustenta toda la simulación del proyecto.

Anexo C
CONFIGURACIONES LABORATORIO GET VPN NOC CORPORATIVO

El anexo presenta las configuraciones finales desarrolladas sobre cada uno de los equipos que componen la topología del laboratorio GET VPN.