RESUMEN – TRABAJO DE GRADO

AUTORES	**DIANA MARCELA PEREZ ORTEGA**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**INGENIERÍA DE SISTEMAS**
DIRECTOR	**YEGNY KARINA AMAYA TORRADO**
TÍTULO DE LA TESIS	**MECANISMOS DE SEGURIDAD A TRAVÉS DE VPN UTILIZANDO DISPOSITIVOS CISCO**

RESUMEN

(70 palabras aproximadamente)

EL TRABAJO DE GRADO MODALIDAD MONOGRAFÍA VA DIRIGIDO CON LA INSTITUCIÓN POLICÍA NACIONAL, INCORPORANDO COMO OFICINA MATRIZ LA CIUDAD DE BOGOTÁ EN DIPON DEL (DEPARTAMENTO DE CUNDINAMARCA) Y COMO SUCURSALES LAS CIUDADES DE OCAÑA Y CÚCUTA DEL DEPARTAMENTO DE NORTE DE SANTANDER; ESTO SURGE CON EL PROPÓSITO DE BRINDAR A LA EMPRESA CONEXIÓN Y DATOS SEGUROS ANEXANDO MÉTODOS DE CONFIABILIDAD, INTEGRIDAD, AUTENTICACIÓN Y TUNELIZACIÓN DE LOS DATOS. EL TIPO DE MONOGRAFÍA PLANTEADA EN ESTA PROPUESTA ES DE TIPO ANÁLISIS DE EXPERIENCIAS YA QUE SE REALIZA A PARTIR DE LOS CONOCIMIENTOS ADQUIRIDOS EN EL CURSO DE PROFUNDIZACIÓN ENTORNOS LAN Y WAN OFRECIDOS POR LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER DE OCAÑA.

CARACTERÍSTICAS

PÁGINAS: 61	PLANOS:	ILUSTRACIONES:	CD-ROM:1

MECANISMOS DE SEGURIDAD A TRAVÉS DE VPN UTILIZANDO DISPOSITIVOS CISCO

AUTOR

DIANA MARCELA PEREZ ORTEGA

Trabajo de grado modalidad monografía para obtener el título de Ingeniero de Sistemas

Director

YEGNY KARINA AMAYA TORRADO

Magister en Ingeniería de Sistemas y Computación.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

INGENIERÍA DE SISTEMAS

Ocaña, Colombia **Enero,2018**

Agradecimientos

Agradezco a Dios sobre todas las cosas por brindarme la oportunidad de culminar de manera satisfactoria mis estudios.

A mi abuela Trina y a mi madre Luz Marina por su esfuerzo, apoyo y motivación cada día para poder lograr tan anhelado sueño.

A toda mi familia que de una u otra manera creyeron y confiaron en mí.

Amigo y jurado especifico de área Fabian Cuesta Quintero por su paciencia y ayuda para culminar con éxito la monografía de trabajo de grado.

También quiero agradecer a la universidad Francisco de Paula Santander Ocaña por brindarme la oportunidad de terminar mis estudios.

Dedicatoria

Dedico este trabajo a cada una de las personas que me apoyaron de manera incondicional y me motivaron para culminar con cada uno de mis objetivos como ingeniera de sistemas.

A mi madre, hermanos y amigos que me enseñaron que a pesar de las adversidades los propósitos y metas se pueden alcanzar.

Índice

Lista de Figuras

Lista de Tablas

Introducción

Esta monografía propone el análisis e implementación de los mecanismos de seguridad para la interconexión de la oficina matriz con las sucursales y la conexión de usuarios remotos hacía las diferentes sedes de la empresa Policía Nacional a través de una Red Privada Virtual (VPN).

Se analizan las necesidades que la empresa requiere para una comunicación segura y confiable, presentando propuesta de VPN`s enmarcado en el protocolo IPv6, debido a la seguridad que ofrece a los proveedores de servicio de internet. El lugar donde se va a llevar a cabo la propuesta involucrara como oficina principal la ciudad de Bogotá en DIPON (Departamento de Cundinamarca) y como sedes sucursales en las ciudades de Ocaña y Cúcuta del departamento de norte de Santander.

En el caso de esta investigación se hace referencia a una Red Privada Virtual, o VPN, de las siglas en ingles de Virtual Private Network. “Es una tecnología en la que su función es crear una extensión segura de una red local (LAN), sobre la red pública mundialmente conocida como internet. El desempeño de las VPN es brindar un canal entre la empresa con sus diferentes oficinas, usuarios que se encuentren distantes, utilizando un recurso elemental como lo es internet, por supuesto con tota la funcionalidad, seguridad y políticas de gestión de una red privada” (Goujon, 2012).

Resumen

La monografía análisis e implementación de los mecanismos de seguridad a través de VPN´s van dirigidos con la Institución Policía Nacional, incorporando como oficina matriz la ciudad de Bogotá en DIPON del (Departamento de Cundinamarca) y como sucursales las ciudades de Ocaña y Cúcuta del departamento de norte de Santander; esto surge con el propósito de brindar a la empresa conexión y datos seguros anexando métodos de confiabilidad, integridad, autenticación y tunelización de los datos. El tipo de monografía planteada en esta propuesta es de tipo análisis de experiencias ya que se realiza a partir de los conocimientos adquiridos en el curso de profundización entornos LAN y WAN ofrecidos por la Universidad Francisco de Paula Santander de Ocaña.

Capítulo 1. Fundamentación teórica de la investigación

1.1 Marco teórico

El desarrollo del trabajo investigativo se enfocó a la institución Policia Nacional, para la cual daremos a conocer un poco de su reseña histórica, misión y visión de la institución, para una mejor comprensión del lector.

1.1.1 Reseña histórica de la Institución Policía Nacional de Colombia

En junio de 1954 se generan unos graves disturbios en la Capital de la República en especial en la Universidad Nacional, la situación se torna incontrolable. Al día siguiente se agravaron los hechos y se suscita una serie de acontecimientos nefastos donde varios estudiantes terminan heridos.

De ahí surge la imperiosa necesidad de crear de forma inmediata por parte del Gobierno Nacional y Mandos Militares una Unidad Táctica preparada para el control de disturbios y motines con personal idóneo para contrarrestar tal accionar.

Es así como se creó el 24 de junio de 1954 el Batallón n. 1 de Policía Militar de la Brigada de Institutos Militares, por decreto n. 1695 firmado por el señor Teniente General Gustavo Rojas Pinilla como presidente de la República.

Desde ese entonces existen los soldados de la Policía Militar en la capital de la República, las primeras instalaciones fueron en el centro de la capital, más adelante por la necesidad locativa se ubica en los terrenos de la Escuela de Ingenieros en Puente Aranda. Desde ese entonces se mantiene su lema principal LEY Y ORDEN.

El principio desde donde se fundamenta la autoridad lo establece el Comando de las FFMM por medio de la orden del día n. 050 art. 185 para el día 8 de septiembre de 1961, donde

confirió autoridad especial a la Policía Militar para ejercer control y vigilancia sobre el personal Militar en actividad y civiles al servicio del Ejército, Armada y Fuerza Aérea, en todos aquellos casos contemplados en el Manual de Policía Militar.

En la actualidad el Batallón de Policía Militar n. 13 está ubicado en la carrera 50 n. 18 06 en el reconocido sector de Puente Aranda, como Institución cuenta con una misión importante en la Capital de la República por ello cuenta con las siguientes compañías: Ayacucho, Córdoba, Dluyer, Espelota, Junín y Santander, las cuales tienen la inmensa responsabilidad de trabajar en la seguridad, protección de la población civil en ocho localidades de la Capital de la República (Mártires, Antonio Nariño, Ciudad Bolívar, Bosa, Kennedy, Fontibón, Puente Aranda, Teusaquillo) y un municipio de Cundinamarca (Soacha). (Ejercito Nacional, s.f).

1.1.2 Misión

El Ejército Nacional conduce operaciones militares orientadas a defender la soberanía, la independencia y la integridad territorial y proteger a la población civil y los recursos privados y estatales para contribuir a generar un ambiente de paz, seguridad y desarrollo, que garantice el orden constitucional de la nación. (Ejercito Nacional, s.f).

1.1.3 Visión

En el año 2030, el Ejército Nacional continuará siendo la fuerza de acción decisiva de la Nación, con capacidad de conducir operaciones autónomas, conjuntas, coordinadas y combinadas, en forma simultánea en dos teatros de operaciones, uno externo y/o uno interno. (Ejercito Nacional, s.f).

Figura 1. Ubicación geográfica de la institución Policía Nacional Bogotá.

Fuente. . Autores del proyecto a través de Google Maps.

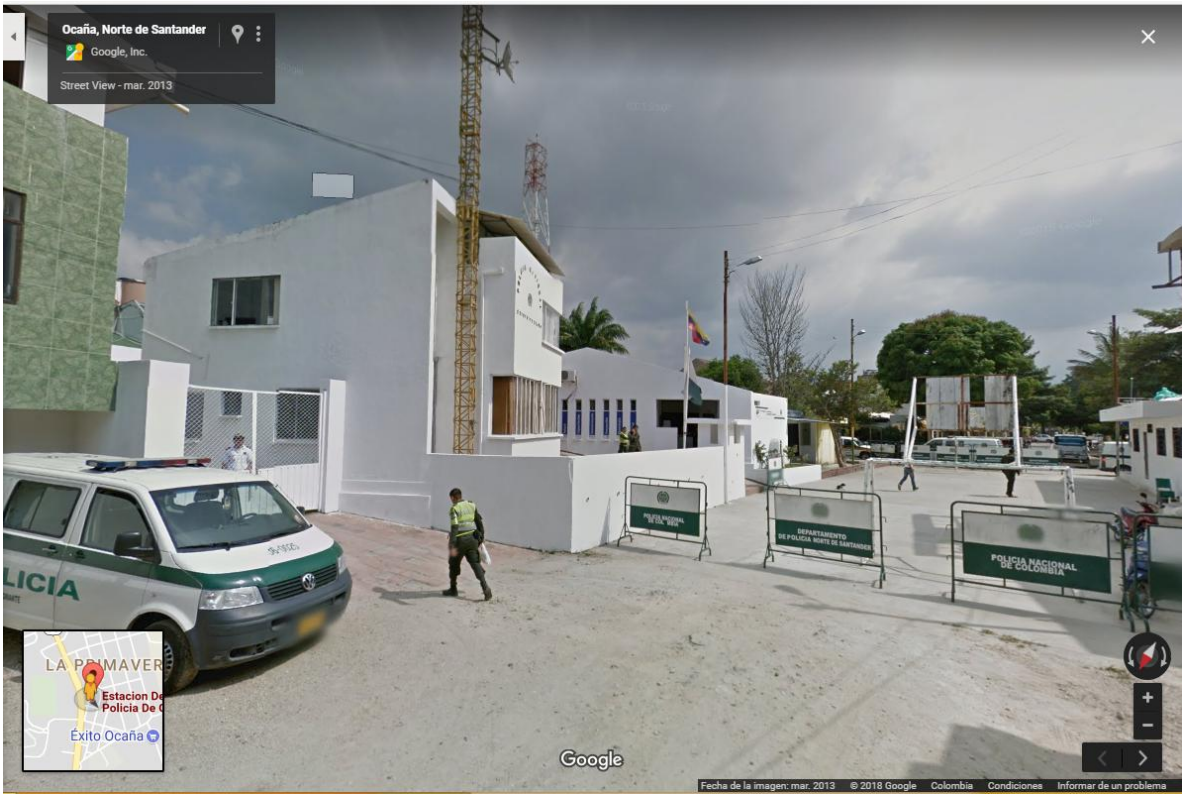

Figura 2. Ubicación geográfica de la institución Policía Nacional Ocaña Norte de Santander.

Fuente. . Autores del proyecto a través de Google Maps.

Figura 3. Ubicación geográfica de la institución Policía Nacional Cúcuta Norte de Santander.

Fuente. . Autores del proyecto a través de Google Maps.

1.2 Bases Teóricos

Para el diseño de la propuesta planteada se lleva a cabo en el laboratorio de Redes y Telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña, en la interconexión de las tres oficinas, la sede de Ocaña y Cúcuta ubicadas en el departamento Norte de Santander, con la sede central en la ciudad de Bogotá en Teusaquillo con el análisis y diseño de la red con el modelo jerárquico de tres capas de cisco.

Para el análisis e implementación de las VPN´s, se basa de la teoría y práctica de los módulos del diplomado de CCNA de la academia de Cisco.

La asignación de dirección se fundamenta en el direccionamiento de IPv6 con un protocolo de encapsulamiento, TUNNEL GRE, para el correcto funcionamiento del envío y recepción de la información brindando confiabilidad y seguridad de los datos.

1.2.1 Protocolo de internet version 6 (IPV6)

IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características. El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta. Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.

Características principales

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.
- Simplificación del formato del Header. Algunos campos del header IPv4 se quitan o se hacen opcionales
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.
- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.
- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.

- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad

Clasificación

- **Unicast** identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección.

Anycast identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast.

- **Multicast** identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

Mecanismos de transición básicos

Los mecanismos de transición son un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de Internet al IPv6 con la menor interrupción posible.

Existen dos mecanismos básicos:

- *Dual Stack*: provee soporte completo para IPv4 e IPv6 en host y routers.

- *Tunneling*: encapsula paquetes IPv6 dentro de headers IPv4 siendo transportados a través de infraestructura de ruteo IPv4.

Dichos mecanismos están diseñados para ser usados por hosts y routers IPv6 que necesitan interoperar con hosts IPv4 y utilizar infraestructuras de ruteo IPv4. Se espera que muchos nodos necesitarán compatibilidad por mucho tiempo y quizás indefinidamente. No obstante, IPv6 también puede ser usado en ambientes donde no se requiere interoperabilidad con IPv4. Nodos diseñados para esos ambientes no necesitan usar ni implementar estos mecanismos.

Dual Stack. La forma más directa para los nodos IPv6 de ser compatibles con nodos IPv4-only es proveyendo una implementación completa de IPv4. Los nodos IPv6 que proveen una implementación completa de IPv4 (además de su implementación de IPv6) son llamados nodos "IPv6/IPv4". Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4, y también operar con nodos IPv6 usando paquetes IPv6.

Tunneling. Los nodos o redes IPv6 que se encuentran separadas por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel. Paquetes IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de paquetes IPv4. Los extremos del túnel son dos direcciones IPv4 y dos IPv6. Se pueden utilizar dos tipos de túneles: configurados y automáticos. Los túneles configurados son creados mediante configuración manual. Un ejemplo de redes conteniendo túneles configurados es el 6bone. Los túneles automáticos no necesitan configuración manual. Los extremos se determinan automáticamente determinados usando direcciones IPv6 IPv4-compatible.

1.3 Marco Conceptual

1.3.1 Red Privada Virtual

Las redes de área local (LAN) son las redes internas de las organizaciones, es decir las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente. Sin embargo, los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está definida por anticipado, lo que significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que a lo largo de la línea, un usuario entrometido "escuche" la red o incluso "secuestre" la señal. Por lo tanto, la información confidencial de una organización o empresa no debe ser enviada bajo tales condiciones.

La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas. Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar Internet como medio de transmisión.

Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de túnel, que significa que los datos se encapsulan antes de ser enviados de manera cifrada. El término Red privada virtual (abreviado VPN) se utiliza para hacer referencia a la red creada artificialmente de esta manera. Se dice que esta red es virtual porque conecta dos redes físicas (redes de área local) a través de una conexión poco fiable (Internet)

y privada porque solo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden "ver" los datos.

Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada. (Vialfa, 2016).

Podemos referir mediante lo investigado que este tipo de red es muy útil para el trabajo en empresas e instituciones educativas, la privacidad de la misma resalta aspectos como la confiabilidad de la información, los sitios virtuales específicos de una especialidad y fundamentalmente acceder a este tipo de servicio con una contraseña y nombre de usuario. Si bien el costo es algo elevado de este tipo de red privada, también proporciona beneficios como:

- ✓ La transparencia y la confiabilidad se observa cuando cada usuario accede a la página, siendo de interés el acceso a documentos y aplicaciones, además de recursos de hardware como scanner, impresoras, lo que asegura la confidencialidad, seguridad e integridad de los datos.
- ✓ Importante también el mencionar la accesibilidad y la reducción de costos al utilizar las VPN.
- ✓ Sin importar el lugar donde se encuentre el usuario puede acceder a la página, estableciendo una amplia comunicación.
- ✓ Accede a diferentes proveedores de internet con su servicio.

Hay que tener en cuenta en las VPN dos características que van a marcar la diferencia entre otras redes ya que cuentan con características específicas que son: la privacidad y la virtualidad.

1-Privacidad

Los recursos de una VPN se separan de la red del portador, lo que permite que los recursos de una VPN no pueden ser utilizadas por otro usuario fuera de la misma. Estas ofrecen permanentemente medidas de seguridad para garantizar que la información interna esté libre de interferencias externas. (Fernandez, 2017).

2-Virtualidad

Es una red las VPN privada lógica, lo que al analizar los usuarios se comunican a través de redes públicas. Estas redes públicas son utilizadas al mismo tiempo las VPN por diferentes usuarios. Lo que se denomina redes troncales a las redes públicas que interactúan con estas. Las VPN en su amplio espectro poseen a diferencias de otras redes privadas, o sea teniendo en cuanta la experiencia en la práctica y los referentes teóricos. (Fernandez, 2017).

1.3.2 Funcionamiento de una Red Privada Virtual (VPN).

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.
La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada.

El equipo remoto le proporciona los datos al servidor VPN en su red y este envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario. (Vialfa, 2016).

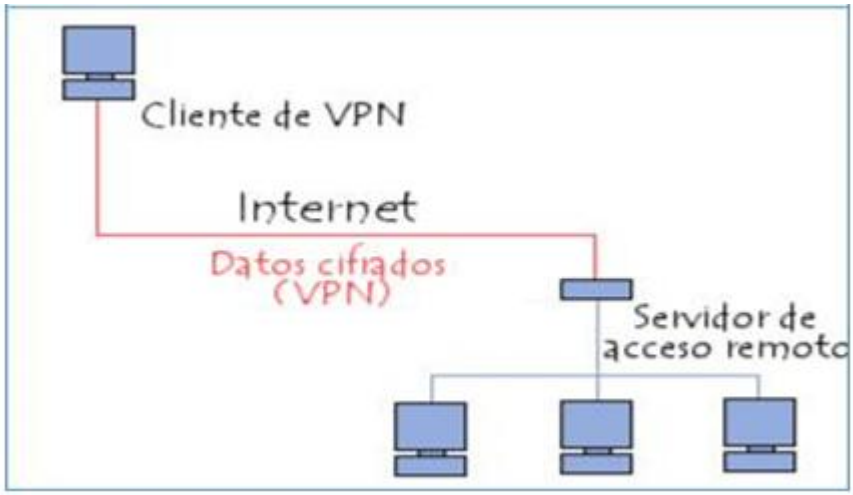

Figura 4. Funcionamiento de una VPN

Fuente: (Ccm, s.f)

1.3.3 Tipos de conexiones mediante vpn

Red Privada Virtual de acceso remoto

Una conexión VPN de acceso remoto permite al usuario que trabaja desde casa o que está de viaje tener acceso a un servidor de una red privada mediante la infraestructura proporcionada por una red pública como, por ejemplo, Internet. Desde el punto de vista del usuario, la VPN es una conexión punto a punto entre el equipo cliente y el servidor de la organización. La infraestructura de la red compartida o pública es irrelevante, ya que aparece lógicamente como si los datos se enviaran a través de un vínculo privado dedicado.

Red Privada Virtual Sitio a Sitio

Una conexión VPN de sitio a sitio (a veces llamada conexión VPN de enrutador a enrutador) permite a una organización tener conexiones enrutadas entre distintas oficinas o con

otras organizaciones a través de una red pública a la vez que se mantiene la seguridad de las comunicaciones. Cuando las redes se conectan a través de Internet, tal como se muestra en la siguiente imagen, un enrutador habilitado para VPN reenvía paquetes a otro enrutador habilitado para VPN a través de una conexión VPN. Para los enrutadores, la conexión VPN aparece lógicamente como un vínculo dedicado en el nivel de vínculo de datos. (Microsoft, 2012).

Una conexión VPN de sitio a sitio conecta dos redes privadas. El servidor VPN proporciona una conexión enrutada a la red a la que está conectada el servidor VPN. El enrutador que realiza la llamada se autentica a sí mismo en el enrutador que responde y, para realizar una autenticación mutua, el enrutador que responde se autentica a sí mismo en el enrutador que realiza la llamada. En una conexión VPN de sitio a sitio, los paquetes enviados desde cualquiera de los enrutadores a través de la conexión VPN por lo general no se originan en los enrutadores. (Microsoft, 2012).

Una conexión VPN de tipo site-to-site que permite interconectar dos redes LAN geográficamente distantes a través de Internet de manera segura. Este tipo de configuración es ideal para interconectar sucursales de una compañía que tienen distintos ISPs para salir a Internet. (Colomès, 2010).

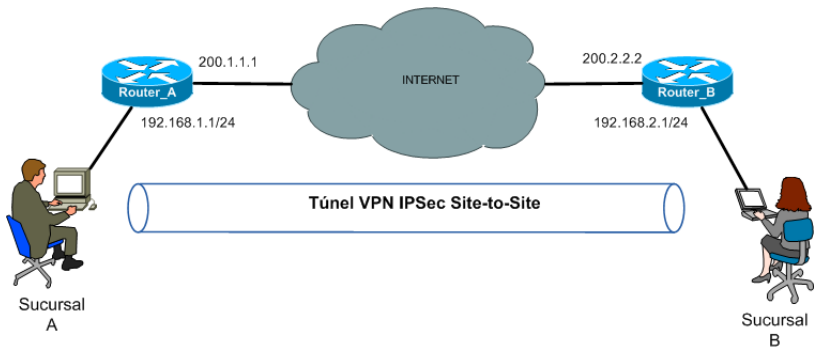

Figura 5. Conexión de punto a punto

Fuente: (Colomès, 2010)

Pasos para configurar la VPN IPsec de tipo site-to-site

1. Se define la fase 1 de IKE (ISAKMP Policy)

2. Se define la fase 2 de IKE (Transform Set)

3. Definir una ACL para seleccionar el tráfico que se irá por la VPN

4. Crear un Crypto Map para asociar los pasos 1, 2 y 3 a una interface de salida.

(Colomès, 2010).

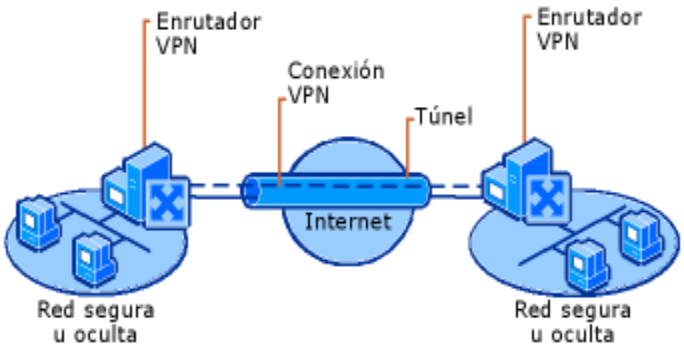

Figura 6. Conexión mediante VPN de dos sitios remotos a través de Internet

Fuente: (Microsoft, 2012)

1.3.3.1 Propiedades de las conexiones VPN

- **ENCAPSULACIÓN:** Los datos privados se encapsulan con un encabezado que contiene información de enrutamiento que permite a los datos recorrer la red de tránsito.
- **Autenticación:** La autenticación para las conexiones VPN puede realizarse de tres formas distintas:

Autenticación en el nivel de usuario con autenticación PPP (Protocolo punto a punto). Para establecer la conexión VPN, el servidor VPN autentica el cliente VPN que intenta realizar la conexión con un método de autenticación PPP en el nivel de usuario y comprueba que el cliente VPN tiene la autorización adecuada. Si se usa la autenticación mutua, el cliente VPN también autentica el servidor VPN, lo que proporciona protección frente a equipos que se hacen pasar por servidores VPN.

Autenticación en el nivel de equipo con Intercambio de claves por red (IKE). Para establecer una asociación de seguridad (SA) de protocolo de seguridad de Internet (IPsec), el cliente VPN y el servidor VPN usan el protocolo IKE para intercambiar los certificados de equipo o una clave previamente compartida. En cualquiera de los casos, el cliente y el servidor VPN se autentican mutuamente en el nivel de equipo. La autenticación de certificados de equipo es un método de autenticación mucho más seguro y, por lo tanto, es muy recomendable. Las conexiones IKE versión 2 o protocolo de túnel de capa dos (L2TP)/IPsec usan la autenticación en el nivel de equipo.

Autenticación del origen de datos e integridad de datos. Para comprobar que los datos enviados en la conexión VPN se originaron al otro extremo de la conexión y no se modificaron durante el tránsito, los datos contienen una suma de comprobación criptográfica basada en una clave de cifrado que solo conocen el destinatario y el remitente. La autenticación del origen de datos y la integridad de datos están disponibles para las conexiones IKE versión 2 y L2TP/IPsec.

- **Cifrado de datos**. Para garantizar la confidencialidad de los datos mientras recorren la red compartida o pública, el remitente cifra los datos y el destinatario los descifra. El proceso de cifrado y descifrado depende de que tanto el remitente como el receptor usen una clave de cifrado común.

Los paquetes interceptados enviados con la conexión VPN en la red de tránsito son ininteligibles para cualquier persona que no tenga la clave de cifrado común. La longitud de la clave de cifrado es un importante parámetro de seguridad. Puede usar técnicas de cálculo para determinar la clave de cifrado. Sin embargo, dichas técnicas requieren mayor capacidad de proceso y tiempo de cálculo a medida que aumenta el tamaño de las claves de cifrado. Por lo tanto, es importante usar claves del mayor tamaño posible para garantizar la confidencialidad de los datos. (Microsoft, 2012).

1.3.4 Protocolos usados en vpn

IPsec: IPsec es una abreviación de Protocolo de Seguridad en Internet. IPsec es un protocolo de VPN que se usa para proteger la comunicación por internet a través de una red IP. Se establece un túnel en un sitio remoto que permite el acceso a tu sitio central. Una IPsec funciona protegiendo la comunicación del protocolo de internet verificando cada sesión y codificando individualmente los paquetes de datos durante la conexión. Hay dos modos en los que opera una VPN IPsec, y son el de transporte y el de túnel. Ambos modos protegen la transferencia de datos entre dos redes diferentes. Durante el modo transporte, se codifica el mensaje en el paquete de datos. En el modo túnel, todo el paquete de datos está encriptado. Un beneficio de usar una VPN IPsec es que también se puede emplear junto con otros protocolos de seguridad para brindar un sistema más robusto.

Aunque una IPsec es una VPN valiosa, una gran desventaja de utilizar este protocolo son las instalaciones costosas y que demoran mucho tiempo en el lado del cliente que deben existir antes del uso. (Frenkel, 2017).

VPN PPTP

PPTP es la abreviatura de Protocolo de Túnel Punto a Punto (en inglés, Point-to-Point Tunneling Protocol). Como su nombre lo indica, una VPN PPTP crea un túnel y captura los datos. Un nombre bastante largo para la VPN más utilizada. Las VPN PPTP son empleadas por usuarios remotos para conectarse a la red de VPN mediante su red de internet existente. Resulta útil para empresas y uso hogareño. Para acceder a la VPN, los usuarios inician sesión con una contraseña aprobada. Las VPN PPTP son ideales para uso personal y empresarial porque no requieren la compra o instalación de hardware adicional y funciones habitualmente ofrecidas como programas complementarios baratos. Las VPN PPTP se usan ampliamente también por su compatibilidad con Windows, Mac y Linux.

Aunque parezca tener muchos beneficios, hay una desventaja de esta VPN, y es que no brinda codificación, que es usualmente la razón por la que uno conseguiría una VPN. Otra desventaja es que depende del PPP o Protocolo de Punto a Punto para implementar medidas de seguridad. (Frenkel, 2017).

VPN L2TP

L2TP es la abreviatura de Protocolo de Establecimiento de Túneles (en inglés, Layer to Tunneling Protocol) y fue desarrollado por Microsoft y Cisco. Las VPN L2TP típicamente están combinadas con otro protocolo de seguridad de VPN para establecer una conexión más segura. Una VPN L2TP forma un túnel entre dos puntos de conexión L2TP, y otra VPN como el protocolo IPSec encripta los datos y se focaliza en asegurar la comunicación entre los túneles.

Una L2TP también es similar a PPTP. Las similitudes existen en términos de su falta de encriptación y en que ambas dependen de protocolos PPP para hacerlo. Comienzan a diferenciarse en relación a la confidencialidad e integridad de los datos. Las VPN L2TP brindan ambos, mientras que las VPN PPTP no. (Frenkel, 2017).

SSL y TLS

SSL significa Secure Sockets Layer y TLS es la abreviatura de Transport Layer Security. Ambas funcionan como un protocolo, utilizadas para crear una conexión VPN. Se trata de una conexión de VPN donde el navegador web funciona como cliente, y el acceso del usuario está restringido a aplicaciones específicas en lugar de poder acceder a toda la red. El protocolo SSL y TLS se utiliza principalmente en sitios web de compras y proveedores de servicios. Una VPN SSL y TLS te brinda una sesión segura desde el navegador de tu PC hacia el servidor de la aplicación. Esto se debe a que los navegadores web cambian a SSL fácilmente y casi no requieren ninguna acción por parte del usuario. Los navegadores ya vienen con SSL y TLS integrado. Las conexiones SSL tienen https al inicio de la dirección URL en lugar de http. (Frenkel, 2017).

VPN MPLS

Las VPN de conmutación por etiquetas multi-protocolo o MPLS (por sus siglas en inglés) son usadas con mayor eficacia para conexiones del tipo sitio a sitio. Esto se debe principalmente por el hecho de que las MPLS son la opción más flexible y adaptable. Se trata de un recurso de base estándar que se usa para acelerar la distribución de paquetes de red en múltiples protocolos. Las VPN MPLS son sistemas que están ajustados a ISP. Una VPN ajustada a ISP es cuando dos o más sitios están conectados para formar una VPN utilizando el mismo ISP. Sin embargo, la mayor desventaja de usar una VPN MPLS es el hecho de que la red no es tan fácil de configurar en comparación con otras VPN. Tampoco es sencillo hacer modificaciones. Por eso, este tipo de VPN generalmente es más costoso. (Frenkel, 2017).

VPN Híbrida

Una VPN híbrida combina MPLS y VPN basada en protocolo de seguridad de internet o IPsec, aunque estos dos tipos de VPN se usan por separado en diferentes sitios. Sin embargo, es posible usar ambas en el mismo sitio. Esto se haría con la intención de utilizar la VPN IPsec como un respaldo de la VPN MPLS.

Las IPsec son VPN que requieren un equipamiento por parte del cliente de algunas cosas mencionadas anteriormente. Este equipamiento generalmente viene en forma de rúter o aparato de seguridad multipropósito. A través de este rúter o aparato se codifican los datos y se forma el túnel VPN tal como mencionamos antes. Comparativamente, las VPN MPLS son utilizadas por un operador, mediante el equipamiento en su red.

Para conectarse a estas dos VPN, se establece un portal para eliminar el túnel IPsec en un lado y trazarlo hacia la VPN MPLS en el otro extremo mientras se preserva la seguridad que esta red se propone brindar.

Las VPN híbridas son utilizadas por empresas principalmente porque utilizar MPLS para sus sitios no sería la opción más apropiada. Hay una gran cantidad de ventajas que las MPLS tienen sobre las conexiones de internet públicas, pero su costo es alto. Por eso, utilizar una VPN híbrida te permite acceder al sitio central a través de un sitio remoto. Las VPN híbridas son en general costosas, pero ofrecen gran flexibilidad. (Frenkel, 2017).

1.3.5 Ventajas de la implementación de una VPN

- EL AHORRO DE COSTOS

Permitir a las empresas como sitio principal compartir Internet con oficinas remotas y usuarios ubicados a largas a distancias.

- ESCALABILIDAD

Permitir adaptar nuevas infraestructura de Internet y dispositivos a las grandes empresas que ya tienen definida su topología, igualmente facilita la adición de nuevos usuarios.

- SEGURIDAD

Las VPN incluye los mecanismos de cifrado avanzado y protocolos de autenticación que protegen los datos del acceso no autorizado, permitiendo que terceros no manipulen la información ya que cuenta con un alto grado de integridad de datos. (Salvador, 2008).

Capítulo 2. Desarrollo del diseño para la simulación de VPN entre las sedes propuestas

2.1 Ubicación geográfica de los puntos a interconectar

Para el desarrollo de la monografía se tendrá en cuenta la ubicación geográfica de las tres sedes a interconectar, esta actividad se realizó a través de la herramienta Google Earth Pro.

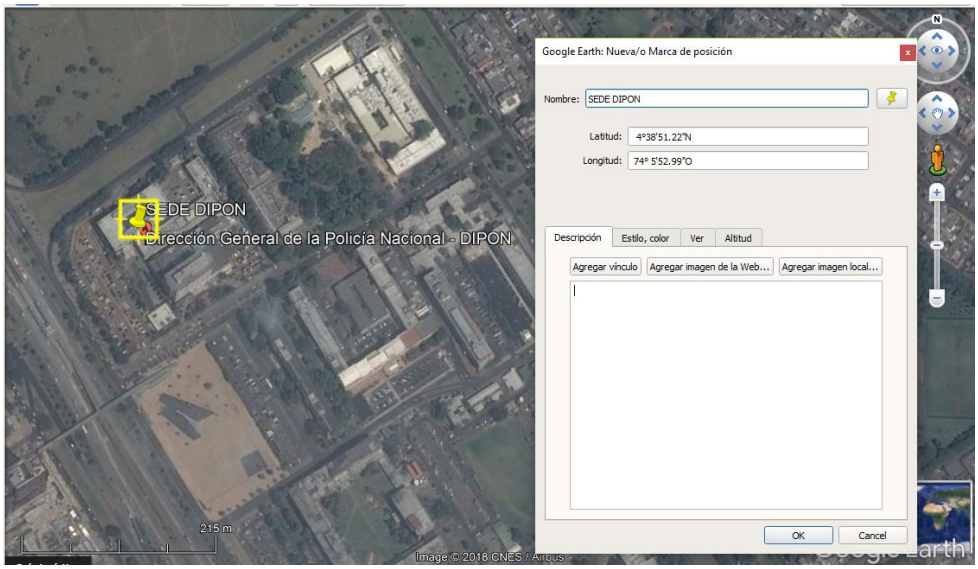

Figura 7. Sede Principal DIPON (Departamento de Cundinamarca)

Fuente. Autor del proyecto

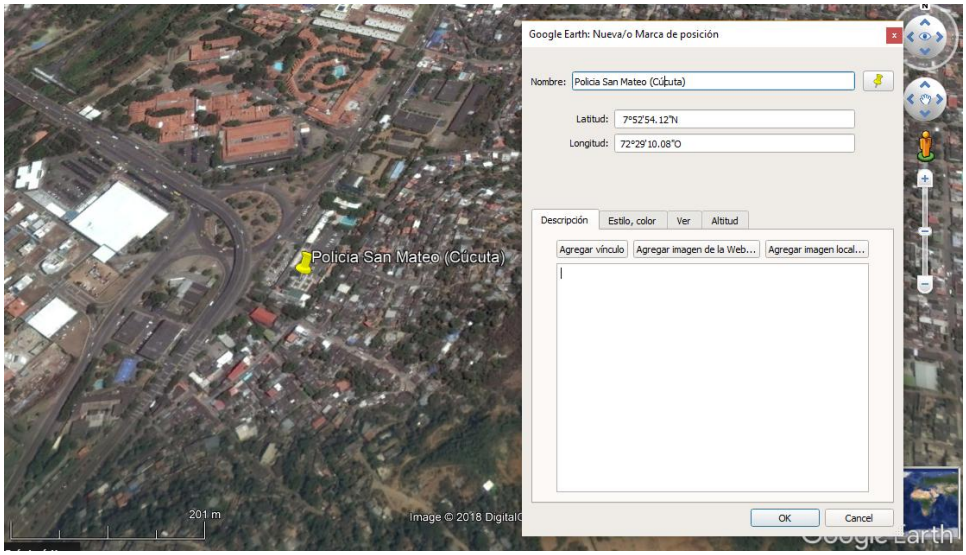

Figura 8. Sede San Mateo Cúcuta (Departamento de Norte de Santander)

Fuente. Autor del proyecto

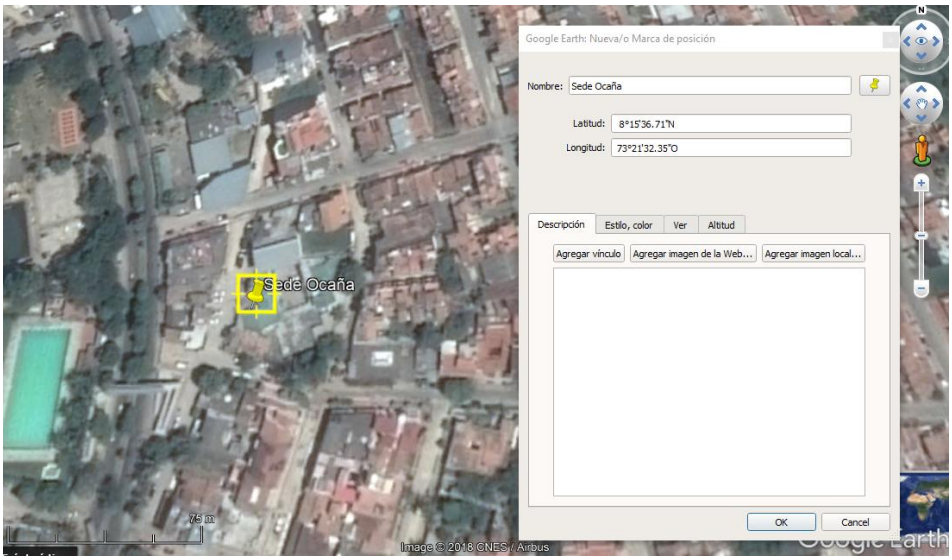

Figura 9. Sede Ocaña (Departamento de Norte de Santander)

Fuente. Autor del proyecto

2.2. Topologia que simula la nube

Teniendo claro la ubicación geográfica de la sedes a interconectar tendremos que simular una red que haga la función de ISP (Proveedor de Servicio de Internet), esta red debe tener como requisito la estructura bajo el protocolo IPv6, de acuerdo a esto simularemos la nube a través de tres routers, y estos podrán comunicarse a través del protocolo de enrutamiento RIP.

En la siguiente figura se observa la topología que simulara la estructura del ISP.

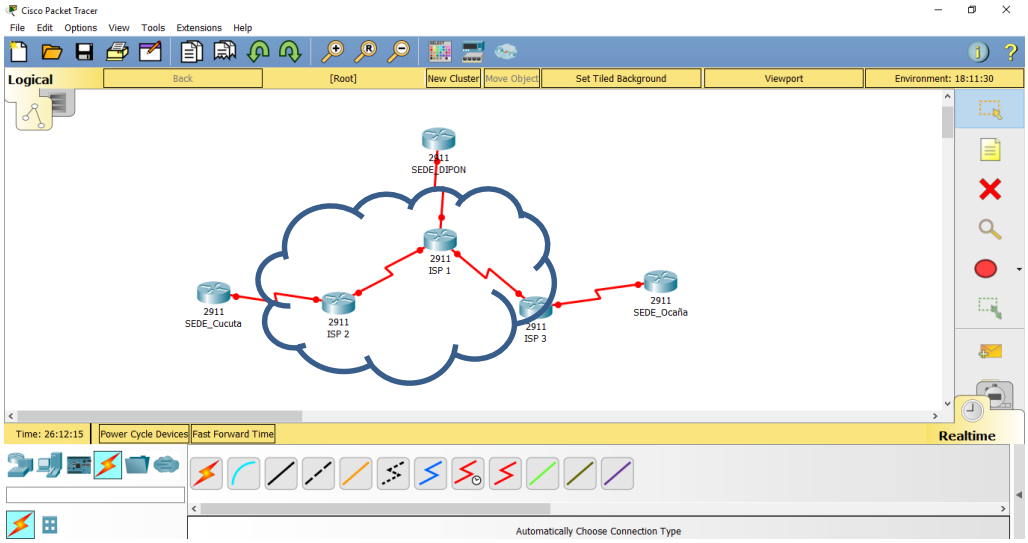

Figura 10. Topología que simula la nube

Fuente. Autor del proyecto

Capítulo 3. Direccionamiento del proveedor de internet en la nube

3.1 Direccionamiento propuesto

Tabla 1. Direccionamiento propuesto

Nodo	Equipo Cisco	Interface	Dirección IPv6
ISP 1	Router 2911	S0/0/0	2001:db8:cafe:6::0/127
		S0/0/1	2001:db8:cafe:7::0/127
		S0/1/0	2001:db8:cafe:8::0/127
ISP 2	Router 2911	S0/0/1	2001:db8:cafe:2::1/122
		S0/0/0	2001:db8:cafe:6::1/127
ISP 3	Router 2911	S0/0/1	2001:db8:cafe:3::1/121
		S0/0/0	2001:db8:cafe:7::1/127

Fuente. Autor del proyecto

3.2 Configuración de los routers

Configuración de los routers que permiten la simulación del ISP en IPv6 con el protocolo de enrutamiento RIP

Nodo ISP 1

Router>enable

```
Router#configure terminal
Router(config)#hotname ISP1
ISP1(config)#ipv6 unicast-routing
ISP1(config)#interface serial 0/0/0
ISP1(config-if)#ipv6 address 2001:db8:cafe:6::0/127
ISP1(config-if)#no shutdown
ISP1(config)#interface serial 0/0/1
ISP1(config-if)#ipv6 address 2001:db8:cafe:7::0/127
ISP1(config-if)#no shutdown
ISP1(config-if)#exit
ISP1(config)#interface serial 0/1/0
ISP1(config-if)#ipv6 address 2001:db8:cafe:8::0/127
ISP1(config-if)#no shutdown
ISP1(config-if)#exit
ISP1(config)#ipv6 unicast-routing
ISP1(config)#ipv6 router rip NUBE
ISP1(config-if)#ipv6 rip NUBE enable
ISP1(config-if)#interface serial 0/0/0
ISP1(config-if)#ipv6 rip NUBE enable
ISP1(config-if)#interface serial 0/0/1
ISP1(config-if)#ipv6 rip NUBE enable
ISP1(config-if)#interface serial 0/1/0
ISP1(config-if)#exit
```

ISP1(config)#exit

ISP1#wr

Building configuration...

[OK]

ISP1#

Nodo ISP 2

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname ISP2

ISP2(config)#ipv6 unicast-routing

ISP2(config)#interface gi

ISP2(config)#interface serial 0/0/0

ISP2(config-if)#ipv6 address 2001:db8:cafe:6::1/127

ISP2(config-if)#no shutdown

ISP2(config-if)#exit

ISP2(config)#ipv6 unicast-routing

ISP2(config)#ipv6 router rip NUBE

ISP2(config-if)#ipv6 rip NUBE enable

ISP2(config-if)#interface serial 0/0/0

ISP2(config)#exit

ISP2#wr

Building configuration...

[OK]

Nodo ISP 3

Router>enable

Router#configure terminal

Router(config)#hostname ISP3

ISP3(config)#ipv6 unicast-routing

ISP3(config)#interface gigabitEthernet 0/0

ISP3(config-if)#ipv6 address 2001:db8:cafe:3::1/121

ISP3(config-if)#no shutdown

ISP3(config)#interface serial 0/0/0

ISP3(config-if)#ipv6 address 2001:db8:cafe:7::1/127

ISP3(config-if)#no shutdown

ISP3(config-if)#exit

ISP3(config)#ipv6 unicast-routing

ISP3(config)#ipv6 router rip NUBE

ISP3(config-if)#ipv6 rip NUBE enable

ISP3(config-if)#interface serial 0/0/0

ISP3(config-if)#exit

ISP3(config)#exit

ISP3#wr

Building configuration...

[OK]

ISP3#

3.3 Vista geográfica

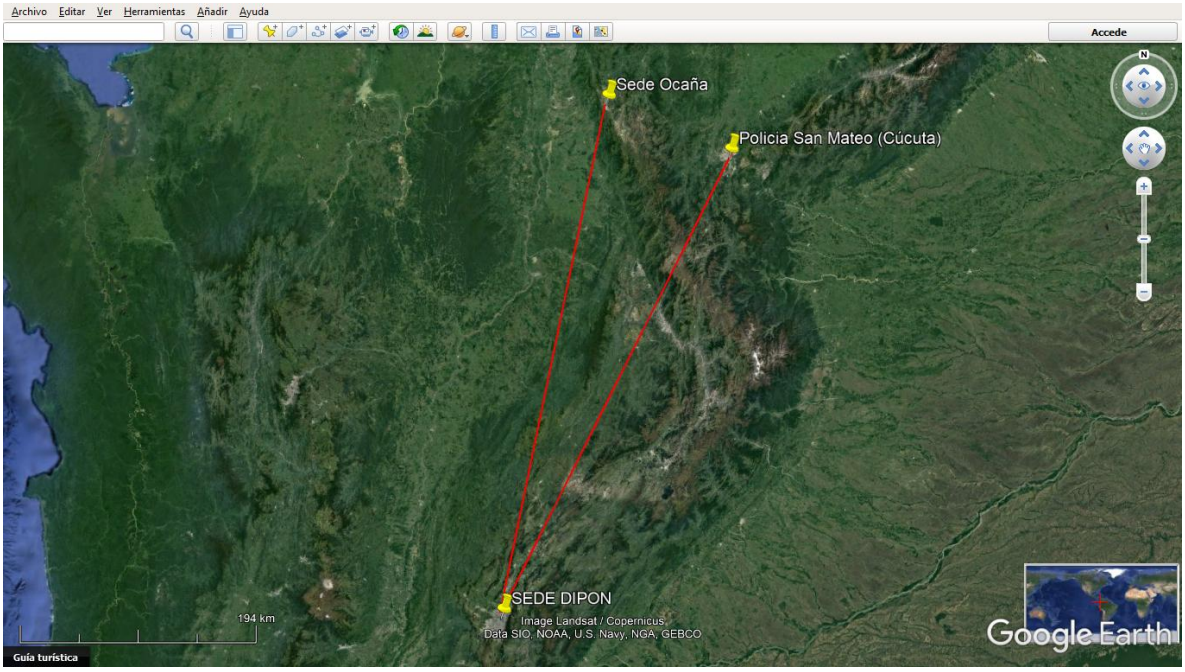

Figura 11. Vista geográfica a través de la herramienta Google Earth

Fuente. Autor del proyecto

Después de tener los tres router que simulan la nube procedemos a realizar la configuración de los tres router que simularan el entorno LAN de los usuarios autorizados para acceder a la VPN.

3.4 Topología De Toda La Red

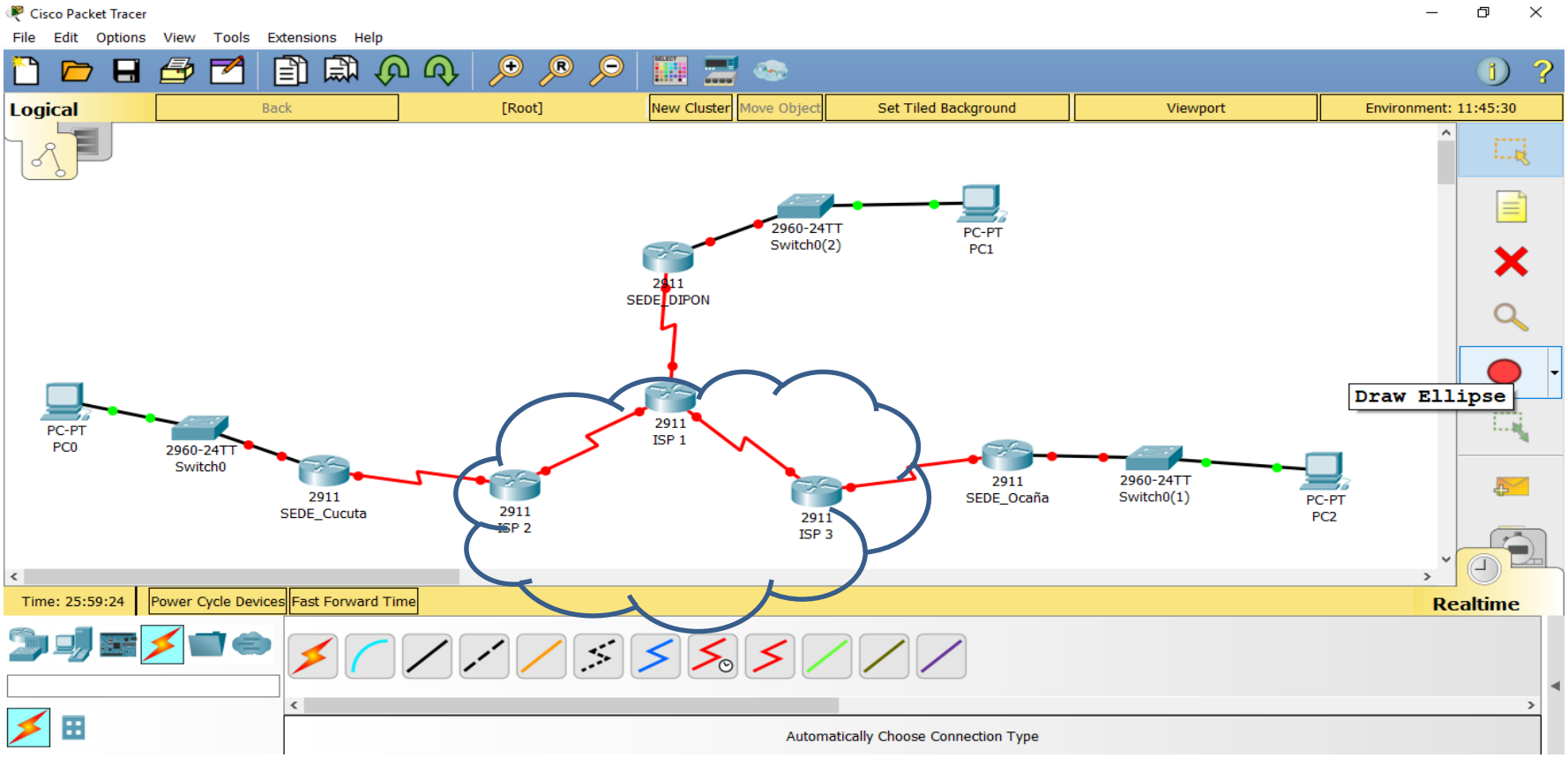

Figura 12. Topología de toda la red

Fuente. Autor del proyecto

3.5 Asignación de direcciones

Tabla 2. Direccionamiento propuesto entre las sedes y los proveedores de internet

Sede	Equipo Cisco	Interface	Dirección IPv6	Cantidad de clientes
DIPON	Router	G0/0	2001:db8:cafe:1::1/121	100
	2911	S0/0/0	2001:db8:cafe:8::1/127	
CUCUTA	Router	G0/0	2001:db8:cafe:2::2/121	100
	2911	S0/0/0	2001:db8:cafe:9::2/127	
OCAÑA	Router	G0/0	2001:db8:cafe:1::1/121	100
	2911	S0/0/0	2001:db8:cafe:7::2/127	

Fuente. Autor del proyecto

3.6 Configuración de los router de las sedes

Sede DIPON

Router>enable

Router#configure terminal

Router(config)#hotname DIPON

DIPON(config)#ipv6 unicast-routing

DIPON(config)#interface gigabitEthernet 0/0

DIPON(config-if)#ipv6 address 2001:db8:cafe:1::1/121

DIPON(config-if)#no shutdown

DIPON(config-if)#exit

DIPON(config)#interface serial 0/0/0

DIPON(config-if)#ipv6 address 2001:db8:cafe:8::1/127

DIPON(config-if)#no shutdown

DIPON(config)#ipv6 unicast-routing

DIPON(config)#ipv6 router rip NUBE

DIPON(config-rtr)#interface gigabitethernet 0/0

DIPON(config-if)#ipv6 rip NUBE enable

DIPON(config-if)#interface serial 0/0/0

DIPON(config-if)#ipv6 rip NUBE enable

DIPON(config-if)#exit

DIPON(config)#exit

DIPON#wr

Building configuration...

[OK]

DIPON#

Sede Cucuta

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname CUCUTA

CUCUTA(config)#ipv6 unicast-routing

CUCUTA(config)#interface gi

CUCUTA(config)#interface gigabitEthernet 0/0

CUCUTA(config-if)#ipv6 address 2001:db8:cafe:2::2/121

CUCUTA(config-if)#no shutdown

CUCUTA(config-if)#exit

CUCUTA(config)#interface serial 0/0/0

CUCUTA(config-if)#ipv6 address 2001:db8:cafe:9::2/127

CUCUTA(config-if)#no shutdown

CUCUTA(config-if)#exit

CUCUTA(config)#ipv6 unicast-routing

CUCUTA(config)#ipv6 router rip NUBE

CUCUTA(config-rtr)#interface gigabitethernet 0/0

CUCUTA(config-if)#ipv6 rip NUBE enable

CUCUTA(config-if)#interface serial 0/0/0

CUCUTA(config)#exit

CUCUTA#wr

Building configuration...

[OK]

Sede Ocaña

```
Router>enable
Router#configure terminal
Router(config)#hostname OCAÑA
OCAÑA(config)#ipv6 unicast-routing
OCAÑA(config)#interface gigabitEthernet 0/0
OCAÑA(config-if)#ipv6 address 2001:db8:cafe:1::1/121
OCAÑA(config-if)#no shutdown
OCAÑA(config-if)#exit
OCAÑA(config)#interface serial 0/0/0
OCAÑA(config-if)#ipv6 address 2001:db8:cafe:7::2/127
OCAÑA(config-if)#no shutdown
OCAÑA(config-if)#exit
OCAÑA(config)#ipv6 unicast-routing
OCAÑA(config)#ipv6 router rip NUBE
OCAÑA(config-rtr)#interface gigabitethernet 0/0
OCAÑA(config-if)#ipv6 rip NUBE enable
OCAÑA(config-if)#interface serial 0/0/0
OCAÑA(config-if)#exit
OCAÑA(config)#exit
OCAÑA#wr
Building configuration...
[OK]
OCAÑA#
```

Con esta configuracion las tres sedes de la institución de policía tienen acceso al servicio de Internet, de acuerdo a esto procedemos a configurar la VPN de tipo sitio a sitio.

La funcionalidad Cisco IOS IPsec proporciona cifrado de datos de red en el nivel de paquete IP, ofreciendo una solución de seguridad robusta y basada en estándares. IPsec proporciona servicios de autenticación y antirreproducción de datos además de los servicios de confidencialidad de datos. Con IPsec, los datos se pueden enviar a través de una red pública sin observación, modificación o suplantación.

3.7 Escenarios de uso general para ipv6 ipsec.

- VPN de sitio a sitio: proteja todo el tráfico de IPv6 entre dos redes confiables
- Tunel seguro configurado: protege el tráfico IPv6 que se está haciendo un túnel a través de una red IPv4 no confiable.
- IPSec también se puede usar para proteger las funciones del plano de control, como IPSec para proteger RIP.

En el ejemplo que se consideró, el túnel protegido por IPSec se configura entre la sede de Bogotá DIPON y la sede Cúcuta y por otro lado la sede Bogotá y la sede Ocaña la idea es que los router pertenecientes a los ISPs no tendrán conocimiento de las subredes privadas.

La VPN de sitio a sitio se configura en el enrutador de la siguiente manera.

Paso 1: configurar la política IKE y la clave previamente compartida entre las sedes del primer brazo

Se configura la misma política ISAKMP en los enrutadores DIPON Y CUCUTA

DIPON # configure terminal

DIPON (config) #crypto isakmp policy 10

DIPON (config-isakmp) #encryption 3des

DIPON (config-isakmp) #grupo 2

DIPON (config-isakmp) #authentication pre-share

DIPON (config-isakmp) #exit

DIPON (config) #crypto isakmp key 0 ipsecvpn dirección ipv6 2001:: 1/128

DIPON (config) #CNTL / Z

CUCUTA # configure terminal

CUCUTA (config) #crypto isakmp policy 10

CUCUTA (config-isakmp) #encryption 3des

CUCUTA (config-isakmp) #grupo 2

CUCUTA (config-isakmp) #authentication pre-share

CUCUTA (config-isakmp) #exit

CUCUTA (config) #crypto isakmp key 0 ipsecvpn dirección ipv6 2002:: 1/128

DIPON (config) #CNTL / Z

Cada enrutador debe configurarse con la misma clave, pero la declaración de configuración debe designar la dirección de la interfaz adecuada en el enrutador par.

Paso 2: configurar un conjunto de transformaciones IPsec y un perfil IPsec. Se Configura el mismo conjunto de transformaciones IPsec y el perfil IPsec en los Router DIPON y CUCUTA

DIPON (config)#crypto ipsec transform-set ipv6_tran esp-3des esp-sha-hmac

DIPON (cfg-crypto-trans)#mode tunnel

DIPON (cfg-crypto-trans)#exit

DIPON (config)#crypto ipsec profile ipv6_ipsec_pro

DIPON (ipsec-profile)#set transform-set ipv6_tran

DIPON (ipsec-profile)#exit

DIPON (config)#

CUCUTA (config)#crypto ipsec transform-set ipv6_tran esp-3des esp-sha-hmac

CUCUTA (cfg-crypto-trans)#mode tunnel

CUCUTA (cfg-crypto-trans)#exit

CUCUTA (config)#crypto ipsec profile ipv6_ipsec_pro

CUCUTA (ipsec-profile)#set transform-set ipv6_tran

CUCUTA (ipsec-profile)#exit

CUCUTA (config)#

Paso 3: configurar un perfil ISAKMP en IPv6. El perfil ISAKMP se configura en los Router DIPON y CUCUTA y garantiza que la declaración de configuración debe designar la dirección de identidad de la interfaz adecuada en el enrutador par.

DIPON(config)#crypto isakmp profile 3des

% A profile is deemed incomplete until it has match identity statements

DIPON (conf-isa-prof)#self-identity address ipv6

DIPON (conf-isa-prof)#match identity address ipv6 2002::1/128

DIPON (conf-isa-prof)#keyring default

DIPON (conf-isa-prof)# exit

DIPON (config)#

CUCUTA(config)#crypto isakmp profile 3des

% A profile is deemed incomplete until it has match identity statements

CUCUTA (conf-isa-prof)#self-identity address ipv6

CUCUTA (conf-isa-prof)#match identity address ipv6 2001::1/128

CUCUTA (conf-isa-prof)#keyring default

CUCUTA (conf-isa-prof)# exit

CUCUTA (config)#

Paso 4: configurar ipsec IPv6 VTI en los router.

DIPON(config)#int tunnel 1

DIPON (config-if)#ipv6 enable

DIPON (config-if)#ipv6 address 2012::1/64

DIPON (config-if)#tunnel source 2001::1

DIPON (config-if)#tunnel destination 2002::1

DIPON (config-if)#tunnel mode ipsec ipv6

DIPON (config-if)#tunnel protection ipsec profile ipv6_ipsec_pro

*Jan 1 01:32:30.907: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

DIPON (config-if)#exit

CUCUTA(config)#int tunnel 1

CUCUTA (config-if)#ipv6 enable

CUCUTA (config-if)#ipv6 address 2012::2/64

CUCUTA (config-if)#tunnel source 2002::1

CUCUTA (config-if)#tunnel destination 2001::1

CUCUTA (config-if)#tunnel mode ipsec ipv6

CUCUTA (config-if)#tunnel protection ipsec profile ipv6_ipsec_pro

*Jan 1 01:32:30.907: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

CUCUTA (config-if)#exit

La configuración para el brazo entre DIPON y OCAÑA es de la siguiente manera

Paso 1: configurar la política IKE y la clave previamente compartida entre las sedes del primer brazo

Se configura la misma política ISAKMP en los enrutadores DIPON Y CUCUTA

DIPON # configure terminal

DIPON (config) #crypto isakmp policy 10

DIPON (config-isakmp) #encryption 3des

DIPON (config-isakmp) #grupo 2

DIPON (config-isakmp) #authentication pre-share

DIPON (config-isakmp) #exit

DIPON (config) #crypto isakmp key 0 ipsecvpn dirección ipv6 2001:: 1/128

DIPON (config) #CNTL / Z

OCAÑA # configure terminal

OCAÑA (config) #crypto isakmp policy 10

OCAÑA (config-isakmp) #encryption 3des

OCAÑA (config-isakmp) #grupo 2

OCAÑA (config-isakmp) #authentication pre-share

OCAÑA (config-isakmp) #exit

OCAÑA (config) #crypto isakmp key 0 ipsecvpn dirección ipv6 2002:: 1/128

OCAÑA (config) #CNTL / Z

Cada enrutador debe configurarse con la misma clave, pero la declaración de configuración debe designar la dirección de la interfaz adecuada en el enrutador par.

Paso 2: configurar un conjunto de transformaciones IPsec y un perfil IPsec. Se Configura el mismo conjunto de transformaciones IPsec y el perfil IPsec en los Router DIPON y OCAÑA

DIPON (config)#crypto ipsec transform-set ipv6_tran esp-3des esp-sha-hmac

DIPON (cfg-crypto-trans)#mode tunnel

DIPON (cfg-crypto-trans)#exit

DIPON (config)#crypto ipsec profile ipv6_ipsec_pro

DIPON (ipsec-profile)#set transform-set ipv6_tran

DIPON (ipsec-profile)#exit

DIPON (config)#

OCAÑA (config)#crypto ipsec transform-set ipv6_tran esp-3des esp-sha-hmac

OCAÑA (cfg-crypto-trans)#mode tunnel

OCAÑA (cfg-crypto-trans)#exit

OCAÑA (config)#crypto ipsec profile ipv6_ipsec_pro

OCAÑA (ipsec-profile)#set transform-set ipv6_tran

OCAÑA (ipsec-profile)#exit

OCAÑA (config)#

Paso 3: configurar un perfil ISAKMP en IPv6. El perfil ISAKMP se configura en los Router DIPON y OCAÑA y garantiza que la declaración de configuración debe designar la dirección de identidad de la interfaz adecuada en el enrutador par.

DIPON(config)#crypto isakmp profile 3des

% A profile is deemed incomplete until it has match identity statements

DIPON (conf-isa-prof)#self-identity address ipv6

DIPON (conf-isa-prof)#match identity address ipv6 2002::1/128

DIPON (conf-isa-prof)#keyring default

DIPON (conf-isa-prof)# exit

DIPON (config)#

OCAÑA(config)#crypto isakmp profile 3des

% A profile is deemed incomplete until it has match identity statements

OCAÑA (conf-isa-prof)#self-identity address ipv6

OCAÑA (conf-isa-prof)#match identity address ipv6 2001::1/128

OCAÑA (conf-isa-prof)#keyring default

OCAÑA (conf-isa-prof)# exit

OCAÑA (config)#

Paso 4: configurar ipsec IPv6 VTI. Configurar IPv6 IPsec VTI en los router

DIPON(config)#int tunnel 1

DIPON (config-if)#ipv6 enable

DIPON (config-if)#ipv6 address 2012::1/64

DIPON (config-if)#tunnel source 2001::1

DIPON (config-if)#tunnel destination 2002::1

DIPON (config-if)#tunnel mode ipsec ipv6

DIPON (config-if)#tunnel protection ipsec profile ipv6_ipsec_pro

*Jan 1 01:32:30.907: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

DIPON (config-if)#exit

OCAÑA(config)#int tunnel 1

OCAÑA (config-if)#ipv6 enable

OCAÑA (config-if)#ipv6 address 2012::2/64

OCAÑA (config-if)#tunnel source 2002::1

OCAÑA (config-if)#tunnel destination 2001::1

OCAÑA (config-if)#tunnel mode ipsec ipv6

OCAÑA (config-if)#tunnel protection ipsec profile ipv6_ipsec_pro

*Jan 1 01:32:30.907: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

OCAÑA (config-if)#exit

Conclusiones

A través del curso de profundización ofrecido por la Universidad Francisco de Paula Santander Ocaña soportado por el laboratorio de redes y telecomunicaciones, se adquirió diferentes competencias enmarcadas en un contexto teórico-práctico aplicable al diseño y configuración de dispositivos Cisco bajo el protocolo IPV6.

Con el análisis sobres las VPN´s se pudo determinar la viabilidad para trabajar sobre la misma infraestructura de red que posee la institución Policía Nacional poder interconectar la oficina principal con sus diferentes sucursales y usuarios remotos proporcionando mayor rapidez, seguridad y confiabilidad.

Mediante la investigación realizada nos pudimos dar cuenta que con el protocolo de seguridad IPsec además de proporcionar servicios de autenticación y confiabilidad los datos se pueden enviar a través de una red pública sin observación, modificación o suplantación.

Se plantea el diseño de una topología basado en IPv6 bajo un protocolo de enrutamiento, RIP, impartido en el curso de profundización como parte de la práctica y su respectiva configuración para hacer más segura la información de la institución Policía Nacional.

Referencias

A. Forouzan, B. (2007). *Transmisión de Datos y Redes de Telecomunicaciones* (Cuarta Edición ed.). Mc Graw Hil.

Ariganello, E. (2014). *REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching.* México: Alfaomega.

Charcotsicas Tsantarliotou, E., & Gimenéz Silva, A. (Febrero de 2012). Recuperado el 11 de Mayo de 2017, de http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAS3510.pdf

Cisco. (2012). Obtenido de https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

Cisco. (2015). Recuperado el 18 de Enero de 2018, de http://mixteco.utm.mx/~resdi/historial/materias/router.pdf

Colomès, P. (7 de OCTUBRE de 2010). *REDESCISCO.NET*. Obtenido de http://www.redescisco.net/sitio/2010/10/07/interconectando-sucursales-mediante-una-vpn-ipsec-site-site/

Comunidad de soporte técnico de Apple. (13 de Marzo de 2015). Recuperado el 5 de Junio de 2017, de https://support.apple.com/es-mx/HT202236

de De Hart, M. E. (14 de Julio de 2003). *MINTIC.* Recuperado el 11 de Mayo de 2017, de http://www.mintic.gov.co/portal/604/articles-3644_documento.pdf

Ejercito Nacional. (s.f). Obtenido de https://www.ejercito.mil.co/?idcategoria=348551

Fernandez, D. (Febrero de 2017). *Repositorio Digital UPS*. Obtenido de https://dspace.ups.edu.ec/handle/123456789/754

Frenkel, A. (27 de febrero de 2017). *vpnMentor*. Obtenido de https://es.vpnmentor.com/blog/diferentes-tipos-de-vpn-y-cuando-usarlas/

Google Earth. (s.f.). Obtenido de https://www.google.com.co/maps/place/Oca%C3%B1a,+North+Santander/@8.252365,-73.3683531,13.25z/data=!4m5!3m4!1s0x8e677beeab6ce443:0x24747bfaf0798150!8m2!3d8.25205!4d-73.3532199?hl=en

Goujon, A. (12 de septiembre de 2012). *WeliveSecurity*. Obtenido de https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

GuilleSQL. (17 de Marzo de 2008). *GuilleSQL Un Portal sobre Microsoft SQL Server en Castellano*. Recuperado el 19 de Mayo de 2017, de http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx

Microsoft. (2012). *Windows Server*. Obtenido de https://technet.microsoft.com/es-es/library/dd469653(v=ws.11).aspx

Salvador. (24 de Mayo de 2008). *Importancia de las VPN en las pequeñas y medianas empresas*. Obtenido de http://redesvirtualesprivadas.blogspot.com.co/

Seoane Balado, E. (2005). *La nueva era del comercio: el comercio electrónico : las TIC al servicio de la gestión empresarial.* IDEASPROPIAS.

Stallings, W. (2004). *Comunicaciones y Redes de Computadores* (Séptma Edición ed.). PEARSON Prentice Hall.

Suarez Pantano, C. A., Duarte López, A. M., & Arcos Moreno, J. E. (2015). Recuperado el 11 de Mayo de 2017, de

http://repository.poligran.edu.co/bitstream/10823/841/1/DISENO%20DE%20UNA%20RED%20DE%20SERVICIOS%20DE%20VOZ%2C%20CONECTIVIDAD....pdf

Vialfa, C. (17 de octubre de 2016). *ccm*. Obtenido de http://es.ccm.net/contents/258-vpn-redes-privadas-virtuales

Apéndice

Equipos ideales para la configuración

- **Router 2911 Cisco**

Figura 13. Router 2911 Cisco

Fuente: (Cisco, s.f)

Los routers son computadoras dedicadas al procesamiento de la interconexión de redes, que no incluyen monitor, ni teclado, ni ratón, por lo que debe comunicarse con ellos de una de las siguientes formas:

- Desde una terminal (PC o estación de trabajo funcionando en modo terminal) conectada a él mediante un cable.
- Mediante un punto de la red. Dado que los routers son los enlaces que mantienen unidas las redes, el diseño de medidas de seguridad dentro de ellos es muy importante; la primera

medida que se debe tomar en cuenta es la asignación de contraseña para no permitir el acceso al público en general y en especial a los hackers. Routers cisco se utilizan las contraseñas para restringir el acceso a:

- El dispositivo.
- La parte EXEC privilegiada (modo habilitar) del entorno del software IOS (Internetwork Operating System).
- El uso de comandos específicos del IOS.

El router es la estructura básica de las redes, que cuenta con las siguientes capacidades:

- Puede soportar simultáneamente diferentes protocolos (Ethernet, Token Ring, RDSI, y otros), haciendo compatible todos los equipos en la capa de red.
- Conecta a la perfección LAN a WAN.
- Filtra al exterior el tráfico no deseado aislando áreas en las que los mensajes se pueden difundir a todos los usuarios de una red.
- Actúan como puertas de seguridad comprobando el tráfico mediante listas de permisos de acceso.
- Asegura fiabilidad, ofreciendo múltiples trayectorias a través de las redes.
- Aprende automáticamente nuevas trayectorias y selecciona las mejores. (Cisco, 2015).

➢ **Switch 2960 Cisco**

Figura 14. **Switch 2960 Cisco**

Fuente: (Cisco, 2012)

Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad.

Existen dos tipos básicos de switches: administrados y no administrados.

Los switches no administrado funcionan de forma automática y no permiten realizar cambios. Los equipos en redes domésticas suelen utilizar switches no administrados.

Los switches administrados permiten su programación. Esto proporciona una gran -exibilidad porque el switch se puede supervisar y ajustar de forma local o remota para proporcionarle control sobre el desplazamiento del tráfico en la red y quién tiene acceso a la misma. (Cisco, 2012).