PROPUESTA PARA LA IMPLEMENTACIÓN DE UNA VPN EN RCN TV

MONOGRAFÍA

LUIS ERNESTO RAMÍREZ PÁEZ

Director:

FELIPE DÍAZ-SÁNCHEZ, PhD

Codirector:

GUSTAVO ALONSO CHICA PEDRAZA, PhD (c)

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ, 2018

Contenido

Lista de Figuras

Lista de Tablas

ACRÓNIMOS

Acrónimo	Definición
VPN	Del inglés Virtual Private Network. Red privada virtual
IPsec	Del inglés Internet Protocol Security. Protocolo de seguridad de internet
SSL/TLS	Del inglés Secure Sockets Layer / Transport Layer Secure. Capa de puertos seguros / Capa de transporte seguro
AHP	Del inglés Analytic Hierarchy Process. Proceso analítico jerárquico
AH	Del inglés Authentication Header. Cabecera de autenticación
ESP	Del ingles Encapsulating Security Payload. Carga útil segura encapsulada
RFC	Del inglés Request For Comments.
DES	Del inglés Data Encryption Standard. Estándar de cifrado de datos.
AES	Del inglés Advanced Encryption Standard. Estándar de cifrado avanzado.
SHA	Del inglés Secure Hash Algorithm.
MD5	Del inglés Message-Digest Algorithm.
PKI	Del inglés Public Key Infrastructure. Infraestructura de clave pública
RSA	Del inglés Rivest Shamir Adleman

RESUMEN

En el siguiente documento se presenta un estudio para la posible implementación de una VPN IPsec en la red privada de la empresa RCN TV, teniendo en cuenta diferentes apartados que puedan influir en la factibilidad del proyecto, además se realiza una comparativa entre VPN IPsec y SSL/TLS, siendo la segunda una de las rivales directas de IPsec en el mercado en cuanto a VPN se refiere. Para esto se deben tener en cuenta factores como: facilidad de instalación, control de usuarios, escalabilidad, encriptación, alcance.

Palabras clave: IPsec, VPN, Control de usuarios, Encriptación, SSL/TLS, escalabilidad.

ABSTRACT

The following document is submitted a study to the possible implementation of an IPsec VPN on the corporate private network RCN TV, taking into account different sections that may have an impact on the feasibility of the project, in addition to a comparison between SSL/TLS and IPsec VPN, being the first one of the IPsec direct rivals in the market with regard to VPN. For this, they must take into account factors such as: ease of installation, user control, scalability, encryption, scope.

Keywords: IPsec VPN, User Control, encryption, SSL/TLS, scalability.

INTRODUCCIÓN

La implementación de una VPN en una empresa de gran tamaño es muy importante y necesaria para el crecimiento, facilidad en la comunicación y transporte de información dentro de la misma, esto siempre y cuando se mantenga la seguridad e integridad de los datos compartidos por medio de la red, para lo cual es necesario un protocolo que permita el cifrado y la protección de la información en las comunicaciones punto a punto; para este caso se tiene dos protocolos de seguridad para el transporte de los datos, el primero es IPsec sobre el cual se piensa centrar esta investigación, y el segundo SSL/TLS que es más utilizado y servirá como referencia para determinar los pros y contras de IPsec, con respecto al resto de sus competidores en el mercado .

Actualmente, la empresa RCN no cuenta con una red VPN, esto es una gran limitante para la organización, ya que todo lo que tenga que ver con acceso remoto, transferencia de archivos y comunicaciones en general se debe hacer por medios no tan seguros y de una manera independiente, lo cual puede generar vulnerabilidades en la red del canal; por estas razones es muy importante tener una red VPN propia con una gestión centralizada, en la que un funcionario decida cuales son los permisos de acceso que debe tener cada integrante del canal.

El problema nace a partir de la necesidad de implementar una VPN en la empresa RCN TV, esto con el fin de facilitar las comunicaciones internas de la misma, Ahora bien, es de gran relevancia realizar un estudio y un análisis sobre la posible implementación de uno u otro tipo de VPN en la empresa, teniendo en cuenta que para este caso se enfatiza en el protocolo IPsec, pero realizando una comparativa con el protocolo SSL/TLS, más común y utilizado alrededor del mundo. Por lo cual se deben tener en cuenta diferentes factores que pueden influir en la decisión final del tipo de implementación a realizar, entre los cuales están, la encriptación, la escalabilidad, el alcance y control de usuario.

Por lo cual al final se tendrán algunas recomendaciones en las que se justifique el por qué la empresa debe o no implementar uno de estos tipos de VPN en su red interna, teniendo en cuenta que al final será la empresa quien determine la factibilidad sobre el proyecto, y tomará este documento como una guía para orientar sus necesidades.

1. MARCO GENERAL DEL PROYECTO

El objetivo de este capítulo es dar las herramientas a los jurados para evaluar la consecución de los objetivos del trabajo de grado y facilitar la lectura del documento. Haga una pequeña introducción al capítulo antes de entrar a abordar los apartados, y esto téngalo en cuenta para el desarrollo de todos los capítulos de su documento.

1.1 OBJETIVOS

Implementar una red privada virtual (VPN[1]) en RCN TV.

- ➢ Identificar y caracterizar los tipos de VPN.
- ➢ Realizar análisis en protocolos de cifrado y seguridad para la comunicación de los tipos de VPN.
- ➢ Analizar las necesidades de la empresa, para determinar cuál VPN se ajusta mejor a los requerimientos.
- ➢ Utilizar método AHP para comparar tipos de VPN e identificar la más factible para su implementación.
- ➢ Proponer tipo de VPN y configuración de la misma sobre firewall FORTINET.

1.2 ALCANCE

El objetivo final de esta investigación es aportar recomendaciones a la empresa sobre los tipos de VPN y cuál puede ser la mejor opción para el respectivo despliegue en las instalaciones de la organización, todo esto sustentado debidamente con la documentación correspondiente, además de la posible implementación de una la VPN en RCNTV usando uno de los métodos más comunes, el cual es a través de un Firewall, esto se explicará más adelante en el documento

[1] Por sus siglas en inglés, Virtual Private Network (VPN).

1.3 METODOLOGÍA

Como primera instancia es necesario identificar las características más importantes de ambos protocolos IPSec y SSL/TLS, para de esta forma tener una base en la cual sustentar los juicios a realizar posteriormente.

Como segunda instancia se identifica la implementación más factible en cuanto al despliegue de la VPN, ya sea a través de un router, un firewall, un software etc. Más adelante serán detalladas cada una de estas alternativas.

Como tercera instancia se tiene la necesidad de comparar dos posibles alternativas para la solución de este problema, por lo cual se requiere de la implementación de algún método que sea capaz de soportar juicios tanto objetivos como subjetivos, valores teóricos como prácticos, y se encuentra como mejor opción el método AHP el cual cómo será detallado más adelante presenta una forma muy simplificada de realizar comparaciones mediante criterios en común de las dos alternativas.

Por último, en concordancia con la segunda instancia, será realizado un manual paso a paso de cómo realizar la respectiva configuración e instalación de la respectiva VPN, teniendo en cuenta la forma de implementación elegida.

2 MARCO CONCEPTUAL

2.1 REDES PRIVADAS VIRTUALES

En primera instancia las redes virtuales (VPN) permiten la interacción entre hosts y usuarios distribuidos geográficamente en diferentes lugares, y la administración de estos por parte de una misma entidad. Estas también permiten la división de una red física en redes virtuales separadas.

Ahora bien, las redes privadas incorporan protección de los datos garantizada entre los hosts de la red virtual, permitiendo conexiones confiables dentro de la red. Con confidencialidad y privacidad, las VPN pueden atravesar redes no confiables, así como compartir redes físicas con partes no confiables.

Las VPN's se pueden crear en base a los siguientes protocolos: MPLS, PPTP, L2TP, IPSec y SSL/TLS; los tres primeros operan en la capa 2 del modelo OSI (enlace de datos) el cuarto en la capa 3 (Red) y el quinto de la capa 4 (Transporte) hasta la capa de aplicación, para este caso se tienen en cuenta los últimos dos. [5] [13]

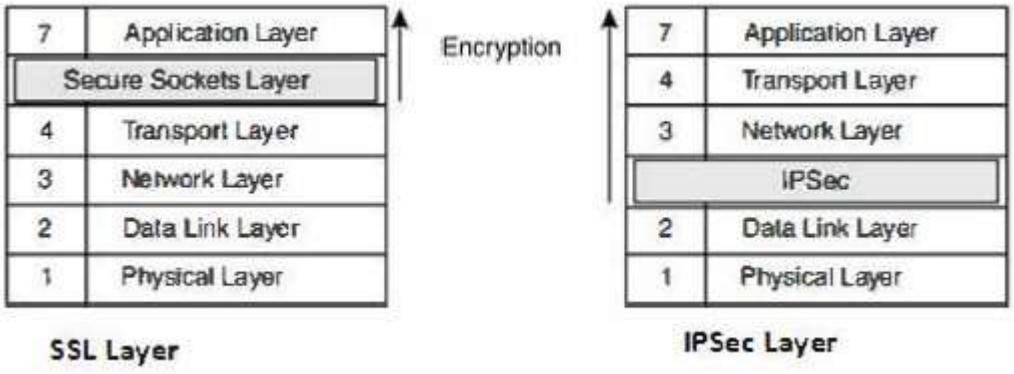

Figura 1: SSL/TLS e IPSec ubicados en el modelo OSI [5]

2.1.1 Arquitecturas VPN

Existen principalmente dos tipos de arquitecturas VPN, las cuales se determinan dependiendo de los requerimientos de la empresa en cuanto a disponibilidad de la VPN y

tipo de conexión, que se puede mantener de manera constante o que se puedan crear y destruir en cualquier instante, para esto se tienen VPN's sitio a sitio y de conexión remota.

2.1.2 VPNS sitio a sitio

Este tipo de VPN se implementa cuando las dos partes de la conexión VPN saben exactamente cuál es la configuración de la VPN con anticipación, de esta manera la conexión permanece estática y sus configuraciones son reiniciadas solo en caso de que ocurra un inconveniente. En la VPN sitio a sitio los gateway de cada red son los encargados de establecer la VPN, es decir, el tráfico IP viaja normalmente desde el host hasta su Gateway, y este es el encargado de realizar el respectivo cifrado y redirigir el paquete a través del túnel VPN el cual se conectará a internet para así llegar al Gateway destino, cuando este reciba el tráfico cifrado se encargará de eliminar los encabezados y descifrar el contenido para así transmitirlo al host destino. [15]

Son usadas generalmente para conectar redes enteras entre sí, por lo cual se crean enlaces WAN a través de una VPN todo esto utilizando la conexión a internet de un ISP local. Este tipo de VPN se puede dividir en VPN intranet y extranet

2.1.3 VPN intranet

Esta se utiliza para la comunicación interna de una organización, es decir, en caso de que una empresa, puede ser una universidad tenga diferentes sedes, entonces mediante está VPN las puede interconectar de una forma segura. [15]

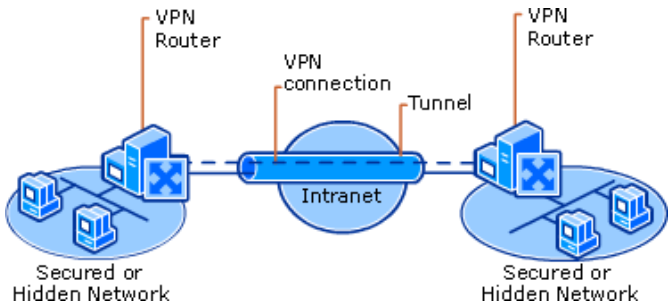

Figura 2: VPN intranet [15]

2.1.4 VPN extranet

Ahora bien, esta arquitectura representa la conexión entre cliente y proveedor, socios o comunidades de interés que implementen una intranet corporativa.

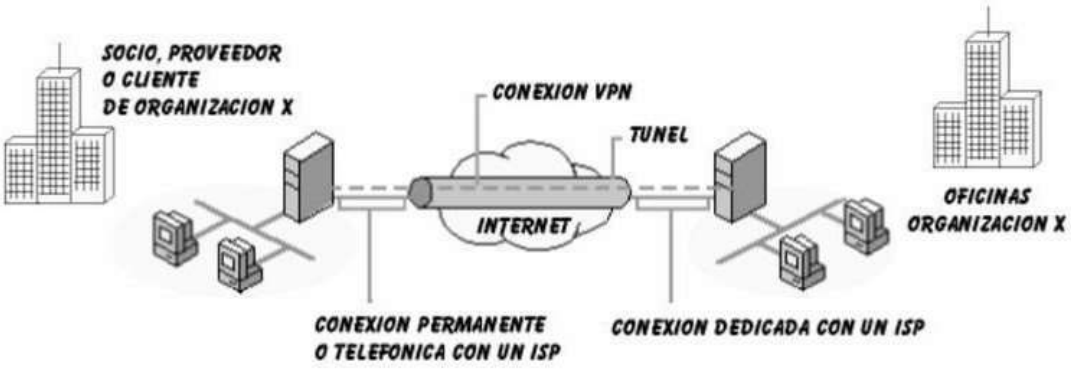

Figura 3: VPN extranet. [15]

2.1.5 VPN de acceso remoto

Por su parte las VPN de acceso remoto cumplen con las demandas de un usuario a distancia, móvil, y de tráfico extranet, ya que le permiten acceder a los recursos de la compañía cuando lo requiera siempre y cuando tenga una conexión a internet.

Esta VPN se implementa cuando la configuración de la conexión no se conoce, es decir no se configura de forma estática, por lo cual mantiene un intercambio dinámico de información.

Para realizar la conexión del host a la red es necesario tener habilitado un cliente VPN, mediante este el usuario es capaz de establecer la conexión con la red corporativa y de esta manera enviar o recibir tráfico hacia o desde la misma. El cifrado del tráfico lo realiza el software del cliente VPN y lo puede descifrar tanto el Gateway de la red como el host destino, esto depende de la configuración de la VPN. [15]

2.1.6 Implementaciones VPN

Una vez realizado el análisis de las arquitecturas utilizadas para una VPN es necesario abordar el apartado de los tipos de implementación; para esto existen diferentes maneras de establecer o crear una VPN, las cuales le permiten al usuario elegir entre tres posibilidades, con diferentes requerimientos de hardware y software, estas son: VPN basadas en Routers, Firewalls y Software.

2.1.7 VPN basadas en routers

En este tipo de implementación se usan routers que tengan la capacidad de establecer una VPN, por lo cual es necesario realizar una de dos acciones, primero se puede instalar directamente en el dispositivo un software que permita el proceso de cifrado, de esta manera los recursos que consuma dicho proceso se tomarán directamente de la CPU y la memoria del router. En un segundo caso se puede insertar una tarjeta externa en el dispositivo, esta se encargará de realizar el cifrado y por lo tanto como hay un nuevo hardware la carga de procesamiento no se aplicará sobre la CPU del procesador, sino que será recibida directamente por la tarjeta externa.

Como se puede observar, la implementación de uno u otro método depende de la capacidad de procesamiento del dispositivo, ya que una sobrecarga de procesos en la CPU podría causar fácilmente que el router se colapse y tenga que ser reiniciado, lo cual sería un gran problema para una empresa que no tenga redundancia y requiera del equipo encendido en todo momento, y aun así, si el equipo puede con la carga adicional, es muy posible que no se obtenga el desempeño esperado por parte del router; por otro lado si se implementa una tarjeta externa, podría ser un poco más costoso que obtener la licencia para un nuevo software, pero el rendimiento del equipo no se vería afectado, por lo cual sería un costo que a largo plazo tendría una buena relación en cuanto a su funcionamiento.

Es necesario verificar que el dispositivo soporte los protocolos de seguridad de internet necesarios para la respectiva implementación de la VPN, estos pueden ser PPTP, L2TP IPSEC, TLS entre otros, todo depende del tipo de VPN que desee implementar el cliente.

2.1.8 VPN basadas en Firewall

Debido a que la mayoría de organizaciones, por no decir todas, se encuentran conectadas a internet a través de un firewall que por lo general es el encargado de realizar el NAT, la forma más común de implementar una VPN es mediante este dispositivo, ya que le permite al usuario usar esta misma infraestructura para establecer la respectiva VPN, lo único que sería necesario añadir para este caso es un software de cifrado en caso de que el firewall no cuente con este, y un software para el cliente en caso de ser necesario, dependiendo del tipo de protocolo a utilizar en la VPN.

Ya que el firewall es un dispositivo como un switch o un router que cuenta con su propia memoria y procesador, es posible que la carga de procesamiento también aumente en caso

de que la cantidad de conexiones mediante VPN sea muy alta, ya que el proceso de cifrado y descifrado consume una gran cantidad de recursos, y esto podría ser un problema mayor, ya que el firewall es el encargado de dar entrada o salida a todos los servicios de la compañía, por lo cual si este falla el daño sería muy grave.

2.1.9 VPN basadas en software

Para este caso por lo general se utiliza un servidor con un sistema operativo como puede ser Windows o Linux que casi siempre viene con un servicio de VPN habilitado, de esta manera la VPN es creada a través del mismo, y se puede mantener una gran cantidad de servicios habilitados, como lo son DNS, servidor web, acceso remoto etc. Para establecer la conexión se utiliza un software en el equipo del cliente.

Una posible desventaja para esta implementación es que la VPN puede ser afectada por las propias vulnerabilidades del sistema operativo, por lo cual es necesario ser muy precavido con los riesgos que se pueden generar, con el fin de mantener la VPN totalmente segura.

2.2 SEGURIDAD EN LAS VPN

Ahora bien, antes de entrar a analizar los distintos protocolos que se pueden utilizar para la implementación de una VPN, es necesario entender cuáles son los parámetros más importantes en cuanto a la seguridad en la transmisión de datos mediante una VPN. Existen muchos apartados que afectan la seguridad en la comunicación, como son: La confidencialidad, integridad, autenticación, disponibilidad, no repudio, no reenvío, entre otros, pero para esta investigación los más importantes y por lo tanto en los cuales se va a profundizar son los tres primeros, ya que estos son los que permiten una conexión segura. [3] [4]

2.2.1 Confidencialidad

Este puede llegar a ser uno de los parámetros más importantes cuando de transmitir información se habla, pero esto depende en gran medida de la sensibilidad de la información que se está tratando, ya que la confidencialidad lo que permite es mantener la información totalmente oculta frente a un tercero que desee acceder a esta y no esté autorizado para hacerlo, esto se logra gracias a algoritmos matemáticos que mediante

claves cifran la información para así dar acceso a esta solo a las personas o entidades que tengan la clave que permita descifrar los paquetes de datos, por lo tanto, si una empresa maneja información poco sensible, este no será el apartado que más le interesará al instalar la VPN. [3] [7]

En la actualidad existen muchos algoritmos de cifrado para garantizar confidencialidad en la información, entre los más destacados se encuentran DES, 3DES y AES, este último es el más seguro ya que entre otras cosas tiene la clave de cifrado más larga, lo cual ayuda a que sea más complicado llegar a descubrir la clave, o deshacer todas las operaciones matemáticas para conseguir la información en texto plano. [14]

Más adelante se profundizará en métodos para el intercambio de claves, con el fin de mantener el cifrado totalmente seguro.

2.2.2 Integridad y Autenticación

Ahora bien, teniendo en cuenta que la información a transmitir debe llegar al receptor exactamente igual a como salió del dispositivo emisor, siempre es necesario una política de seguridad que permita verificar la validez y autenticidad de la información recibida, esto quiere decir que si la información fue alterada durante el trayecto, o fue interceptada por un tercero y reenviada, el receptor tenga la capacidad de identificar que esto ha ocurrido y de esta manera se descarte el paquete y se solicite un reenvío del mismo.

La forma más común y utilizada para asegurar la integridad y autenticación de un paquete es conocida como hash; un hash es un algoritmo que toma una entrada de datos cualquiera y los convierte en un “único” valor de longitud fija, y que a la vez representa a ese conjunto de datos de manera exacta, lo cual quiere decir que si el conjunto de datos cambia la más mínima variable el valor del hash cambiará totalmente, pero esto no siempre se cumple, la veracidad de esta afirmación está sujeta al tipo de algoritmo utilizado para realizar el respectivo hash de un determinado paquete de datos, debido a que el hash tiene una longitud fija, entonces no se pueden obtener una cantidad ilimitada de valores a la salida, lo cual puede causar que dos entradas diferentes obtengan un mismo hash a la salida, a esto se le llaman colisiones; la mejor manera para evitar este tipo de errores es aumentando el tamaño del valor a la salida, de esta forma la probabilidad de que dos entradas generen el mismo valor de salida se reduce cada vez más. Con esta función se cubren tanto el factor

de la integridad como el factor de la autenticación, de esta manera se asegura una fuente confiable e información totalmente válida. [3] [8] [12]

Los algoritmos hash más utilizados en la actualidad son los SHA (Secure Hash Algorithm), existen 3 versiones de este algoritmo: la primera fue descartada totalmente hace muchos años, ya que fueron descubiertos graves fallos en su seguridad; la segunda se estableció en el 2002 y desde entonces se ha estandarizado como uno de los algoritmos hash más seguros, la tercera y última se presentó alrededor del 2015 por lo cual aún se muestra como una alternativa a la segunda versión, pero no ha llegado para reemplazarla.

2.2.3 No reenvío

Para este apartado, se tiene en cuenta un tema relacionado a la autenticación, debido a que el objetivo de este es evidenciar cuando un tercero ha interceptado el paquete puede que lo haya modificado o no y decide reenviarlo para que llegue a su destino final como se observa en la siguiente imagen:

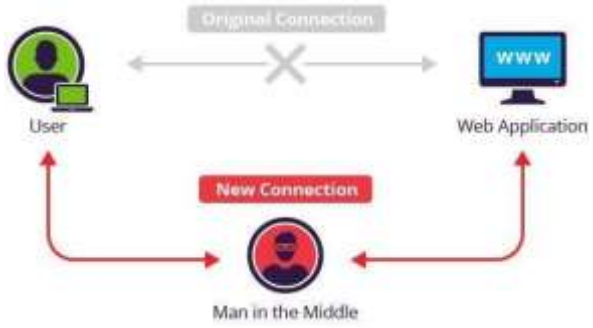

Figura 4: Man in the middle [22]

Una de las formas para evitar este tipo de ataque es inicializar un contador en cada paquete que se transmite, así como en el receptor y en el emisor, de esta manera cuando se inicia la transmisión de paquetes el primer paquete tendrá un número de secuencia en 1, el segundo en 2 y así sucesivamente, en caso de que llegue un paquete con un número de secuencia anterior el receptor identifica esto como un error y descarta automáticamente el paquete.

2.2.4 Intercambio de claves

Como bien se mencionó anteriormente, para el cifrado de un paquete de datos es necesaria una clave, en algunos casos más de una, esta clave debe ser compartida al inicio de la conexión, siendo una de las partes más importantes y difíciles al establecer la VPN, ya que los equipos no han tenido una conexión anterior, por lo cual no se conocen y sería muy fácil para un atacante interceptar la clave y obtener acceso a esta ya que no se puede realizar ningún tipo de cifrado aún. Se debe aclarar que sin esta clave no se debe realizar ningún tipo de transmisión que involucre información sensible. [27]

Ahora bien, actualmente se ha estandarizado un protocolo que se encarga del respectivo intercambio de claves de una forma segura, ya que en ese momento el canal es totalmente inseguro.

El protocolo Diffie-Hellman fue desarrollado por Whitfield Diffie y Martin Hellman, este se encarga del intercambio de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima, es decir, no autenticada. Su seguridad radica en la extrema dificultad para calcular las operaciones utilizadas para hallar las respectivas claves. [27]

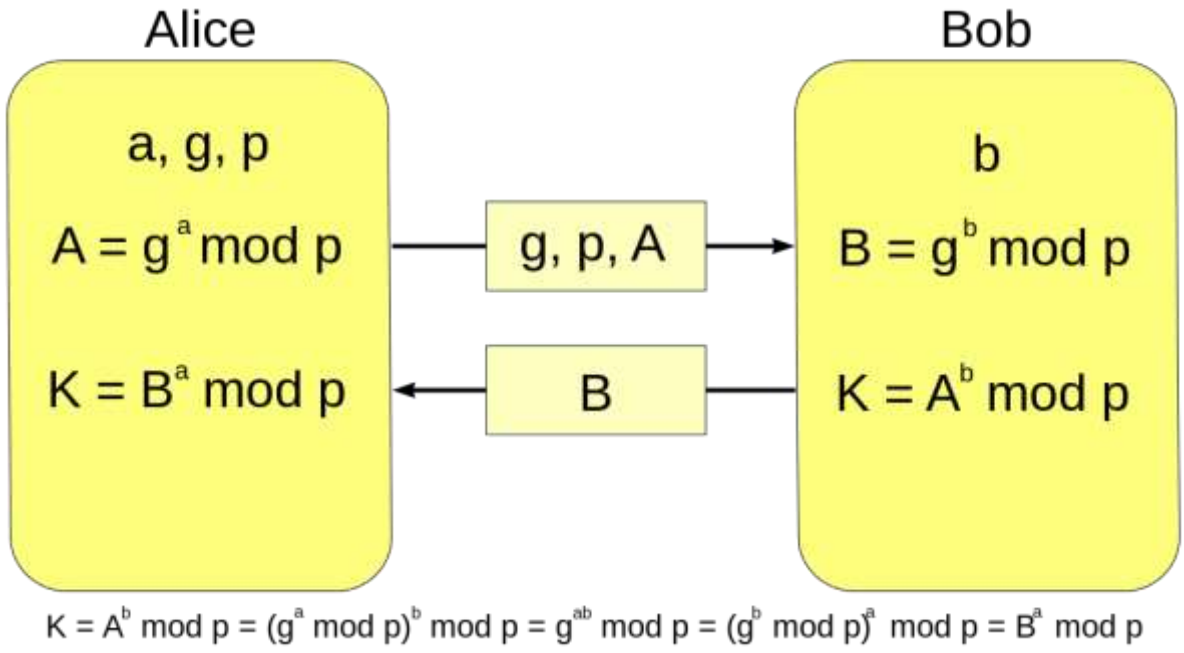

Figura 5: Diffie-Hellman [25]

1. Entonces para hallar la clave primero Alice elige dos números, el primero *p* es primo por lo general muy grande, alrededor de 300 dígitos, y luego un numero aleatorio *g* que debe ser menor a *p,* estos dos se los comparte a Bob, no importa si alguien puede ver esto números, ya que no implican una vulnerabilidad.
2. Ahora Alice elige otro número aleatorio *a (*este no lo comparte con Bob*),* este debe ser menor a *p* y aplica la ecuación $A = g^a * mod(p)$, este número *A* también se lo debe enviar a Bob.
3. Luego Bob también debe elegir un número privado *b* que debe ser menor a *p* y aplica la siguiente ecuación $B = g^b * mod(p)$*,* una vez hecho esto comparte *B* con Alice.
4. Por último Alice debe aplicar $K = B^a * mod(p)$ y Bob debe aplicar $K = A^b * mod(p)$, con esto ambos deben obtener el mismo valor, y esa será la clave que utilizarán para cualquier tipo de cifrado.

Por otro lado, si se desea usar un cifrado asimétrico, es decir que involucre una clave pública, y una clave privada, se ha estandarizado para esto el protocolo RSA. Este protocolo funciona mediante el uso de números primos y una serie de operaciones permite hallar las dos claves para cada parte, como se mencionó anteriormente una privada y una pública, el uso de estas dos claves se retomará más adelante.

2.3 PROTOCOLO VPN IPSEC (INTERNET PROTOCOL SECURITY)

Una de las principales preocupaciones al atravesar una red pública es la seguridad de los datos. Es decir, como se puede prevenir los ataques malignos en una conexión VPN.

El cifrado es una de las maneras más comunes para proteger los datos; Este se puede dar por medio del despliegue de dispositivos de cifrado/descifrado en cada ubicación. IPSec es un conjunto de protocolos desarrollados bajo los estándares del IETF para conseguir servicios seguros a través de redes IP de conmutación de paquetes. Internet es la red pública de conmutación de paquetes más grande del mundo. Además, un túnel VPN desplegado sobre la red pública de internet puede significar un gran ahorro para una empresa, en comparación con una línea punto a punto arrendada. [14]

Continuando con lo anterior, IPSec provee autenticación, integridad, control de acceso y confidencialidad. Además, permite que la información intercambiada entre dos sitios

remotos pueda ser cifrada y verificada. Las dos arquitecturas VPN mencionadas anteriormente pueden ser desplegadas usando IPSec.

EL protocolo IPSec se usa para la creación de túneles cifrados IP, de un sitio a otro a través de una red insegura.

Antes de hablar sobre los pasos que sigue IPsec para el establecimiento de un canal seguro, es necesario conocer algunos conceptos, el primero es IKE; (Internet Key Exchange), cuyo propósito es permitir que dos dispositivos intercambien la información requerida para lograr una comunicación segura. Este opera por medio se SAs (Security Associations) las cuales son negociadas a través de ISAKMP (Internet Security Association and Key Management Protocol), el cual es un protocolo criptográfico que soporta varios métodos para el intercambio de llaves. En IKE el uso de ISAKMP se centra en dos procesos, primero el intercambio de llaves, y segundo, la negociación de los parámetros SAs, una vez se han sido establecidos, los SA son guardados en una base de datos llamada SPD (Security Policy Database), allí se guardan las políticas que han sido negociadas anteriormente mediante los SA. [14] [17]

En la primera fase se usa el protocolo IKE (Internet Key Exchange), el cual se encarga de autenticar los pares y de establecer un canal seguro entre los mismos, para así habilitar el intercambio de IKE. IKE realiza las siguientes funciones:

- Autenticación y protección de la identidad de los pares IPSec.
- Negociación y coincidencia en la política IKE SA para la protección del intercambio IKE.
- Realizar una autenticación a través del protocolo Diffie-Hellman, en el cual se realiza un intercambio de claves que deben coincidir.
- Establecer un túnel seguro para negociar los parámetros de la segunda fase.

En la segunda fase se debe negociar los parámetros de IPSec SA (Security Associations) para establecer el túnel IPSec. Se realizan las siguientes funciones:

- Negociar los parámetros IPSec SA protegidos por un IKE SA existente.
- Establecer los IPSec SA.
- Re-negociar periódicamente los IPSec SAs para mantener la seguridad.
- Opcionalmente realizar un intercambio adicional de Diffie-Hellman.

Los parámetros SA en IPsec son los encargados de describir cómo las entidades utilizarán los servicios de seguridad para comunicarse de forma confiable; en este se definen apartados como el algoritmo para el cifrado o para la integridad. [17]

Después de que la segunda fase esté completa y el modo rápido haya establecido los parámetros IPSec SAs, la información se intercambia a través del túnel IPSec. Los paquetes son cifrados y descifrados usando el método especificado en los SAs.

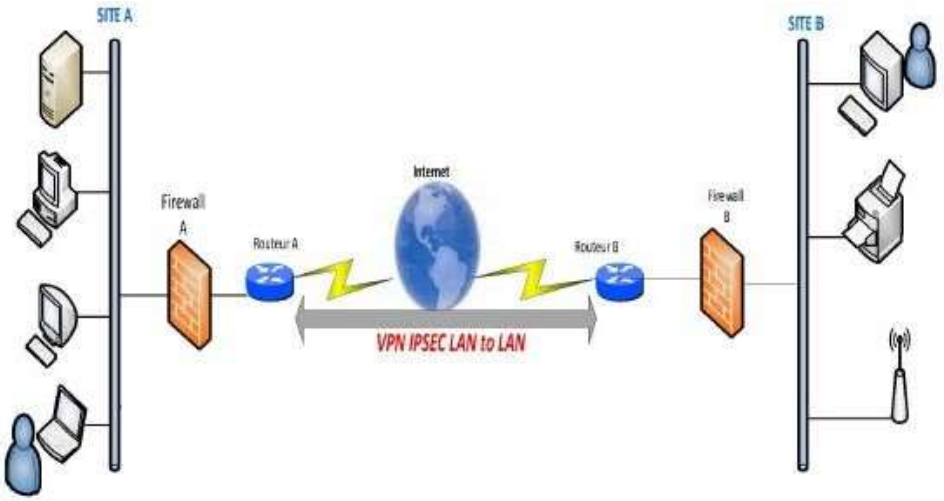

Figura 6: Topología VPN IPSec [14]

Políticas de uso en IPSec:

Primera Fase

- Main Mode
- AES
- SHA-2
- DH-Group 2
- SA Lifetime (seconds)

Segunda Fase

- Esp Tunnel mode
- AES
- SHA-2

- PFS
- DH Group 2
- SA Lifetime (Seconds)

Dentro de los problemas y debilidades de IPSec se encuentran dos principales:

- Direcciones dinámicas (no reconoce los pares)
- NAT/PAT

Cuando se usa NAT, el paquete pasa a través del dispositivo NAT, entonces la dirección de origen del paquete cambia, se presenta incompatibilidad entre los identificadores IKE y las direcciones de origen detectadas, de este modo se invalida el paquete.

Para lo anterior se ha creado un estándar definido por la RFC 3947, en el cual se define el NAT Traversal, que permite realizar la traducción de direcciones sin afectar la cabecera del datagrama, de tal manera que el hash no se invalide y el paquete pueda llegar a su destino.

2.3.1 Modos de Cifrado

El protocolo IPsec tiene la capacidad de utilizar varios métodos para el cifrado de cada uno de los paquetes a enviar, para esto usa algoritmos que implican realizar una determinada cantidad de operaciones con una llave que permitirá a su vez descifrar el paquete; los protocolos más utilizados son: DES, 3DES y AES, este último es el más reciente y más seguro en la actualidad, ya que utiliza una mayor cantidad de bits para la llave de cifrado, por consiguiente, mientras más larga sea la clave, más complejo es el algoritmo de cifrado. [4] [5]

DES (Data Encryption Standard)

Este algoritmo fue uno de los primeros en ser estandarizado como FIPS (Federal Information Proccessing Standard), es decir que Estados Unidos lo anunció públicamente como un estándar para el uso por parte de organizaciones no militares; pero a su vez generó mucha controversia, ya que tenía una longitud de clave relativamente corta y se sospechaba que tenía una puerta trasera para el uso de la NSA.

DES es un algoritmo de cifrado por bloques, es decir que divide la información en bloques de longitud fija, y uno por uno toma cada bloque de texto plano y lo cifra con la llave o clave

asignada, una vez se aplica la llave al bloque, se produce otro bloque de igual tamaño pero cifrado, para descifrar el bloque se aplica el proceso inverso con la misma llave y de esta manera se obtiene el bloque en texto plano. Para DES la longitud de cada bloque es de 64 bits, y la longitud de la llave es de 56 bits.

3DES (Data Encryption Standard)

3DES se refiere a la versión avanzada del protocolo DES, ya que este realiza triple cifrado DES.

Este surgió cuando se descubrió que la llave que utilizaba DES era demasiado corta, lo cual lo hacía muy vulnerable a ataques de fuerza bruta, por lo cual TDES como también se le llama, fue elegido como una alternativa para aumentar la longitud de la llave de cifrado sin necesidad de cambiar el algoritmo. La clave para este caso se triplica a 168 bits, pero solo 112 son efectivos para el cifrado del bloque, y así como la clave el proceso también se debe triplicar, por lo cual cada bloque de 64 bits se cifra tres veces.

AES (Advanced Encryption Standard)

Este algoritmo es uno de los más utilizados y seguros en la actualidad; además es el cifrado que utiliza la NSA para asegurar sus propios documentos; fue desarrollado por dos criptógrafos belgas, Daemen y Rijmen, y se conoce como “Rijndael”.

El algoritmo funciona con varias sustituciones, permutaciones y transformaciones lineales, las cuales se aplican a bloques de 16 bytes, todas las operaciones se repiten varias veces, en series llamadas rondas, durante cada ronda una clave circular única se calcula a partir de la clave principal de cifrado y se utiliza en los cálculos, es decir que cada ronda tiene su clave circular única. Además, el cambio de un único bit en la clave o en el bloque de texto plano, da como resultado un bloque de texto cifrado totalmente diferente, lo cual le da una ventaja sobre el cifrado tradicional.

Existen tres tipos de AES: AES-128, AES-192 y AES-256, lo que varía en cada versión es la longitud de la clave, 128, 192 o 256 bits, se calcula que el ataque para descifrar una clave AES de 128 bits con un ordenador de última generación tomaría más tiempo que la presunta edad del universo, por lo cual aún no se conoce ningún ataque factible contra AES.

2.3.2 Modos de autenticación e integridad

La autenticación como se mencionó anteriormente es uno de los parámetros más importantes en la seguridad de las VPN, ya que este le permite al cliente verificar que el paquete recibido realmente proviene de la fuente original, y no ha sido alterado durante el trayecto hacia su destino final. Esto se logra mediante un hash; Para el caso de IPsec se usan dos algoritmos hash muy conocidos a nivel mundial: SHA (Secure Hash Algorithm) y MD5 (Message-Digest Algorithm 5).

SHA (Secure Hash Algorithm)

Este algoritmo fue presentado en el año 1993 como SHA-0 y ha venido evolucionado en SHA-1 uno de los más utilizados pero que terminaría por mostrarse muy inseguro y poco confiable, después llego SHA-2 que fue muy parecido a su antecesor pero que logró un valor de salida de un mayor tamaño, específicamente 224, 256, 384 y 512 bits, superando de esta manera los reducidos 160 bits que llegó a ofrecer SHA-1 en su momento y ofreciendo así una mayor seguridad y una posibilidad más baja de generar colisiones, hasta llegar al SHA-3, el más reciente presentado en el año 2015, muy diferente a sus dos primeras versiones, pero que no ha llegado a reemplazar a SHA-2 el cual no ha mostrado ningún tipo de vulnerabilidad desde su presentación en el año 2002, sino que simplemente se mantiene como un seguro en caso de que falle la implementación de SHA-2.

MD5 (Message-Digest Algorithm 5)

MD5 es un algoritmo que funciona de una manera muy similar a SHA-1 y SHA-2 pero que genera una vulnerabilidad aún mayor a la de SHA-1 usando un tamaño de salida de tan solo 128 bits, por esto mismo en el año 2004 fue demostrado que el uso de este algoritmo representa un gran riesgo para la transmisión segura de información, en la actualidad se recomienda el no uso de este algoritmo.

2.3.3 Modos de Conexión

IPsec ha definido dos modos de operación para establecer la VPN entre los dispositivos: modo transporte y modo túnel. [14]

Modo Transporte

En este modo solo la carga útil (payload) es cifrada o autenticada; el enrutamiento permanece intacto, ya que no se cifra ni se modifica la cabecera IP. Este se utiliza para las conexiones Host to Host

Modo Túnel

En este modo se cifra tanto la carga útil como la cabecera IP, esto indica por consiguiente que se debe re encapsular el paquete IP, para que de esta manera el enrutamiento pueda funcionar. Este se utiliza para comunicaciones Red a Red, es decir que llega solamente hasta el router que delimita la LAN de la empresa.

2.3.4 Protocolos

Ahora bien, una vez se ha determinado el modo de operación a utilizar se tienen los protocolos que van a actuar sobre estos canales, por un lado está AH (Authentication Header) y por el otro está ESP (Encapsulation Security Payload).

Authentication Header

Este protocolo de seguridad fue creado para garantizar la integridad y autenticación de los datagramas IP sin ningún tipo de encriptación, es decir no garantiza la confidencialidad de los paquetes, por lo cual los datos se envían en texto plano. El AH se basa en la integración de un campo adicional al datagrama IP, este hace posible que el receptor verifique la autenticidad e integridad del paquete, lo anterior gracias a un HMAC (Hash Message Authentication Code) que se calcula a través de un algoritmo hash que opera sobre una clave secreta, de esta manera si el HMAC de origen no coincide con el HMAC en el destino, el paquete será invalidado y se descartara; como se mencionó anteriormente, si se aplica NAT al datagrama IP este invalida el hash automáticamente, por lo cual se debe aplicar el método NAT-T. El formato del AH es el siguiente: [1] [18]

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Figura 7: Formato AH [1]

Aquí se definen 6 campos:

Next Header, es un campo de 8 bits, el cual identifica el tipo de carga útil que viene después del AH. El valor de este campo es elegido de una serie de números definidos en la STD-2, definido por la IANA.

Payload Length, este campo de 8 bits especifica el tamaño del AH en palabras de 32 bits (unidades de 4 bytes).

Reserved, este campo de 16 bits está reservado para un futuro uso, y debe estar todo en ceros.

SPI (Security Parameters Index), campo de 32 bits con un valor aleatorio, que en combinación con la dirección ip de destino y con el protocolo AH, identifica el SA para ese datagrama únicamente.

Sequence Number, este campo de 32 bits contiene un valor en constante crecimiento, y se utiliza para evitar la repetición del paquete.

Authentication Data, en este campo de tamaño variable se ubica el ICV (Integrity Check Value) para ese paquete, este es el valor utilizado para la verificación del paquete.

Ahora bien, la ubicación del AH dentro del datagrama IP depende del modo de operación:

En el modo transporte se ubica entre la cabecera original y la carga útil de esta manera:

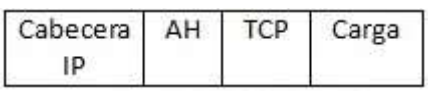

Figura 8: AH en el modo transporte [1]

En el modo túnel es necesaria nueva cabecera ip ya que se encapsula todo el datagrama, por lo cual se tiene de la siguiente manera: [18]

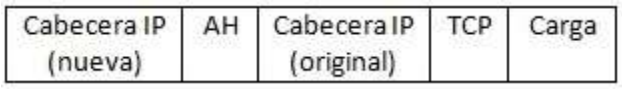

Figura 9: AH en el modo túnel [1]

Encapsulation Security Payload

ESP fue diseñado principalmente para garantizar la confidencialidad de los datos, pero también puede proveer autenticación. El principio de ESP se basa en generar un nuevo datagrama IP en el cual la carga útil, y ocasionalmente la cabecera son cifrados, por lo cual el principal objetivo es garantizar la confidencialidad, pero si se requiere también se puede garantizar tanto autenticidad como integridad; entre los algoritmos más utilizados están DES y 3DES. [2]

A continuación se tiene el formato para el paquete ESP:

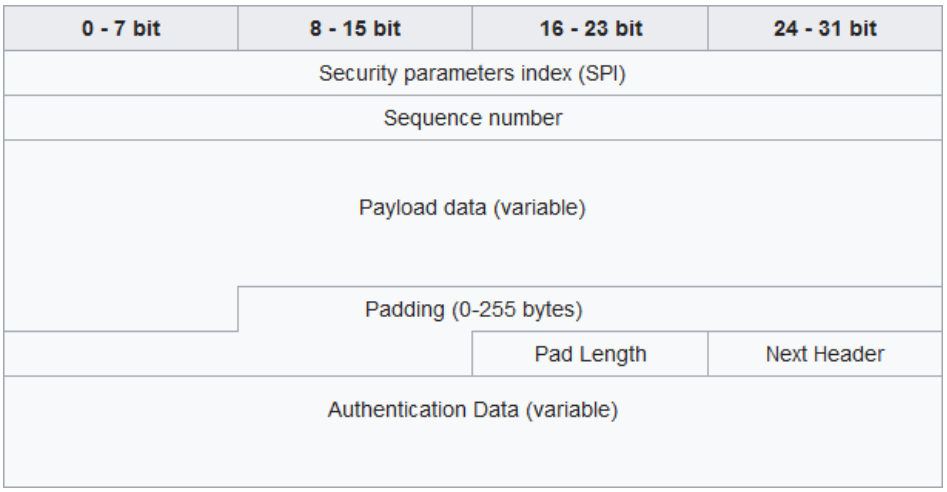

Figura 10: Formato paquete ESP [2]

En este se definen 7 campos:

SPI (Security Parameters Index), en este se identifican los parámetros de seguridad junto con la dirección ip.

Sequence Number, Un valor en constante aumento, utilizado para evitar posibles repeticiones.

Payload Data, la información a transferir.

Pad Length, es el tamaño del relleno en bytes.

Next Header, en este campo se identifica el protocolo de los datos transferidos.

Authentication Data, valor utilizado para la autenticación del paquete.

Si servicio de integridad es seleccionado, entonces el cálculo de este abarca, el SPI, el Sequence Number y los datos de la carga útil. [2]

Si el servicio de confidencialidad es seleccionado (Siempre), entonces se realiza el cifrado sobre la carga útil, excepto por cualquier dato de sincronización criptográfica que se pueda incluir.

Una vez analizados todos los componentes del protocolo IPsec así se vería su estructura

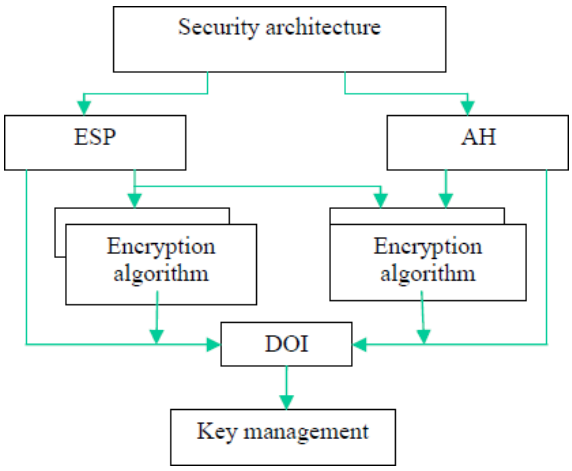

Figura 11: Estructura de IPsec [13]

2.4 PROTOCOLO VPN SSL/TLS (SECURITY SOCKET LAYER)

SSL/TLS es una serie de protocolos de seguridad en los datos sobre internet también conocido como TLS el cual es la versión más reciente de este, desarrollado por la compañía Netscape, este ha sido ampliamente usado para la autenticación y transmisión de información entre aplicaciones web y un servidor. Este protocolo trabaja sobre la capa de aplicación del modelo TCP/IP. Provee soporte de seguridad en la transmisión de datos. SSL/TLS sigue los parámetros del sistema PKI (Public Key Infrastructure), el cual será detallado más adelante; además usa algoritmos no simétricos RSA, los cuales permiten realizar el cifrado de la información mediante claves públicas y privadas, todo esto se logra mediante la selección de números primos aleatorios del orden de 10^200, con los cuales se realizan una serie de operaciones y así se hallan las claves públicas y privadas. [3]

SSL/TLS incluye tres protocolos principales, handshaking protocol, record protocol y warning protocol; El primero se utiliza para determinar los parámetros del cifrado durante la comunicación entre el cliente y el servidor, el segundo realiza la función de encapsulamiento, compresión, cifrado y transporte en general de los paquetes, y por último se tiene el protocolo de alerta que se encarga de informar cuando se ha terminado la conexión o cuando ocurre algún tipo de error durante la comunicación. [13]

La estructura de SSL/TLS es la siguiente:

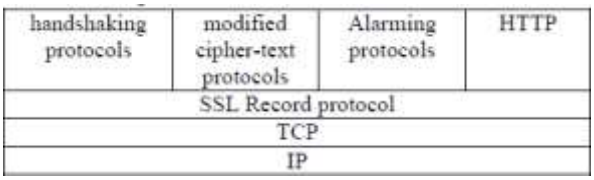

Figura 12: Estructura de SSL/TLS

EL propósito principal de SSL/TLS es proveer privacidad y confiabilidad en la comunicación a nivel de aplicaciones. La conexión se divide en dos estados, primero el handshake en el cual el servidor se autentica y la llave de cifrado para proteger los datos es generada; en la segunda se realiza el respectivo encapsulamiento, cifrado y transmisión de los datos. Siempre se debe completar el proceso de handshake antes de transmitir cualquier paquete de datos.

2.4.1 PKI (Public Key Infrastructure)

Esta infraestructura es un estándar en el cual se mencionan cuáles son las mejores prácticas para un intercambio de información seguro, entre estos están el cifrado, el intercambio de claves y la firma o certificado digital.

El cifrado recomendado es con clave asimétrica, es decir, no utiliza una sola clave sino dos, para mayor seguridad, por ejemplo, si B va a enviar un mensaje a A, primero que todo A debe compartir su clave pública a B, de esta manera B cifra el mensaje con la clave pública de A y lo envía a A, una vez este lo reciba lo puede descifrar con su clave privada, como se observa en la figura 13. [19]

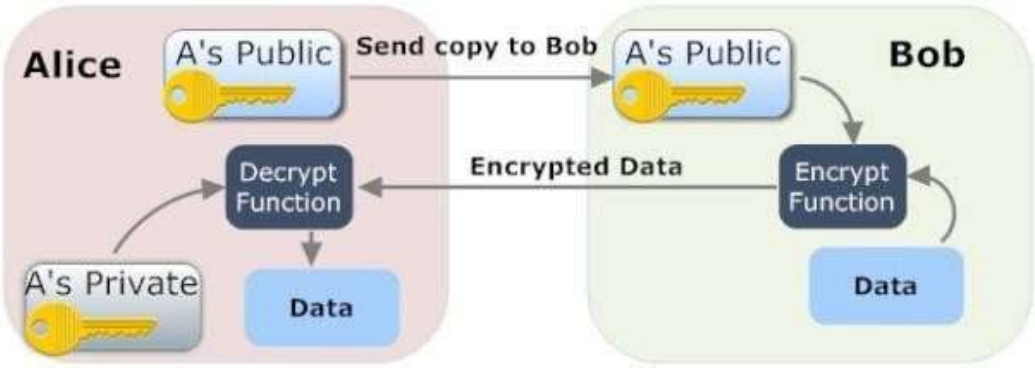

Figura 13: Cifrado asimétrico [26]

Pero lo anterior no sería del todo seguro si las dos partes de la comunicación no fueran capaces de autenticarse frente a su receptor/emisor, por lo cual, SSL/TLS resuelve este problema utilizando un tercero de confianza, es decir una autoridad de certificación (CA) confiable, que actúe como intermediario, de esta forma para que el receptor confíe en el emisor, éste debe tener firmado su certificado público por una CA de confianza, de esta manera la comunicación se mantiene lo más segura posible.

Un ejemplo claro de estos certificados se da en la comunicación navegador-servidor, para esta se dan los siguientes pasos con el fin de asegurar la transmisión de datos, donde N es navegador y S es servidor: [20]

1. N solicita el identificador a S
2. S envía el certificado público
3. N comprueba el certificado
4. N comprueba la validez del CA

5. Si el certificado es correcto y el CA es una entidad de confianza, N debe verificar que el dominio del sitio con el que se está comunicando sea el mismo que aparece en el certificado
6. Una vez confirmado todo esto N puede estar seguro de que el servidor es auténtico y no es una suplantación.

Certificados digitales

Un certificado digital o electrónico es un fichero informático que permite verificar la identidad de un sitio web en internet, de esta manera el cliente está seguro de que se está conectando con la página oficial y no con una falsificada o clonada, por ejemplo, a continuación, está el certificado digital del banco de Bogotá

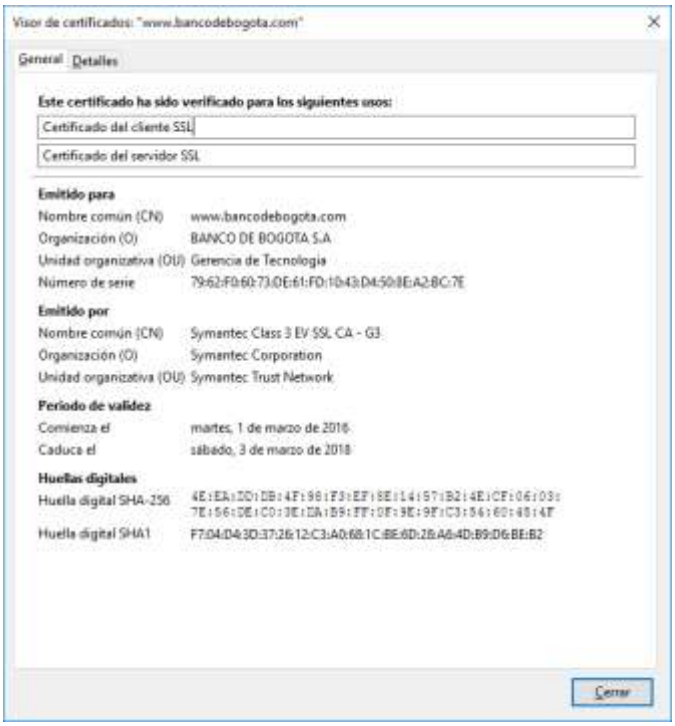

Figura 14: Certificado digital banco de Bogotá

Como se puede observar en el certificado, se presentan los datos de la organización para la cual es emitido el certificado y los datos de la organización que emite el certificado, esta se conoce como autoridad certificadora, además se muestra el periodo de validez del certificado y las huellas digitales que identifican únicamente a esa organización, esto para evitar posibles falsificaciones del sitio web. [23]

El uso del certificado digital es de gran importancia cuando se desea acceder a un sitio web donde posiblemente se manejen datos sensibles en cuanto a la información del cliente, por lo cual la mayoría de sitios web manejan su certificado digital para garantizar la seguridad en el tratamiento de la información.

2.4.2 Modos de Cifrado, autenticación e integridad

Básicamente en este tema SSL/TLS usa los mismos algoritmos implementados por IPsec tanto para el cifrado como para la autenticación e integridad; estos son: DES, 3DES y AES para cifrado y SHA, MD5 para autenticación e integridad.

2.4.3 Categorías SSL/TLS

A continuación serán descritos tres ámbitos principales sobre los cuales se puede desempeñar SSL/TLS:

Proxy en capa de aplicación

Estos proxys se convierten en la manera más simple de implementar SSL/TLS, ya que se basan en la funcionalidad de SSL/TLS usada por las aplicaciones existentes, pero que generalmente solo soportan el correo y el tráfico basado en web.

Sin embargo, para agregar una mayor funcionalidad a esto, se tiende a habilitar el servicio web, así se pueden aplicar otras funciones como la trasferencia de archivos

Redirección de protocolos

Este funciona descargando un software para el cliente, el cual será instalado localmente y se encargará de redirigir el tráfico hacia el túnel SSL/TLS, este mecanismo es más flexible que los proxys mencionados anteriormente, pero no se mantienen en el ámbito clientless (no cliente). Este puede soportar cualquier aplicación que trabaje con puertos fijos TCP o UDP, incluso en algunas implementaciones puede soportar aplicaciones con puertos dinámicos. [13]

Potenciadores de control remoto

Esta es la forma más flexible de implementar una VPN SSL/TLS, funciona potenciando los protocolos de control remoto, como los servicios de Windows o citrix, esto se logra agregando la funcionalidad VPN SSL/TLS y el soporte Web Browser. Así cualquier

aplicación puede ser agregada a la VPN SSL/TLS si ha sido agregada a la aplicación de control remoto. De esta manera la aplicación en el escritorio remoto funciona a través del túnel SSL/TLS.

Ahora bien, a continuación se observa un diagrama del intercambio de datos entre un usuario y la red interna de la empresa:

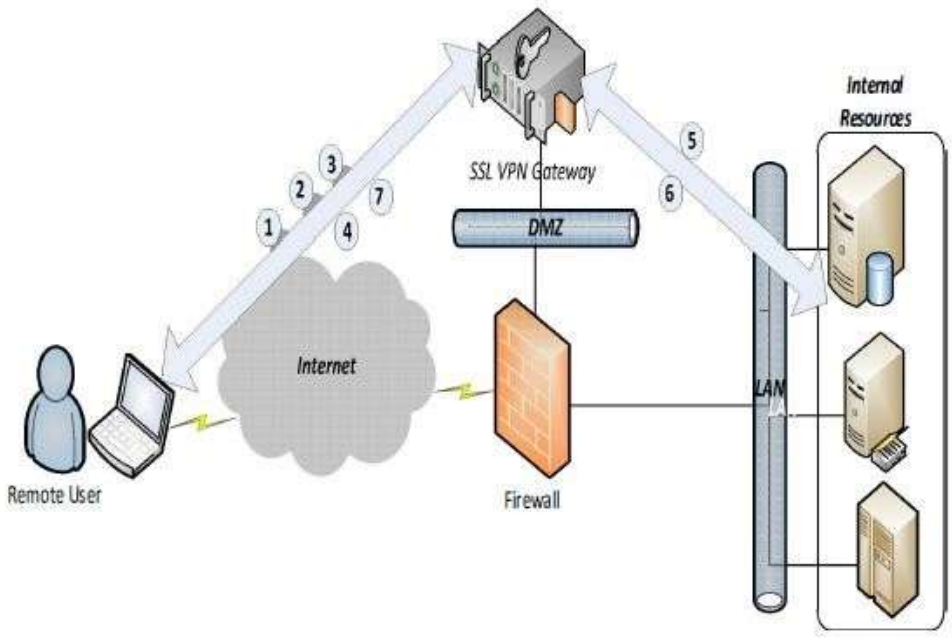

Figura 15: Conexión SSL/TLS [19]

1. EL usuario establece la conexión con el puerto 443 del servidor.
2. El usuario proporciona sus credenciales usando la interfaz web.
3. El usuario puede ver la lista de recursos que están disponibles en su perfil.
4. Selecciona el recurso al que quiere acceder y envía una solicitud al servidor a través de la conexión SSL/TLS
5. El Gateway de la VPN SSL/TLS recibe la solicitud y verifica si el usuario tiene acceso a este recurso, en caso de que lo tenga, entonces reenvía una solicitud al servidor en texto plano.
6. El servidor envía la respuesta al Gateway en texto plano.
7. Finalmente, el Gateway de la VPN SSL/TLS envía la respuesta al usuario final a través del túnel SSL/TLS.

Ahora bien, se debe tener en cuenta que dependiendo del recurso al que se desea acceder, se debe usar un método de conexión diferente, los métodos son los siguientes: Clientless, Thin Client y Tunnel Mode:

2.4.4 Clientless

Este modo proporciona un acceso seguro a los recursos de contenido web; es muy útil para acceder a más contenido del que se esperaría acceder en un navegador web, como acceso a internet, bases de datos y herramientas online que implementan una interfaz web.

2.4.5 Thin Client

Se puede definir como cliente ligero, este amplía la capacidad de las funciones criptográficas, del navegador web, para permitir el acceso remoto a servicios basados en TCP, como POP3, SMTP, IMAP, Telnet, SSH entre otras.

2.4.6 Tunnel Mode

Este modo ofrece un amplio soporte a aplicaciones a través del cliente VPN SSL/TLS descargado dinámicamente para VPN web. Este túnel provee una VPN SSL/TLS con una configuración centralizada y de fácil soporte, además le da al usuario un acceso a prácticamente cualquier aplicación. [13]

2.5 POSIBLES ATAQUES SOBRE UNA RED VPN

Debido a que una VPN transporta una gran cantidad de información que por lo general es muy sensible, puede que algún tercero intente atacar la red con el fin de robar la información, interrumpir la comunicación o alterar la información, por lo cual es necesario conocer cuáles son los tipos de ataques más comunes y cómo prevenirlos.

2.5.1 Session Hijacking

En este tipo de ataques el individuo (atacante) es capaz de robar el identificador de sesión que usa el usuario para ingresar a una página web, en este caso se refiere al inicio de sesión que requiere un cliente para conectarse a la VPN, ya sea mediante una navegador web o mediante un software específico, teniendo en cuenta que es más probable que robe las credenciales si el usuario está ingresando por un navegador web, ya que este es más inseguro que un software cliente el cual está hecho especialmente para establecer una conexión VPN. [22]

Existen varias formas de robar este identificador, entre las más comunes están: ataque por fuerza bruta y sniffing.

Ataque por fuerza bruta

En el ataque por fuerza bruta, se intenta ingresar a la VPN probando identificadores al azar hasta encontrar alguno que le dé acceso a esta, como en el caso de un algoritmo hash, mientras más largo sea el identificador más difícil será encontrar un valor que concuerde con el identificador original y se pueda acceder a la VPN.

Sniffing

El sniffing es una forma de espiar el tráfico que se transmite por la red a la que está conectado el cliente, de esta manera el atacante podría hallar el identificador de sesión de una manera más fácil y rápida, lo único que necesita es estar conectado a la red del cliente e instalar un software que permita realizar un escaneo profundo sobre la red.

Para este caso el cliente debe usar una conexión https de tal manera que el tráfico se mantenga cifrado y un usuario no autorizado no pueda acceder a este.

Man in the Middle

Este es uno de los ataques más conocidos y tal vez más difíciles de evitar, se trata de un tercero que intercepta una conexión cliente-servidor o cliente-cliente, en la cual este atacante desvía el trayecto del paquete transmitido para así recibirlo y poder acceder a este para modificarlo o simplemente para obtener la información, después de esto vuelve e enviar el paquete hacia su destino final, esperando que el receptor no se percate de lo que acaba de ocurrir. [22]

La forma más fácil de realizar este ataque es suplantando una de las dos partes, por lo general el servidor, de esta manera el cliente cree estar conectado con el servidor, pero en realidad está conectado con la computadora del atacante, así el atacante puede robar toda la información que desee sin que el cliente llegue a advertir que ha estado enviando su información a un destino totalmente desconocido.

Spoofing

Esta modalidad de ataque se basa en la suplantación de identidad de tal manera que el cliente se conecte o envíe tráfico al destino incorrecto, este se diferencia del MITM debido a que en este caso no se realiza el reenvío de los paquetes, así el atacante simplemente recibe el tráfico y cuando cree que no necesita más información o el cliente advierte que ha estado enviando información a un servidor equivocado se termina la conexión. Este tipo de ataque se puede dar por: IP, ARP, DNS, Web, Email, estos son los más comunes. [22]

IP Spoofing

La suplantación de IP consiste en sustituir la dirección IP de origen que contiene un paquete TCP/IP, de esta forma los mensajes enviados a un destino determinado parecerá que han sido enviados desde un origen legítimo, pero las respuestas a estos mensajes las recibirá el host o servidor al que corresponde la IP legalmente.

Esto puede ser usado para ataques DoS (Denial of Service) en los que un atacante envía grandes cantidades de mensajes de petición, como un ping por ejemplo a la dirección broadcast teniendo como IP origen una IP perteneciente a otro host que es a quien se desea atacar, de esta manera cuando las peticiones sean respondidas, todos los mensajes de respuesta llegarán al host que tiene asignada la dirección IP origen que ha sido colocada intencionalmente en todos los paquetes enviados, de esta manera el objetivo se verá inundado por una cantidad de tráfico muy alta que hará colapsar su procesamiento.

ARP Spoofing

En este caso se suplanta la identidad mediante la falsificación de la tabla ARP, de esta manera el usuario envía paquetes a una dirección MAC equivocada.

Como bien se sabe la tabla ARP es la encargada de relacionar una IP con una dirección MAC, es decir, si un dispositivo se quiere conectar con otro mediante su IP este envía una trama ARP-request a la dirección de broadcast preguntando quien tiene la IP correspondiente y solicitando la MAC de ese equipo, el equipo que posee la IP le responde con un ARP-reply y mediante este le envía la dirección MAC a la cual se debe conectar; estos datos son guardados por el dispositivo en una tabla llamada tabla ARP, así cuando en una próxima ocasión necesite conectarse nuevamente con el mismo dispositivo ya sabrá hacia dónde debe dirigir el paquete.

Ahora bien, para realizar el spoofing el atacante envía uno o varios ARP-reply al objetivo intentando así modificar los registros de la tabla ARP, de esta manera si se modifica la MAC de una IP específica es posible que el atacante reciba el tráfico, lo escanee y lo reenvíe a su destino real, si así lo desea.

DNS Spoofing

Para este caso el atacante falsifica las entradas de una relación nombre de dominio-IP ante la consulta de resolución de nombre, es decir mediante una IP falsa acceder a cierto nombre de dominio o viceversa. Para esto es necesario acceder al servidor DNS y modificar los registros, así cuando el usuario crea estar accediendo a una página web legitima sin darse cuenta está accediendo a una página web falsa donde sus datos personales corren peligro.

Web Spoofing

El web spoofing se realiza únicamente sobre páginas web, y su objetivo es suplantar una página web para que la víctima ingrese a este pensando que está accediendo a la página web legitima, así el atacante puede escanear las credenciales del usuario sin que este advierta lo que está ocurriendo.

Esto se logra mediante distintas aplicaciones por lo general en un software libre como Linux.

Email Spoofing

Es uno de los más simples y difíciles de detectar ya que se basa en la suplantación de una dirección de correo electrónico, mediante esta práctica es posible difundir una noticia falsa, o solicitar datos a personas fingiendo ser una entidad bancaria o algo similar.

2.5.2 Virus o Malware

Una de las formas más comunes del robo de información es un virus o malware de cualquier tipo, como un troyano, un spyware, un gusano, entre otros, ya que si el cliente tiene alguno de estos en su computadora y este accidentalmente se infiltra en uno de los paquetes enviados a la LAN de la VPN, fácilmente toda la empresa puede llegar a ser afectada por este malware, que puede borrar información, corromper archivos o robar información, por lo cual es muy importante que tanto el cliente como el servidor cuenten con un buen antivirus siempre actualizado. [22]

2.5.3 DoS (Denial of Service)

Como ya se mencionó anteriormente este ataque se da mediante el envío de muchas peticiones a un mismo destino, esto con el fin de colapsar los servicios e inundar la red de una cantidad de tráfico que no sea capaz de manejar, este ataque es muy común y afecta de una manera drástica a toda la red.

Consideraciones de seguridad

- Se debe usar un firewall para la protección a través de la VPN.
- Sistemas para detección de intrusos o de prevención, son necesarios para evitar posibles ataques en la red.
- Es necesario un anti-virus tanto en los clientes remotos como en los servidores de la red, que se mantengan siempre actualizados, con el fin de evitar cualquier tipo de malware.
- Se debe llevar un registro de las conexiones que se establecen entre los servidores y los clientes, para futuras revisiones.
- Los sistemas inseguros con ausencia de autenticación no deben ser permitidos
- Se debe dar la capacitación pertinente a los encargados de la administración de la red y usuarios y tener personal de soporte para cualquier eventualidad.
- Se deben establecer políticas de seguridad que permitan controlar y administrar la VPN de una forma correcta.
- Evitar el uso de Split tunneling (concepto que representa la conexión a dos redes por parte de un dispositivo al mismo tiempo).

Características al elegir una VPN

- Elegir un sistema de autenticación robusto, como RADIUS, tarjetas inteligentes, tokens, etc.
- Aplicar sistemas de cifrado confiables, que utilicen una clave de gran tamaño para asegurar la confidencialidad.
- Considerar el uso de antivirus que sean capaces de trabajar sobre la VPN.
- Buscar soporte de autenticación sitio a sitio mediante certificados digitales.

3 DESARROLLO COMPARATIVO

Ahora bien, después de haber detallado las características más importantes de los protocolos IPsec y SSL/TLS es necesario realizar un análisis comparativo en el cual se relacionen los aspectos más importantes al desplegar una VPN, para lo cual será utilizado un método o proceso llamado AHP (por sus siglas en inglés Analytic Hierarchy Process) Proceso Analítico Jerárquico, pero antes que nada se deben entender que son los problemas de decisión o selección multicriterio, y a partir de estos desarrollar la teoría del AHP para aplicarla al proceso que implica la toma de decisiones llevada a cabo en este trabajo.

3.1 PROBLEMAS DE DECISIÓN MULTICRITERIO

La toma de una decisión multicriterio es uno de los problemas más comunes en la vida real, pero que en la mayoría de los casos termina siendo muy complicado de resolver. Este se da cuando en una actividad es necesario evaluar un conjunto de alternativas en función de una cantidad determinada de criterios, donde con gran frecuencia se produce conflicto entre unos y otros. El responsable de tomar una decisión se ve enfrentado a un sinfín de factores que pueden afectar la elección final, desde factores anímicos, familiares y sociales hasta factores económicos y de información sobre cada alternativa.

Para evitar esto es de vital importancia que el responsable se centre solamente en el impacto que puede causar su decisión en el funcionamiento y desempeño de un proceso dentro de una organización que requiera la mejor alternativa costo/beneficio. Por lo cual es necesario recolectar toda la información adecuada sobre cada una de las posibles opciones para al final tomar la mejor decisión.

Esto dará como resultado un análisis totalmente objetivo en el cual se tendrán en cuenta solamente criterios que involucren las alternativas relacionadas, y de esta forma se aíslen los demás factores.

Ahora bien, la complejidad que requiere el análisis de los diferentes criterios o factores ha llevado al desarrollo de herramientas que permitan abordar el problema de una forma sistemática y científica buscando así favorecer el proceso y ayudar al responsable de tomar la decisión. Entre estas herramientas o modelos se encuentra el AHP, el cual mediante

simples matemáticas beneficiará en gran medida la elección que tome el encargado de resolver el problema.

3.2 PROCESO DE ANÁLISIS JERÁRQUICO (AHP)

Este fue desarrollado en los años 60 por el profesor Thomas Saaty y ha sido extensivamente estudiado y mejorado desde entonces.

El AHP es una alternativa para estructurar, medir y sintetizar. Se presenta como un método matemático para evaluar diferentes alternativas cuando se tienen en cuenta diferentes criterios, y se basa en el conocimiento sobre cada uno de estos en las diferentes opciones.

El AHP permite a los usuarios descomponer un problema de decisión en varios sub-problemas que pueden ser comprendidos más fácilmente y además se pueden analizar de forma independiente, así, teniendo diferentes alternativas todas se relacionan entre ellas usando un solo criterio a la vez. [30]

Escala	**Definición**	**Explicación**
1	Igualmente preferida	Los dos criterios contribuyen igual al objetivo
3	Moderadamente preferida	La experiencia y el juicio favorecen un poco a un criterio frente al otro
5	Fuertemente preferida	La experiencia y el juicio favorecen fuertemente a un criterio frente al otro
7	Muy fuertemente preferida	Un criterio es favorecido muy fuertemente sobre el otro. En la práctica se puede demostrar su dominio

9	Extremadamente preferida	La evidencia favorece en la más alta medida a un factor frente al otro

Tabla 1: Escala de comparación Saaty

Como primera medida es necesario definir un árbol jerárquico, en el cual se definen 4 niveles; como primer nivel o nivel cero, se encuentra el objetivo del proyecto, en el segundo nivel se describen cuáles son los criterios globales, pero para ser más específico se requiere al menos un tercer nivel en el cual se definan unos subcriterios, por último en el cuarto nivel se tienen las alternativas sobre las cuales se desea trabajar, de esta manera se logra simplificar al máximo la forma de comparación de ambas alternativas, si se desea es posible agregar más niveles en los que haya criterios de los subcriterios, tantos como se crea prudente, y suficientes para tomar la mejor decisión. [31]

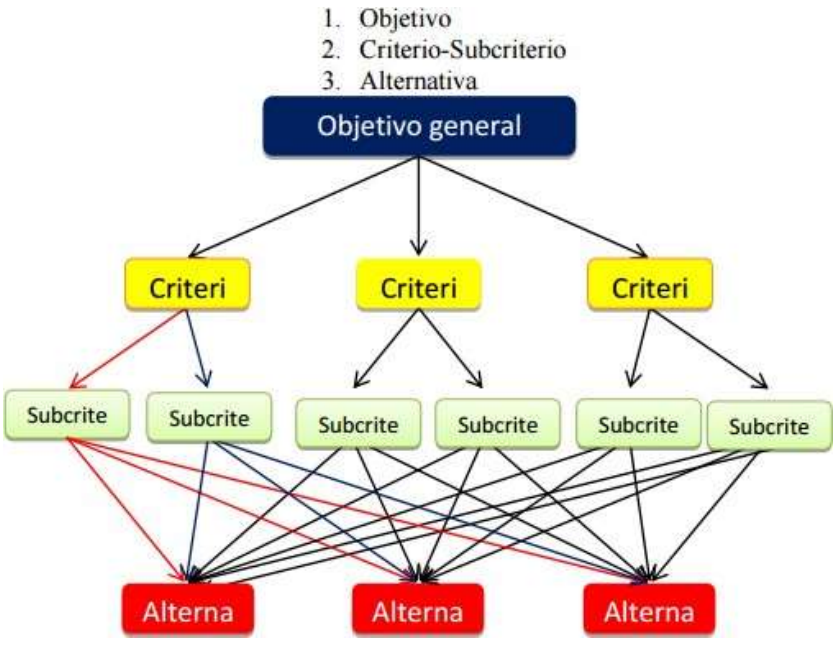

Figura 16: Árbol Jerárquico [31]

Una vez se tenga el árbol, será necesario realizar dos tipos de comparaciones, en la primera se realiza la comparación entre criterios y entre subcriterios, esto quiere decir que se toman los criterios del segundo nivel y se comparan entre ellos, después se toman los subcriterios de cada criterio y se comparan independientemente, es decir, solo se toman subcriterios de un criterio específico para ser comparados, todo esto mediante valores de preferencia, y

con el fin de hallar los vectores de preferencia para cada criterio y subcriterio, es decir, el peso de cada uno.

La segunda parte se basa en la comparación por pares de cada uno de los subcriterios con respecto a cada una de las alternativas, es decir se toma un subcriterio y este se enfrenta en cada una de las alternativas, después de esto se debe normalizar la tabla y obtener el promedio para cada normalización, esto para identificar cual es el vector de prioridad (peso) de cada subcriterio en cada alternativa; se debe tener en cuenta que siempre la sumatoria de los vectores de prioridad de la matriz que se está ejecutando debe dar como resultado 1. [32]

Lo anterior se realiza mediante valores de preferencia (ver tabla 1), por ejemplo, se tienen los criterios C1 y C2, entonces se debe definir qué tanto se prefiere un criterio sobre el otro, esto con un valor que puede ser 1,3,5,7 o 9, lo cual en una tabla se vería representado de la siguiente manera.

COMPARACIÓN CRITERIOS SEGUNDO NIVEL					
	C1	**C2**	**Norm1**	**Norm2**	**Vector P**
C1	1	5	0,8333333	0,833333	0,8333333
C2	1/5	1	0,1666667	0,1666667	0,1666667
Suma	1,2	6	1	1	1

Tabla 2: Comparación de criterios

COMPARACIÓN SUBCRITERIOS DEL CRITERIO 1					
	SC1	**SC2**	**Norm1**	**Norm2**	**Vector P**
SC1	1	1	0,5	0,5	0,5
SC2	1	1	0,5	0,5	0,5
Suma	2	2	1	1	1

Tabla 3: Comparación de subcriterios

Como se puede observar en la tabla anterior en el criterio C1, se define de mayor importancia sobre el criterio C2 en una relación de 5, y el criterio C2 se define en una relación de ⅕.

Si la matriz es igual o mayor a 3x3 se debe tener en cuenta la consistencia de la misma, la cual permite identificar que los juicios de los expertos sean coherentes, es decir, que si C1>C2 y C2>C3, entonces C1>C3, si esto no aplica se estaría trabajando con una matriz inconsistente, la cual no arrojaría el resultado más exacto, para comprobar esto se tienen las siguientes ecuaciones: [32]

Primero se debe tener en cuenta el índice de consistencia aleatorio RI el cual se toma de la siguiente tabla, donde n es el tamaño de la matriz.

N	1	2	3	4	5	6	7	8
RI	0	0	0,525	0,882	1,115	1,252	1,341	1,404

Tabla 4: Tabla de índice de consistencia aleatorio [32]

A partir de esto se debe hallar λmax, el cual Se obtiene de la multiplicación de la matriz de las sumatorias por la matriz de los vectores de prioridad es decir:

COMPARACIÓN CRITERIOS SEGUNDO NIVEL					
	C1	**C2**	**Norm1**	**Norm2**	**Vector P**
C1	1	5	0,8333333	0,833333	0,8333333
C2	1/5	1	0,1666667	0,1666667	0,1666667
Suma	1,2	6	1	1	1

Tabla 5: Hallar λmax

para este caso λmax= [1,2 6] * [0,83333 0,1666667] = 2

después de esto se debe hallar el CI:

$$CI = \frac{\lambda max - n}{n-1} = 0$$

por último, se debe hallar CR el cual nos permite identificar si la matriz es consistente, para n=3 0,05, para n=4 0,08, para n=5 0,10, si el valor de CR es superior al indicado para cada posible n, entonces se deben reconsiderar los juicios de los expertos.

$$CR = \frac{CI}{RI} = 0$$

este juicio se debe realizar sólo para matrices 3x3 en adelante, ya que como se observa en una matriz 2x2 no es posible que exista algún tipo de inconsistencia.

Después de haber realizado la primera comparación, se debe realizar la comparación por pares para cada alternativa, es decir tomar cada subcriterio y asignar una preferencia según la alternativa.

subcriterio1					
	IPsec	**SSL**	**Norm1**	**Norm2**	**VP**
IPsec	1	1	0.5	0.5	0.5
SSL	1	1	0.5	0.5	0.5
Suma	2	2	1	1	1

Tabla 6: Comparación por pares para cada subcriterio

Realizado lo anterior para cada uno de los subcriterios que se tienen ya se puede pasar a la última parte del proceso, la cual consiste en hallar los pesos globales para cada una de las alternativas.

Este se halla tomando el peso para cada subcriterio, multiplicado por el peso para cada criterio, es decir Pglobal=0,5*0,8333333=0,4166665, donde 0,5 es el peso para el subcriterio 1, y 0,833333 es el peso para el criterio1, se realiza el mismo procedimiento para todos los subcriterios con su respectivo criterio, una vez hallados los pesos globales se realiza la suma ponderada entre los pesos globales y el vector de prioridad local para cada alternativa, es decir el vector de prioridad hallado en la comparación por pares de cada subcriterio en relación a cada alternativa, este cálculo dará como resultado en porcentajes el valor de preferencia de cada una de las alternativas el cual igualmente debe sumar 1 o 100, dependiente de la escala. [32]

Una vez realizado este procedimiento, el cliente tiene una ayuda que le permite eliminar alternativas y dejar las más probables a un lado, para así poder realizar otro estudio que crea pertinente o elegir inmediatamente la alternativa con mayor prioridad.

Está herramienta es de gran utilidad, pero requiere de una gran cantidad de información sobre cada una de las alternativas, de esta manera la comparación en función del criterio será mucho más fácil de realizar, y arrojará resultados con mayor exactitud.

3.3 Comparación de criterios

Para realizar la respectiva comparación de los criterios es necesario especificar cuáles son, y describir las características por las cuales se les asigna el valor de preferencia indicado.

En primera instancia serán enumerados los 5 criterios principales que a su vez se dividen en un segundo nivel, y a continuación se realizará la respectiva descripción:

1. Seguridad
   -1.1 Cifrado
   -1.2 Autenticación
   -1.3 Integridad
2. Acceso
   -1.1 Usabilidad
   -1.2 Interfaz de acceso
3. Instalación
   -1.1 Configuración
   -1.2 Instalación
   -1.3 Soporte Apps
4. Mantenimiento
   -1.1 Facilidad
   -1.2 Costos
   -1.3 Escalabilidad
5. Tunel real (SSL/TLS host to host - IPsec GW to GW)
   -5.1 GW to GW
   -5.2 Host to Host

3.3.1 Seguridad

Como ya se mencionó anteriormente este puede ser uno de los apartados más importantes para una organización en el momento de implementar una VPN, este puede ser dividido en

tres factores mencionados anteriormente, como lo son, Cifrado, Autenticación e Integridad, los cuales fueron descritos en el apartado 3.2.1 y 3.2.2,

- Cifrado (Maximizar): llega a ser uno de los parámetros más importantes cuando de transmitir información se habla, pero esto depende en gran medida de la sensibilidad de la información que se está tratando, ya que la confidencialidad lo que permite es mantener la información totalmente oculta frente a un tercero que desee acceder a esta y no esté autorizado para hacerlo, el cifrado se logra mediante los protocolos DES, 3DES y AES que como ya se mencionó anteriormente son implementados tanto en IPsec como en SSL/TLS.

- Autenticación e integridad (Maximizar): Estos dos puntos se tratan como uno solo ya que los protocolos que se usan actualmente para garantizar integridad y autenticación son los mismos, SHA y MD5, que ya se trataron en un apartado anterior y al igual que el cifrado se usan del mismo modo tanto para IPsec como para SSL/TLS

3.3.2 Acceso

Este criterio permite evaluar la facilidad y la seguridad que se implementa al ingresar a la VPN desde un lugar aleatorio y desde un dispositivo aleatorio, ya que ambos son necesarios pero cada uno resulta ser inversamente proporcionalmente a su complemento, a continuación se observará el porqué de esto.

- Usabilidad (Minimizar): Cuando se desea acceder a la VPN la primera impresión es la facilidad que tiene el usuario para ingresar de una forma rápida y sencilla, a nadie le gustan los accesos complicados y lentos, por lo cual en este punto SSL/TLS presenta la ventaja sobre IPsec, ya que su acceso se puede considerar como el más sencillo y rápido, donde se requiere solamente de un dispositivo con conexión a internet y un navegador web preferiblemente (Firefox, Chrome, Safari), de esta forma el usuario mediante una dirección IP y claro está un usuario y una contraseña accede a su VPN, si lo desea también puede verificar el certificado digital y ya estará adentro.

  Por su parte IPsec presenta un acceso mucho más engorroso y complicado, donde solamente se puede utilizar el dispositivo autorizado por la empresa con el software

indicado (el cual depende del dispositivo que forma la VPN), además de utilizar, luego de esto se necesita el usuario y la contraseña y en algunos casos un segundo factor de autenticación, que se puede traducir en un código de una cantidad de dígitos determinada que solo se puede usar una vez.

- Interfaz de acceso (Maximizar): Para esto se tiene en cuenta el proceso al cual debe recurrir el usuario para acceder a la VPN, como ya se mencionó anteriormente, en ambos casos se tiene un ingreso básico de usuario y contraseña, pero este puede variar dependiendo del protocolo implementado.
  Para el caso de IPsec es necesario tener instalado un software específico en un dispositivo que ya ha sido autorizado previamente, por lo cual, esto genera un nivel de seguridad mayor, además de esto también es posible incluir un segundo factor de autenticación, que se traduce en un código de una cantidad de dígitos determinada que solo se puede usar una vez, y que permitirá al software comprobar que la persona que desea acceder tiene los permisos necesarios; Entonces son 4 factores que afectan el control de acceso para una VPN IPsec (usuario y contraseña, Software, Hardware y segundo factor de autenticación).

  Por su parte SSL/TLS solo tiene un segundo factor de seguridad para el control de acceso, este se conoce como certificado digital, el cual ya fue mencionado en el apartado 2.4 (Protocolo SSL/TLS).

3.3.3 Instalación

En este apartado se desea analizar la complejidad de la instalación y configuración de una VPN para cada uno de los protocolos (IPsec y SSL/TLS), esto incluye tanto hardware como software.

- Instalación (Minimizar) se debe tener en cuenta mediante qué tipo de dispositivo se desea crear la VPN, actualmente se usan en su gran mayoría los firewalls de la empresa para la creación de la VPN, ya que es uno de los métodos más seguros y eficientes, puesto que no requiere de software ni hardware adicional, y el tráfico se mueve a través del dispositivo que le da seguridad a toda la red interna de la compañía, por lo cual da una gran garantía al túnel que se desea crear.

- Configuración (Minimizar): Ahora bien, la configuración dentro del firewall para IPsec y SSL/TLS no es muy compleja, más adelante se realizará un ejemplo de cómo configurar los dos tipos de VPN en un firewall Fortinet; pero por otro lado, la configuración en los dispositivos remotos se hace un poco más tediosa para una VPN IPsec, esto debido a que es necesario instalar software adicional y configurar el mismo para que el acceso sea permitido, caso contrario en SSL/TLS, el cual permite acceder a la VPN teniendo a disposición solamente un navegador web, y permitiendo el acceso desde cualquier dispositivo con una conexión a internet, lo cual reduce en gran medida la complejidad en la instalación y configuración.

- Soporte de apps (Maximizar): Para este aspecto se debe abordar la capa de del modelo OSI en la cual trabaja cada uno de los protocolos, de esta manera se puede analizar cuál es el soporte en relación a las aplicaciones.

  IPsec entra directamente en la capa 3 lo cual significa que es capaz de soportar cualquier aplicación o recurso al cual se desee acceder, esto le da una ventaja muy importante sobre SSL/TLS, el cual, si bien es capaz de acceder a muchas aplicaciones, al entrar directamente sobre la capa de aplicación, restringe en cierto modo la cantidad de aplicaciones a las que tiene acceso, las cuales en su gran mayoría son basadas en web.

3.3.4 Mantenimiento

El mantenimiento está muy relacionado con la instalación y configuración de cada uno de los protocolos, ya que un mantenimiento se basaría en actualizaciones de software, adición y eliminación de usuarios, verificación de certificados digitales, entre otros.

- Costos (Minimizar): El costo se basa en dos parámetros principales, la mano de obra de la persona encargada de realizar el mantenimiento, teniendo en cuenta que si es para IPsec será mucho más demorado que para SSL/TLS, y la nueva compra de licencias en caso de ser necesario, donde para IPsec se da un costo adicional si se utiliza el segundo factor de autenticación que en fortinet se conoce como fortitoken, y en SSL/TLS el costo adicional se presenta en los certificados digitales.

- Facilidad (Minimizar): Ya que el costo está directamente conectado con la dificultad para realizar el mantenimiento, queda claro que para SSL/TLS se presenta una mayor facilidad para realizar el mantenimiento que para IPsec.

- Escalabilidad (Maximizar): Cual es la capacidad de cada uno de los protocolos para escalar en usuarios y aplicaciones, es decir, si la empresa desea o necesita añadir usuarios o aplicaciones a su VPN tiempo después de haber sido instalada, cuál va a ser el grado de complejidad para cada uno de estos aspectos.

  Con IPsec es más fácil añadir nuevas aplicaciones, ya que como se mencionó anteriormente al trabajar sobre la capa de ip directamente, es capaz de soportar la mayoría de aplicaciones por no decir todas; ahora bien, agregar un nuevo usuario requiere de un trabajo más complejo, ya que es necesario aparte de crear el usuario en el firewall, instalar el software necesario en el equipo del cliente, y configurarlo de la manera correcta, esto le da un punto positivo pero a su vez un punto negativo en el aspecto de la escalabilidad.

  Por otra parte, SSL/TLS se puede quedar corto en cuanto a la escalabilidad en aplicaciones, debido a que si no soporta ciertas aplicaciones no habrá forma alguna de utilizarlas, pero en el tema de los usuarios, solo será necesario crearlos en el respectivo firewall, y agregarlos al grupo correspondiente para que así se puedan usar inmediatamente.

3.3.5 Túnel VPN

Cuando se implementa una VPN se genera un túnel cifrado por el cual viaja todo el tráfico que comparten cliente y servidor, es importante analizar hasta dónde llega este túnel, para esto se tienen dos opciones principales, un túnel Gateway to Gateway o Host to Host.

En cuanto al protocolo IPsec el túnel es Gateway to Gateway, es decir que la puerta de enlace de cada red será la encargada de encriptar y desencriptar el tráfico que llegue o salga de ese punto, en caso de que exista solo un gateway y del otro lado un host, como en el caso de un firewall y un cliente respectivamente, el túnel será cifrado entre estos dos puntos.

Por su parte, SSL/TLS implementa un túnel cifrado Host to Host, es decir que el tráfico se encripta y desencripta en los destinos finales y no en las puertas de enlace como se mencionó en el caso anterior.

4.4 Resultados

A continuación se observan los resultados de cada procedimiento iniciando por la comparación de los criterios de segundo nivel o criterios generales.

COMPARACIÓN GENERAL						
	1	**2**	**3**	**4**	**5**	**VP**
1	1	2	5	6	5	0,452304982
2	0,5	1	3	5	3	0,270895626
3	0,2	0,333333333	1	0,333333333	0,333333333	0,061360375
4	0,166666667	0,2	3	1	0,5	0,09059684
5	0,2	0,333333333	3	2	1	0,124842178
SUMA	2,066666667	3,866666667	15	14,33333333	9,833333333	1

Tabla 7: Comparación criterios Generales

A continuación se observa la tabla de comparación para los criterios específicos o subcriterios, teniendo en cuenta que estos se comparan independientemente por cada criterio general.

SEGURIDAD				
	1.1	**1.2**	**1.3**	**VP**
1.1	1	5	3	0,64794686

1.2	0.2	1	0.5	0,122181965
1.3	0,333333333	2	1	0,229871176
SUMA	1,533333333	8	4.5	1

Tabla 8: Comparación subcriterios de seguridad

ACCESO			
	1.1	**1.2**	**VP**
1.1	1	0,2	0,166666667
1.2	5	1	0,833333333
SUMA	6	1,2	1

Tabla 9: Comparación subcriterios de Acceso

INSTALACIÓN				
	1.1	**1.2**	**1.3**	**VP**
1.1	1	3	0,333333333	0,260497956
1.2	0,333333333	1	0,2	0,106156324
1.3	3	5	1	0,63334572
SUMA	4,333333333	9	1,533333333	1

Tabla 10: Comparación subcriterios de Acceso

MANTENIMIENTO				
	1.1	**1.2**	**1.3**	**VP**
1.1	1	0,5	0,25	0,137287664
1.2	2	1	0,333333333	0,239487608
1.3	4	3	1	0,623224728

SUMA	7	4,5	1,583333333	1

Tabla 11: Comparación subcriterios de Acceso

TÚNEL			
	1.1	**1.2**	**VP**
1.1	1	1	0,5
1.2	1	1	0,5
SUMA	2	2	1

Tabla 12: Comparación subcriterios de Acceso

CONSISTENCIA DE LAS MATRICES						
	Seguridad(3)	**Acceso(2)**	**Instalación(3)**	**Mantenimiento(3)**	**Túnel(2)**	**General (5)**
RI	0,525	0	0,525	0,525	0	1,115
LAMBDA	3,005394525	2	3,055361493	3,025480368	2	5,428801794
CI	0,002697262	0	0,027680747	0,012740184	0	0,107200448
CR	0,005137643	0	0,052725231	0,024267017	0	0,0961439

Tabla 13: Consistencia de las matrices

Todos los cálculos realizados se pueden observar en el archivo anexo que se tiene en excel.

Así pues, las prioridades quedan de la siguiente manera:

IPSEC: 57,1779401 %

SSL/TLS: 42,8220599 %

3.4 CONFIGURACIÓN VPN'S

Ahora bien, debido a que la empresa RCN TV cuenta con un firewall de la marca FORTINET, el cual es utilizado para mantener seguros los servicios que tienen que salir hacia internet, además de filtrar el tipo de tráfico que puede ingresar o salir de la red corporativa teniendo en cuenta la Ip origen o destino, entre otras aplicaciones más; este dispositivo como ya se mencionó anteriormente, permite la creación de una VPN ya se con el protocolo IPsec o con el protocolo SSL/TLS, esto da la facilidad de implementar la VPN sin necesidad de comprar software o hardware adicional, ya que la licencia con la que se cuenta da acceso a estas funcionalidades hasta por tres años.

A continuación se presentará un paso a paso de cómo realizar la respectiva configuración de la VPN en ambos protocolos, para que esto sirva de guía en caso de que se desee adoptar este tipo de red.

3.4.1 Configuración VPN IPsec

1. Como primer paso se debe realizar la creación de un rango de direcciones, este rango pertenece al rango de IP que se utilizan dentro de la red del canal, se pueden crear varios rangos si es necesario. Esto se realiza en la pestaña "Policy & Objects" >> "Objects" >> "Addresses"; allí será necesario añadir un nombre, la subred con su respectiva máscara, la interfaz por la cual se podrán ser vistas esas IP, que para evitar inconvenientes será por efecto "any", y si se desea se puede agregar un comentario.

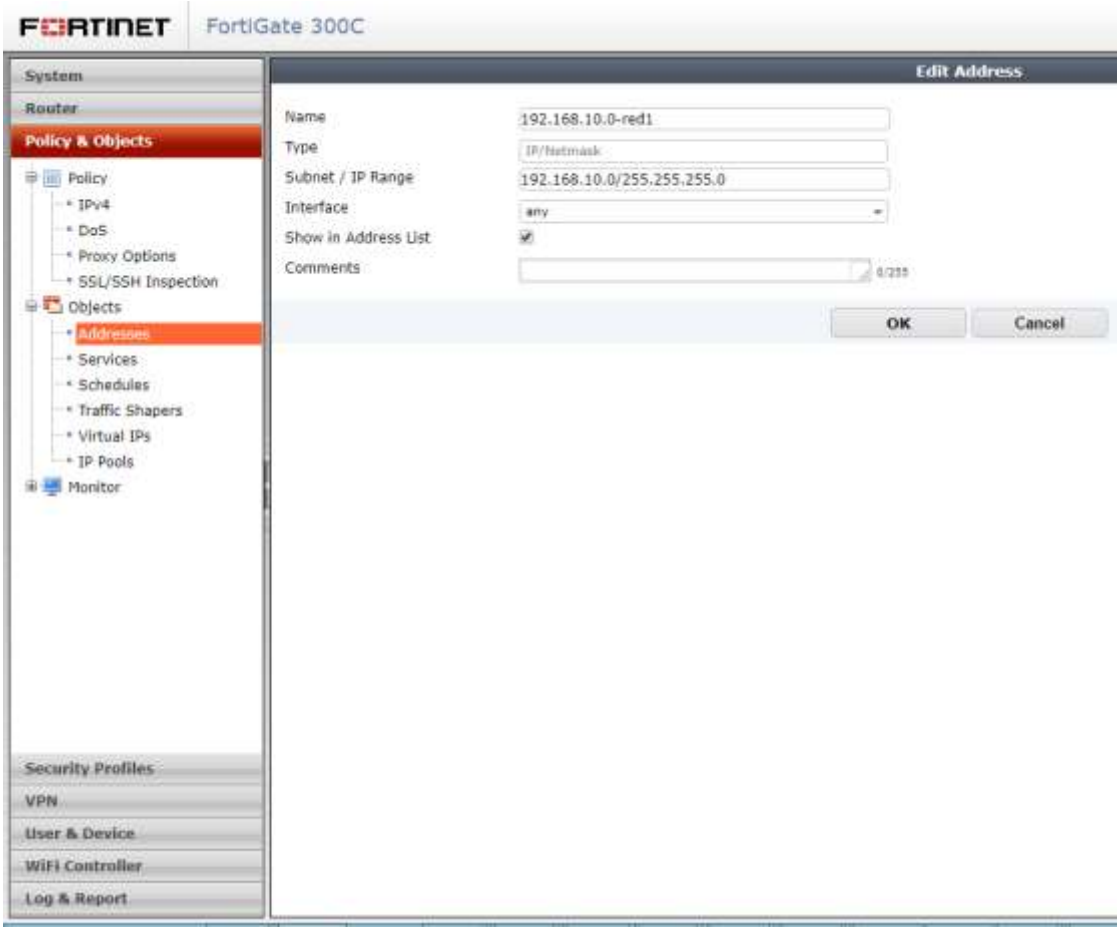

Figura 17: Creación de pool de IP

2. En este caso se realiza la creación de una segunda red corporativa a la cual tendrá acceso la VPN, del mismo modo que se realizó en el paso anterior.

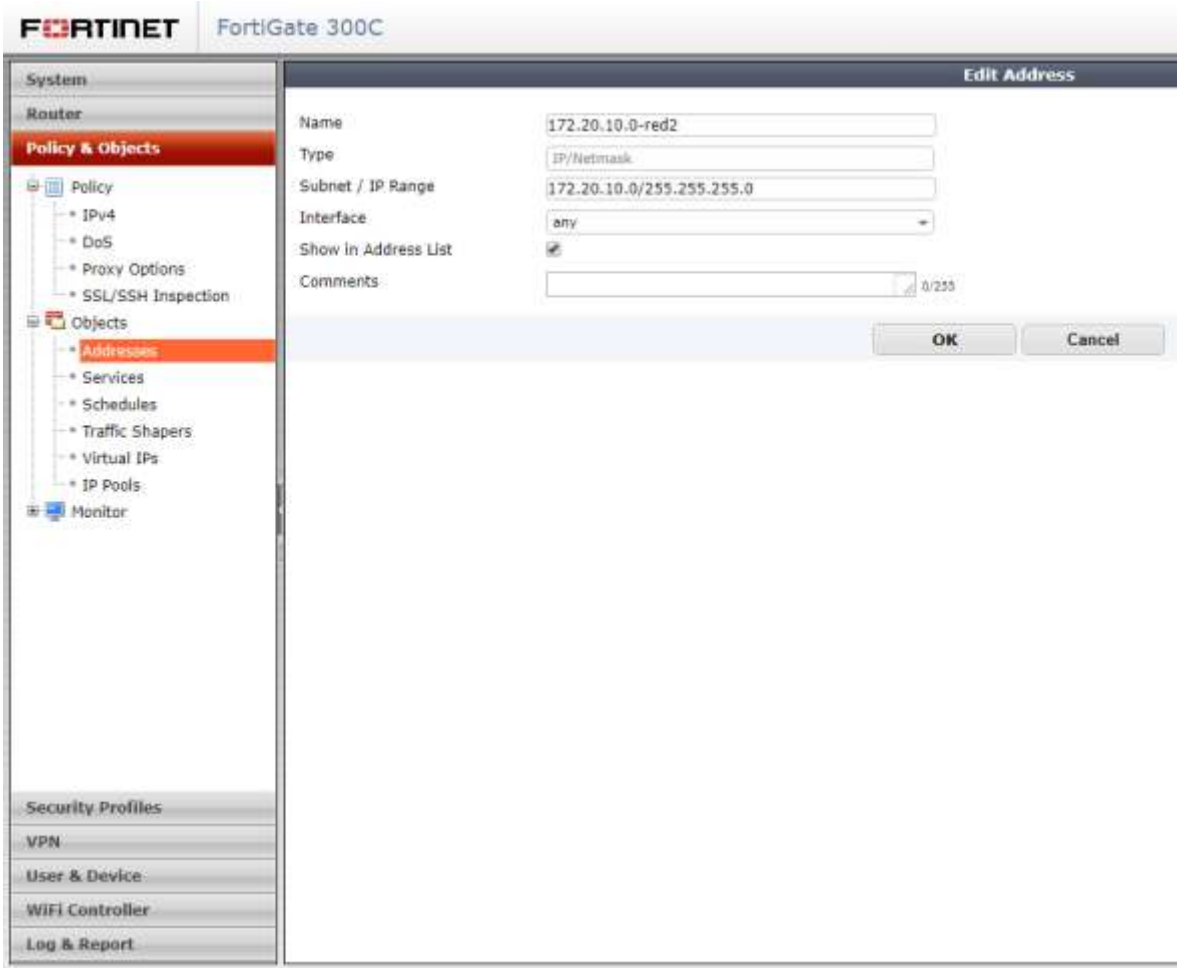

Figura 18: Creación de pool de IP

3. Ahora bien se debe crear un pool de direcciones, de este pool se tomarán las direcciones IP que serán asignadas a cada uno de los usuarios que accedan a la VPN, de preferencia se debe utilizar un rango de direcciones privadas, esto se realiza de la misma forma que se realizaron los dos pasos anteriores.

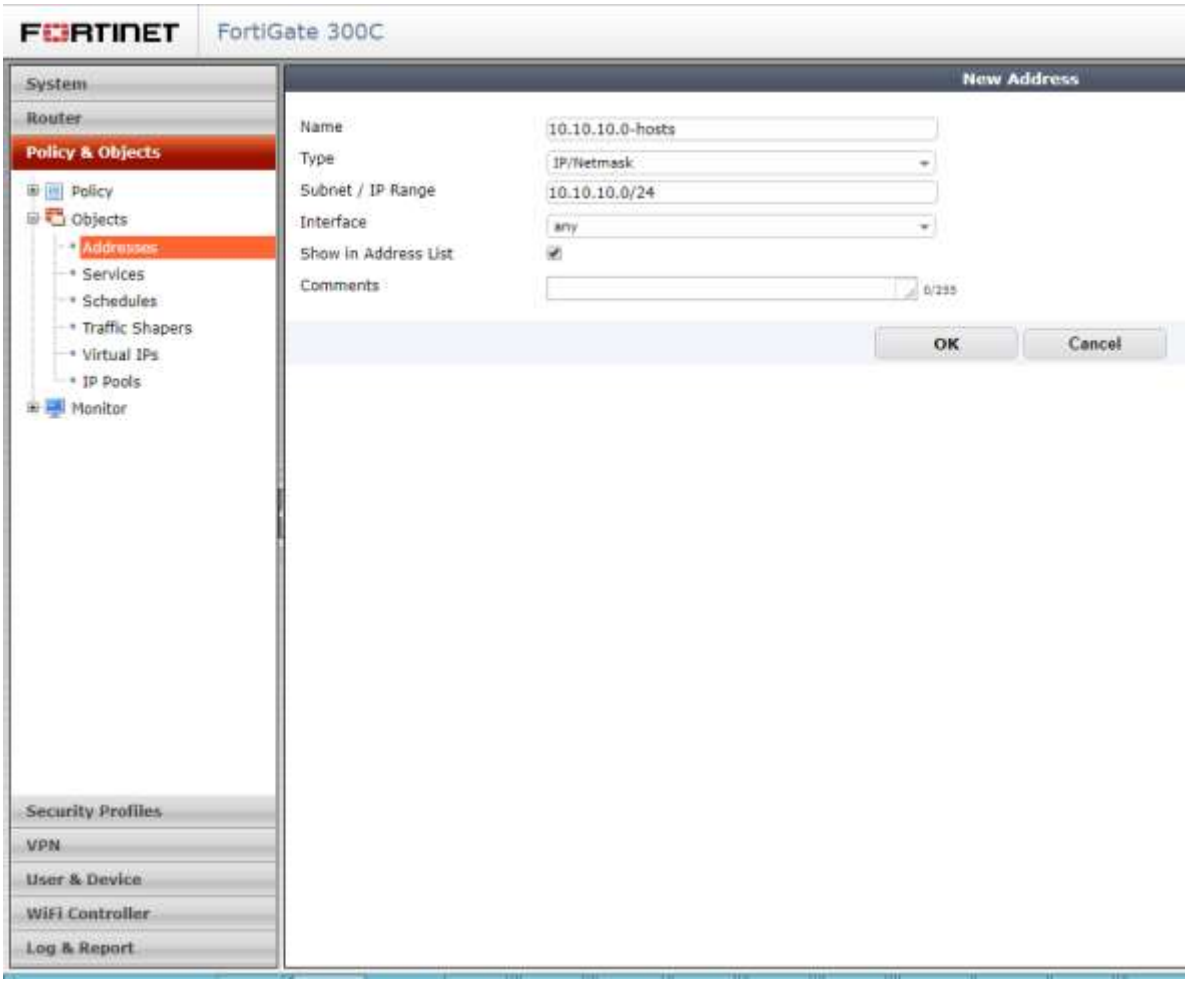

Figura 19: Creación de pool de IP

4. Después de haber creado todos los rangos de direcciones necesarios, se deben crear los usuarios que podrán acceder a la VPN, entonces en la pestaña “User & Device” >> “User” >> “User Definition” en la parte superior está la opción de crear nuevo usuario; lo primero que se solicita es especificar qué tipo de autenticación tendrá el usuario, como se puede observar se pueden usar distintos tipos de autenticación remota, como lo son RADIUS, TACACS+ y LDAP, todos estos métodos ofrecen una mayor seguridad, pero para este caso se realizará una autenticación local, entonces se deja la opción “Local User”.

Figura 20: Selección tipo de usuario

5. En el siguiente paso se solicita el nombre el usuario y su contraseña, esto para la respectiva autenticación.

Figura 21: Creación de usuario "luis"

6. Después se solicita una dirección de correo electrónico, para efectos de confirmación y comunicación, y si se desea se puede realizar una confirmación vía mensaje de texto.

Figura 22: Adición de correo para usuario "luis"

7. Por último se da la opción de habilitar automáticamente el usuario, o dejarlo creado pero deshabilitado, y además se da la opción de como ya se mencionó anteriormente utilizar un segundo factor de autenticación, conocido en Fortinet como Fortitoken, este sistema requiere que el usuario ingrese un código aleatorio válido para una sesión, para poder ingresar a la VPN. Este servicio tiene un costo agregado por parte Fortinet ya que no viene incluido en la licencia original.

Figura 23: Habilitar usuario "luis"

8. Después de crear tantos usuarios como sean necesarios, se creará un grupo de usuarios, para así facilitar la configuración al momento de crear la VPN, esto se hace en la pestaña "User & Device" >> "User" >> "User Groups", allí se da en la opción para crear nuevo grupo y se tiene lo siguiente, donde se solicita el nombre del grupo, el tipo del grupo, que para este caso es "Firewall", los usuarios que pertenecen a este grupo, y por último si se está utilizando algún tipo de autenticación remota se encuentra la opción para agregar el servidor remoto con el cual se desea conectar.

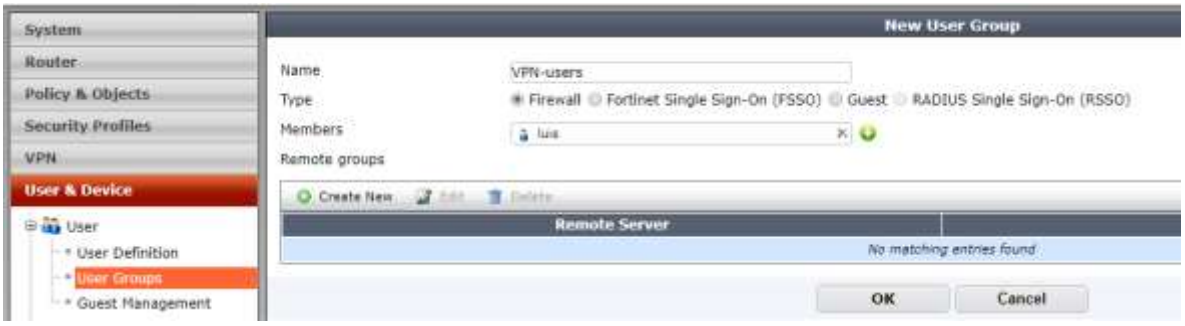

Figura 24: Creación grupo de usuarios "VPN-users"

9. Ahora bien, ya teniendo todo lo necesario se procederá a la configuración de la respectiva VPN, esto se hace en la pestaña "VPN" >> "IPsec" >> "Tunnels"; entonces para la creación de la VPN primero se requiere la plantilla del tipo de VPN, en este caso se realiza una VPN dialup, esto debido a que el otro punto de la VPN es un host, por lo cual este tendrá una dirección dinámica. En caso de que en el otro lado de la conexión estuviera un dispositivo que actuará como Gateway se utilizaría una plantilla Site to Site.

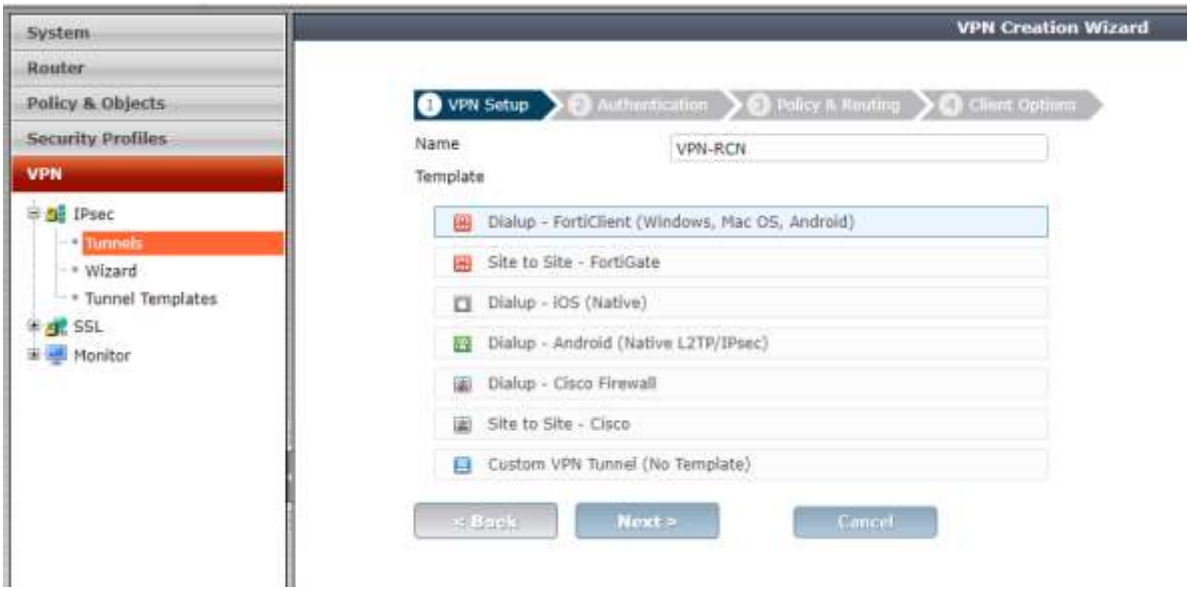

Figura 25: Selección tipo de VPN

10. Después se solicita especificar cuál es el puerto por el cual ingresará la conexión VPN, es decir el puerto que tiene conexión hacia internet, para este caso es “port1”, el método de autenticación se configura como “Pre-shared Key”, esta clave se debe tener presente, ya que será utilizada en la primera conexión con la VPN, y por último asignar el grupo de usuarios que se creó anteriormente.

Figura 26: Configuración VPN IPsec

11. Ahora bien, se debe especificar la interfaz que tiene conexión con la red interna de la empresa en este caso el port 2, se deben asignar los rangos de IP a los que tendrá acceso la VPN, es decir los que se crearon en el paso 1 y 2, después se pedirá especificar el rango de IP que será usado para asignar a los clientes de la VPN, además en caso de ser necesario se podrán asignar DNS diferentes a los que vienen por defecto.

Figura 27: configuración VPN IPsec

12. En este caso se configuran preferencias de los usuarios, como guardar la contraseña, conexión automática con la VPN y no cerrar la conexión automáticamente.

Figura 28: Configuración VPN IPsec

13. Después de crear la VPN es necesario crear una política dentro del Firewall que le permite a los clientes de la VPN acceder a todos los servicios que requieran, entonces se

configura la interfaz de entrada como la VPN creada, las direcciones origen “all”, los usuarios serán los del grupo ya creado anteriormente, interfaz de salida es la interfaz que se conecta a la red interna del canal, direcciones destino “all” ya que las direcciones están restringidas directamente dentro de la configuración de la VPN, servicios permitidos “ALL” o se pueden filtrar si así se desea, el protocolo NAT debe estar habilitado, y si se desea se pueden activar los perfiles de antivirus, web filter, application control etc., esto para mayor seguridad en la conexión.

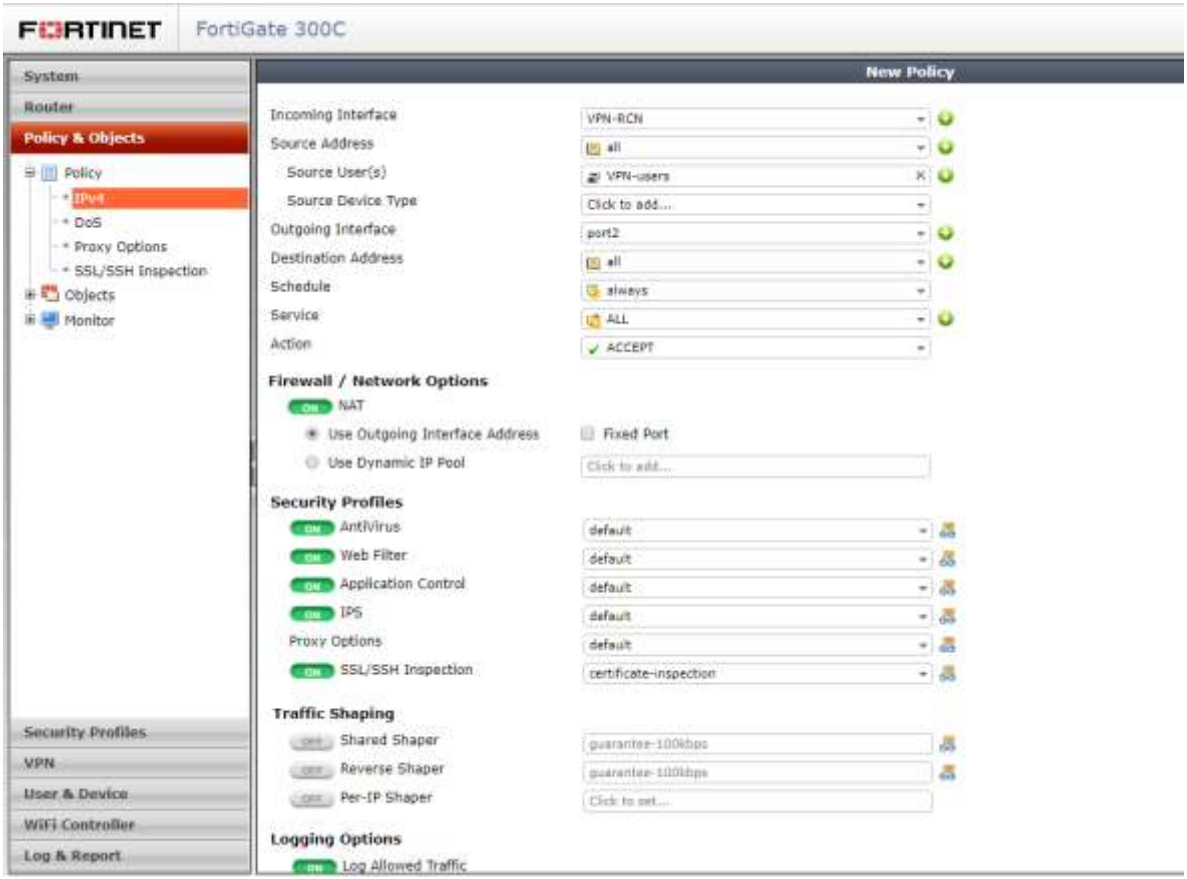

Figura 29: Configuración políticas para VPN IPsec

14. Por último se debe dejar la política habilitada para que así la VPN funcione de manera correcta

Figura 30: Configuración políticas para VPN IPsec

15. Una vez realizada la configuración en el firewall es necesario ingresar al equipo del cliente y realizar la respectiva instalación del software necesario para que este pueda ingresar a la VPN, para el caso de Fortinet se requiere FortiClient, el cual se descarga totalmente gratis desde la página www.fortinet.com.

16. Ahora bien, en la pestaña “Remote Access” se accede a la opción “Configure VPN”, la cual aparece en el centro de la ventana.

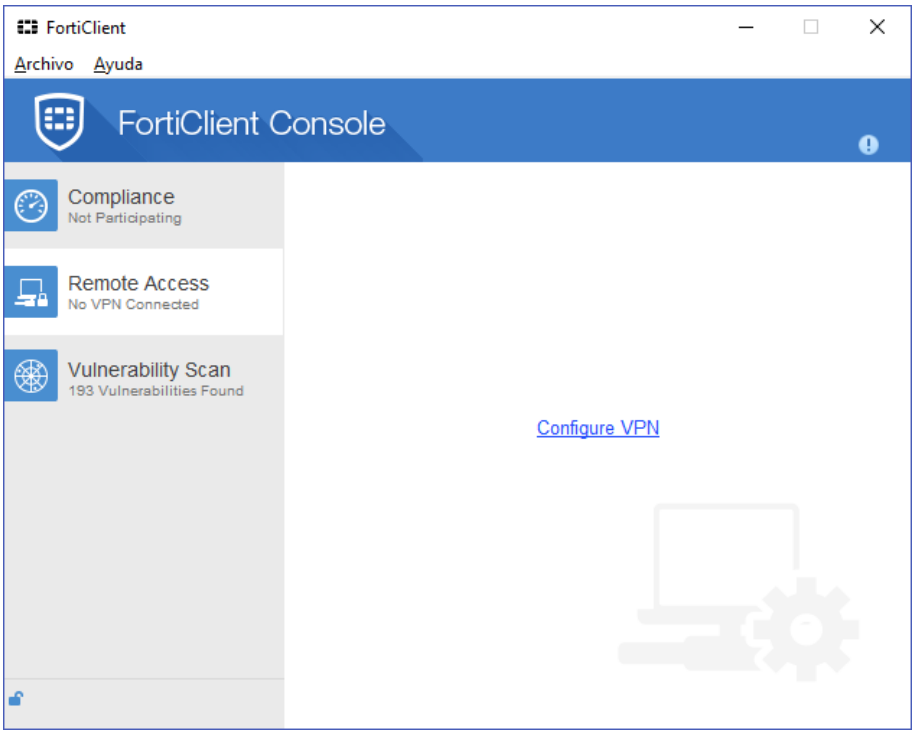

Figura 31: Configuración FortiClient para VPN IPsec

17. Una vez allí se elige la opción “IPsec VPN” en la cual se solicitará ingresar un nombre para la conexión, la ip del gateway remoto, en este caso la ip pública del firewall de la empresa, el método de autenticación y clave asignados en el paso 10, y por último se podrá elegir si guardar o no las credenciales del usuario.

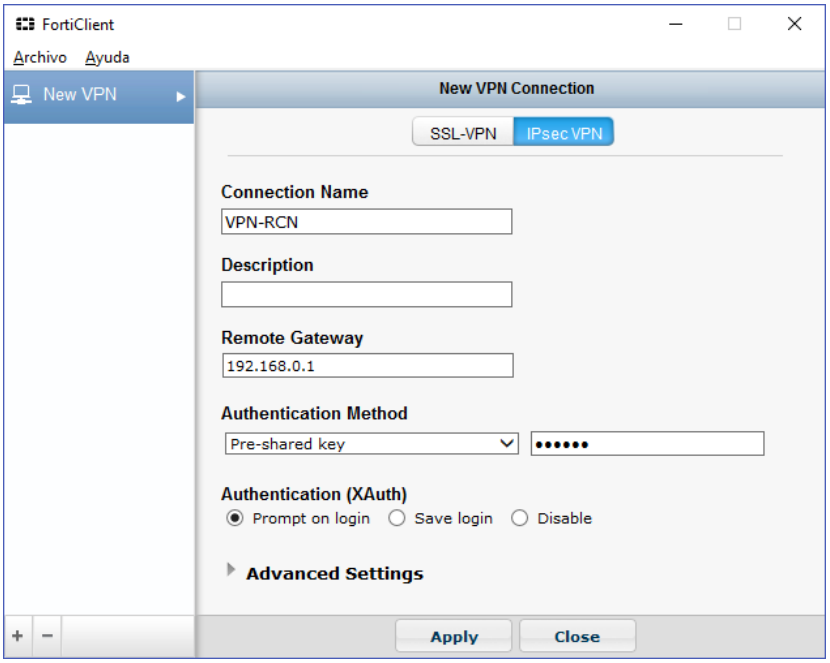

Figura 32: Parámetros conexión VPN IPsec.

18. Además de lo anterior, es posible realizar configuraciones avanzadas en las cuales se puede especificar el método de cifrado, así como el método de autenticación, el tiempo de vida de la clave o key, si se desea realizar verificación de la conexión con el otro extremo de la VPN y si se desea aplicar o no el NAT Transversal, esto para la fase 1 de las dos que utiliza IPsec en su conexión.

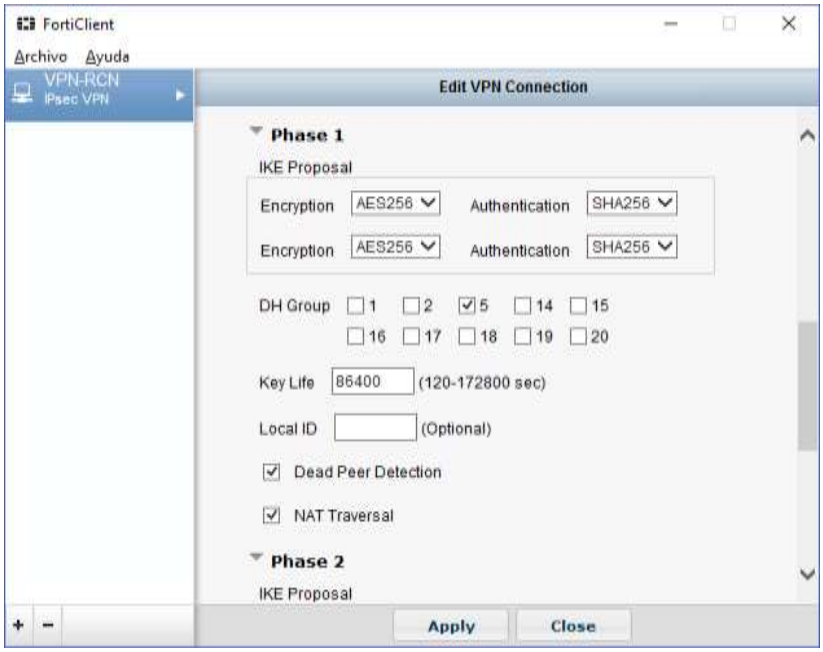

Figura 33: Parámetros conexión VPN IPsec.

19. Así mismo en la fase 2 se pueden especificar los métodos de cifrado y autenticación, el tiempo de vida de la clave o key, pero además se puede habilitar la detección de repeticiones y por último habilitar PFS (Perfect Forward Secrecy) el cual es un protocolo que garantiza que una clave de una sesión anterior que sea comprometida no afectará en ningún modo la sesión actual o sesiones futuras.

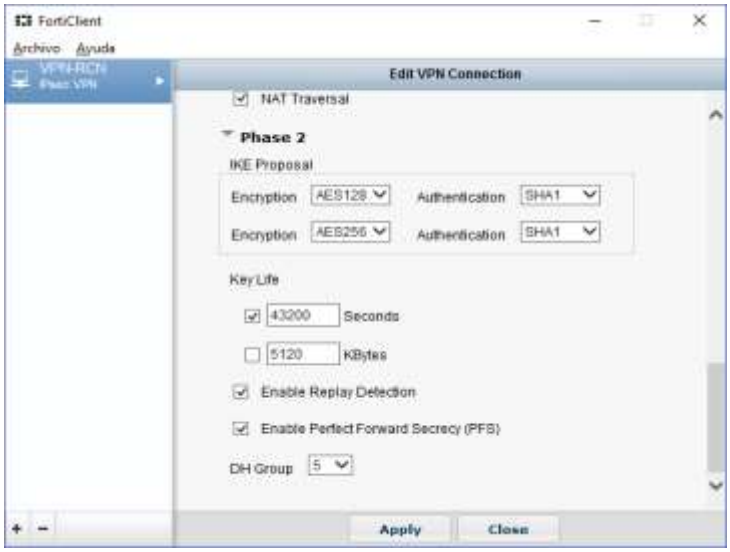

Figura 34: Parámetros conexión VPN IPsec.

20. Realizado lo anterior, se aplican los cambios y automáticamente se tiene la opción para ingresar el usuario y la contraseña creados en el paso 5, hecho esto se tendrá conexión con la VPN.

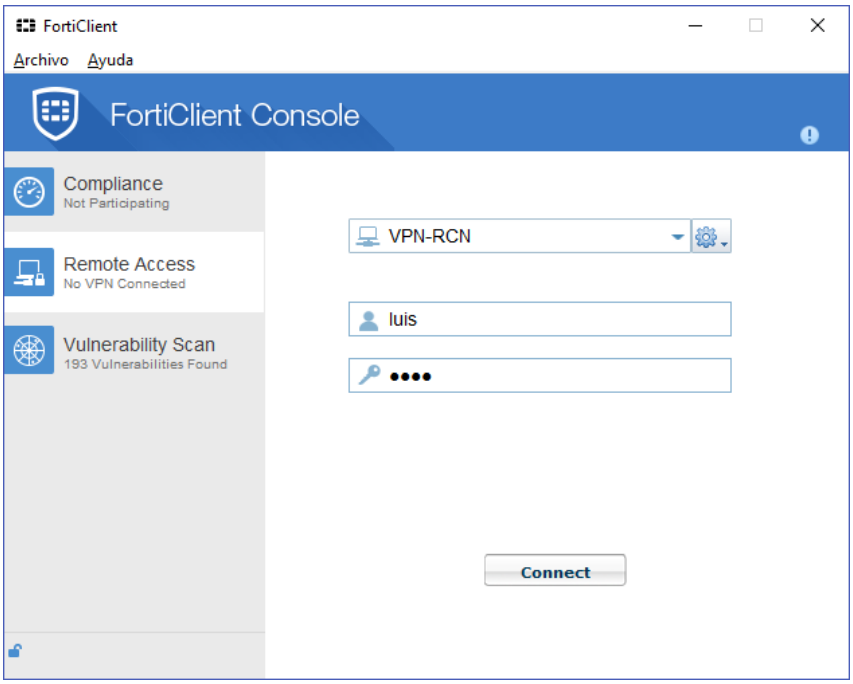

Figura 35: Acceso a VPN IPsec

3.4.2 VPN SSL/TLS

1. En primera instancia es necesario configurar el portal de acceso que tendrá la VPN, esto se configura en la pestaña “VPN” >> “SSL” >> “Portal”, y se edita la opción “full access”, allí se habilita la opción “Enable Tunnel Mode” y se configura la interfaz web que tendrá la VPN.

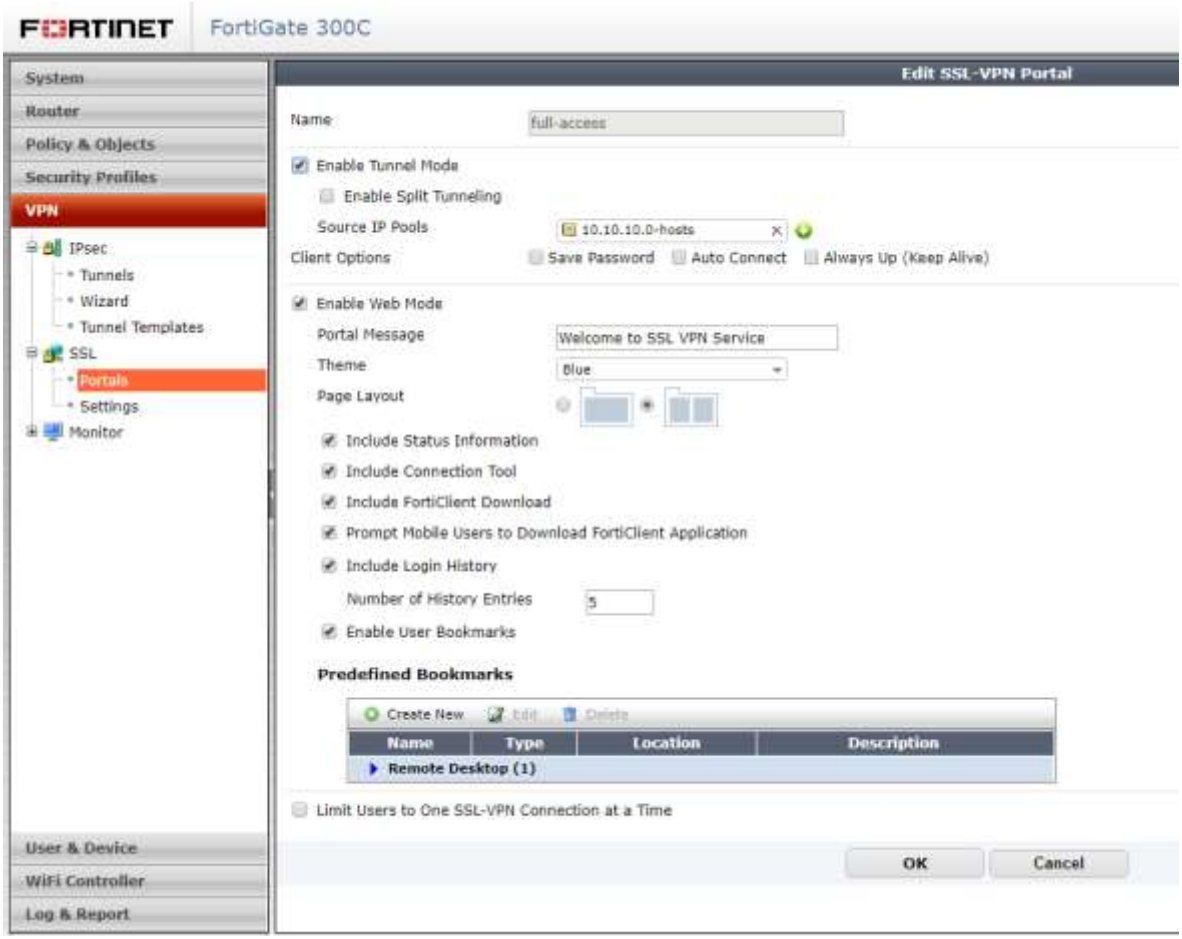

Figura 36: Configuración portal web SSL/TLS.

2. Además se crea un perfil para acceder por RDP a un host, pero además de esto se pueden agregar funciones adicionales a las que se pueda acceder desde el portal web, allí se pide la categoría, un nombre para el perfil, el host destino, las dimensiones de la pantalla, un usuario y una contraseña, que debe corresponder con los usuarios creados más adelante.

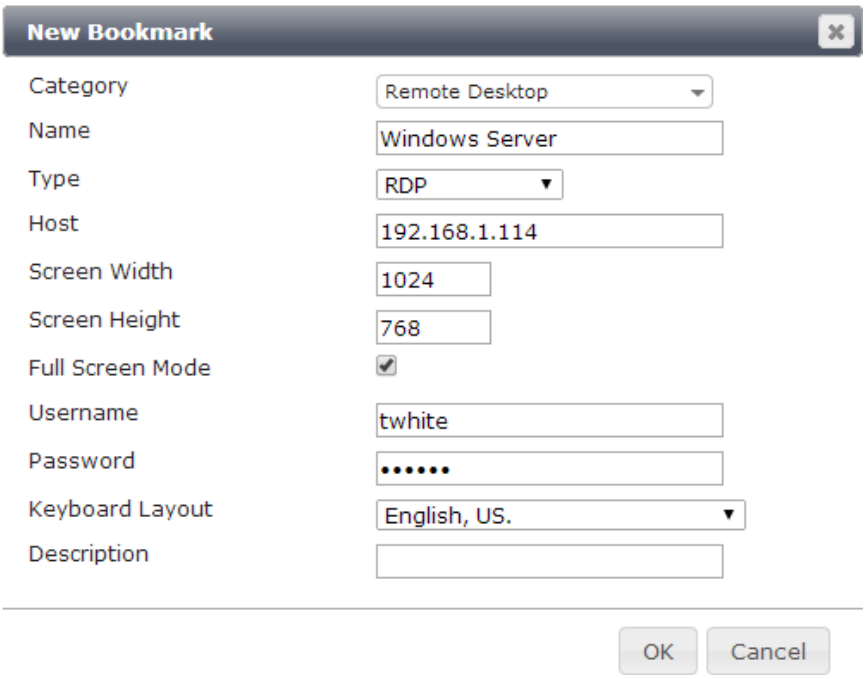

Figura 37: Configuración aplicación remote desktop para VPN SSL/TLS.

3. Los usuarios deben ser creados de la misma forma que se realizó en los pasos 4-7 en la sección 3.4.1 Configuración VPN IPsec, al igual que la creación del grupo de usuarios que se realizó en el paso 8 del mismo apartado.

4. Después de esto se deben configurar los parámetros de la VPN, esto se realiza en la pestaña “VPN” >> “SSL” >> “Settings”, allí se solicita especificar el puerto del firewall que tiene conexión a externa es decir a internet, el puerto por el cual se desea realizar la conexión, en este caso 4443, se debe verificar que este puerto no interfiera con ningún otro servicio, también se pueden especificar los host que tendrán acceso a esta VPN si así se desea, además de definir el tiempo máximo de sesión inactiva, por otra parte se puede agregar un certificado digital o bien continuar con el certificado que emite Fortinet; después se debe asignar el rango de direcciones que serán asignados a los clientes VPN marcando la opción “Specify custom IP ranges” y agregando allí el rango de IP, este se crea de la misma forma que se hizo en el paso 3 de la sección 4.4.1 Configuración VPN IPsec, por último se debe agregar el grupo de usuarios creado en el paso anterior.

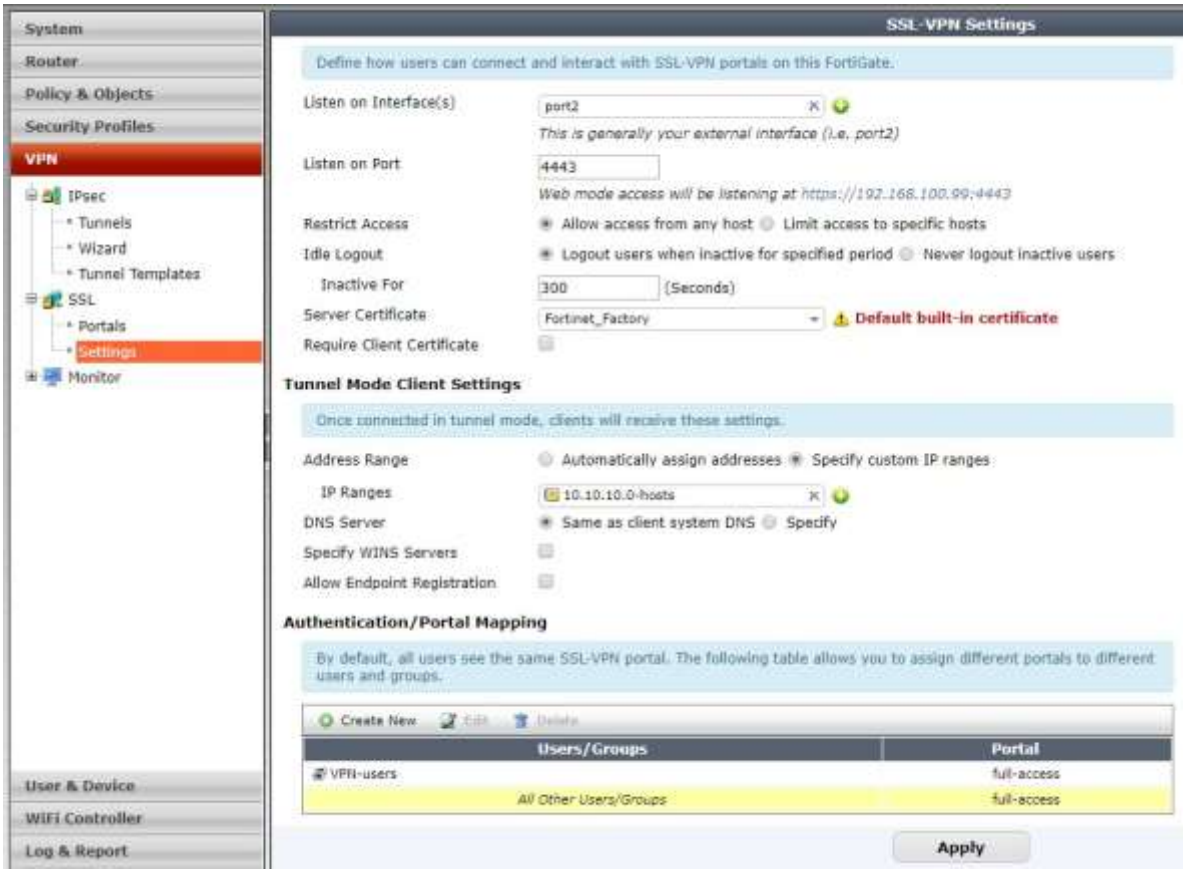

Figura 38: Configuración VPN SSL/TLS

5. Ahora bien, es necesario crear dos políticas para esta VPN una para que los usuarios VPN puedan acceder a la red interna de la organización, y otra para que la VPN SSL tenga acceso a internet, entonces esto se realiza en la pestaña “Policy & Obects” >> “Policy” >> “IPv4”, allí se asigna como interfaz de entrada “ssl.root”, direcciones origen se ponen todas, en los usuarios se especifica el grupo de usuarios creado anteriormente, la interfaz de salida será la interfaz que tiene conexión con la red interna, dirección destino todas y servicios todos, además se especifica que debe usar NAT.

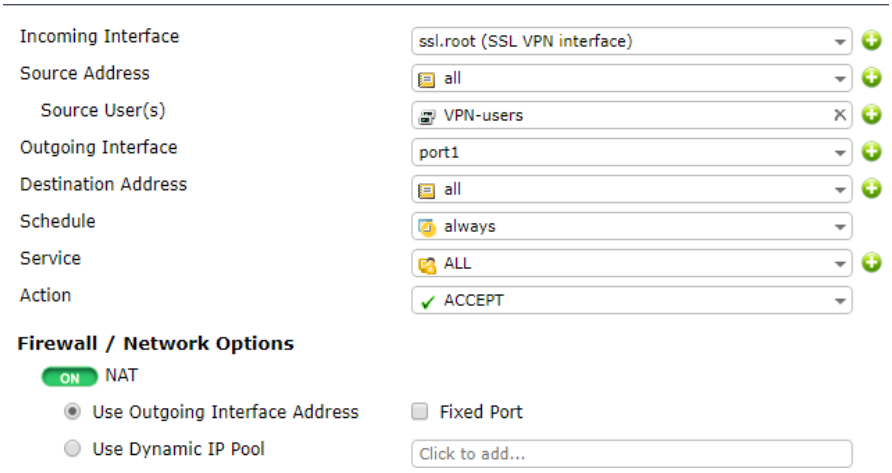

Figura 39: Política para acceder a la VPN SSL/TLS

6. Ahora la segunda política se crea de la misma forma, se mantiene la interfaz de entrada como “ssl.root”, y la interfaz de salida será el puerto que tiene conexión a internet, no se debe especificar el grupo de usuarios y en el resto de opciones se selecciona “all”

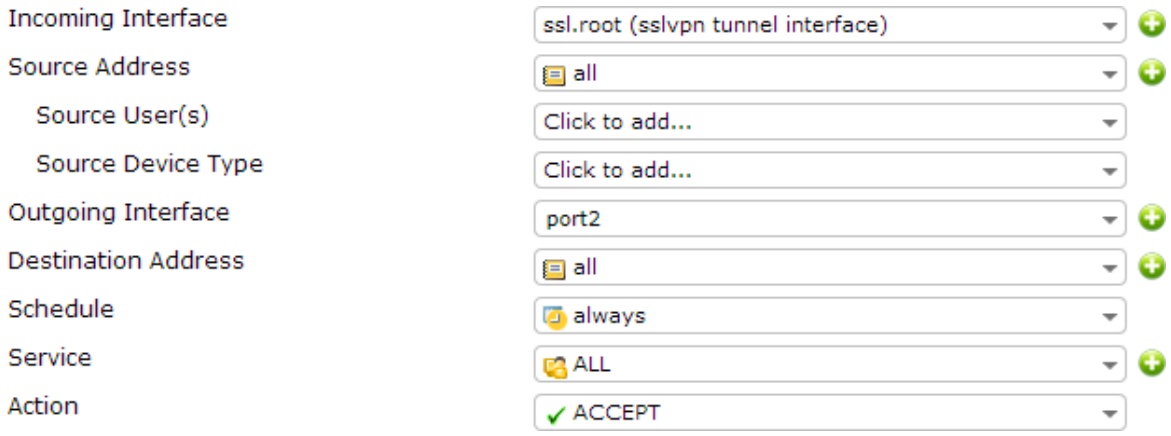

Figura 40: Política para conexión a internet VPN SSL/TLS

7. Por último solo será necesario acceder a un navegador web como Chrome, Mozilla, Safari entre otros, e ingresar la dirección https://”ip del firewall”:”puerto especificado”, que para este caso sería http://192.168.100.99:4443, esto automáticamente redirige la dirección al

portal web de la VPN pidiendo un usuario y una contraseña asignados a esa VPN.

3.5 RECOMENDACIONES

Una vez terminado todo el proceso de análisis sobre ambos protocolos, tanto IPsec como SSL/TLS, se tienen las bases necesarias para poder brindar la respectiva recomendación sobre la posible implementación de la VPN dentro de la empresa.

En primera instancia debido a la gran cantidad de información sensible que se maneja dentro de la entidad, a todos los riesgos que puede correr la organización si se llegase a filtrar información confidencial, es absolutamente necesario implementar el protocolo con mayor seguridad, que para este caso vendría siendo IPsec, ya que mantiene la información totalmente segura mediante los protocolos de cifrado, autenticación e integridad ya mencionados, y además hace que el ingreso a la VPN se totalmente seguro mediante el software que implementa y los factores de autenticación que solicita.

Por otra parte, sería absolutamente necesario establecer unas políticas de uso para esta conexión de tal modo que los usuarios y credenciales de acceso no se vean vulnerables en ningún momento, no se deberían usar dispositivos que no estén certificados por el experto en redes dentro de la empresa para realizar la conexión remota, solo equipos que hayan sido verificados y aprobados por el área respectiva.

Si así se cree necesario se puede implementar una VPN SSL/TLS para una conexión mucho más eficaz y ágil solo para compartir información que no represente ningún tipo de riesgo para la integridad de la organización, de esta forma, se pueden tener dos tipos de conexión y se puede definir que usuarios deberían trabajar sobre cada tipo de VPN.

Por último, se recomienda adoptar unas políticas de seguridad internas, con un mayor control y un consolidado sobre los accesos que tiene cada uno de los trabajadores de la organización a información sensible sobre procesos que se llevan dentro de la empresa, o la estructura de la red interna, los cuales pueden ser usados en su contra si no se mantiene el control adecuado.

En futuras ocasiones se podría realizar un análisis a los procesos que se llevan cuando se hace un cambio dentro de la infraestructura de red, ya que en varias ocasiones se ha encontrado que las áreas encargadas de esto no tienen la comunicación necesaria para que el proceso sea en común acuerdo y no se presenten desacuerdos.

3.6 CONCLUSIONES

En cuanto a seguridad en el transporte de datos se encuentran protocolos que claramente dominan el mercado del cifrado la integridad y la autenticación de la información, así mismo se demuestra que estos son de uso masivo y más importante aún, por entidades del gobierno que manejan información extremadamente sensible, por lo cual se muestran casi 100% confiables frente a posibles ataques de agentes externos, sin embargo, toda esta seguridad no serviría en lo absoluto sin unas políticas de seguridad y buenas prácticas dentro de la empresa al momento de hacer uso de estas herramientas.

El protocolo IPsec termina por ser mucho más seguro en cuanto a las políticas de seguridad que implementa para el acceso a la VPN, ya que se basa en diferentes parámetros para confirmar que la persona que está intentando acceder tiene todos los permisos necesarios y no representa ningún riesgo para la seguridad de la empresa, todo esto debido a que cualquier posible intruso necesita algo más que un usuario y una contraseña para realizar el respectivo acceso, como el dispositivo de alguien autorizado que tenga instalado el respectivo software y además en caso de aplicar, el código de seguridad que se puede implementar en este tipo de VPN si así se desea.

Por su parte SSL/TLS es un protocolo muy práctico a la hora de acceder a la VPN ya que los requisitos para el ingreso son tan básicos como un navegador y un ingreso con usuario y contraseña, lo cual la hace una herramienta con una interfaz de acceso muy simple y fácil de usar, de tal manera que desde cualquier parte del mundo con una conexión a internet y un computador, tablet, teléfono, o cualquier dispositivo que soporte un navegador con Adobe Flash Player sea posible acceder a dicha VPN.

El método AHP se presenta como una alternativa bastante útil y además muy completa para la comparación de diferentes alternativas presentadas para un problema, de esta forma la estructura jerárquica presentada como: objetivo, criterios, subcriterios y alternativas permite simplificar al máximo las comparaciones y dar con un resultado muy exacto con la ayuda de diferentes expertos en el campo a tratar.

Un firewall es tal vez la mejor forma que se tiene para realizar una VPN, esto debido a que el mismo tiene acceso a toda la red interna de la empresa, es un dispositivo especializado en la seguridad de las redes, y además no incurre en costos adicionales ya que entre los servicios que incluye la licencia actual, se tienen tanto VPN IPsec como SSL/TLS, por lo cual se presenta como la solución perfecta para la implementación de la VPN.

Cada uno de los protocolos tiene sus campos de fortaleza debilidad, pero es al final los pesos que se da a cada criterio y subcriterio lo que determina cuál será la mejor opción para realizar la implementación de la VPN en la empresa, esto debido a que los pesos son los que dan la importancia de cada criterio, por lo cual si un determinado subcriterio tiene mayor peso el impacto generado en el resultado final será mucho mayor.

Es importante que los pesos de cada criterio y subcriterio se den por parte de expertos en el tema, esto debido a que existen muchos juicios que son subjetivos y que no pueden obtenerse de manera matemática, por lo cual alguien que no tenga un gran conocimiento del tema no puede realizar un juicio que además de ser consistente sea totalmente confiable.

REFERENCIAS

[1]. S. KENT, *RFC 2402: IP authentication heade*r, 1998.

[2]. S. KENT, *RFC 4303: IP Encapsulating security payload,* 2005.

[3]. T. DIERKENS, E. RESCORLA, *RFC 5246: The transport layer security protocol version 1.2,* 2008.

[4]. S. KENT, K. SEO, *RFC 4301: Security architecture for the internet protocol.*

[5]. A. LAKBABIi, G. ORHANOU, *VPN IPsec & SSL Technology,* Université Mohammed V - Agdal, Faculté de sciences - Rabat, Portugal, 2012.

[6]. W. HUANG, *The research of VPN on WLAN*, Hebei University of Engineering, China, 2010.

[7]. M. MAZLAN, R.RAHMAN, *Technical comparison analysis of encryption algorithm on Site-to-Site, IPSec VPN,* Faculty of Electrical Engineering, Universiti Teknologi MARA, Malasia, 2010.

[8]. J. LU, C. DONG, *Study on the application of a VPN technology based on IPSec in the modern universities,* Department of Computer Science, Northeast Petroleum University, China, 2011.

[9]. A. LAGUIDI, A. HAYAR, *Secure HeNB network management Based VPN IPSec*, University Hassan II Casablanca, Francia, 2012.

[10]. D. PALOMARES, D. MIGAULT, *High availability for IPSec VPN platforms: ClusterIP evaluation,* Institut Telécom*,* Telécom SudParis, Francia, 2013.

[11]. G. QUAN-DENG, L. YI-HE, *Dynamic IPsec VPN architecture for private cloud services,* College of Computer Science, Neijiang Normal University, China, 2012.

[12]. O. ADEYINKA, *Analysis of problems associated with IPsec VPN Technology*, University of East London, UK, 2008.

[13]. H. MAO, L. ZHU, *A comparative research on SSL VPN and IPSEC VPN*, Oujiang College, Wenzhou University, China, 2012.

[14]. Protocolo IPsec, web-site visitado en Abril de 2018- http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

[15]. Tipos de arquitectura VPN, web-site visitado en Marzo de 2017 - https://iw114grupo03.wikispaces.com/2.+TIPOS+DE+ARQUITECTURA+VPN

[16]. How does NAT-T works with IPsec web-site visitado en Marzo de 2018 https://supportforums.cisco.com/t5/security-documents/how-does-nat-t-work-with-ipsec/ta-p/3119442

[17]. IPsec security associations (SAs) web-site visitado en Diciembre de 2018 - http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=7

[18]. Cabecera de autenticación, web-site visitado en Marzo de 2018 https://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzaja/rzajaahheader.htm?cp=ssw_i5_54

[19]. ¿Qué es el PKI? web-site visitado en Febrero de 2018, Samuel Noriega https://www.certsuperior.com/Blog/aqua-es-el-pki

[20]. Criptografía e infraestructura de clave pública, web-site visitado en Febrero de 2018 https://windowserver.wordpress.com/2011/02/26/criptografa-e-infraestructura-de-clave-pblica-pki/

[21]. Seguridad de las sesiones en php: session hijacking, web-site visitado en Enero de 2018 http://www.arumeinformatica.es/blog/seguridad-de-las-sesiones-en-php-session-hijacking/

[22]. VPN security flaws an its prevention, web-site visitado en Enero de 2018 https://www.clickSSL/TLS.net/blog/vpn-security-flaws-and-its-prevention

[23]. Qué es un certificado SSL/TLS y cómo funciona, web-site visitado en Enero de 2018 https://blog.neothek.com/blog-neothek/que-es-un-certificado-SSL/TLS-y-como-funciona/

[24]. Security association database, web-site visitado en Enero de 2018 - http://what-when-how.com/ipv6-advanced-protocols-implementation/security-association-database-ipv6-and-ip-security/

[25]. Algoritmo de intercambio de claves diffie-hellman, web-site visitado en Enero de 2018 - http://wiki.elhacker.net/seguridad/criptograf%C3%ADa/algoritmo-diffie-hellman

[26]. ¿Qué es RSA? web-site visitado en Enero de 2018 - https://seguinfo.wordpress.com/2007/09/14/%C2%BFque-es-rsa/

[27]. Diffie-Hellman vs RSA comparing key exchange algorithms web-site visitado en Enero de 2018 - http://searchsecurity.techtarget.com/answer/Diffie-Hellman-vs-RSA-Comparing-key-exchange-algorithms

[28]. SSL VPN for remote users, visitado en Febrero de 2018 - http://cookbook.fortinet.com/ssl-vpn-for-remote-users/

[29]. IPsec VPN with forticlient, visitado en Febrero de 2018 - http://cookbook.fortinet.com/ipsec-vpn-forticlient/

[30]. J. OSORIO, *EL PROCESO DE ANÁLISIS JERÁRQUICO (AHP) Y LA TOMA DE DECISIONES MULTICRITERIO. EJEMPLO DE APLICACIÓN,* Universidad tecnológica de Pereira, Colombia, 2008.

[31]. AHP visitado en marzo de 2018 - http://evaluador.doe.upv.es/wiki/index.php/AHP

[32]. G. CHICA, *Estudio y Análisis de la Viabilidad de la Implementación de Tecnología PLT (Power Line Telecommunications) en Colombia, en el Ámbito de la Transmisión de Datos Sobre Redes de Baja Tensión,* Departamento de ingeniería de Sistemas e Industrial, Universidad Nacional de Colombia, Colombia, 2012.