UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXÁMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistema

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMA

TEMA:

Estudio de las redes privadas virtuales VPN para soporte a usuarios remotos del sistema informático del cuerpo de bomberos de la ciudad de Montalvo.

EGRESADO:

Yuley Yessenia Martínez Chang

TUTOR:

Ing. Narcisa Crespo Torres.

AÑO 2017

INTRODUCCIÓN

A medida que pasa el tiempo la tecnología va evolucionando cada día más y más, por este motivo se ha visto la necesidad de crear, desarrollar e implementar nuevos sistemas informáticos, para lograr que la información transmitida por los diferentes canales sean seguros, debido a la importancia de la información.

Por otra parte, en la actualidad las redes han sido el punto clave de la inseguridad, que las personas mal intencionadas quieren tener acceso a información que no les compete, las redes han reducido en gran escala costos y tiempo a las empresas siendo una gran ventaja para las organizaciones.

Por este motivo el Cuerpo de Bomberos del Ciudad Montalvo ha implementado la conexión VPN (Red Privada Virtual), con el fin de que la información viaje de forma segura hacia su destino, los problemas que actualmente presenta la VPN dentro de la Institución son que el personal de la Institución no puede acceder a la red desde los smartphone u ordenadores portátiles.

Otro problema que se ha manifestado es que de acuerdo con el cambio que se presentó dentro del Cuerpo de Bomberos de la Ciudad Montalvo, de ser autónomos pasó a ser municipal, y hubo la obligación de hacer cambio de proveedor de servicio internet haciendo esto que la VPN deje de funcionar, debido a que el nuevo proveedor no ofrece IP públicas causando molestia a la hora de funcionar la VPN.

También se puede decir que el personal del Cuerpo de Bomberos de la Ciudad Montalvo no cuenta con muchos conocimientos sobre temas informáticos, provocando esto

que no se use de una manera adecuada la VPN, por lo que la persona que está encargada de la administración o manipulación de la VPN no tiene muchos conocimientos sobre ella.

Frente a los diferentes problemas que se han suscitado dentro del establecimiento se harán las siguientes preguntas:

- ¿De qué manera funciona la VPN en el Cuerpo de Bomberos de la Ciudad de Montalvo?
- ¿Cómo se puede acceder a la VPN desde los smartphone u ordenadores portátiles?
- ¿De qué manera está capacitado el personal del Cuerpo de Bomberos para la manipulación de la VPN?

El presente caso de estudio se realiza para dar a conocer de una manera más a fondo sobre los problemas que presenta la VPN, el cual se estará planteando el objetivo general y los objetivos específicos.

- Investigar los diferentes ISP (Proveedores de Servicio de Internet) que brinden las direcciones IP públicas para tener salida al mundo en este caso internet para el mejor funcionamiento de la VPN.
- Analizar las falencias que se presentan a la hora de tener la conexión VPN desde los smartphone u ordenadores portátiles, para que haya una mejor comunicación entre los administrativos de la Institución.
- Evaluar el nivel de conocimiento del personal del Cuerpo de Bombero de la Ciudad de Montalvo en el manejo de la VPN.

Recordando que una VPN es una red privada que es utilizada por internet, permitiendo realizar la conexión de diferentes organizaciones a una solo red, la información que viaja por

los canales es cifrada para que solo las personas autorizadas en este caso el cliente y el servidor de acceso remoto tengan acceso a ella y no por personas mal intencionado.

Una conexión VPN es realizada punto a punto debido a la inseguridad que existen en estos tiempo, por este motivo se ha visto la necesidad de implementar estos tipos de VPN, la principal característica que presenta las VPN, es que utilizan túneles para el traspaso de la información debido que solo los extremos, son los encargados de autentificar el acceso a la misma.

Es de vital importancia mencionar que las redes privadas deben de cumplir ciertos requerimientos como se puede mencionar la autentificación de usuario, administración de dirección, encriptación de datos y administración de claves.

Las limitaciones de la presente investigación determinan que su objeto de estudio es: el funcionamiento adecuado que la VPN debe brindar a la Institución para una mayor seguridad, disponibilidad e integridad al momento de acceder a la información en el Cuerpo de Bomberos. Su campo de acción está determinado por el lugar donde se desarrollará esta investigación, que es en la Ciudad de Montalvo.

DESARROLLO

El Cuerpo de Bomberos fue fundado en el año de 1939 actualmente cuenta con 37 bomberos entre rentados, voluntarios y apoyo está ubicado en la Av. Antonia de la Bastida entre Babahoyo y 10 de Agosto, lo que esta entidad se dedica es al cobro de permiso de funcionamiento a los locales comerciales, donde se lleva un registro o una base de datos de cada negocio, también se extiende permiso de construcción, permiso de plan de contingencia, capacitaciones en contra incendio, rescate y primeros auxilios.

En la actualidad el Cuerpo de Bomberos consta con una red LAN cableada la misma que brinda servicio de internet en una parte de la Institución dado que la otra parte de la arquitectura está conformada por una red inalámbrica cuenta con 5 computadoras con procesadores core i3 con su respectiva impresora.

El Cuerpo de Bombero de la Ciudad de Montalvo cuenta con dos áreas una administrativa y otra operativa, el área administrativa es la que se dirige a diferentes parte de la Provincia, la misma que al viajar tiene acceso a la información que se encuentra en la Institución, en esto momentos se ha presentado problemas al no poder tener acceso a la VPN debido al cambio de proveedor puesto que se ha tenido que realizar llamadas para que dicha información de suma importancia sea enviada por correos electrónicos personales, pero por este medio no es seguro dado que la información puede ser robada o clonada.

Actualmente el proveedor que está brindando el servicio de internet es CNT, el mismo que trabaja con protocolo PPPOE (Protocolo Punto a Punto sobre Ethernet o Point to Point Protocol Over Ethernet), siendo que este protocolo no trabaja con VPN a consecuencia de que trabaja con una serie de códigos que da el proveedor de telefonía, así mismo dicho ISP

actúa con direccionamiento IP dinámico del rango privado de ellos, es decir, cada día es asignada diferentes IP dado que causa problemas al no dejar una sola dirección IP fija para la VPN cabe recalcar que la VPN trabaja con una dirección IP fija.

Por este inconveniente se va a realizar un estudio de las redes privadas virtuales VPN para soporte a usuarios remotos del sistema informático del cuerpo de bomberos de la ciudad de Montalvo.

La problemática que se presenta es la falta de accesibilidad de parte de los funcionarios, del Cuerpo de Bomberos de la Ciudad de Montalvo con la Red Privada Virtual siendo que al no poder tener acceso a la información causaría grandes problemas y gastos muchos mayores.

Al realizar un enfoque directo a los puntos que se van a tratar acerca de los problemas del no acceso a la información se podrá dar una posible solución al problema presentado, se debe de conocer cuáles son los tipos de redes que existen en nuestro medio.

Según la tecnología de transmisión

- Redes Broadcast o de difusión
- Redes Point To Point o redes punto a punto

Según el tipo de transferencia

- Redes de transmisión simple
- Redes Half Duplex
- Redes Full Duplex

Según el tamaño y la extensión geográfica son las que se van a estudiar para que haya un mejor funcionamiento de la VPN.

- Redes LAN (Red de Área Local): son redes locales que cubren hasta 200 metros de distancia comúnmente estas redes son instaladas dentro de una misma institución ya que su cobertura no es muy extensa.
- Redes MAN (Red de Área Metropolitana): esta red cubre alrededor de uno a siete kilómetros de distancia se sitúan dentro de una ciudad.
- Red WAN (Red de Área Mundial): esta red puede comunicar un continente, un país con otros.

Una red virtual es una red privada manejada por internet en la que ninguna persona no autorizada puede acceder a ella, es una red de conexión punto a punto donde la información que es trasmitida por este canal es encriptado para mayor seguridad y solo el cliente y el servidor de acceso remoto tienen acceso a dicha información. VPN (Red Privada Virtual), " es una red privada que utiliza la internet para conectar con seguridad usuarios o sitios remotos, en lugar de usar líneas dedicadas, una VPN utiliza una conexión virtual enrutada a través de internet en enlaces de banda ancha." (Vasquez, 2014, pág. 18)

Según (Marqués, 2016, pág. 3) "Una VPN es una red privada virtual. Esto quiere decir que entre otras funciones, puede realizar el rol de una línea dedicada o red privada (segura), sin serlo físicamente, debido a la seguridad que ofrece."

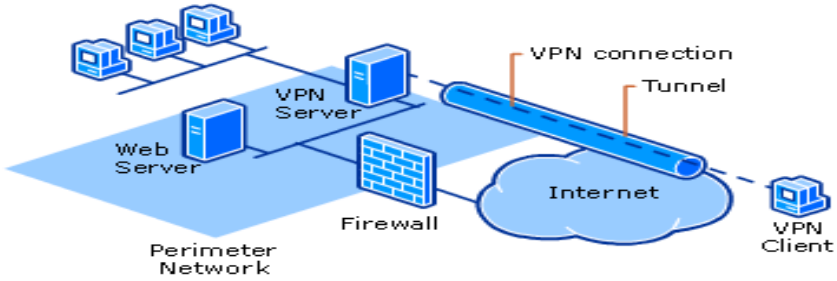


Figura 1. Esquema de cómo está estructurada la VPN en el Cuerpo de Bombero de la Ciudad de Montalvo. Vulnerabilidad sobre servicios de VPN. (2015).

En la (Figura 1) está mostrando como está diseñada la VPN en el Cuerpo de Bomberos de la Ciudad de Montalvo, la misma que cuenta con un servidor VPN la persona responsable o encargado de manipular siendo este el primer jefe, también se cuenta con el servicio de internet dado esto por CNT (Corporación Nacional de Telecomunicaciones), el cliente servidor en este caso la tesorera, la que es encargada de realizar las actividades del Cuerpo de Bomberos, adicionalmente la red consta de un corta fuego encargado de proteger la red de cualquier ataque de afuera bloqueando el acceso.

La tecnología de las VPN se basa en elementos para la protección de las diferentes privacidades dentro de la red manteniendo la confiabilidad y calidad se puede mencionar los siguientes elementos.

- Seguridad
- Calidad de Servicio
- Gestión

Para conectar una VPN se debe de tener en cuenta que existen dos tipos de VPN.

VPN de acceso remoto: esta conexión permite que los usuarios puedan acceder a un servidor de red privada desde el lugar que se encuentre a través de una red pública como internet, al realizar esta conexión punto a punto entre el cliente y el servidor remoto el cliente tendrá

acceso a la información siempre y cuando el servidor tenga registrado al cliente de lo contrario no podrá acceder.

VPN de sitio a sitio: permite tener conexión enrutada de una organización pero en distintas ciudades o sucursales a través de una red pública haciendo esto como una red WAN extensa utilizando propiedades de Tunneling (Túnel), encriptación, autenticación y cifrado de datos con esto mantendría todas las seguridades necesarias para que la información que viaje por ese medio sea segura.

Una vez conocido cuales son los tipos de VPN se realiza el análisis que el Cuerpo de Bomberos trabaja bajo una conexión de acceso remoto, permitiendo esto una conexión punto a punto entre el servidor y el cliente, continuamente se describe las propiedades de la VPN de sitio a sitio de las redes privadas virtuales en el cual está trabajando en la actualidad.

Tunneling (Túnel): consiste en que los puntos finales cliente/servidor estén de acuerdo con el mismo túnel de transferencia utilizando los diferentes protocolos basados explícitamente en datagramas en pocos palabra se puede decir que túnel es el medio en que la información es transmitida. Existen diferentes protocolos de túnel:

- PPTP (Protocolo de Túnel Punto a Punto): este protocolo consiste en que las tramas son creadas y encapsuladas mediante un paquete de datos IP (Protocolo de internet) con el protocolo punto a punto permitiendo esto conectarse a una conexión de igual a igual un equipo remoto siendo que el paquete que es enviado encapsulado viaje dentro del datagrama.

- L2TP (Protocolo de Túnel de Capa Dos): según (Sivianes Castillo, y otros, 2010) “es un protocolo de capa 2 basado en PPP e incluye características de PPTP y L2F. Surge como resultado del trabajo del IETF (RFC 2661)”
- IPSec (Seguridad de Protocolo de Internet): este protocolo mejora en gran escala la seguridad mediante algoritmos de cifrados fuertes utilizando también un sistema de autentificación más amplia, se puede decir que este mecanismo posee dos métodos de encriptación uno que es de modo túnel cifrando la cabecera y la carga de cada uno de los paquetes que se envíen y el otro de modo transporte este en cambio solo cifra la carga del paquete enviado.

La Encapsulación Según (Perez, 2009, pág. 406) “encapsulación con la tecnología VPN los datos privados se encapsulan con un encabezado que contiene información de enrutamiento que permite a los datos recorrer la red de tránsito.”

(Perez, 2009, pág. 406) Afirma que la autentificación:

Adquiere una primera forma denominada autentificación en el nivel de usuarios con autenticación PP. Para establecer la conexión VPN, el servidor VPN autentifica al cliente VPN que intenta realizar la conexión con un método de autenticación en el nivel de usuario de protocolo punto a punto y comprueba que el cliente VPN tiene la autorización adecuada.

Cifrados de datos: esto quiere decir cuando la información es enviada por el túnel el remitente cifra los datos y al llegar al destino es descifrada utilizando una clave de cifrado común.

Una vez tenido en cuenta cuales son las propiedades de conexión de las redes privadas virtuales se dirigirá a los requerimientos básicos que se debe cumplir al momento de emplear una VPN para conectar las redes virtuales dentro de la red.

- Autenticación de usuario: Verifica la identidad del usuario-cliente y si el usuario no está registrado dentro del servidor restringe su acceso a la VPN dando aviso al servidor, además la VPN mediante el registro de auditoría se deberá saber quién accedió a la VPN en que momento y a que información accedió.
- Administración de dirección: la red privada virtual designara una dirección al cliente para que pueda tener acceso a la red privada teniendo en cuenta que las direcciones privadas asignadas deban mantenerse.
- Encriptación de datos: la información o los datos que se envíen a través del túnel o la red privada deberá ser encriptado o cifrada, para que solo sean leídos por los usuarios autorizados y no interceptados por intrusos.
- Administración de claves: las red privada deberá proporcionar o generar las diferentes claves de codificación para cada cliente y cada servidor teniendo en cuenta que estas deberán ser renovadas o actualizadas cada cierto tiempo
- Soporte de protocolo técnico: la red privada deberá soportar los protocolos comunes utilizados dentro de la red pública entre estos protocolos está incluido el protocolo de internet entre otros.

Tipos de conexión de las redes privadas virtuales que se pueden mencionar son las siguientes:

Conexión de acceso remoto: es realizada por un usuario o cliente mediante ordenador, que desean realizar la respectiva conexión a una red privada una vez hecha la conexión mediante la VPN, los paquetes que son enviados cifradamente son originados explícitamente a los

clientes de acceso remoto y este debe ser autentificada por el servidor de acceso remoto, una vez hecha esta secuencia el servidor deberá realizar la autentificación ante el cliente.

Conexión de router a router: esta conexión es realizada por un router conectándose a una de las redes privadas establecidas en la institución los router no son originarios de los paquetes enviados por los diferentes router de la red sino que el router que hace la llamada tiene que autentificarse frente al router que responde y viceversa sirviendo esto también para la intranet.

Según (USERSHOP, 2008, pág. 107) un router "es el dispositivo encargado de unir dos redes de forma segura y precisa, que pueden o no encontrarse a una distancia considerable una de otra."

Una intranet según (Sánchez Estrella & Herrero Domingo, 2014, pág. 3) "es una red de área local, es decir, de uso exclusivo de una determinada organización, por lo que solamente los equipos informáticos de esta pueden acceder a ella."

Conexión de firewall a firewall: esta conexión se realiza por uno de los firewall conectándose simultáneamente a unas de las redes privadas, el usuario podrá enviar los paquetes mediante internet sin ningún problema debido que el firewall que está haciendo la llamada, tiene que realizar la autentificación frente al firewall que está respondiendo y de la misma manera el firewall que responde debe de realizar la autentificación con el firewall que realiza la llamada.

Según (Gaumé, 2016, pág. 374) firewall es un dispositivo lógico o físico que comprueba los datos entrantes o salientes que van o vienen de redes externas como internet. Así pues, un firewall le permite prevenir los ataques de hackers o programas malintencionados que intentan tomar el control del equipo de una manera u otra.

Figura 2. Cómo funciona un firewall. Valdivia, C. (2014)

En la (Figura 2) muestra cómo funciona el firewall dentro de la red, es decir, el firewall es el encargado de administrar todos los datos que hay en la conexión de internet, de entrada y salida permitiendo bloquear el acceso, permitir el acceso o desviar el acceso a otro lado, también el firewall bloquea páginas por las cuales el servidor da orden del no acceso a ciertas páginas como se muestra en la figura.

VPN en entornos móviles: esta conexión se debe establecer cuando el punto de la red privada virtual, no se encuentra fijo a una sola dirección IP sino más bien tiene movimiento por distintas redes para no perder la sesión segura dentro de la VPN, como sea posible entre estás pueden estar las redes de datos de operadores móviles o los diferentes puntos de acceso de una red wifi, además estas conexiones son utilizadas en la gestión de equipos técnicos para la seguridad pública, siendo en gran parte adaptadas por personas profesionales que tienen la necesidad de tener una conexión fiable .

Una dirección IP (Protocolo de Internet) según (Torrente Artero, 2013) “es una etiqueta numérica formada por cuatro cifras, de valores entre 0 y 255 separados por un punto, que

identifica a la tarjeta de red de un dispositivo (computadora, placa Arduino Ethernet, etc.) dentro de la red de tipo TCP/IP."

Para el diseño de nuestra VPN se tiene que tener en cuenta las posibles demandas que se pueda presentar. Según (Castro Gil, Díaz Orueta, Alzórriz Armendáriz, & Sancristobal Ruiz, 2014) "qué tipo de tráfico se va a trasmitir que aplicaciones usarán la RPV, con qué frecuencia, con que necesidades de cifrado."

Dentro de las demandas se ha mencionado algunas aplicaciones que se pueden utilizar para las redes privadas virtuales.

- Cisco AnyConnect: permite crear y gestionar redes privadas virtuales para ordenadores o smartphone. (tuexpertoIT.com, 2010)
- Remobo: facilita la conexión entre varios equipos garantizando la seguridad del acceso cifrando las comunicaciones cliente/servidor disponible para Windows, Mac y Linux. (Lopez, 2013)

Ventajas que se tiene de las redes privadas virtuales que nos favorecen a la Institución Reducción de costo: cuando se utiliza líneas dedicadas sitio a sitio o punto a punto, era necesario establecer un enlace dedicado entre casi todos los puntos de la Institución, con esto el número de líneas era mucho mayor y el costo a su vez ahora permiten remplazar cada línea privadas por otras menos costosas y al mismo tiempo reduce el número de líneas utilizadas.

- Las líneas dedicadas permiten la conexión de diferentes localizaciones de forma segura teniendo acceso a internet, posibilitando la transmisión de datos a grandes velocidades con una conexión punto a punto.

Mejora de la seguridad: la mayorías de redes hoy en día utilizan los protocolos TCP/IP que no son tan seguros dado que los datos son enviados en código ASCII haciendo esto que sea fácil de descifrar las redes privadas virtuales utilizaran cifrados criptográficos incrementando la seguridad del envió de información.

Según (Lajara Vizcaíno & Pelegrí Sebastiá, 2011, pág. 215) el objetivo de TCP/IP "es establecer una interconexión entre redes para proporcionar servicios de tal manera que para el usuario parezca que solo hay una única red homogénea."

Integración de los datos: con esto permitirá reducir costos, dado que se integraran dos redes de una misma institución en una sola ya que se habrá la comunicación adecuada entre ambas.

Una vez conocidos todos los términos que trabaja una VPN se debe tener en cuenta que son los protocolos PPPOE que trabaja la telefonía CNT, que son las IP públicas, IP privadas y las IP dinámicas cómo funcionan cada uno de ellos para el buen funcionamiento de la VPN.

Una PPOE (Protocolo Punto a Punto sobre Ethernet) según (Jorge, 2014) "es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cable módem y DSL."

Según (Padial, 2016) una IP pública "son aquellas que permiten que cada dispositivo conectado a una red pueda ser identificado. Cuando un dispositivo se conecta a internet se le asigna una dirección IP de las que disponga su proveedor de acceso (ISP, Internet Service Provider)"

La IP privada se la puede denominar según (Aguilera & Morante, 2012) “es un identificador único del ordenador en la red. Cada ordenador conectado a su enrutador tendrá una IP privada y todas las IP privadas de la misma red en un mismo momento deben ser diferentes.”

Figura 3. Diferencia entre IP pública e IP privada.

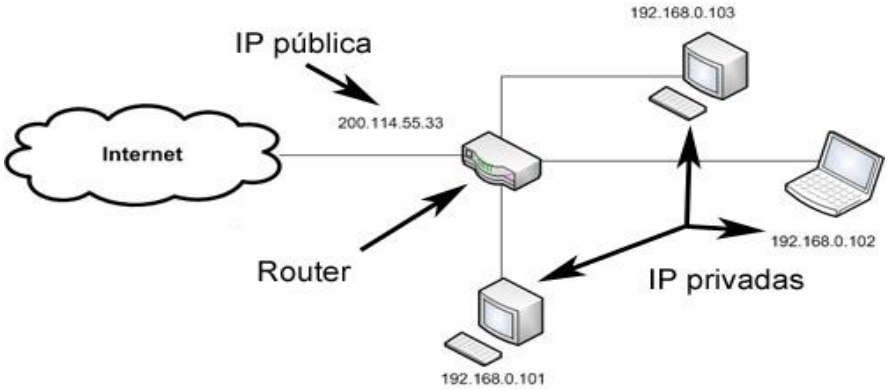


Figura 3. Diferencia entre IP pública e IP privada. Padial, J. (2016).

En la (Figura 3) detalla la diferencia entre una IP pública y una IP privada se establece que una IP publica es asignada por un proveedor de servicio de internet en cualquier lugar del mundo a los usuarios para la conexión a internet, las IP privadas son aquellas que la IANA (Internet Assigned Numbers Authority o Autoridad para Asignación de Números de Internet) estableció que no pueden ser utilizadas para internet, más bien son utilizadas internamente por las diferentes organizaciones dentro de la misma teniendo diferentes clases de IP.

También se debe de tener en consideración qué importancia tiene el usuario remoto dentro de la VPN y hacernos la pregunta ¿Qué es un usuario remoto?, ¿Qué es un servicio de acceso remoto?, ¿Cuál es la ventaja de tener un servicio de acceso remoto?, ¿Será que un usuario remoto es fiable dentro de la Organización?

Según (Techopedia, s.f.) “un usuario remoto es un usuario que está operando un dispositivo de hardware o software para acceder desde un lugar fuera de las instalaciones.”

Ante lo mencionado se puede decir que un usuario remoto no es más que una persona accediendo a otra computadora desde cualquier parte que se encuentre, teniendo permiso al acceso a los diferentes documentos, archivos, etc. Que se encuentran en el otro lado del software siempre y cuando este tenga su usuario y contraseña.

Un servicio de acceso remoto según (Caballero & Caballero Artigas, 1997) es el equipo que recibe las llamadas remotas y las conecta a la red de área local central. El hardware del servidor de acceso remoto debe ser fiable y eficiente, y disponer de una arquitectura bien diseñada.

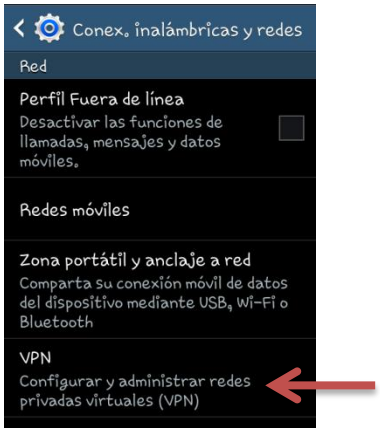
Las principales ventajas que se pueden mencionar dentro del servicio de acceso remoto son:

- Los servicios de acceso remoto son considerados los servicios más seguros debido a que el usuario y el equipo tienen la necesidad de acceder mediante una solicitud de conexión es decir usuario y contraseña, en el momento de tráfico de información el acceso es supervisado cuidadosamente para que no se suscite ninguna interferencia.
- Otra ventaja que se presenta es que la mayoría de las empresas utilizan este servicio dado que es más fácil el manejo.
- Bajo costo en el mantenimiento ya que no hay la necesidad de la utilización de otros equipos de servicio costosos o realizar contratación de otro personal para que maneje el sistema.

Dentro del estudio de caso también se ha visto la necesidad de tener el acceso a la VPN desde los smartphone, tablet u ordenadores portátiles debido a que no existe dicha conexión de la VPN con Android se debe de seguir los siguientes pasos:

- Abrir el menú de ajustes
- Desde ajustes se pulsa “más redes” para que se desplace el resto de opciones relacionadas con la conectividad.
- Se pulsa sobre VPN para abrir la configuración y administrar las redes privadas virtuales (VPN). Se verá una pantalla como la siguiente figura 5.

Figura 5

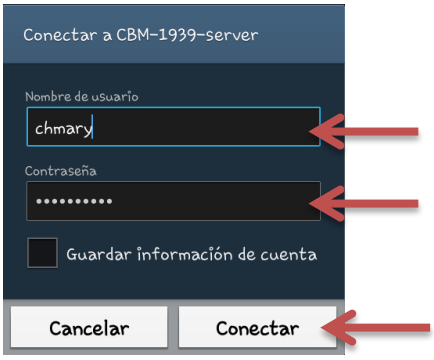


Fuente propia

- Se presiona sobre el botón “+” para que se muestre la pantalla de configuración de la nueva conexión VPN.
- Se deberá ingresar el nombre que se dará a la red, el tipo de conexión y la dirección IP del servidor. Se pulsa guardar para que se guarden los cambios y aparecerá la nueva conexión en la lista.

- Para conectarse se deberá pulsar sobre la misma e ingresar el usuario y la contraseña del servidor como se muestra en Figura 8. Luego se procede a pulsar en conectar.

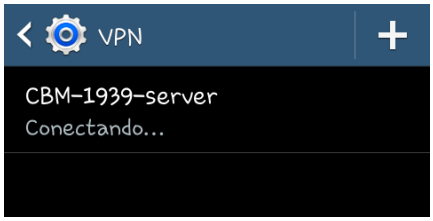
Figura 8



Fuente propia

- Se establecerá la conexión con el servidor después de unos segundos se estará navegando por internet. (MOVILZONA, s.f.)

Figura 9



Fuente Propia

Una forma sencilla de saber si nuestra VPN está funcionando es escribir la dirección IP en el navegador de google y tendrá que mostrar la dirección IP de la VPN si esta no nos muestra esto indicará que la VPN tiene problemas como se muestra figura 10.

Figura 10

Fuente propia

CONCLUSIÓN

Como resultado del análisis del caso de estudio es posible concluir que la Red Privada Virtual en el Cuerpo de Bomberos de la ciudad de Montalvo.

- Existe la necesidad de que adquieran un nuevo proveedor de servicio de internet por motivo que este nuevo proveedor brinde IP públicas para que la VPN funcione correctamente.
- Se llegó al análisis de realizar una nueva configuración dentro del servidor para crear nuevos usuarios remotos y puedan acceder a la VPN desde los smartphone u ordenadores portátiles.
- Existe la necesidad de que haya una persona encargada de administrar la VPN, de manera que esta tenga un mejor conocimiento sobre el mismo.
- Es necesario de que el personal que trabaja en el área administrativa del Cuerpo de Bomberos del Cantón Montalvo tengan una capacitación más a fondo del manejo adecuado de la Red Privada Virtual.
- Utilización de una aplicación como Cisco Any Connect esta permitirá crear y gestionar redes privadas virtuales para ordenadores o smartphone disponible para Windows, Mac y Linux.

Bibliografía

(s.f.).

Aguilera, P., & Morante, M. (2012). Internet, mantenimiento y redes (Ofimática y proceso de la información). En P. Aguilera, & M. Morante, *Internet, mantenimiento y redes (Ofimática y proceso de la información)* (pág. 18). Editex.

Areitio, G., & Areitio, A. (2009). *Información, Informática e Internet: del ordenador personal a la Empresa 2,0.* España : Editorial Visión Libros.

Caballero, J. M., & Caballero Artigas, J. M. (1997). Redes de banda ancha. En J. M. Caballero, & J. M. Caballero Artigas, *Redes de banda ancha* (pág. 272). Barcelona: Marcombo.

Castro Gil, M. A., Díaz Orueta, G., Alzórriz Armendáriz, I., & Sancristobal Ruiz, E. (2014). PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES. En M. A. Castro Gil, G. Díaz Orueta, I. Alzórriz Armendáriz, & E. Sancristobal Ruiz, *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES* (pág. 597). Editorial UNED.

Gaumé, S. (2016). Mantenimiento y reparación de un PC en red (4ª edición). En S. Gaumé, *Mantenimiento y reparación de un PC en red (4ª edición)* (pág. 490). Barcelona: Ediciones ENI.

Jorge. (27 de Octubre de 2014). *ClubEnsayos*. Recuperado el 18 de Abril de 2017, de Configuracion de una Antena: https://www.clubensayos.com/M%C3%BAsica-y-Cine/Configuraci%C3%B3n-De-Una-Antena/2144025.html

Lajara Vizcaíno , J. R., & Pelegrí Sebastiá, J. (2011). Labview : entorno gráfico de programación. En J. R. Lajara Vizcaíno, & J. Pelegrí Sebastiá, *Labview : entorno gráfico de programación* (pág. 470). Barcelona: Marcombo.

Lopez, J. (28 de Octubre de 2013). *Hipertextual*. Recuperado el 3 de Abril de 2017, de Las mejores herramientas para trabajar desde casa con VPN: https://hipertextual.com/archivo/2013/10/trabajar-casa-con-vpn/

Marqués, G. (2016). *IPsec y redes privadas virtuales.* Lulu.com.

MOVILZONA. (s.f.). *MOVILZONA*. Recuperado el 30 de Mayo de 2017, de Cómo configurar una conexión VPN desde un smartphone Android: https://www.movilzona.es/tutoriales/android/conectividad/como-configurar-una-conexion-vpn-desde-un-smartphone-android/

Padial, J. (16 de Octubre de 2016). *curiosoando*. Recuperado el 28 de Abril de 2017, de ¿Cuál es la diferencia entre IP pública e IP privada?: https://curiosoando.com/cual-es-la-diferencia-entre-ip-publica-e-ip-privada

Perez, M. (2009). *Windows Server 2008 : instalación, configuración y administración.* RC Libros.

Sánchez Estrella, Ó., & Herrero Domingo, R. (2014). Aplicaciones básicas de ofimática. En Ó. Sánchez Estrella, & R. Herrero Domingo, *Aplicaciones básicas de ofimática* (pág. 152). Madrid: Ediciones Paraninfo, S.A.

Sivianes Castillo, F., Sánches Antón, G., Ropero Rodríguez, J., Rivera Romero, O., Benjumer Mondéjar, J., Barbancho Concejero, J., & Romero Ternero, M. D. (2010). *Servicios en Red.* Madrid: Editorial Paraninfo.

Techopedia. (s.f.). *Techopedia*. Recuperado el 05 de Mayo de 2017, de Remote user: https://www.techopedia.com/definition/5554/remote-user

Torrente Artero, Ó. (2013). Arduino : curso práctico de formación. En Ó. Torrente Artero, *Arduino : curso práctico de formación* (pág. 588). Madrid: RC Libros.

tuexpertoIT.com. (3 de Marzo de 2010). *tuexpertoIT.com*. Recuperado el 3 de Abril de 2017, de Cisco AnyConnectuna aplicación de cliente de redes para ordenadores y smartphones: https://www.tuexpertoit.com/cisco-anyconnect-una-aplicacion-de-cliente-de-redes-para-ordenadores-y-smartphones/

USERSHOP. (2008). Reparación de componentes. En USERSHOP, *Reparación de componentes* (pág. 240). USERSHOP.

Vasquez, J. (2014). *Libro científico: Investigaciones en tecnologias de información informatica y computación.* EE.UU.: Palibrio.

ANEXO

Anexo 1. Dialogo sobre el funcionamiento de la VPN