UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

Facultad de Contaduría y Administración

Facultad de Ciencias Químicas e Ingeniería

Maestría en Tecnologías de la Información y la Comunicación

Integración de un entorno de comunicación por medio de una red virtual privada con IPSec.

TESIS QUE PARA OBTENER EL GRADO DE

MAESTRO EN TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN

Presenta:

I.C. ÁNGEL ISAAC CARVAJAL GONZÁLEZ

Bajo la dirección de:

DRA. CARELIA GUADALUPE GAXIOLA PACHECO

TIJUANA, BAJA CALIFORNIA, MEXICO **JUNIO 2014**

Índice de Contenido

Índice de Figuras

Índice de Tablas

RESUMEN

La presente tesis de caso práctico tiene como propósito la integración de un entorno de comunicación de datos por medio de una red virtual privada con IPSec para el flujo de la información entre las sucursales o los puntos de ventas y la unidad corporativa de la empresa Tecnicentro Royal S.A. de C.V., en el cual se rediseñó la infraestructura de red para la comunicación de los datos para las 29 sucursales en la zona noroeste del país de México. La manera en que se llevó a cabo la solución tecnológica de la red de datos está basada en la metodología PPDIOO de Cisco, el cual brindó las etapas de operación para la integración de una nueva red de comunicación entre los distintos puntos. Se inició con la preparación y la recopilación de la información de la infraestructura de la red para poder llevar a cabo una correcta planeación, en la parte del diseño se buscó seguir las mejores prácticas para elaborar la infraestructura de red necesaria para la integración de la tecnología nueva. Se partió de un escenario de prueba en una de las sucursales con la intensión de hacer las mediciones necesarias y los ajustes para los demás puntos de ventas, el cual arrojó la configuración necesaria que sirvió como base para los otros dispositivos de comunicación. Los resultados mostraron que hubo una reducción considerable del gasto en los servicios de internet mensualmente, debido a que ya solo se requiere contar con un único servicio en los puntos de ventas, el cual incrementó la estabilidad y conectividad en la red alámbrica como también en la red inalámbrica WIFI tanto para el personal interno como la red de visita. Con respecto a la gestión de la red se obtuvo una cantidad de herramientas para la administración de la misma, el cual da oportunidad de aplicar políticas de filtrado web, monitoreo y acceso a ciertos usuarios de forma remota. Finalmente, se aportó una gama de opciones para la integración de nuevas tecnologías, debido al nuevo canal o medio de comunicación que cumplió con las expectativas de accesibilidad, conectividad y rendimiento de la red de comunicación.

Palabras clave: Integración, Red Privada Virtual, IPSec, PPDIOO

ABSTRACT

This thesis aims case study integrating a data communication environment through a Virtual Private Network with IPSec for the flow of information between branches or outlets and corporate business unit Tecnicentro Royal SA de CV , which the network infrastructure for the communication of the data for the 29 branches in the northwest of the country of Mexico was redesigned . The way it was carried out the technological solution of the data network is based on Cisco PPDIOO methodology, which provided the steps of operation for the integration of new communication network between points. It began with the preparation and compilation of the information network infrastructure to carry it out properly planning on the part of the design sought to follow best practices to develop the network infrastructure for the integration of technology new. We started a test scenario in one of the branches with the intention of making the necessary measurements and adjustments for other outlets, which produced the necessary configuration that served as the basis for other communication devices. The results showed that there was a considerable reduction in spending on internet services monthly, because since only required to have a single service at points of sales , which increased stability and connectivity to the wired network but also in the WIFI wireless network for both internal staff and network cards. With regard to the management of the network a number of tools for managing it, which gives opportunity to apply web filtering policies, monitoring and access to certain users remotely was obtained. Finally, a range of options for the integration of new technologies, due to the new channel or media that meet the expectations of accessibility, connectivity and performance of the communication network is provided.

Keywords: Integration, Virtual Private Network, IPSec, PPDIOO

Capítulo I. Introducción

1.1. Antecedentes

Con el inicio de la revolución tecnológica en la década de los 60’s, surgió la necesidad de transportar la información de un lugar a otro en un menor tiempo a través de canales de comunicación que fueran efectivos para el flujo de los datos mediante el uso de las redes distribuidas. Una parte fundamental para el éxito de la comunicación global de la información fue el nacimiento de Internet, que aumentó considerablemente la interconexión entre los diferentes dispositivos electrónicos alrededor del mundo, debido a la alta velocidad en el tráfico de los datos que podía ser compartida y transmitida.

La importancia de tener una comunicación entre los distintos puntos en un lapso corto de tiempo y a su vez por un medio de transmisión seguro, da entrada a que las organizaciones a nivel mundial decidan integrar dentro de su red local dispositivos de comunicación, para poder así tener un flujo de la información de una manera ágil y aún costo menor.

Con el avance progresivo de la tecnología de Internet hubo un incremento en la comunicación pública, debido a que fue una forma práctica de cubrir grandes distancias de transmisión y con accesibilidad al medio. La comunicación en las redes públicas cumplía con el objetivo de mantener conectadas las distintas redes de computadoras por un mismo canal de transmisión que pudiera compartir información y distintos servicios propios de la red local. La comunicación en las redes privadas ofrece a las organizaciones un medio para transmitir la información debido a que podrán tener conectadas sus diferentes redes locales con un acceso al medio controlado para ciertos usuarios o dispositivos electrónicos.

En la actualidad las organizaciones son cada vez más dependientes de sus redes de información y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. Por lo cual requieren un medio de comunicación que sea confiable y seguro para el flujo de información propio de la organización.

La tecnología de redes privadas virtuales se considera muy interesante para cualquier organización que necesite incrementar la conectividad de sus redes locales y disminuir

los costos de servicios tanto en el mantenimiento como en la administración. Debido que la pueden encontrar en cualquier lugar y conectarse en los sitios con servicio de Internet para así lograr que los usuarios puedan estar conectados con mayor seguridad a la red de la organización y aprovechar los recursos internos que brinda para los usuarios finales.

La importancia de la tecnología de redes privadas virtuales en las organizaciones se ha convertido en una parte primordial para las organizaciones que cuentan con unidades en distintos lugares con grandes distancias de recorrido para la transmisión de la información. Por lo cual se apoyan en este tipo de tecnologías como un medio seguro del flujo de los datos, sin embargo, la clave principal que ofrece este tipo de tecnología es su capacidad de utilizar redes de comunicación públicas en lugar de manejar líneas privadas rentadas.

En el año de 1982 nace en la ciudad de Tijuana B.C. la Empresa Tecnicentro Royal, en el giro de servicio automotriz, fué la primera sucursal que ofreció servicios integrales para el área automotriz como son, los servicios de mantenimiento, diagnósticos, la venta y la reparación de las llantas, entre una infinidad de servicios dedicados a mantener el funcionamiento de los automóviles para los clientes particulares o de las empresas de la región.

Hoy en día, la empresa Tecnicentro Royal S.A. de C.V. cuenta con 29 puntos de venta, ubicadas en distintos puntos estratégicos para la adquisición del capital y de los recursos compartidos. Dichas sucursales se encuentran en los principales estados del norte del país como son el estado de Baja California, Baja California Sur, Sonora, Sinaloa y Nayarit.

El próspero crecimiento que ha tenido en las aperturas de las sucursales en los últimos años la ha convertido en una de las organizaciones empresariales referentes de su giro, brindándole la oportunidad de lograr el reconocimiento a nivel local, regional y nacional.

Debido al exitoso crecimiento empresarial que ha tenido desde su primera sucursal hasta el día de hoy, se ha visto en la necesidad de integrar los medios de comunicación que lo

apoye en la transmisión de la información que se genera en las distintas sucursales de la empresa. Asimismo, requiere que los sistemas tecnológicos los auxilien para realizar la comunicación con los diferentes puntos de generación de los datos a su unidad central, para así tener concentrada la información generada de las ventas, los servicios y los mantenimientos efectuados.

Por otra parte, en la actualidad existen distintos casos de éxito con implementaciones sobre la tecnología de redes virtuales privadas en las empresas, que requieren tener un medio de comunicación confiable y con una estabilidad en su conexión. En Marzo del 2006, fue presentado un caso práctico para una empresa comercializadora, titulado Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPSec, por Trujillo, E. donde se expone un estudio de la situación organizacional y tecnológica de la Empresa Comercializadora y la forma de implementar la tecnología VPN de manera exitosa (Trujillo, 2006).

Dicho trabajo, está estructurado en 5 capítulos para expresar la manera que definió la resolución y la muestra de los resultados. En el Capítulo I presenta una reseña teórica elemental de los conceptos relacionados con la tecnología de VPN, como es la introducción a las tecnologías de acceso a Internet y enlaces privados, diferentes tipos de conexiones de la actualidad y la tecnología WAN.

El Capítulo II comprende de la arquitectura tecnológica de la VPN, los túneles y la revisión de las funcionalidades aplicadas que ofrece el manejo del protocolo IPSec. En el Capítulo III se muestra un estudio de la situación de la organización y el área de tecnologías de la información.

El Capítulo IV se indica la implementación de un prototipo VPN, con los posibles escenarios en su integración, el cual se muestra en la Figura 1. De manera óptima para el tráfico de la información y comunicación. Finalmente en el Capítulo V, indica una amplia conclusión del tema y unas recomendaciones que se deben de tomar en cuenta al momento de implementar la tecnología de VPN.

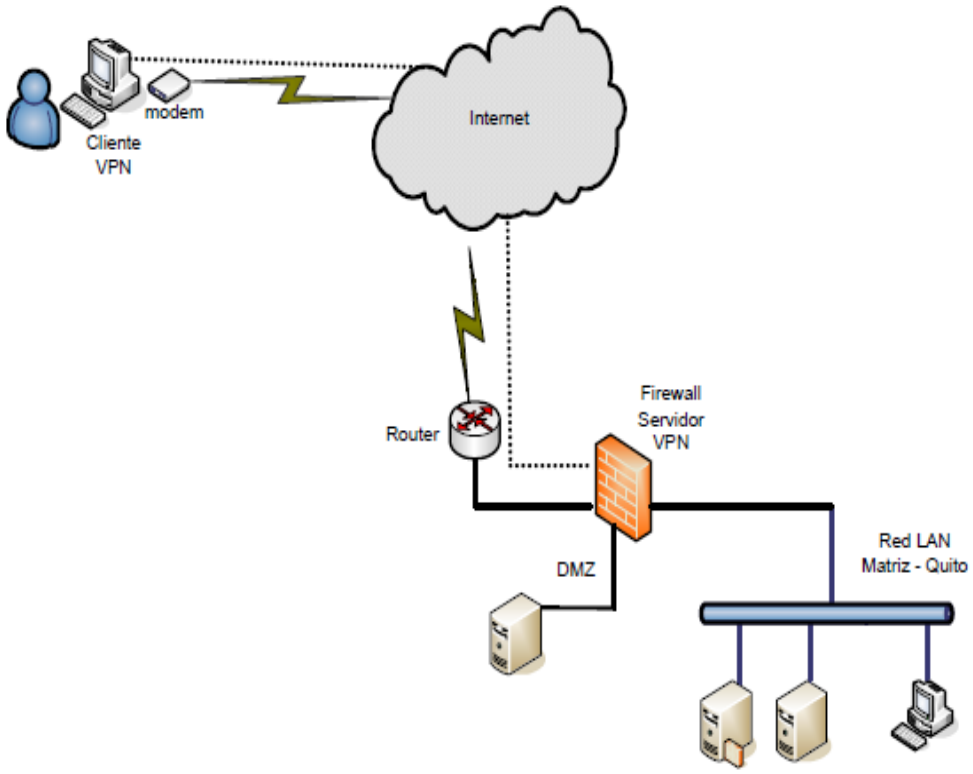


Figura 1. Escenario de acceso remoto del prototipo de VPN (Trujillo, 2006)

Aguado y Nivon (n.d.) Utiliza la tecnología de VPN como medio de transmisión para resolver los inconvenientes de conectividad entre los empleados móviles dentro y fuera de las instalaciones de televisión Metropolitana Canal 22.

El método propuesto para una configuración de VPN con nivel de capa 3 con acceso remoto y el protocolo IPsec para un óptimo transporte de los datos a través de un medio seguro, se ilustra en la Figura 2 de una manera general. La propuesta del esquema general de la red de VPN de acceso remoto para el canal 22 tiene un cifrado simétrico en la opción del protocoló AES para una mayor seguridad e incrementar el cifrado y descifrado de los datos (Aguado y Nivon, n.d.).

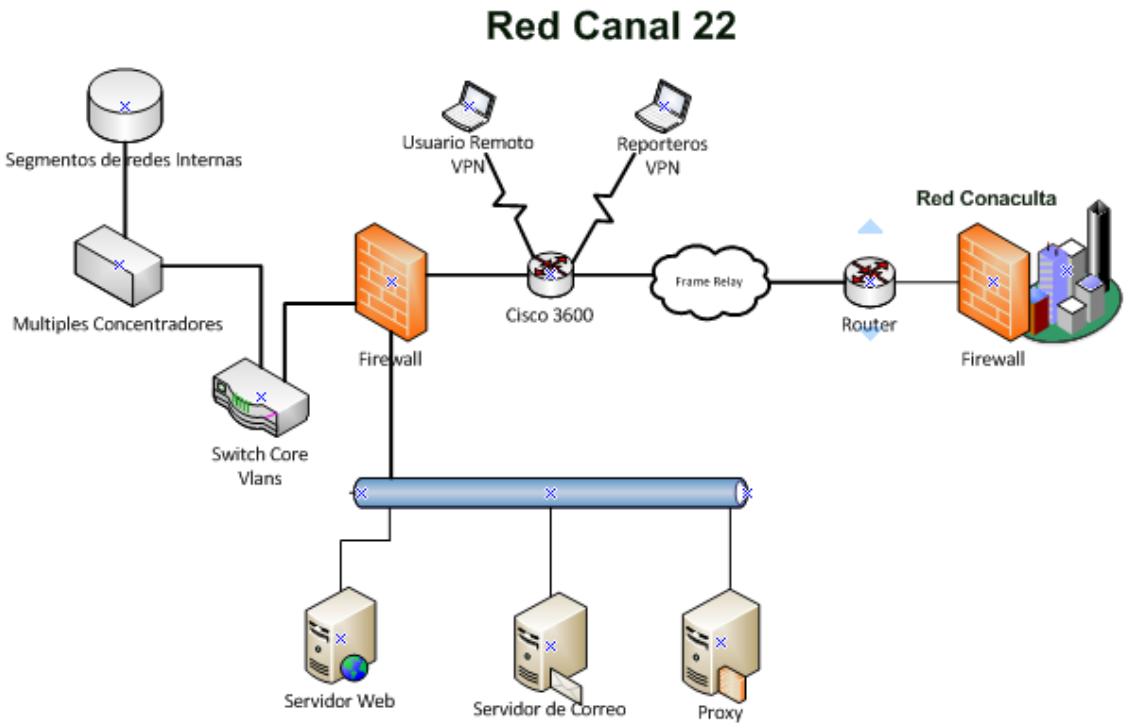


Figura 2. Red local de acceso remoto con la tecnología VPN. (Aguado y Nivon, n.d.).

La tecnología de VPN aporta una red altamente robusta debido a que permite implementar de manera segura y a un bajo costo para la empresa una red de comunicación escalable y ágil en la conectividad (Aguado y Nivon, n.d.).

1.2. Planteamiento del problema

La tecnología de la información de los últimos tiempos constituye una herramienta muy importante para el avance progresivo de cualquier empresa, debido a la gama de opciones que ofrece para la manipulación y la gestión de su propia información. Cada mejora tecnológica hace necesario para las empresas estar a la vanguardia con las últimas innovaciones que los apoyen en los procesos, los procedimientos y la productividad para una mejora continua.

A finales del año 2012, surge la necesidad en la empresa Tecnicentro Royal S.A. de C.V. de mejorar e integrar una nueva tecnología en sus instalaciones de red, debido al constante cambio tecnológico de los últimos tiempos, y aunado a la alta competitividad del mercado que da la pauta para integrar o no integrar una nueva tecnología en la infraestructura de la red de datos de la empresa.

Con el constante surgimiento y el alza de las nuevas sucursales o los puntos de venta en la empresa en los últimos años, es necesario mejorar la comunicación de la información en cada una de ellas, debido al incremento en el flujo de los datos que tiene que ir de un punto a otro para obtener la información referente de los productos y los servicios. Por lo cual, debido a ese crecimiento en la transmisión de los datos, se ha vuelto una comunicación inestable y poco confiable para los sistemas de información internos.

Cada uno de los inconvenientes que se presentan referente a la transferencia de la información se ve directamente reflejado en la productividad y en las mediciones internas que tiene cada sucursal, el cual provoca un impacto mayor al momento de hacer la evaluación y la revisión de la operatividad en cada uno de los ciclos y para la toma de decisiones de las personas encargadas.

A continuación se describen los problemas que refleja el tener una infraestructura de red que no cumpla con las expectativas ni el panorama actual de lo que requiere la empresa para la comunicación de su información. Tales inconvenientes son:

- Incremento en los costos de operatividad, debido a que tiene que aumentar el gasto al contratar personal externo para la revisión de las fallas en la red.

- Complejidad e inflexibilidad en la infraestructura de la red con respecto a la expansión.
- Retardo en la transmisión de la información operativa de las sucursales y el corporativo.
- Indirectamente se tiene una disminución en la productividad del personal de ventas, debido a que los sistemas fallan por no tener conectividad y a ellos se les ve reflejado en no contar con las listas de precios de los artículos y los servicios actualizados
- Poca movilidad para el personal interno con respecto a la conectividad de internet en las sucursales, debido a no contar con servicio de internet por causas del dispositivo o modem.

Dentro de las múltiples fallas que se puedan tener en la parte de la comunicación operativa de los datos de la empresa, existe la preocupación en el departamento de sistemas de la parte tecnológica y con respecto a los servicios técnicos, que tiene que garantizar en la infraestructura de red actual, entre los que se mencionan:

- Poca administración de la red ante fallos, mantenimiento y cambios.
- Constantes fallas en la redes inalámbricas del personal interno y los clientes, debido que los dispositivos que brindan el servicio de internet se traban o se desconfiguran con el pasar del tiempo
- Al momento de implementar un cambio en el sistema, se tiene que llevar a cabo en cada una de las computadoras de la empresa.
- Desconexiones continuas en la red en el momento que el personal de soporte técnico aplica la revisión de los folios para las estaciones remotas.
- Saturación en el tráfico de la red ante amenazas internas como externas.
- Incrementa el tiempo y el costo de las actividades del soporte técnico para la resolución de fallas.

1.3. Objetivo general

El presente caso práctico tiene como objetivo integrar un entorno de comunicación de datos por medio de una red virtual privada con IPSec para el flujo de la información entre las sucursales y el corporativo de la empresa Tecnicentro Royal S.A. de C.V.

1.3.1 Objetivos específicos

- Elaborar el diseño de la infraestructura de red de datos para el manejo de la información por medio del túnel de la red virtual privada.
- Estructurar la red de comunicación inalámbrica para el personal operativo de las sucursales y los clientes.
- Integrar un sistema de autenticación de usuarios para los equipos de comunicación que se conecten a la red operativa e inalámbrica por medio de clientes remotos VPN.
- Proporcionar movilidad al personal de la Empresa para el uso de los diferentes sistemas y servicios integrados.
- Reducir la cantidad de servicios DSL contratados en las sucursales.
- Mejorar la gestión de la red en el departamento de sistemas con diversas herramientas que apoyen al monitoreo de los servicios, para aplicar las políticas de usabilidad y actualizaciones de los sistemas.
- Homologar la segmentación de la red para las sucursales.

1.3. Justificación

Los constantes avances tecnológicos de la actualidad brindan a la empresa Tecnicentro Royal S.A. de C.V., la oportunidad de estar a la vanguardia con las innovaciones tecnológicas para sus procesos operativos y técnicos de la información. La misma globalización del mercado exige a dicha empresa el uso de la tecnología de punta para una óptima competitividad y crecimiento progresivo. Por lo cual, es de suma importancia la integración de un medio de comunicación tecnológico que apoye con la integridad y un ágil flujo en la transmisión de la información.

Por tal motivo, el integrar una nueva tecnología en la red que auxilie a mejorar la forma en la que se hace las comunicaciones en los diferentes puntos de la empresa, trae con ello beneficios y servicios para la gestión de la infraestructura de la red. Debido a que la misma demanda de mejorar día con día ha tenido como consecuencia un incremento en el tráfico de la información que se procesa.

El implementar un canal como medio de transmisión que cumpla con la demanda del tráfico de la información producido en la misma infraestructura de la red de la empresa, apoya a reducir considerablemente los múltiples inconvenientes presentados en la actualidad.

Los beneficios que aportará el mejoramiento de la red se citan en las siguientes características:

- Confiabilidad del medio de transmisión.
- Estabilidad de los servicios de comunicación.
- Conectividad administrable.
- Flexibilidad ante los cambios y las configuraciones de la red.
- Optimización de los recursos e integración de nuevos servicios.
- Reducción de gastos operativos técnico ante fallos de la red.
- Brindar movilidad controlada al personal operativo de la empresa.
- Agilizar el tráfico de la red interna.

Para el caso de la parte técnica, le incrementaría las herramientas al departamento de sistemas de la empresa, debido a la gama de opciones que le brinda el tener una infraestructura de red que conecte a los distintos sitios y que los auxilie a mejorar cada uno de los servicios que utilizan acceso a la red y requieren ser transmitidos en un tiempo corto.

Las aportaciones tecnológicas que brindará la tecnología de VPN al estar integrada a la red de la empresa son descritas en los siguientes puntos:

- Estabilidad en las redes operativas inalámbricas para el personal interno como a su vez para los clientes externos.
- Reducción de gastos en servicios de internet.
- Incrementa la administración de la infraestructura de la red.
- Disminuye el tiempo de conexión para los casos que requiera la conectividad a los equipos remotos para revisar algún folio en el área de soporte técnico.
- Integra un canal de comunicación para la integración de nuevos sistemas de la red para los diferentes departamentos de la empresa.
- Mejora la integración de nuevas actualizaciones de los sistemas internos en cuestión de la continuidad y accesibilidad al medio.
- Movilización al personal operativo y administrativo para que se pueda conectar fuera de la infraestructura de red de una manera controlada.

Capítulo II. Marco teórico

2.1. Introducción

Hoy en día, el gran interés que experimenta las nuevas tecnologías de comunicación para las empresas, han llevado a la necesidad de contar con diversos medios de comunicación que optimicen la forma de expresar los datos a través de un canal rápido y seguro en cualquier parte donde exista acceso a una conexión de datos. La comunicación entre los dispositivos electrónicos y las personas es un factor crítico para el éxito de una gran cantidad de procesos o referencias las actividades empresariales que se ejecutan en la actualidad (Tittel, 2004).

2.2. La importancia de Internet

Los orígenes de Internet se remontan como un proyecto de investigación en las redes de conmutación de los paquetes dentro de un ámbito militar, a finales de los años sesenta el departamento de la defensa de los Estados Unidos llegó a la conclusión de que su sistema de comunicaciones era demasiado vulnerable y estaba basado en la comunicación telefónica y por lo tanto en una tecnología denominada de conmutación de circuitos, que establece enlaces únicos y un número limitado entre importantes nodos o centrales (Stallings, 2005).

Como alternativa a través de su Agencia de Proyectos de Investigación Avanzados decidió estimular las redes de computadoras mediante las becas y el apoyo a los departamentos de informática de numerosas universidades y algunas empresas privadas. Esta investigación condujo a una red experimental de cuatro nodos que arrancó en Diciembre de 1969 y se denominó ARPA net (Stallings, 2005).

El objetivo principal por el cual empezó el proyecto era para poder contar con un sistema de comunicación estable y capaz de comunicar a los diferentes estados del país en el caso de que los sistemas telefónicos fallaran y se quedaran incomunicados (López y Novo, 2000).

ARPA desarrolló una nueva tecnología denominada conmutación de paquetes cuya principal característica reside en fragmentar la información, dividirla en porciones de una determinada longitud. Cada paquete lleva asociada una cabecera con datos

referentes al destino, origen, códigos de comprobación, etc. Así, el paquete contiene información suficiente para encaminarse hacia su destino en los distintos nodos que atraviese. El camino a seguir no está preestablecido de forma que si una parte de la red cae o es destruida, el flujo de paquetes será automáticamente encaminado por nodos alternativos. Los códigos de comprobación permiten conocer la pérdida o la corrupción de paquetes estableciéndose un mecanismo que permite la recuperación (Stallings, 2005).

Este sistema de transmisión reúne múltiples ventajas:

- Fiabilidad.
- Distribución.
- Encriptación.

Al igual que los equipos o las conexiones también se evolucionó en los servicios que ofrecía ARPANET, ya que si bien al principio sólo permitía ejecutar programas en modo remoto.

En 1972 se introdujo un sistema de correo electrónico que liberó a los usuarios de la dependencia de los husos horarios y supuso un sorprendente aumento en el tráfico generado, convirtiéndose en la actividad que mayor volumen generaba en contra de las previsiones iníciales.

Para que las computadoras pudieran comunicarse entre sí es necesario que todos ellos envíen y reciban la información de la misma manera. La descripción de los pasos a seguir se denomina "protocolo". Este protocolo proporcionaba un sistema independiente de intercambio de datos entre computadoras y redes locales de distinto origen (Gliger y Olifer, 2009).

Durante los años ochenta Internet creció hasta incluir el potencial informático de las universidades y centros de investigación, lo que unido a la posterior incorporación de empresas privadas, organismos públicos y asociaciones de todo el mundo, supuso un fuerte impulso para Internet que dejó de ser un proyecto con protección estatal para convertirse en la mayor red de computadoras del mundo, formada por más de cincuenta

mil redes, cuatro millones de sistemas y más de setenta millones de usuarios (Gliger y Olifer, 2009).

Se estima un crecimiento del censo de usuarios de Internet de aproximadamente un diez por ciento mensual, se deduce que para el año dos mil se superarían los trescientos millones de usuarios conectados a la 'Red de redes'. Internet no es simplemente una red de computadoras conectadas entre sí. Se trata de una asociación de miles de redes conectadas entre sí. Todo ello da lugar a la red de redes, en la que una computadora de una red puede intercambiar información con otro situado en una red remota.

Este espectacular crecimiento se debe a la notable mejora en la facilidad de uso de los servicios ofrecidos dado que aun manteniéndose los servicios originales de transferencia de archivos, correo electrónico o acceso remoto.

2.3. La tecnología en la red virtual privada

Que es una VPN?

La red privada virtual (VPN) es un medio de comunicación de datos privado que por lo general se integra sobre una red pública que habitualmente es Internet, encargándose interconectar dos subredes de manera remota mediante un túnel virtual por donde será transmitida de manera encapsulada los paquetes (Andrés, 2006).

La tecnología de red que aporta la VPN como la extensión de una red interna de una organización sobre una red LAN, aumenta la variedad de servicios a través del medio que puede ofrecer en sus diferentes unidades. En la Figura 3, se muestra una estructura general de comunicación con la tecnología de VPN en un entorno corporativo.

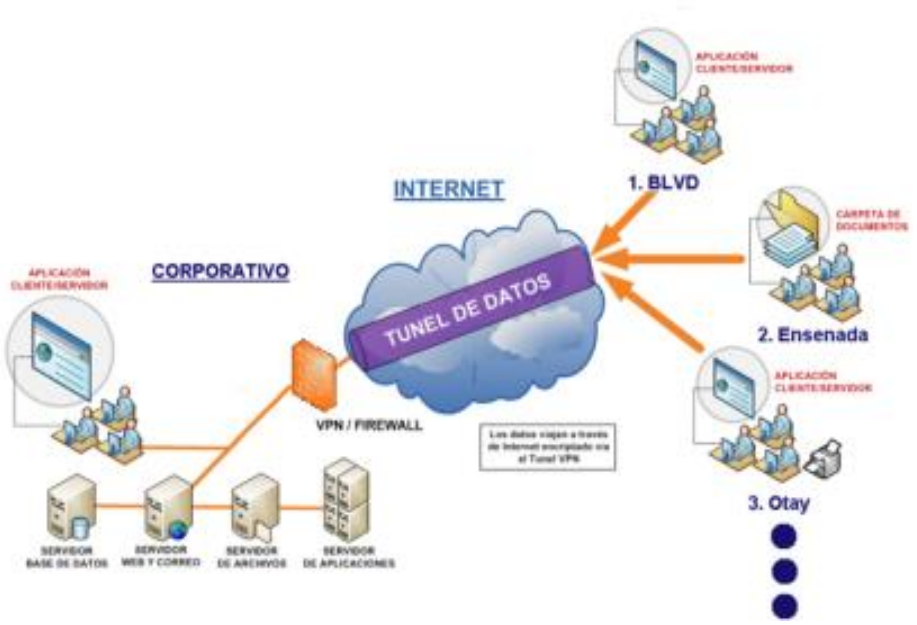


Figura 3. Esquema general de una VPN corporativa.

Los requerimientos de una VPN que ofrece en conjunto de los protocolos de comunicación y los servicios que establece el funcionamiento de los túneles o los medios de transmisión que en ocasiones puede cambiarse alguno.

- Autenticar usuarios, realiza una validación de la identidad del usuario que se va a conectar para poder restringir o dar acceso a la red. Donde solo podrán entrar los usuarios que cumplan con una autenticación correcta.

- Administrar las IPs, apoya a la asignación de una dirección IP al usuario autenticado en la red privada y que la dirección IP otorgada cumpla con los rangos establecidos previamente en la configuración.

- Encriptar los datos, transforma los datos que serán enviados por una red pública y que solo el destinatario pueda desencriptar la información.

- MultiProtocolo, que sea capaz de utilizar una variedad de protocolos compatibles en la red pública para el transporte de la información por el medio.

2.3.1. Tipos de VPN.

Existen dos formas en que se puede implementar la tecnología de redes privadas virtuales basada en un entorno por dispositivos o hardware y la otra por medio de sistemas de software. Donde cada una de ellas ofrece características y elementos propios, aunque el punto fundamental que se tiene que tener en cuenta es el protocolo que se implemente (Huidobro y Rolda, 2004).

Utilizar la VPN basada en dispositivos electrónicos dedicados que han sido específicamente diseñados con los parámetros ideales para un óptimo rendimiento, ya que los procesos están aplicados al funcionamiento de la red. En la Figura 4, se ejemplifica un esquema general de la conexión que utiliza como medio de conexión un dispositivo por hardware.

Este tipo de dispositivos por hardware por lo general son más seguros y fáciles de utilizar, entre los principales fabricantes que ofrecen una alternativa diversa se destacan los de Cisco, Juniper, Fortinet, CheckPoint, entre otros (Huidobro y Rolda, 2004).

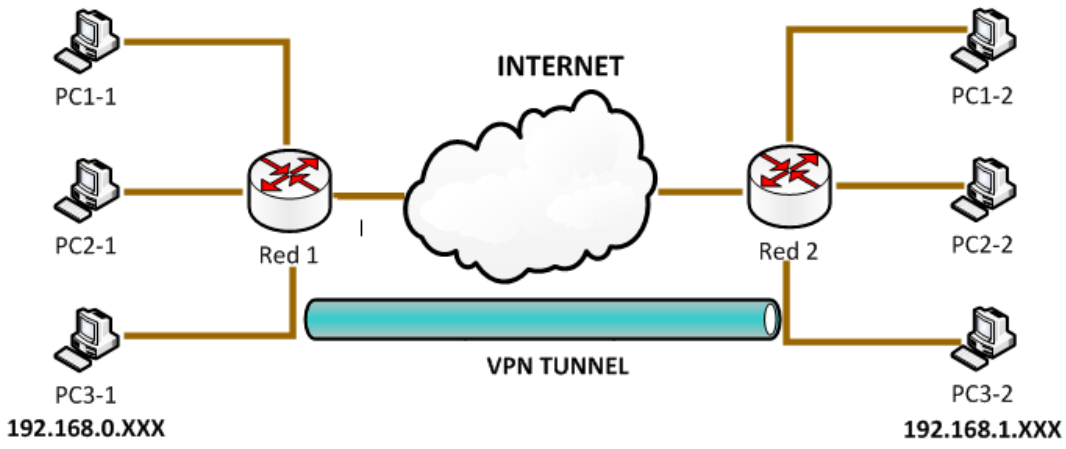


Figura 4. Esquema general de una VPN por hardware (Huidobro y Rolda, 2004).

Para el caso de la VPN que se basa en software, esta reúne una diversidad de aplicaciones que permite realizar la implementación de una red virtual privada y son independientes de la arquitectura o sistema operativo utilizado. En la Figura 5, se muestra una forma general de la utilización de la tecnología de VPN basada en

software. En la actualidad existen diversas herramientas de software que son catalogadas como libre distribución y otras que son de fabricante.

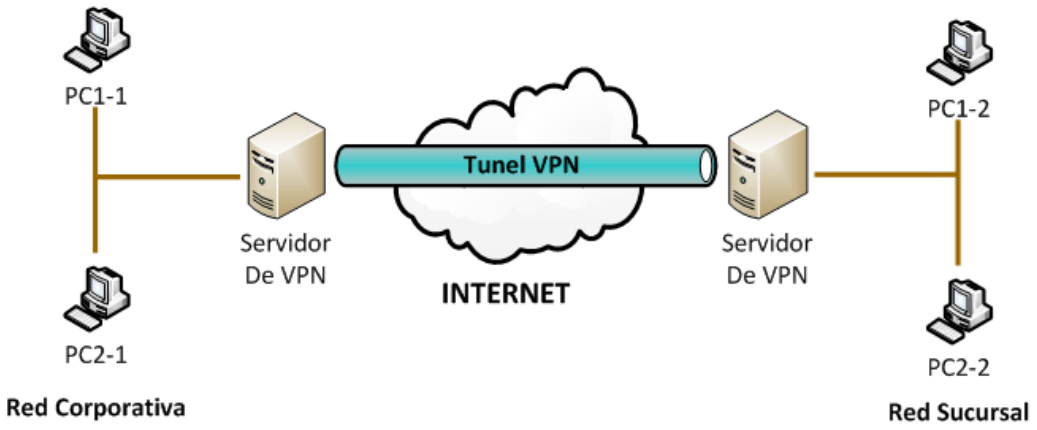


Figura 5. Esquema general de una VPN por software.

Existen diferentes tipos tecnologías que se puede implementar en una VPN, de los cuales podemos destacar:

- IPsec: Internet Protocol Security Tunnel Mode
- PPTP: Point to Point Tunneling Protocol
- L2TP: Layer To Tunneling Protocol

El establecimiento de un canal de comunicación privado sobre una infraestructura de acceso público brinda la seguridad y la confidencialidad en la información que se trasmite a través del medio, sin que sea alterada por personas no autorizadas. Otro beneficio posible es poder controlar el ancho de banda de los accesos al medio y poder incrementar el número de usuarios conectados sin implicaciones dentro de la infraestructura establecida (Forouzan, 2002).

2.4. Modelo de referencia OSI

A principios de los años 80 los fabricantes informáticos más importantes del momento se reúnen para unificar diferencias y recopilar la mayor información posible acerca de cómo poder integrar sus productos hasta el momento compatible entre si y exclusivos

para cada uno de ellos. Como resultado de este acuerdo surge el modelo de referencia OSI, que sigue los parámetros de hardware y software donde logra la integración multi-fabricante (Tittel, 2004).

- En el año 2009 Ariganello, E., indica una forma de cómo opera los dispositivos en una red. En la cual se hace referencia para crear e implementar estándares de red, dispositivos y esquemas de internet.

El modelo OSI divide a la red en diferentes capas con el propósito de que cada desarrollador trabaje específicamente en su campo sin tener necesidad de depender de otras áreas. En la Figura 6, se muestra el conjunto de capas en la que se clasifica el modelo OSI (Tittel, 2004).

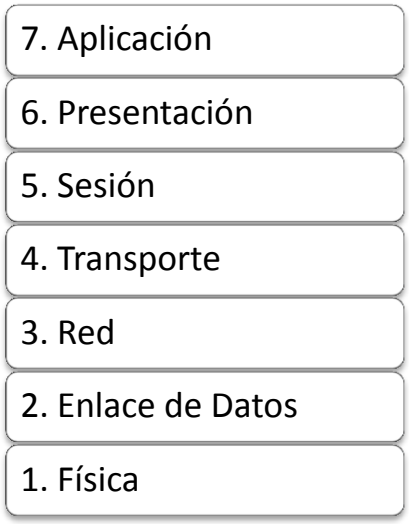


Figura 6. Capas (Tittel, 2004).

Cada una de estas capas presta servicio a la capa inmediatamente superior, el cual la capa de aplicación es la única que no lo hace ya que al ser la última capa su servicio está directamente relacionado con el usuario (Stalling, 2000).

2.4.1. Descripción de las siete capas

Capa 1: Física

Es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es unidireccional o bidireccional.

Capa 2: Enlace de datos.

Puede decirse que esta capa traslada los mensajes hacia/desde la capa física a la capa de red. Esta capa define como son los cuadros (Frames), las direcciones y las sumas de control (Checksum) de los paquetes Ethernet.

Capa 3: Red.

Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada (Routing), tarea esta que puede ser complicada en redes grandes como Internet, pero no se ocupa para nada de los errores o pérdidas de paquetes. Para Schawartz, (1994), define la estructura de direcciones y rutas de Internet. A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta.

Capa 4: Transporte.

Esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y la naturaleza del envío de los datos como indica Tanenbaum, (1997). Esta capa define como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos, los numera correlativamente y los entrega a la capa de red para su envío.

Durante la recepción es responsable de reordenar los paquetes recibidos fuera de secuencia y también puede funcionar en sentido inverso multiplexado una conexión de

transporte entre diversas conexiones de datos. Este permite que los datos provenientes de diversas aplicaciones compartan el mismo flujo hacia la capa de red.

Capa 5: Sesión.

Es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, aunque en realidad son pocas las aplicaciones que hacen uso de ella.

Capa 6: Presentación.

Esta capa se ocupa de los aspectos semánticos de la comunicación donde se establece los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. P.E. describe como pueden transferirse números de coma flotante entre equipos que utilizan distintos formatos matemáticos. Para Schawartz, (1994), ésta capa es buena candidata para implementar aplicaciones de criptografía.

Capa 7: Aplicación.

Esta capa describe como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotas, transferencia de archivos, etc.).

2.5. Tipos de redes

- **Red pública**: Se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

- **Red privada**: Una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

- **Red de área personal:** Es una red de computadoras usadas para la comunicación entre los dispositivos de la computadora cerca de una persona.

Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros.

Las PAN se pueden utilizar para la comunicación entre los dispositivos personales o para conectar con una red de alto nivel y el Internet.

- **Red de área local**: una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización. Para los propósitos administrativos, las redes locales de nivel grande se divide generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroups es un grupo de las computadoras que comparten un sistema común de recursos dentro de un LAN.

- **Red del área del campus**: Se deriva a una red que conecta dos o más LAN los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

- **Red de área metropolitana**: Consiste en conectar redes locales entre sí a alta velocidad, como si fuera la misma red.

- **Red de área amplia**: Es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono.
  Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

Los túneles de VPN, son los canales de comunicación a través del cual fluye la información de manera cifrada, sin que cualquier otro elemento ajeno al origen y destino de la conexión pueda interpretar los datos que viajan a través de él (Ford y Kim, 1998).

2.6. Modelos de redes privadas virtuales.

Existen diferentes escenarios en donde se puede implementar la tecnología de redes privadas virtuales dependerá de la situación y características de la red. Cada una de las situaciones estará puesto en el tipo de red que sea necesario conectar en de forma punto a punto, dos o más oficinas remotas entre sí o varios clientes contra una única oficina remota.

2.6.1. Punto a punto

Este tipo de conexión se representa mediante dos usuarios remotos van a establecer un túnel a través de una red insegura. Ya que está establecida la comunicación de los datos, inicia el intercambio entre ellos de forma cifrada y segura donde el destinatario será el único que podrá decodificar la información. En la Figura 7, puede observarse una conexión de punto a punto.

En este escenario se puede establecer un canal de comunicación seguro con otra persona que se encuentre en cualquier parte con el objetivo de poder enviarle o recibir la información de forma confidencial.

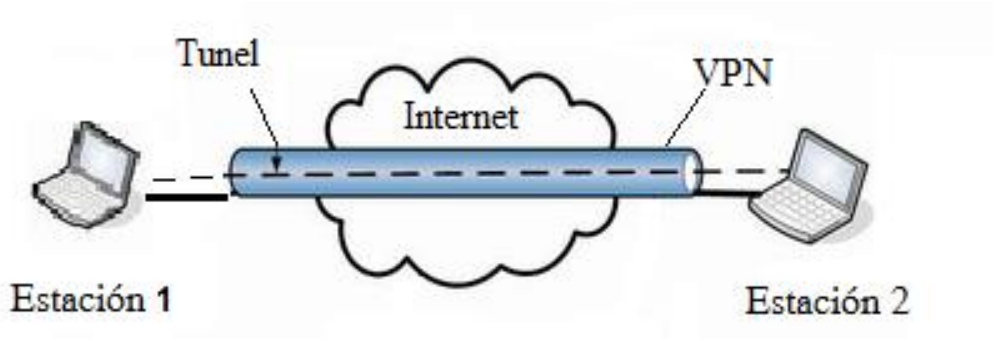


Figura 7. Diagrama de una VPN de punto a punto.

2.6.2. LAN a LAN

En una VPN LAN a LAN, dos redes remotas van a establecer un medio de comunicación a través de una red insegura, una vez establecido el canal privado, los datos son transmitidos entre ambos gateways viajaran cifrados mediante el túnel. En la Figura 8, se ha establecido un túnel VPN entre la red remota 1 y la red remota 2, el cual maneja Internet como vínculo de acceso.

Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local donde se comparte el recurso o servicios propios de la red conectada.

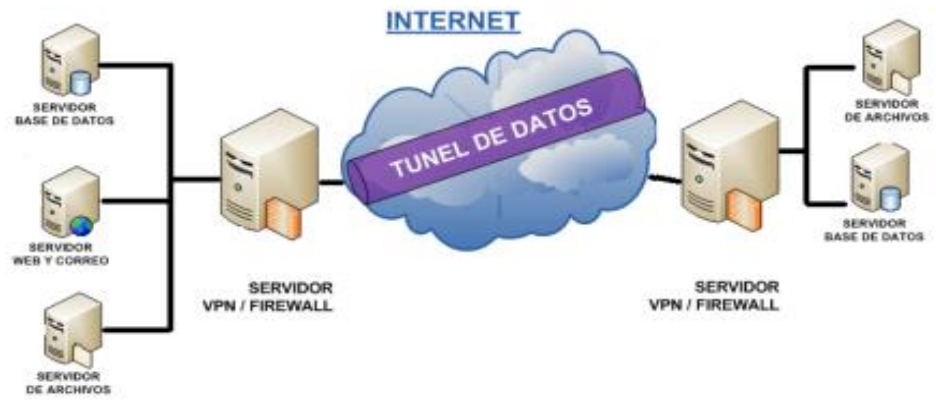


Figura 8. Esquema de una VPN de LAN a LAN (Araya, Carvajal y Llico, n.d.).

Con el acceso remoto VPN se puede dar disponibilidad de varias sedes en distintos lugares geográficos, el cual la información viajara encriptado exclusivamente entre dos puntos finales y de esta forma cifrar y enviar a través del túnel al destinatario la información (Araya, Carvajal y Llico, n.d.).

2.6.3. LAN a Road Warrior

En este tipo de escenarios de comunicación, uno o más usuarios remotos van a establecer un enlace virtual contra una Gateway con el objetivo de acceder a los recursos situados detrás de este. En la Figura 9, puede observarse que dos usuarios

remotos han establecido en túneles VPN contra la red remota de forma de enviar y recibir los datos de forma privada a través de la red insegura (Alonso, 2006).

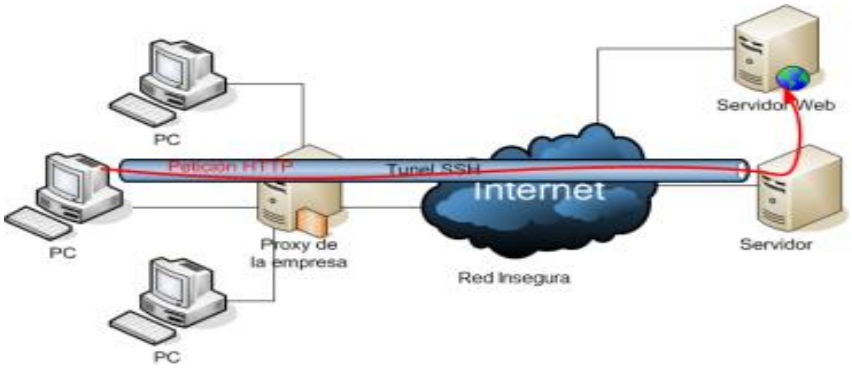


Figura 9. VPN LAN a Road Warrior (Alonso, 2006).

2.6.4. VPN interna

Este tipo de esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo acceso remoto y utiliza Internet como medio de conexión, donde emplea la misma red LAN para aislar las zonas y servicios de la red interna. En la Figura 10, se presenta un esquema general para ejemplifica una VPN Interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (Alonso, 2006).

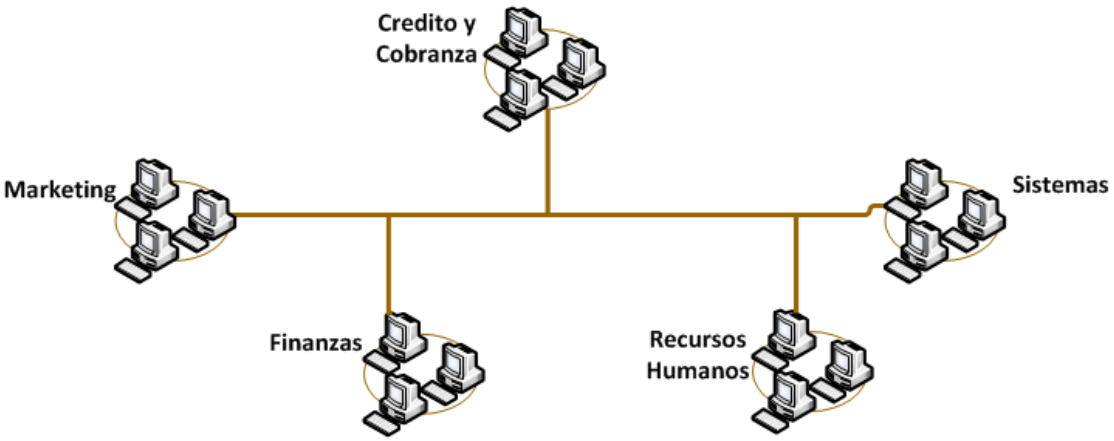


Figura 10. Escenario de una VPN interna (Alonso, 2006).

Es de suma importancia cuidar la seguridad al manejar escenarios de VPN Interna debido que la mayoría de los inconvenientes está relacionada con intrusos dentro de la red de la Empresa. Una VPN entre departamentos puede ayudar a encontrar esos requerimientos de confidencialidad (Alonso, 2006).

2.7. Técnica de tunelización

La tunelización elabora un medio de comunicación dentro del canal que se maneja en una red de datos con la tecnología de VPN para establecer una conexión privada que atraviese de un punto a otro. Aunque, no proporciona un mecanismo dentro del canal de comunicación para mantener fuera el tráfico de red no deseado, para este caso lo que se realiza es cifrar antes todo el paquete que sale en un extremo de la red VPN. El extremo receptor descifra la parte cifrada del paquete y reenvía éste hacia la red conectada a la VPN donde las únicas dos direcciones conocidas de los paquetes son las direcciones de los extremos del túnel VPN (Tittle, 2004).

Es una técnica que usa una infraestructura entre diferentes redes de comunicación para la transferencia de los datos entre una red a otra. La información se puede transportar como tramas de otro protocolo y encapsulación de las tramas con una cabecera adicional en vez de enviarla como en la parte inicial. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dicho paquetes.

Las tecnologías de tunelización son:

- IPSec
- PPTP
- L2TP
- MPLS
- ATMP
- IPX

Entre los más utilizados en la actualidad está el IPSec, PPTP, MPLS, entre otros.

2.8. Protocolo IPSec

IPSec es un acrónimo de IP Security y se trata de un protocolo cuyo objetivo es proporcionar seguridad y autentificación para las comunicaciones que utilicen el protocolo IP. Es un protocolo de seguridad a nivel de red que se sitúa entre IP y los protocolos de transporte. De esta manera proporciona seguridad a la capa de transporte y de aplicación según el modelo de referencia TCP/IP. Si tomamos el modelo de referencia OSI, IPSec proporcionaría seguridad desde el nivel 3 o nivel 4.

IPSec es un conjunto de estándares del IETF para incorporar servicios de seguridad en IP y que responde a la necesidad creciente de garantizar un nivel de seguridad imprescindible para las comunicaciones entre empresas y comercio electrónico (López y Novo, 2000).

2.8.1. El origen del protocolo IPSec

Los orígenes de este protocolo se remontan al año 1994, en la Comisión de Arquitectura de Internet realizaron un informe que llevaba por título "La seguridad en la arquitectura de Internet". Según dicho informe la opinión generalizada sobre Internet era que carecía de mecanismos para una mayor seguridad. Se identificaron diversas áreas para implementar dichos mecanismos, como la intrusión no autorizada, control de tráfico de red y formas para cifrar y autentificar una comunicación entre dos máquinas cualesquiera dentro de la red.

Estas preocupaciones se vieron confirmadas en otro informe más tardío, de 1998, del Equipo Informático de Emergencia y Respuesta en el que figuraba una extensa lista de incidentes relacionados con la seguridad de Internet.

Los ataques más serios eran los relacionados con la técnica de suplantación de IP, aunque también se incluían diferentes formas de intrusión y espionaje del tráfico de paquetes, mediante las cuales los atacantes leían información concerniente a identificación y contraseña dentro de un sistema, bases de datos y otra información de tipo confidencial.

Fue por estas razones por las cuales la IAB incluyó cifrado y autentificación como características estrictamente necesarias en la nueva versión del protocolo IP (IPv6). Sin embargo se diseñaron de forma que pudieran ser usadas en versiones previas del protocolo IP como el muy extendido IPv4 (Tanenbaum, 1997).

2.8.2. Servicios de IPSec

IPSec proporciona tres servicios:

- Una función únicamente de autentificación denominada Authentication Header (AH), es decir, cabecera de autentificación,

- Una función de autentificación y/o cifrado llamada Encapsulating Security Payload (ESP) que equivale a carga encapsulada de forma segura y por última.

- Una función de intercambio de claves en un principio contemplada por el protocolo ISAKMP/Oakley, pero que finalmente fue integrado en el protocolo IKE.

En una VPN tanto el cifrado como la autentificación son deseables ya que es importante asegurar:

- Qué usuarios no autorizados se introduzcan en la red.

- Qué terceras partes que practiquen la escucha o espionaje de comunicaciones en la red pública IP puedan leer mensajes enviados por la VPN.

En concreto, AH facilita integridad sin conexión, autentificación propiamente dicha y un servicio opcional para evitar el reenvío de paquetes. ESP puede proporcionar confidencialidad (cifrado) y ocultación limitada del flujo de tráfico así como los servicios ya mencionados de AH. El ESP es invocado, es obligatorio que al menos uno de los dos servicios sea utilizado.

Estos dos protocolos pueden ser usados independientemente o de forma combinada. Las diferentes combinaciones se utilizan para aumentar el nivel de seguridad de IPSec. Por ejemplo, ESP puede proporcionar los dos servicios, en cambio, AH tan sólo puede facilitar uno de ellos, pero se diferencia de ESP en que, al autentificar puede también ocultar determinados campos de la cabecera de un paquete IP. Aunque en general se utiliza ESP, una combinación de ESP para cifrado y AH para autentificación proporciona un grado adicional de seguridad.

2.8.3. Modo transporte

En modo transporte, sólo la carga útil del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; Sin embargo se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera.

2.8.4. Modo Túnel

Los paquetes IP son cifrados y autenticados debido que deben ser encapsulados en un nuevo paquete IP para que funcione el enrutamiento. El propósito de este modo es establecer una comunicación segura entre dos redes remotas sobre un canal inseguro.

2.8.5. Protocolo AH

El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Esto es, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros (Raya, 1997).

Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser

un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo. AH es realmente un protocolo IP nuevo, y como tal el IANA le ha asignado el número decimal 51. Esto significa que el campo Protocolo de la cabecera IP contiene el valor 51, en lugar de los valores 6 o 17 que se asocian a TCP y UDP respectivamente. Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, flags, offset y checksum (ST-Pierre & Stephano, 2005).

La porción de IPSec encargada de la gestión de claves incluye la elección y distribución de claves secretas para cifrado simétrico. La arquitectura IPSec obliga a que cualquier producto IPSec soporte dos tipos de administración de claves:

Manual: el administrador de una red dada configura manualmente cada sistema con sus propias claves para que coincidan entre sí. Es práctico para entornos pequeños y relativamente estáticos.

Automático: un sistema automático permite la creación de claves para SAs en base a una petición y da servicio al uso de claves en grandes sistemas distribuidos con una configuración en permanente cambio.

El protocolo por defecto definido para la distribución de claves en IPSec fue el conocido como ISAKMP/Oakley, que hace referencia a los dos módulos que permiten el intercambio de claves y ambos se integran en un esquema más general IKE.

Protocolo de determinación de claves Oakley**:** Oakley es un protocolo de intercambio de claves basado en el algoritmo Di-e-Hellman, pero con ciertas medidas adicionales de seguridad. En particular el algoritmo Di-e-Hellman por sí solo no autentifica a dos usuarios que intercambien claves, por lo que el protocolo es vulnerable a ataques de suplantación. Oakley incluye mecanismos para evitar este problema.

ISAKMP especifica un marco para el intercambio de claves en Internet junto con los protocolos capaces de negociar atributos de seguridad.

ISAKMP por sí mismo no dicta el uso de un algoritmo de intercambio de claves; en lugar de ello, ISAKMP consiste de un conjunto de tipos de mensajes que permiten el uso de una serie de algoritmos. Oakley es el algoritmo de intercambio de claves en concreto que apareció con la versión inicial de ISAKMP (Raya, 1997).

2.9. Redes inalámbricas.

La transmisión inalámbrica se ha convertido en un medio de comunicación muy popular años, debido a las características y las ventajas que ofrece a los usuarios para una conexión de datos a un entorno de red y a la libertad de movilidad de la misma conexión (Garcia, 2008).

Los principales factores que maneja una transmisión inalámbrica son los siguientes:

- Alta disponibilidad.
- Escalabilidad.
- Manejabilidad.
- Seguridad.
- Bajo costo de operación.
- Ventajas de instalación.
- Fiabilidad en entornos complejos.

El funcionamiento de una red inalámbrica es muy parecido a lo que se maneja en las redes alámbricas o en la redes de área local tradicionales donde en lugar de utilizar un cableado par trenzado o fibra óptica, utiliza la luz infrarroja o la radiofrecuencia para tener un mayor alcance y una cobertura más amplia en su transmisión.

Las redes inalámbricas tienen muchas ventajas para entornos pequeños, medianos o de gran escala debido a los beneficios y las características que ofrece tanto en la conectividad y la transparencia de la comunicación. Aunque una red inalámbrica no elimina la necesidad de los proveedores de servicios de Internet del todo, debido a que en muchos de los casos se requiere conectividad con el exterior para mantener comunicación en distintos puntos y el utilizar redes inalámbricas en un entorno empresarial o domestico es mucho más económico que utilizar ancho de banda WAN o

cualquier otra servicio de conexión por medio de fibra óptica y radio frecuencia (Carballar, 2004).

En la actualidad existen organizaciones especializadas que rigen la maneja de utilizar y manejar las redes inalámbricas basados en normas y estándares que detallan el funcionamiento de la tecnología inalámbrica.

La estandarización inalámbrica ofrece los siguientes beneficios:

- Interoperabilidad.
- Conectividad
- Operatividad.

El instituto de ingeniería eléctrica y electrónica abreviado como IEEE es una asociación mundial de ingenieros que elaboran las guías técnicas para el correcto uso de dicha tecnología. La mayoría de los estándares oficiales están financiados por el gobierno y la industria lo que incrementa la cooperación y la implementación a nivel internacional (Roldán, 2004).

La norma IEEE 802.11 establece el estándar para las redes inalámbricas y se refiere a una familia de protocolos de comunicación, dentro de los protocolos más utilizados actualmente se destacan los siguientes:

- 802.11a: 5 GHz, 54 Mbps.
- 802.11b: 2.4 GHz, 11 Mbps.
- 802.11d: dominios normativos múltiples.
- 802.11e: calidad de servicio.
- 802.11f: protocolo de interpunto de acceso.
- 802.11g: 2.4 GHz, 54 Mbps.
- 802.11h: selección dinámica de frecuencia.
- 802.11i: seguridad.
- 802.11j: canales de 5 GHz.
- 802.11k: medición.
- 802.11m: mantenimiento.
- 802.11n: alta velocidad.

El 802.11 es un estándar inalámbrico que especifica la conectividad de los dispositivos de comunicación dentro de un área local y define el uso de las dos capas inferiores del modelo OSI (Cabezas y Gonzalez, 2010).

La alianza Wi-Fi es una asociación internacional sin fines de lucro encargada de certificar la interoperabilidad entre los productos de las redes inalámbricas basados en las especificaciones del IEEE802.11. El logotipo Wi-Fi CERTIFIED indica que el equipo ha cumplido con rigurosas pruebas de interoperabilidad para asegurar que los distintos proveedores operen de manera adecuada (Ariganello, 2009).

Capítulo III. Metodología

3. Metodología

En esta etapa del caso práctico y con respecto a la manera en que se llevará a cabo una solución tecnológica para la empresa Tecnicentro Royal S.A. de C.V., se toma como base fundamental los procesos que ofrece la metodología PPDIOO de Cisco para guiar y definir el camino por el cual se integra una mejora en la tecnología de la red.

Cabe señalar que estará establecido por 6 etapas descritas en la Figura 11, que apoyará a determinar los procesos en la integración de una solución tecnológica.

Figura 11. Etapas de la metodología PPDIOO

Cada una de las etapas del proceso de integración del proyecto representa una parte importante para el éxito del mismo, debido que determina las actividades mínimas requeridas por la tecnología y la complejidad que tendrá la red.

3.1. Preparación

En la presente etapa se aplicará distintas técnicas y herramientas para la recolección de la información necesaria para comprender el funcionamiento actual de la red de comunicación de la empresa, como también de los procesos y las actividades que se llevarán a cabo en las diferentes sucursales o unidades de negocio de la empresa.

Con el motivo de alcanzar exitosamente la recolección de la información, se aplicará varias técnicas y herramientas de recopilación de información descritas en la Figura 12, que apoya a obtener los datos de manera más rápida y precisa.

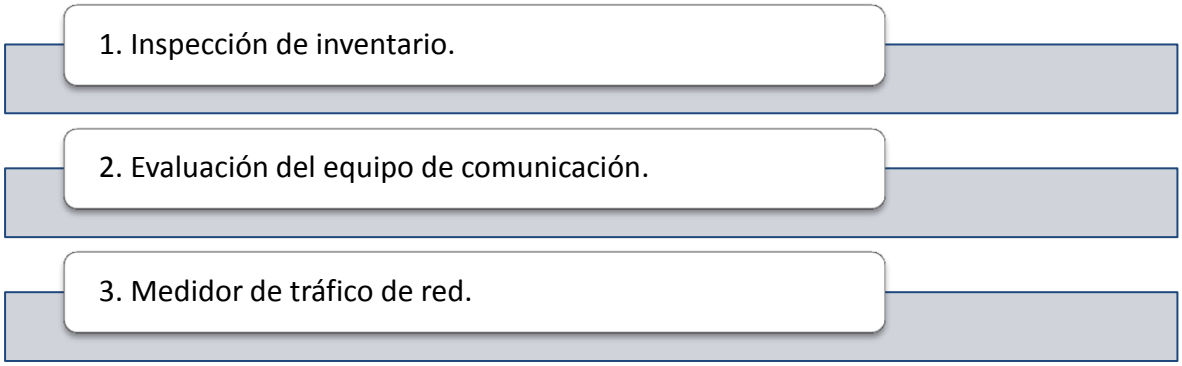


Figura 12. Técnicas y herramientas de recopilación de información

Cada uno de estas herramientas aporta información valiosa y conocimiento sustentable sobre la situación que vive la organización con respecto a su infraestructura de red.

Una parte que es vital para conocer con precisión, es el aplicar correctamente los medidores de tráfico de red en el corporativo como unidad central de información y en cada una de las sucursales pertenecientes a la empresa. Con el fin de saber que tráfico es transmitido en la red de comunicación actual y localizar puntos por mejorar en la infraestructura de red.

Con la finalidad de establecer las dimensiones correspondientes a los equipos de comunicación con los que dispone la empresa, será necesario realizar una actualización a los diversos equipos de cómputo y dispositivos electrónicos que requiera estar conectado a la red.

3.2. Planeación

Después de conocer los datos de red de la empresa, esta etapa apoyará a determinar las necesidades de la infraestructura de red y poder determinar una forma de acción para solucionar dicha problemática. Donde se podrá ejemplificar de manera clara los puntos vulnerables de la conexión y elaborar información estadística para el sustento de la solución a integrar en la infraestructura de red.

Cada uno de los datos será analizado para determinar si la implementación de la solución propuesta es adecuada para la resolución de los inconvenientes actuales en la conexión de red de la empresa. Cabe indicar que las mediciones de tráfico mostrará un panorama específico del tráfico de información que se maneja en cada una de las sucursales.

3.3. Diseño

En esta fase se inicia la preparación del esquema de red a seguir durante la implementación de la solución, donde se especifica la manera de la conexión ideal para la integración de la infraestructura de red. La base del conocimiento parte de las especificaciones de la red que anteriormente fueron recopiladas para identificar el modelo de red que sea idóneo en la empresa.

Luego se elabora el esquema de red idóneo, también esta etapa se encargará de realizar la adquisición y el seguimiento de los dispositivos que se utilizaran para la conexión de la red virtual privada en la unidad corporativa y las diferentes sucursales.

3.4. Implementación

Durante esta fase se configura el dispositivo central de la información en la unidad corporativa de la empresa, donde se integrará como referencia el diseño de la infraestructura de red elaborado anteriormente para una conexión de VPN exitosa. Cabe indicar, que después de tener lista la configuración de la unidad central se inicia la instalación de cada dispositivo en cada una de las sucursales.

3.5. Operación

Durante esta etapa se llevará a cabo la verificación de la implementación en cada una de las sucursales y en la unidad del corporativo, donde se realiza mediciones que indique que la comunicación de la información entre dispositivos es la correcta. Cada una de las pruebas de conectividad entre los diferentes dispositivos se llevará acabado en base a los requisitos de red para la validación de la información.

3.6. Optimización

En esta última etapa se envuelve una administración proactiva donde se idéntica y resuelve las cuestiones que afecten a la red, el cual se puede crear algunas modificaciones al diseño de la red en caso de ser necesario, para mejorar el desempeño y la estabilidad de la red. La verificación adecuada en esta etapa, resuelve una gran variedad de situaciones que pueden presentarse una vez integrada la nueva red a su entorno.

Capítulo IV. Desarrollo

4. Desarrollo

Debido a la gama de posibilidades que en la actualidad se tiene para generar información representativa de la estructura de comunicación de datos en la red, es importante partir por reconocer el panorama actual y la influencia de los datos dentro de la infraestructura de red.

Por lo cual se parte como primera etapa en la preparación con la recopilación de la información necesaria con respecto a dispositivos conectados en la red y además cada dato vital en el proceso del reconocimiento de la red.

Por lo cual se divide en 3 procesos, como son:

- Inventario de los dispositivos electrónicos que actualmente están conectados.
- Selección y evaluación de los equipos de comunicación con apoyo del proveedor de tecnología de información.
- Integrar un medidor del tráfico de datos de la red que apoyo a identificar el flujo de información.

El proceso de inventario de los equipos de cómputo al momento es parte importante para conocer el panorama actual del estado de la red y la carga en cuestión de los dispositivos que requieren servicio de red, ya sea para uso de la red interna en las diferentes unidades de negocio, como en la unidad central de información.

La recolección de la información en la parte de inventario está divida en dos categorías de las cuales son:

- Equipos de comunicación de internet (Módems).
- Dispositivos de comunicación:

    - Laptop
    - PC de escritorio.
    - Dispositivos Móviles.
    - Impresoras y Scanner.

Cada una de las categorías de los dispositivos a inventariar, son clave para definir la capacidad de los equipos de comunicación que se pondrán en cada sucursal, debido al tamaño que se maneje en cantidad de equipos conectados en la red local y las personas que cuenten con acceso vía remota a los diferentes servicios y procesos propios de la operación diaria.

En la Tabla 1. Se muestra la cantidad de equipos de comunicación que da servicio de internet para la red operativa y la de visita.

Tabla 1. Inventario de módem operativos y visita.

Equipos Operativos	Equipos para Visitas	Total
29	25	52

La representación porcentual de lo que abarca la cantidad total de equipos que ofrecen el servicio de internet en las sucursales de la empresa, esta ejemplificada en la Figura 13, que indica el valor en porcentaje de los equipos.

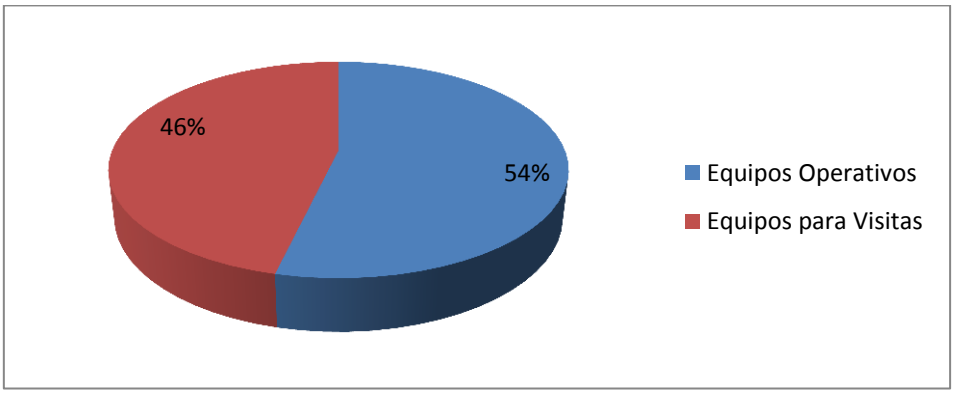


Figura 13. Cantidad de equipos de comunicación de Internet

La cantidad de inventario de los dispositivos que brinda el servicio de internet de la estructura de comunicación con la que cuenta actualmente la empresa está divida en dos grupos según la función o el área a la que va dirigida.

La recolección de información para el inventario de los dispositivos de comunicación está representada con las características de los equipos de cómputo, como también de los diferentes dispositivos. La Tabla 2 Inventario de la tienda de Obregón, representa la estructura de los datos obtenidos de los diversos dispositivos electrónicos.

Tabla 2. Inventario de la sucursal de Obregón.

No.	Sucursal	Perfil	Tipo
1	Tersa Obregón	Contabilidad	Escritorio
2	Tersa Obregón	Contabilidad	Portátil
3	Tersa Obregón	Ventas	Escritorio
4	Tersa Obregón	Ventas	Escritorio
5	Tersa Obregón	Gerente	Escritorio

Para la Tabla 3. Inventario general de equipos de comunicación, representa las cantidades de equipo con el que cuenta el grupo.

Tabla 3. Inventario general de equipos de comunicación.

Laptop	PC Escritorio	Impresoras	Otros (IPAD, Celulares)
122	153	95	50
		Total:	**420**

4.1. Herramientas de monitoreo de la red

Para obtener información correspondiente al tráfico de la red y a sus distintos equipos de transmisión y comunicación que la componen, se utiliza diferentes medidores de la red en distintos puntos de la infraestructura. Actualmente, cada uno de los puntos es totalmente independiente por lo cual cada sitio remoto genera su propia problemática que serán analizados para determinar el factor que influye en el deterioró de los servicios de comunicación.

La configuración con la que se parte en cada equipo de cómputo se lleva mediante el sistema por aplicación llamada Logmein, el cual registra cada uno de los dispositivos con el usuario y contraseña de acceso al mismo. En la Figura 14, se ejemplifica la plataforma vía web correspondiente a la página del Logmein.

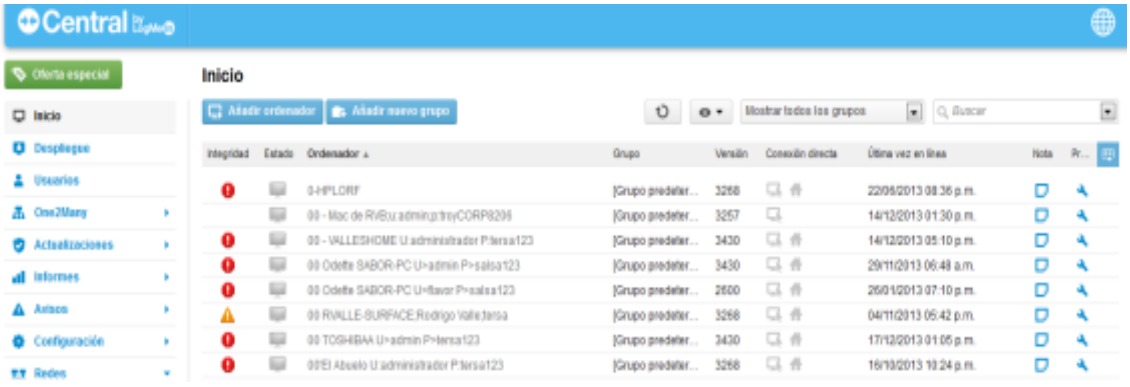


Figura 14. Plataforma de monitoreo

Cada uno de los equipos integrado en la plataforma de Logmein ofrece un monitoreo del tráfico que se genera y a su vez se mide la conectividad en un periodo de tiempo que auxilie a determinar la efectividad de la infraestructura de la red en cada puntos remotos. La referencia del enlace que tendría con la unidad central como punto de almacenamiento de la información generada en cada sitio, es llevada por aplicaciones que trasmiten información a través de internet.

En el corporativo se emplea el monitor de tráfico que trae el equipo UTM de Fortinet 60c donde se conectan los sitios remotos. La Figura 15, identifica el tráfico diario que se tiene en la unidad central, y la cantidad de información que se procesa.

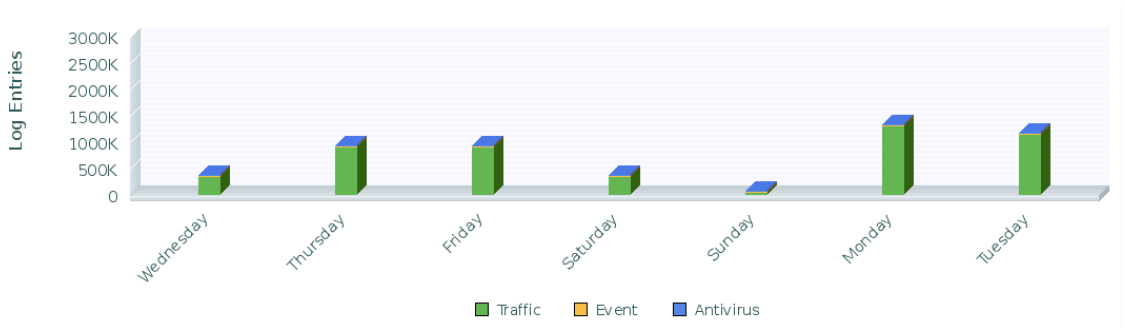


Figura 15. Medidor de tráfico diario

4.2. Comparación de equipos de comunicación VPN.

En la actualidad existe una gama de fabricantes de equipos de comunicación unificada que brindan servicios de rendimiento, velocidad de procesamiento de datos, seguridad ante amenazas y una amplia gama de soluciones de acceso remoto escalables que se ajusta a todos los tamaños, desde las pequeñas y medianas empresas hasta las grandes corporaciones globales.

Basado en los resultados de investigación que presenta la empresa Gartner con respecto al mercado UTM, el cual reconoce a los principales fabricantes y hace un enfoque en la importancia de la capacidad de los dispositivos y recientemente a la incorporación de soporte Wireless LAN seguro. En la Figura 16, se presenta el cuadrante según Gartner sobre los principales líderes del mercado UTM.

La importancia de los líderes de este mercado, tanto en la fabricación como en la distribución de productos UTM, responde a las necesidades de las empresas de cualquier tamaño. Entre las características comunes se incluye fiabilidad, rendimiento y un producto fácil de configurar, instalar y administrar. Aunque en los últimos años, se puede tener apoyo de consultores externos al fabricante que son expertos en realizar las tareas de integración en una empresa.

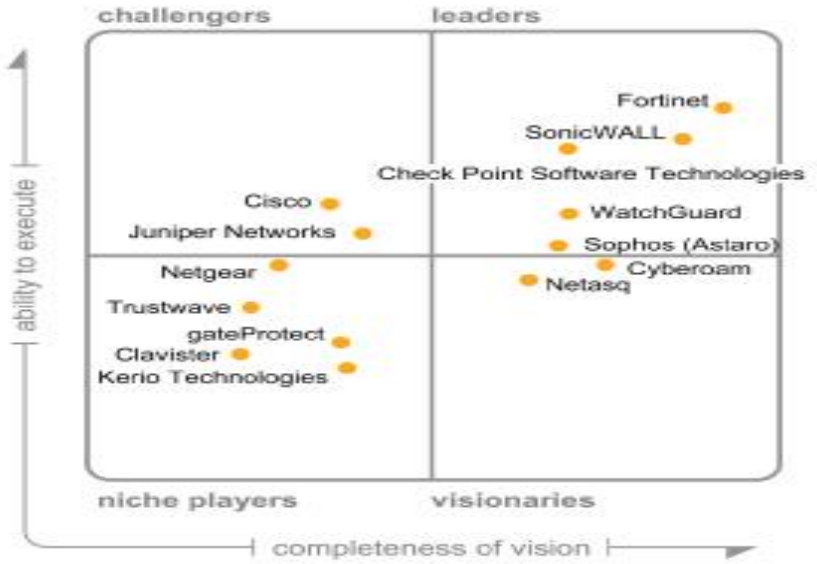


Figura 16. Cuadrante UTM

Los resultados del análisis de Gartnet, reconoce como Líderes a Fortinet, SonicWall, Checkpoint Software Technologies, WachtGuard y Sophos; en el área de Challengers ha situado a Cisco y Juniper Networks;

En el cuadrante de Jugadores de Nicho ha identificado a Netgear, Trustwave, gateProtect, Clavister y Kerlo Technologies; en el espacio de Visionarios ha ubicado a Netasq y Cybercam.

Para efecto del reducir la lista de proveedores posibles en equipos de comunicación, se analiza a los principales líderes del cuadrante de Gartnet como es Fortinet, Checkpoint y Cisco. Debido a dispositivos que cumplen con los requisitos internos en la empresa. En la Tabla 4, se muestra la lista de equipos sugeridos para integrar al proyecto. Donde se aproximan a las necesidades y servicios necesarios.

Tabla 4. Lista de equipos VPN.

Fabricantes	Equipo
Cisco	Cisco 887
Checkpoint	UTM 1140
Fortinet	FortiGate 60CM

4.2.1. Fabricantes de equipos de comunicación de red

CISCO 887

Los equipos de comunicación de servicios integrados de Cisco serie 800 combinan datos, seguridad y servicios inalámbricos en un mismo dispositivo fácil de usar y gestionar.

Los equipos de comunicación de servicios integrados de Cisco serie 800 admiten:

- Servicios simultáneos a altas velocidades de banda ancha, por lo cual se obtiene un máximo de uso de la conexión.
- Seguridad robusta que reduce los riesgos asociados a virus y otras amenazas contra la seguridad.
- Compatibilidad de la red virtual privada para personal en sitio y conexiones a distancia con un acceso seguro a los recursos de la empresa a través de una conexión segura.
- Conectividad de red inalámbrica que permite acceder a las aplicaciones y la información.

Los equipos de comunicación de servicios integrados de Cisco Serie 800 ofrecen una amplia gama de funciones y características, que incluye:

- Opción de conexiones de WAN 10/100 Mbps o ADSL2/2+
- Switch gestionado 10/100 Mbps de 4 puertos

- Sólidas funciones de seguridad, que incluyen cortafuegos Cisco IOS y compatibilidad con VPN
- Conectividad inalámbrica opcional

Los modelos 881, 887 y 888 de Cisco añaden:

- Opción de conexiones WAN VDSL2 y G.SHDSL
- Prevención de intrusiones con servicios IP avanzados
- Filtrado de contenido de Cisco IOS
- VPN multipunto dinámica de Cisco (DMVPN), VPN de transporte cifrado en grupo de Cisco (GET VPN) y VPN SSL

Los modelos 891 y 892 de Cisco añaden:

- Alto rendimiento para un acceso de banda ancha segura.
- Conexiones en distintos puntos.
- Punto de acceso inalámbrico 802.11n opcional de alta velocidad.
- Compatibilidad opcional con 4 puertos de switch Power over Ethernet (PoE)

A continuación se presenta la Figura 17. Con la imagen del equipo físicamente.

Figura 17. Equipo Cisco 887

FortiGate 60C

El dispositivo de seguridad contra múltiples amenazas FortiGate 60C ofrece una flexibilidad y seguridad para la oficina remota, sucursal o una pequeña oficina. Combina un hardware de alto rendimiento con el almacenamiento incluido y opciones de expansión innovadoras como el soporte de redes inalámbricas de banda ancha.

También provee protección simplificada con servicios de seguridad con una profundidad y amplitud sin precedentes, dentro de los beneficios que se puede encontrar al utilizar este dispositivo, se puede mencionar:

- Segmenta el tráfico interno y garantiza la seguridad total para el tráfico de perímetro consolidado con un rendimiento de protección de Gigabit combinado con puertos internos y puertos WAN dedicados.
- Almacenamiento interno de registros e informes gráficos, optimización WAN y el almacenamiento en caché de Web.
- Implementa redes seguras de manera rápida y fácil con soporte para banda ancha inalámbrica basada en USB.
- Simplifica la administración de seguridad, informes y análisis, y la reducción de los gastos operativos con la disponibilidad de la solución de gestión centralizada con FortiManager y FortiAnalyzer.

Características:

- Rendimiento de Firewall (512 / 1518 bytes paquetes UDP) de 1 Gbps
- Rendimiento de Firewall (64 bytes paquetes UDP) de 1 Gbps
- IPSec VPN (AES-256 + SHA-1): 70 Mbps
- Antivirus: rendimiento de 20 Mbps
- IPS: rendimiento de 60 Mbps
- Interfaces totales de red: 8
- Interfaces Switch de GbE internas: 5
- Interfaces dedicadas WAN 10/100: 2
- Interfaz dedicada DMZ 10/100: 1
- Incluye 4 GB de almacenamiento en Tarjeta SD HC Clase 6 (soporta hasta 32

GB, a partir de 4GB se pueden almacenar logs y hacer reportes, a partir de 16 GB además Web Cache y optimización WAN)

A continuación se presenta la Figura 18. Con la imagen del equipo físicamente.

Figura 18.Equipo Fortigate 60C

CheckPoint UTM 1140

Seguridad UTM integral para oficinas y entornos industriales

- Se integra protección de clase empresarial, IPS, VPN, NAC, filtrado de URL, Anti-malware y seguridad en los mensajes.
- Seguridad integral.

Alta disponibilidad y rendimiento

- Gigabit Firewall rendimiento y multi-densidad de puertos Gigabit de aumento de la demanda de ancho de banda
- Alta disponibilidad y balanceo de carga para la conectividad persistente y la disponibilidad del servicio

Características

- Integración con Firewall e IPS
- Conectividad
- Anti-malware y seguridad en la mensajería.
- Filtrado Web
- Control de acceso a la red controlado.

En la parte de VPN, el equipo cuenta con las siguientes especificaciones mostradas en la Tabla 5, donde se indica los servicios que ofrece con respecto al manejo de la tecnología de red virtual privada. En la Tabla 6, se muestra las especificaciones de red que soporta los diferentes modelos del fabricante.

Tabla 5. Especificaciones a la conexión de VPN.

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Remote Access Software Cliente	Compruebe Punto final Punto de Seguridad VPN, SecureClient, SecuRemote, L2TP IPsec VPN			
Sitio a sitio VPN	✓			
VPN de acceso remoto	✓			
Túneles VPN	400 (con gestión)			
Perfiles VPN de acceso remoto	Ilimitado			
Perfiles VPN de sitio a sitio	Ilimitado			
IPSec Características	Acelerada por hardware DES, 3DES, AES, MD5, SHA-1, Hardware Generador de números aleatorios (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), compresión de IPSec, IPSec NAT Traversal (NAT-T)			
L2TP VPN Servidor	✓			

Tabla 6. Especificaciones de red.

	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Estándares admitidos	IP estática, DHCP, PPPoE, PPTP, Telstra, L2TP			
Backup ISP y equilibrio de carga	✓			
Respaldo de acceso telefónico	Serial	USB, Serie		
Traffic Shaper (QoS)	Avanzada *			
Failover automático Gateway (HA)	✓ *			
Enrutamiento dinámico *	OSPF, BGP, RIP			
Multicast Routing *	DVMRP, PIM SM v2			
Servidor de impresión	n / a	✓		

Las especificaciones técnicas con respecto a las redes inalámbricas que soporta el equipo, están descritas en la Tabla 7.

Tabla 7. Especificaciones del inalámbrico.

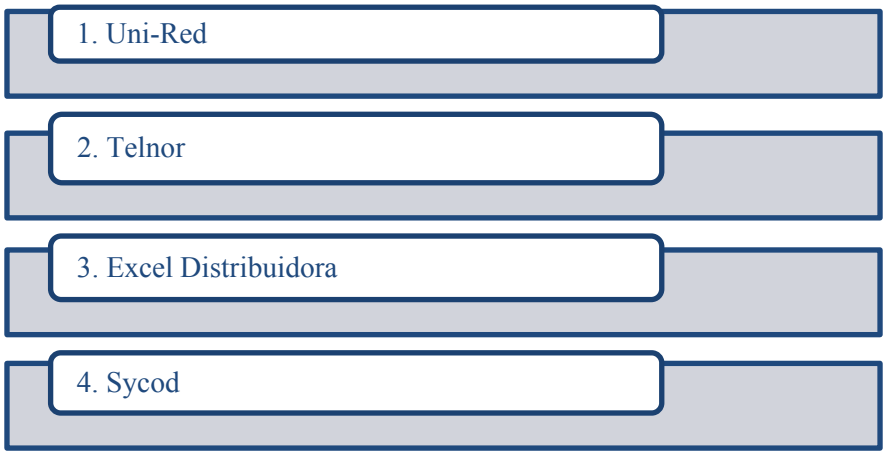
	UTM-1 Edge N	UTM-1 Edge NW	UTM-1 Edge N ADSL	UTM-1 Edge NW ADSL
Protocolos inalámbricos		802.11b (11 Mbps), 802.11g (54 Mbps), 802.11n (300Mbps)		802.11b (11 Mbps), 802.11g (54 Mbps), 802.11n (300Mbps)
Seguridad inalámbrica		VPN de forma inalámbrica, WEP, WPA2 (802.11i), WPA-PSK, 802.1x		VPN de forma inalámbrica, WEP, WPA2 (802.11i), WPA-PSK, 802.1x
Sistema de Distribución Inalámbrico (WDS)		✓ *		✓ *
Múltiples puntos de acceso		✓ *		✓ *

4.3. Revisión de los equipos UTM.

El proceso siguiente en la recolección de los datos está representado por una fase fundamental en el éxito de la comunicación por medio de conexión, como es el equipo que se utilizara para realizar dicho trabajo.

Lo cual se convoca a proveedores de la región que brindan soporte en la compra y configuración de los equipos de comunicación que se requiere para hacer la conexión entre los diferentes sitios remotos. En la Tabla 8, Proveedores del servicio. Se identifica las empresas que brindan el tipo de servicio de telecomunicaciones que se requiere.

Tabla 8. Proveedores del servicio de equipo de comunicación.



Cada una de las propuestas de equipos para realizar una VPN por parte de los diferentes proveedores de la región, está enfocada en la conectividad con servicios extras. Como son que brinde una administración básica de los usuarios, monitoreo de los paquetes que pase por el equipo, filtrado de contenido, bloqueo de páginas web, conexión remota y que utilice el protocolo IPSec.

En la Tabla 9, Análisis de la propuesta de Telnor con respecto al equipo que proponen para realizar la conexión entre los diferentes sitios.

Tabla 9. Ventajas y desventajas de la propuesta de Telnor

Proveedor Telnor
Equipo
Equipo marca Cisco que integra Firewall, VPN e IPS. **Ventajas:** El equipo propuesto cumple con las necesidades para implementarlo. Y cuenta con un fuerte soporte por parte del proveedor en cuestión de fallos o garantía. **Desventajas:** Están muy enfocados en conectividad y se perdería el lado de administración.
Equipo Central: Secure Manager
Equipo Sucursales: Cisco 887

En la Tabla 10. Análisis de la propuesta de Uni-Red con respecto al equipo que proponen para realizar la conexión entre los diferentes sitios.

Tabla 10. Ventajas y desventajas de la propuesta de Uni-Red

UNIRED
Equipo
Equipo marca Fortinet que integra Firewall, VPN e IPS **Ventajas:** El equipo cumple con las características y requerimientos necesarios para realizar el proyecto. La propuesta incluye equipo para todas las sucursales, consola de administración y portes. **Desventajas:** La consola de admón. que incluye la propuesta es una renta anual comparado con Excel y/o SYCOD.
Equipo Central: CheckPoint 4205
Equipo Sucursales: CheckPoint 1120

En la Tabla 11. Análisis de la propuesta de Excel con respecto al equipo que proponen para realizar la conexión entre los diferentes sitios.

Tabla 11. Ventajas y desventajas de la propuesta de Excel Distribuidora.

EXCEL Distribuidora
Equipo
Equipo marca Fortinet que integra Firewall, VPN e IPS. **Ventajas:** El equipo cumple con las características y requerimientos necesarios para realizar el proyecto. Al adquirir los equipos son propiedad de la empresa. La propuesta incluye equipo para todas las sucursales, consola de administración y reportes. **Desventajas:** La propuesta del equipo para sucursales es más pequeña y el modelo es más antiguo al comparar con Unired y/o SyCod.
Equipo Central: FortiGate-100D
Equipo Sucursales: Fortigate-20C ADSL, Fortigate-60C ADS
Administración: Fortimanager-300D, FortiAnalizer-200D

En la Tabla 12. Análisis de la propuesta de Sycod con respecto al equipo que proponen para realizar la conexión entre los diferentes sitios.

Tabla 12. Ventajas y desventajas de la propuesta de SyCOD

SYCOD
Equipo FortiGate marca Fortinet que integra Firewall, VPN e IPS. **Ventajas:** El equipo cumple con las características y requerimientos necesarios para realizar el proyecto.
Equipo Central: FortiGate-100D
Equipo Sucursales: Wireless 802.11a
Administración: Fortimanager -400D, FortiAnalizer-400C

Cada una de las propuestas de equipos para realizar una VPN por parte de los diferentes proveedores de la región, está enfocada en la conectividad con servicios extras. Como

son que brinde una administración básica de los usuarios, monitoreo de los paquetes que pase por el equipo, filtrado de contenido, bloqueo de páginas web, conexión remota y que utilice el protocolo IPSec.

El proveedor elegido para el apoyo de dicho proyecto, será el de Unired. Debido que cuenta con experiencia en el manejo de equipo, tanto en configuración como en instalación. Adicional, el integrar su equipo propuesto brinda el beneficio de adquirir el equipo arrendamiento, que es de gran ayuda para el estado financiero de la empresa en la actualidad.

4.4. Elección del equipo

Basado en las características propias de cada uno de los equipos mostrados en el documento, y en lo que se requiere para integrar a la red actual de la empresa. Se considera propio el equipo de Checkpoint UTM 1140 applicance, debido a la gama de funciones con la que cuenta, tanto en la parte de conectividad de red como también en la parte de la administración y seguridad de los datos que brinda el equipo.

Sin duda cada fabricante ejemplifica servicios muy potentes que resultan de gran ayuda para la protección y conexión de red de cualquier organización. La elección del equipo de Checkpoint también, está sustentada por el soporte que brindara el proveedor local que nos auxiliara en la parte técnica del equipo para una efectiva implementación.

4.5. Elección de la topología y los componentes de red

La topología nos indica la forma en que están conectados los diferentes equipos (nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como un ordenador o una impresora. Un nodo también puede ser dispositivo o equipo de la red como un concentrador, conmutador o un router. El cual, nos auxilia a mantener controlada la estructura de la red de una manera lógica y física.

4.5.1. Elección de la topología

Debido a que se cuenta con diferentes sitios remotos en toda la parte noroeste del país, es vital ejemplificar una correcta forma de organizar los componentes de red que lleven la comunicación de datos en cada uno de los puntos o enlaces remotos de conexión. Es por ello, que una elección incorrecta de la forma de comunicación, nos puede dar como resultado perdida de información entre los diferentes puntos.

Para el diseño de la estructura de red se analiza la topología de estrella, para la parte del esquema general entre cada uno de los dispositivos remotos. El utilizar esta topología brinda elementos y ventajas considerables en comparación de las otras, el cual debido a la misma necesidad de la empresa de integrar nuevas soluciones en la red interna. Lleva a considerar la integración de un punto central que brinde los servicios a cada una de las unidades o sucursales de la empresa.

El esquema general de la estructura de red, seria representada en la Figura 19. Que ejemplifica la conexión corporativa como unidad central con la de las sucursales.

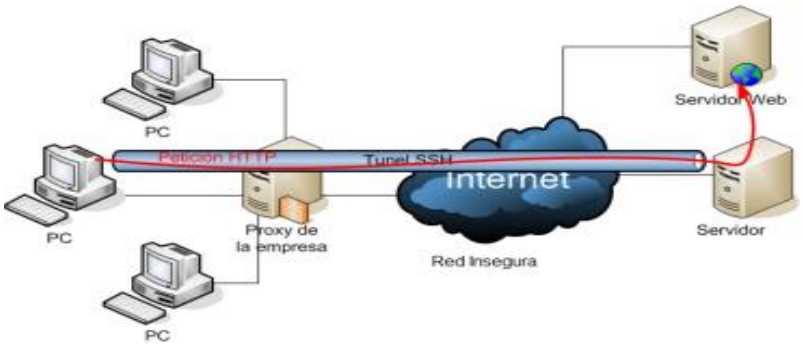


Figura 19. Esquema elemental de la red.

4.5.2. Componentes de red.

De manera general los componentes están enfocados en los dispositivos que se utilizaran para llevar acabo las conexiones de la red en cada punto. En total serán 29 dispositivos UTM CheckPoint que estarán en cada una de las sucursales y unidades del grupo, y otro para la unidad concentradora en el corporativo.

Características de las sucursales.

Cada una de las sucursales que imparten servicio para Tecnicentro Royal, cuentan con una infraestructura de red básica y un servicio de internet de 4 MB. Debido que la misma demanda de mejorar día con día, ha tenido un incremento considerablemente en el tráfico de la información que se procesa y se envía al corporativo para su tratamiento.

Requerimientos para una VPN

Se necesita un conjunto de protocolos de comunicación y servicios que establece el funcionamiento de los túneles o medios de transmisión que en ocasiones puede cambiarse alguno.

- Autenticar usuarios, realiza una validación de la identidad del usuario que se va a conectar para poder restringir o dar acceso a la red. Donde solo podrán entrar los usuarios que cumplan con una autenticación correcta.

- Administrar las IPs, apoya a la asignación de una dirección IP al usuario autenticado en la red privada y que la dirección IP otorgada cumpla con los rangos establecidos previamente en la configuración.

- Encriptar los datos, transforma los datos que serán enviados por una red pública y que solo el destinatario pueda desencriptar la información.

- MultiProtocolo, que sea capaz de utilizar una variedad de protocolos compatibles en la red pública para el transporte de la información por el medio.

4.6. Diseño del entorno de comunicación

La estructura de red para el procesamiento de la información toma como base, la información recolectada anteriormente del presente trabajo. Para así, poder plantear una forma de conexión que sea lo más estable posible y facilite la administración dela red y la posibilidad de integración de distintas tecnologías de información.

El segmento de red que tendrá está clasificado en nivel C, el cual parte de bloques para acomodar los dispositivos de impresión, escáner, equipo de cómputo y cámaras análogas. En la Tabla 13, representa la relación de IPs que tendrá cada uno de los servicios en los sitios remotos.

Tabla 13. Relación de IPs en los equipos principales

No.	Posición del Sitio	Sucursal	Zona	Computo	DVR	Impresora
1	**1**	Boulevard	Tijuana	192.168.11.10	192.168.11.30	192.168.11.50
2	**2**	Plaza	Ensenada	192.168.12.10	192.168.12.30	192.168.12.50
3	**3**	Otay	Tijuana	192.168.13.10	192.168.13.30	192.168.13.50
4	**4**	Rosarito	Tijuana	192.168.14.10	192.168.14.30	192.168.14.50
5	**5**	Benito Juárez	Mexicali	192.168.15.10	192.168.15.30	192.168.15.50
6	**6**	La Mesa	Tijuana	192.168.16.10	192.168.16.30	192.168.16.50
7	**7**	Forjadores	BCS	192.168.17.10	192.168.17.30	192.168.17.50
8	**8**	Cedis	Tijuana	192.168.18.10	192.168.18.30	192.168.18.50
9	**9**	San Quintín	BCS	192.168.19.10	192.168.19.30	192.168.19.50
10	**11**	Abasolo	BCS	192.168.21.10	192.168.21.30	192.168.21.50
11	**12**	Morelos	Sonora	192.168.22.10	192.168.22.30	192.168.22.50
12	**13**	Obregón	Sonora	192.168.23.10	192.168.23.30	192.168.23.50
13	**14**	Mochis	Sinaloa	192.168.24.10	192.168.24.30	192.168.24.50
14	**15**	Periférico	Sonora	192.168.25.10	192.168.25.30	192.168.25.50
15	**16**	Río	Tijuana	192.168.26.10	192.168.26.30	192.168.26.50
16	**17**	Insurgentes	Tijuana	192.168.27.10	192.168.27.30	192.168.27.50
17	**18**	Culiacán	Sinaloa	192.168.28.10	192.168.28.30	192.168.28.50
18	**19**	Cortés	Ensenada	192.168.29.10	192.168.29.30	192.168.29.50
19	**21**	López Mateos	Mexicali	192.168.31.10	192.168.31.30	192.168.31.50
20	**22**	Justo Sierra	Mexicali	192.168.32.10	192.168.32.30	192.168.32.50
21	**23**	Lienzo Charro	Mexicali	192.168.33.10	192.168.33.30	192.168.33.50
22	**24**	Cabo	BCS	192.168.34.10	192.168.34.30	192.168.34.50
23	**25**	Santa Lucía	Ensenada	192.168.35.10	192.168.35.30	192.168.35.50
24	**27**	Tepic	Nayarit	192.168.37.10	192.168.37.30	192.168.37.50
25	**28**	San Lucas	BCS	192.168.38.10	192.168.38.30	192.168.38.50
26	**29**	Santa Rosalía	BCS	192.168.39.10	192.168.39.30	192.168.39.50

27	**30**	Encinas	Sonora	192.168.40.10	192.168.40.30	192.168.40.50
28	**31**	Tecate	Tijuana	192.168.41.10	192.168.41.30	192.168.41.50
29	**33**	Lázaro Cárdenas	Mexicali	192.168.43.10	192.168.43.30	192.168.43.50

En la Figura 20, se representa de manera general la estructura de red. Indicada por zona geográfica del país. Donde cada una de los sitios remotos está homologado a su referencia de sitio de apertura de la sucursal.

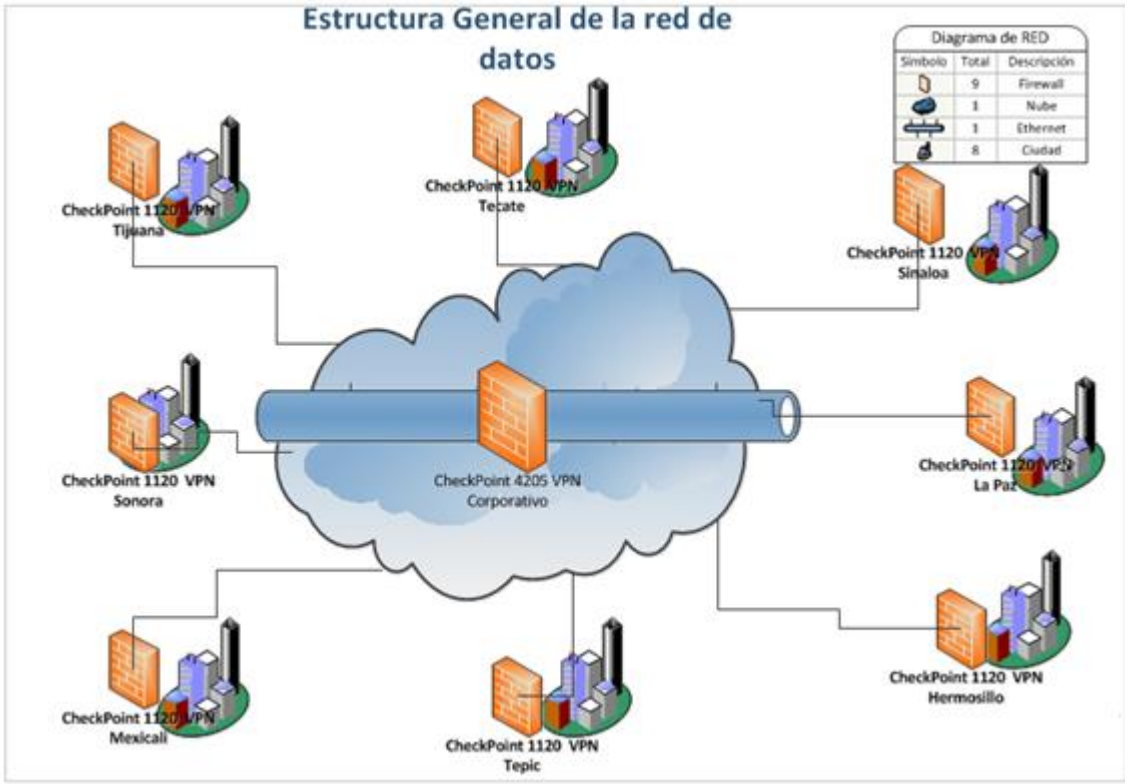


Figura 20. Diseño general de la red

4.7. Equipo central UTM

El dispositivo de comunicación que estará en la unidad central, que recibirá las conexiones de los diferentes sitios remotos estará ubicado en el corporativo. Las ventajas que lleva el tenerlo ubicado en un punto neutro con una sucursal es de vital importancia, debido que los servicios que ofrece y manejo de las aplicaciones está centrada en esta unidad.

Únicamente tendrá acceso al equipo UTM Checkpoint R77 el departamento de tecnología de la comunicación de la empresa mediante la siguiente liga http://192.168.1.233. La Figura 21, muestra la pantalla de acceso del dispositivo, el cual brinda oportunidad de revisión del entorno de red.

Figura 21. Página web de acceso al equipo Checkpoint R77

La configuración del equipo central, con lleva la actualización correspondiente de los parches del firmware con los que cuente el fabricante. Como también, la asignación de IP local y la IP pública por la cual se conectara los sitios remotos e integraran túneles para formar la VPN. Para la Figura 22, se indica la configuración de las interfaces del equipo tanto en la IP local como la pública. Para lo cual, se toma rangos de IPs asignados al grupo de equipos de comunicación del centro de comunicación de la empresa.

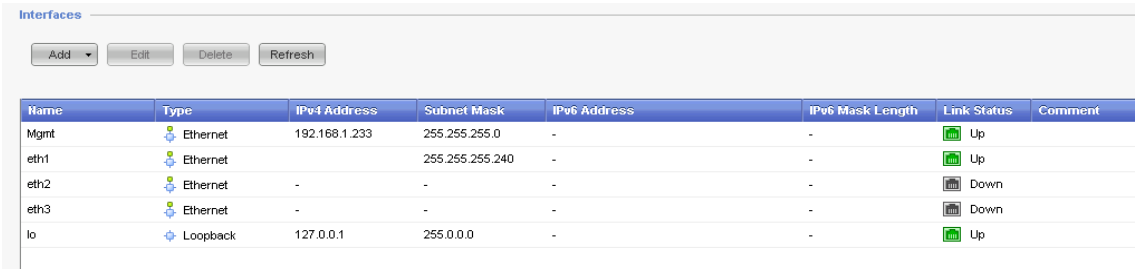


Figura 22. Interfaces del equipo administrador

Los datos que lleva el manager está representado en la Figura 23, el cual indica los parámetros que tiene el equipo central en el nombre del dispositivo, el dominio por el cual será reconocido la red y el primer DNS Server por default que manera.

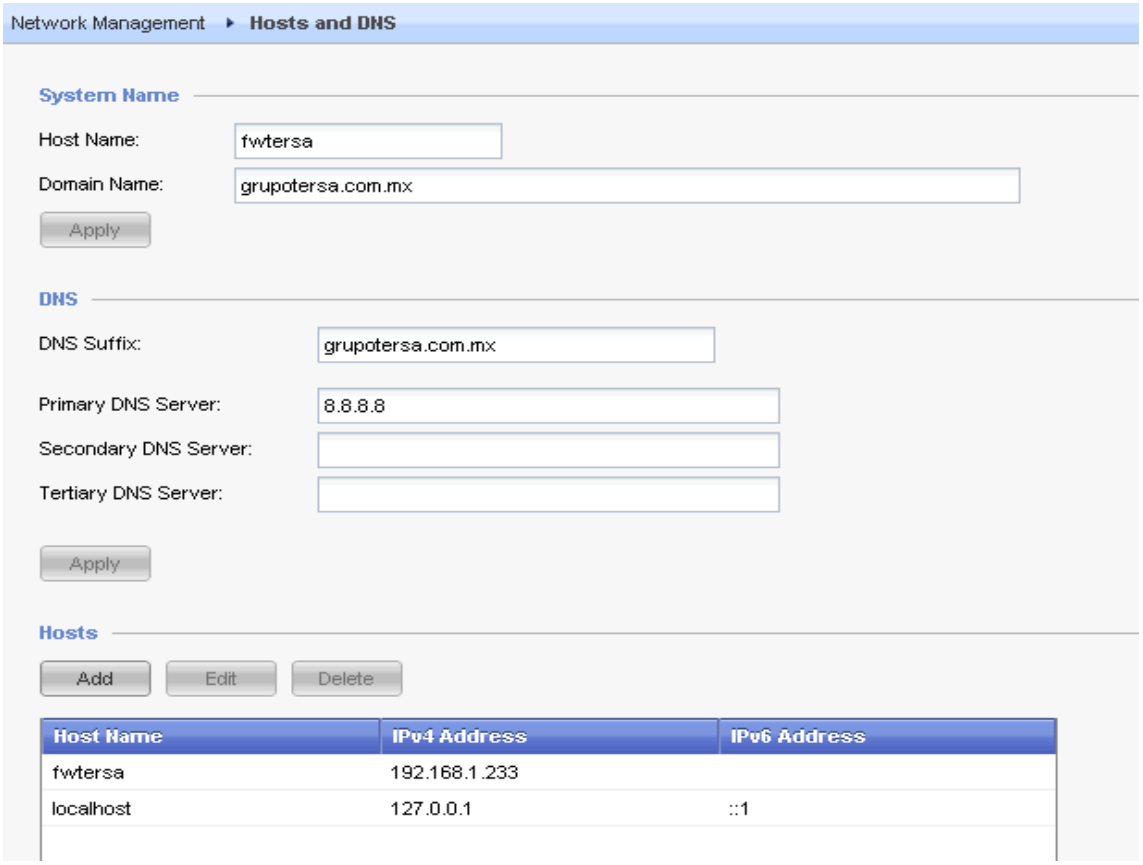


Figura 23. Configuración del manager

4.8. Equipo en el sitio remoto UTM Checkpoint.

Para entrar al equipo remoto en cada una de las sucursales de la empresa, es vía página web mediante el uso del protocolo https con el puerto 4434. La Figura 24, representa la pantalla de acceso del equipo.

Figura 24. Página web de acceso al equipo Checkpoint 1100

La configuración del sitio remoto estará basado en los parámetros recopilados en cada una de las sucursales, el cual se cambiara los DSL infinitum por este equipo. El cual brinda beneficios antes mencionados.

Uno de los requisitos para la conexión del equipo Checkpoint 1100 en la línea de infinitum de internet, es contar con la cuenta infinitum de la línea contratada en Telnor, el cual se manejara una conexión PPPOE en el ASDL. En la Figura 25, se indica el módulo de configuración que se tiene que agregar al equipo de la sucursal para que pueda conectarse a Internet una vez conectado el servicio de Infinitum.

Por default el equipo lo trae deshabilitado, por lo cual es necesario habilitarlo y configurarlo con los parámetros de la línea infinitum y también un parámetro estándar para los proveedores de internet como es el VCI y VPI.

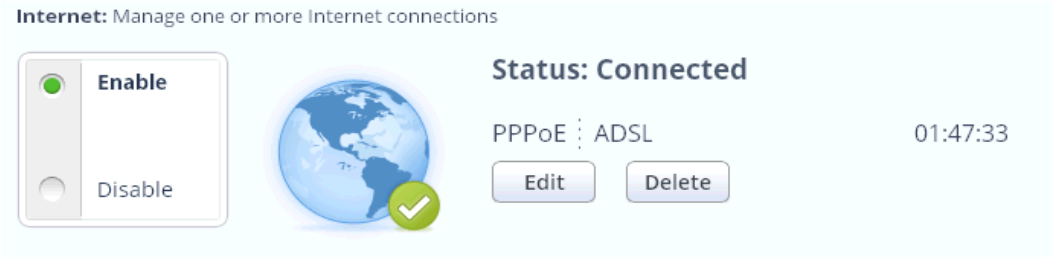


Figura 25. Conexión PPPoE en la sucursal

Los parámetros de configuración que tiene asignado el equipo de la sucursal, parte de homologar la subred al número de la sucursal. Para formar en cada punto remoto, un acceso identificable y sencillo de administrar. En la Figura 26, se indica la parte configurada con respecto a la sub red correspondiente para la tienda de Blvd. Aunque los demás sitios remotos tendrán una subred parecida, contaran con semejanzas y una forma de asignación de IP administrables.

Dentro de la configuración en el equipo de la sucursal, se maneja por el rango de funciones, por mencionar un caso, el servidor pertenece la IP con terminación 10, el DVR con terminación 30 o el equipo Checkpoint con terminación 1. La IP dinámica disponible para asignar a los dispositivos conectados a la red por medio de una conexión alámbrica o inalámbrica comprende de la termina 101 a la 200.

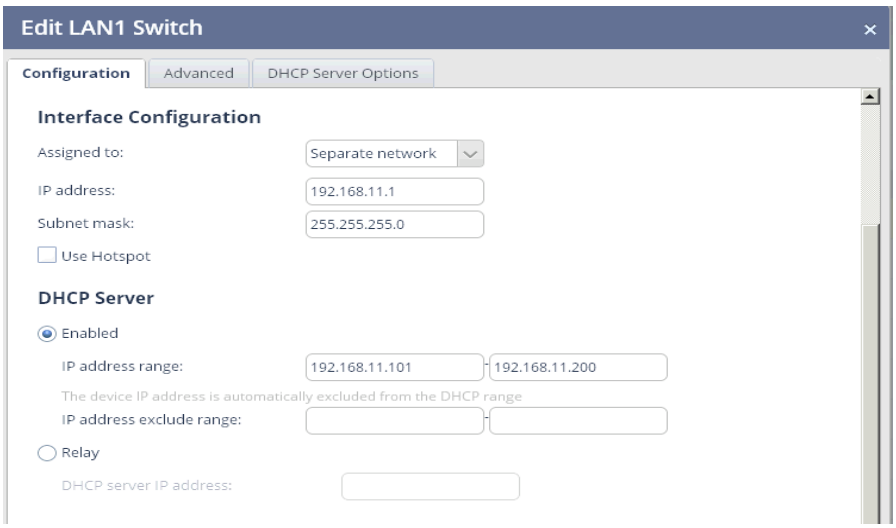


Figura 26. Parámetros de la red alámbrica

4.9. Redes inalámbricas operativas y clientes.

Una parte importante dentro de las configuraciones de los equipos Checkpoint 1100 appliance, es correspondiente a los servicios inalámbricos que pueda tener tanto para la red operativa y para la red de visitantes, en el apartado del dispositivo trae forma de configurar redes inalámbricas el cual está relacionado en la Tabla 14. Que representa la configuración de la prueba piloto en la tienda de Blvd.

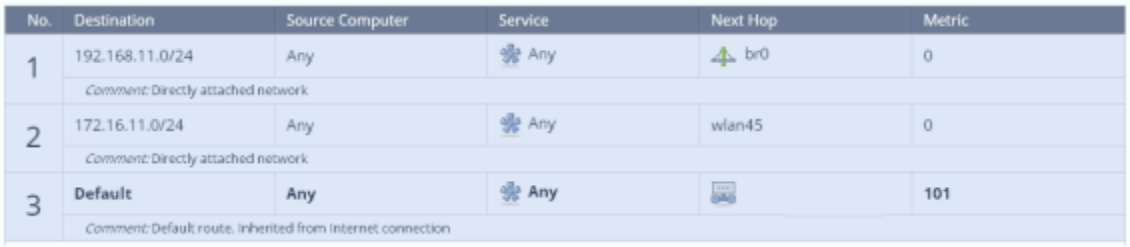
Tabla 14. Relación del SSID del inalámbrico de la sucursal

Red Inalámbrica	
Nombre de la Red	**Rango de IP**
Tersa	192.168.11.101 - 200
Tersa-Visitas	172.16.11.101 - 200

Para la Figura 27, se muestra la configuración propia del equipo para la red de clientes y el rango de IP que tendrá, cabe indicar que la red de Tersa y Tersa-Visitas no se podrán enlazar una con la otra debido que tienen diferentes parámetros por cuestión de seguridad. El SSID de Visitas y Tersa tendrá la seguridad WPA como medio de protección para el acceso a la red.

Figura 27. Parámetros de la red inalámbrica de visitas

Los parámetros finales en el equipo UTM, lo representa en la Figura 28. El cual se ruteo las direcciones que serán valida tanto para la red alámbrica como para la red inalámbrica.



No.	Destination	Source Computer	Service	Next Hop	Metric
1	192.168.11.0/24	Any	Any	br0	0
	Comment: Directly attached network				
2	172.16.11.0/24	Any	Any	wlan45	0
	Comment: Directly attached network				
3	**Default**	**Any**	**Any**		**101**
	Comment: Default route. Inherited from Internet connection				

Figura 28. Configuración de la red inalámbrica de visitas

Capítulo V. Resultados

5.1. Resultados

Dado que el proceso de desarrollo integró una variedad de puntos en el entorno de comunicación en cada punto remoto de la empresa Tecnicentro Royal S.A de C.V., el cual culmina con una serie de datos que reflejan el panorama general después de tener implementada la tecnología de VPN en la empresa. A lo cual, se partió con la reducción de dispositivos DSL de manera global con resultado directamente en la factura del servicio de internet.

La Tabla 15, refleja el ahorro correspondiente a la cantidad de servicio de internet contratado con Telnor, para satisfacer la necesidad de conexión al exterior y propiamente a la comunicación de la estructura de red. Dicha reducción en los equipos de comunicación a internet, refleja un 39% del gasto en la mensualidad total de la cuenta maestra correspondiente a servicio de Internet de la empresa. El cual se refleja en la Figura 29, que indica la cantidad porcentual final de los DSL Infinitum.

Tabla 15. Cantidad de equipos con Internet Infinitum

Equipos Operativos	Equipos para Visitas	Total
29	3	32

Aunque, el equipo que se utiliza en cada sitio remoto cuenta con la opción de tener dos redes inalámbricas configuradas, para el caso de las sucursales que requerían por la cantidad de máquinas con la que cuentan tener una adicional para fines de respaldo de servicio en caso de que uno no funcione se pueda usar el otro.

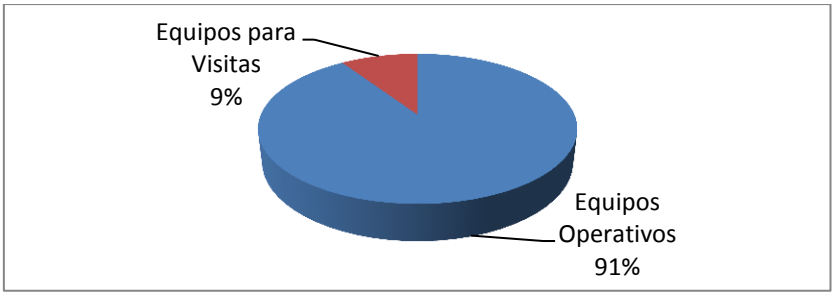


Figura 29. Cantidad que abarca el servicio de Internet Infinitum

Además, de los equipos restantes de los servicios de internet quedó configurado en los equipos Checkpoint forma que se utiliza para medir el traáfico correspondiente, para determinar y recolectar datos en aquellas líneas de infinitum que requiera incrementar o disminuir la velocidad de subida y bajada. Y para fines de manejar la información a través de la red, fue requerido homologarla a 4 MB de descarga con 760 KB de subida. Con excepción de la unidad central que cuenta una velocidad de subida y bajada de 10 MB aproximadamente.

El tráfico generado en la unidad central, se puede ver reflejado en la Figura 30 que indica la cantidad de kbits que fueron procesados por el equipo. Para la Figura 31, refleja la reducción de los recursos usados y la cantidad de tráfico procesado por el equipo central.

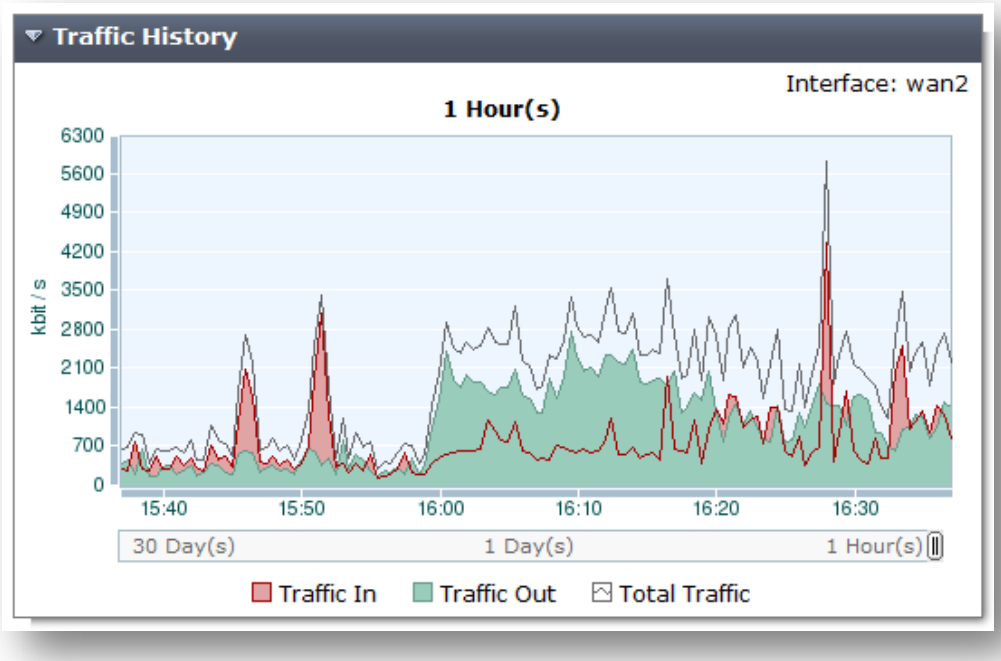


Figura 30. Tráfico entrante y saliente de la red

Por lo cual, el tráfico generado por cada paquete de información que es transmitido por el túnel de la VPN con lleva una reducción considerable del tiempo de retardo de llegar a su destino.

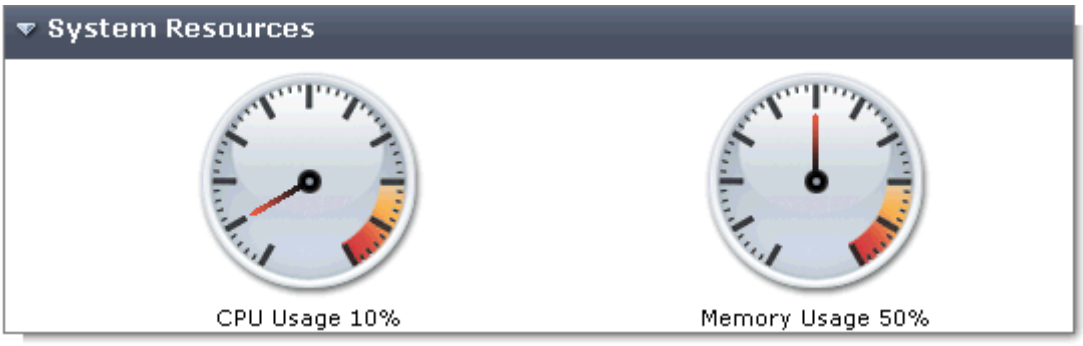


Figura 31. Recursos en CPU y memoria de uso del equipo central

El poder homologar cada rango de IP utilizado en los sitios remotos y en la unidad central, facilita la integración y la administración de los dispositivos de red. En la Tabla 16, se indica los parámetros en IP con lo que cuenta el servidor de cada sucursal, el cual es utilizado para ingresar vía remota o por medio de VNC.

Tabla 16. Relación de IP en los servidores remotos

No.	Posición del Sitio	Sucursal	Zona	Server
1	**1**	Boulevard	Tijuana	192.168.11.10
2	**2**	Plaza	Ensenada	192.168.12.10
3	**3**	Otay	Tijuana	192.168.13.10
4	**4**	Rosarito	Tijuana	192.168.14.10
5	**5**	Benito Juárez	Mexicali	192.168.15.10
6	**6**	La Mesa	Tijuana	192.168.16.10
7	**7**	Forjadores	BCS	192.168.17.10
8	**8**	Cedis	Tijuana	192.168.18.10
9	**9**	San Quintín	BCS	192.168.19.10
10	**11**	Abasolo	BCS	192.168.21.10
11	**12**	Morelos	Sonora	192.168.22.10
12	**13**	Obregón	Sonora	192.168.23.10
13	**14**	Mochis	Sinaloa	192.168.24.10
14	**15**	Periférico	Sonora	192.168.25.10
15	**16**	Río	Tijuana	192.168.26.10
16	**17**	Insurgentes	Tijuana	192.168.27.10
17	**18**	Culiacán	Sinaloa	192.168.28.10
18	**19**	Cortés	Ensenada	192.168.29.10
19	**21**	López Mateos	Mexicali	192.168.31.10
20	**22**	Justo Sierra	Mexicali	192.168.32.10
21	**23**	Lienzo Charro	Mexicali	192.168.33.10
22	**24**	Cabo	BCS	192.168.34.10
23	**25**	Santa Lucía	Ensenada	192.168.35.10
24	**27**	Tepic	Nayarit	192.168.37.10
25	**28**	San Lucas	BCS	192.168.38.10

26	**29**	Santa Rosalía	BCS	192.168.39.10
27	**30**	Encinas	Sonora	192.168.40.10
28	**31**	Tecate	Tijuana	192.168.41.10
29	**33**	Lázaro Cárdenas	Mexicali	192.168.43.10

Cabe indicar, que la asignación de cada una de las direcciones IP está relacionada al número de sucursal en turno. Con la idea de facilitar la identificación de cada uno de los equipos computo, y poder reducir el tiempo de atención en el área de soporte técnico. Otra configuración donde impacta directamente es en los sistemas internos con los que cuenta la empresa, debido que estos constantemente envían información importante como son las facturas, datos del cliente, inventario de equipo, impresiones, entre otras cosas.

También, el homologar las direcciones IPs para los equipos de videograbación DVR auxilia definitivamente para el departamento de riesgos de la empresa, debido que podrán entrar a la página web del DVR y revisar las grabaciones. Esto, se tiene que llevar a cabo al estar conectado en cualquier red inalámbrica o alámbrica de Tecnicentro Royal, S.A. de C.V. En la Tabla 17 se indica la relación de IPs que tiene el DVR en cada punto remoto.

Tabla 17. Relación de las direcciones IPs de los DVR

No.	Posición del Sitio	Sucursal	Zona	DVR
1	**1**	Boulevard	Tijuana	192.168.11.30
2	**2**	Plaza	Ensenada	192.168.12.30
3	**3**	Otay	Tijuana	192.168.13.30
4	**4**	Rosarito	Tijuana	192.168.14.30
5	**5**	Benito Juárez	Mexicali	192.168.15.30
6	**6**	La Mesa	Tijuana	192.168.16.30
7	**7**	Forjadores	BCS	192.168.17.30
8	**8**	Cedis	Tijuana	192.168.18.30
9	**9**	San Quintín	BCS	192.168.19.30
10	**11**	Abasolo	BCS	192.168.21.30
11	**12**	Morelos	Sonora	192.168.22.30
12	**13**	Obregón	Sonora	192.168.23.30
13	**14**	Mochis	Sinaloa	192.168.24.30
14	**15**	Periférico	Sonora	192.168.25.30
15	**16**	Río	Tijuana	192.168.26.30
16	**17**	Insurgentes	Tijuana	192.168.27.30

17	**18**	Culiacán	Sinaloa	192.168.28.30
18	**19**	Cortés	Ensenada	192.168.29.30
19	**21**	López Mateos	Mexicali	192.168.31.30
20	**22**	Justo Sierra	Mexicali	192.168.32.30
21	**23**	Lienzo Charro	Mexicali	192.168.33.30
22	**24**	Cabo	BCS	192.168.34.30
23	**25**	Santa Lucía	Ensenada	192.168.35.30
24	**27**	Tepic	Nayarit	192.168.37.30
25	**28**	San Lucas	BCS	192.168.38.30
26	**29**	Santa Rosalía	BCS	192.168.39.30
27	**30**	Encinas	Sonora	192.168.40.30
28	**31**	Tecate	Tijuana	192.168.41.30
29	**33**	Lázaro Cárdenas	Mexicali	192.168.43.30

Luego de tener integrado un entorno de comunicación entre los puntos remotos y la unidad central, es importante vigilar el tráfico generado en dicha red. Mediante revisiones constantes que auxilien a detectar posibles vulnerabilidades o virus que afecte la integridad de la información y de la red. Para la Figura 32, se ejemplifica las 10 estaciones con más tráfico entrante y saliente generado en una semana, el cual sirve de parámetro para detectar grandes cargas de información o quien genera mucho flujo de información.

Los 10 flujos de tráfico más destacados (esta semana)

Nombre de cliente	ID de cliente	Sent	Received	Total
CLN-Vts02	096-274-348	1 324 560 KB	29 971 KB	1 354 531 KB
CLN-SupCred	097-002-872	26 206 KB	1 159 689 KB	1 185 894 KB
CLN-SupCred	097-002-872	20 532 KB	875 437 KB	895 969 KB
CLN-SupCred	097-002-872	15 474 KB	704 114 KB	719 588 KB
CLN-Vts02	096-274-348	699 961 KB	16 045 KB	716 006 KB
CLN-Vts02	096-274-348	558 871 KB	12 922 KB	571 793 KB
CLN-SupCred	097-002-872	12 022 KB	546 058 KB	558 080 KB
CLN-Vts02	096-274-348	429 917 KB	9 815 KB	439 733 KB
CLN-Vts02	096-274-348	405 928 KB	9 239 KB	415 167 KB
15 - Her Perif-Serv	092-644-386	266 007 KB	47 185 KB	313 192 KB

Figura 32. Los principales 10 equipos que generan trafico entrante y salientes

Capítulo VI. Conclusiones

6.1. Conclusión

Mediante el avance tan ágil que se ha tenido en la última década con respecto a la tecnología de la información y la comunicación, se considera que las organizaciones o empresas de cualquier giro requieren estar siempre en constante cambio para que no se vean afectadas en su producción y así poder competir en el mercado global.

Para el presente trabajo de caso práctico donde se integra la tecnología de VPN a la empresa Tecnicentro Royal S.A. de C.V., que cuenta con múltiples accesos o sucursales, se considera que fue de vital importancia el claro entendimiento de lo que abarcaba este tipo de tecnología en la estructura de comunicación y la gama de beneficios que tendrían con el avance del tiempo y con la aplicación de diferentes sistemas tecnológicos de la actualidad. Tanto para medir factores determinantes que apoyen en la toma de decisiones o simplemente programas enlazados que recopilen de mejor manera la información.

Dentro de los beneficios adquiridos, al contar con una estructura de red estable y ajustada a las necesidades propias del trabajo que día a día lleva la empresa, son el concentrar, de cada una de las sucursales, los datos de las ventas hechas al momento, información de inventarios de mercancía, monitoreo de las cámaras y una infinidad de tareas y sistemas para la recopilación de los datos.

Uno de los retos que dio rumbo al trabajo como fase preliminar fue la aceptación de los directivos de la empresa misma para que apostaran al cambio en la estructura de comunicación de la información que se llevaba; ya que sin duda todo cambio genera incertidumbre y temor para cualquier persona, y más aún en procesos que están activos y generan ganancias. Aunque parecia, en su momento, que ya se podía vivir con un entorno donde la red se caía seguido, había perdida de información, lentitud en resolución de inconvenientes en la red y temas relacionados por las debilidades de la estructura de transmisión del momento, la propuesta de este proyecto, brindó la oportunidad de preparar, recopilar y proponer una solución eficaz ante los retos continuos de esparcimiento en la red en base a la necesidad del momento sin ningún argumento teórico o documentación que lo sustentara.

El tener una recopilación de los datos de la red de forma adecuada, dio la oportunidad de comprender los puntos fuertes y débiles de la estructura que se manejaba, dónde se tenía que atacar y ajustar para fortalecerla. También, el identificar la cantidad de dispositivos que estarían conectados a la red para determinar qué tipo de servicios de internet era el idóneo para satisfacer el requerimiento de ancho de banda. Además, dichos datos sirvieron para proponer un diseño a la medida de la empresa que cumpliera con el flujo de la información y la estructura de red, el cual dio paso a poder seleccionar el equipo de comunicación que hiciera el trabajo de la transmisión de la información en cada uno de los puntos.

Donde se analizó cada uno de los dispositivos UTM que cumplieran con los requisitos de la red deseada y rasgos propios en las configuraciones de las redes inalámbricas. El cual se tuvo un ahorro del 39 % de los servicios de internet infinitum en la cuenta maestra, esto llevo a quitar 20 equipos de comunicación y a la cancelación del servicio por ya no ser necesario. Estos equipos fueron los correspondientes a las redes inalámbricas de visita que se usaban en cada sucursal, ya con el nuevo equipo instalado brindó la oportunidad de configurarlo para dos redes y así poder reducir considerablemente el gasto de internet en la cuenta maestra de la empresa.

Cada una de las sucursales cuenta actualmente con dos redes inalámbricas, una para el personal de tersa que va a la sucursal y otro para los clientes que requieran acceso a internet para consultas básicas, el cual fueron asignados usuarios para ingresar a cada una de las redes, con un nivel de seguridad que ofrece la encriptación WPA2. Otro aporte fundamental en la estructura de la red fué el homologar el direccionamiento de IP en cada una de las sucursales para que así fuera más práctico de administrar para el departamento de sistemas. Dicho direccionamiento se colocó por subredes a cada una de las sucursales, el cual podrán ser entrar vía remota o simplemente comunicarse por el mensajero interno.

Se considera que el impacto del presente trabajo fue muy significativo para la empresa, tanto en la forma de trabajo y en la manera el flujo de la información. Aunado a esto la reducción de gasto en los servicios de internet y sin duda la base o medio de comunicación que servirá como camino para mandar información de nuevas aplicaciones o mejorar el tráfico actual.

6.2. Recomendaciones y trabajo futuro.

La tecnología VPN está en constante cambio y evolución en base a lo que ofrece Internet, debido a esto la empresa Tecnicentro Royal, S.A. de C.V. debe continuar en búsqueda de mejorar y ajustar la infraestructura de red del momento. Con la plena intención de mejorar los medios y canales de transmisión de los datos y así poder competir ante los retos del momento.

Hoy en día existen servicios que en un futuro muy cercano ofrecerán semejanzas al manejar la tecnología VPN, como es los servicios en la nube, sitios remotos de hospedaje de información, alta disponibilidad de la información entre otros buenos servicios que se pueden complementar con lo actual, y poder hacer una mezcla sin necesidad de quedar rezagados y llevar en cualquier lugar la información de la empresa para la toma de decisiones.

Dentro del panorama de los equipos Checkpoint que fueron implementados, está el de poder contar con equipos propios en un futuro o en la terminación del contrato por arrendamiento que se tiene en la actualidad por 3 años con el proveedor de Uni-Red. El cual conlleva la renegociación de contrato una vez finalizado y la consideración de buscar en un plazo de 6 años otra solución que incremente la conectividad y la movilidad de la información.

El mantener actualizada la documentación de la infraestructura de red, lleva a mejorar la administración y resolución de posibles fallos que surjan. Es necesario llevarlos al día e integrar los parámetros de medición constante que ayude a mantener estable la conexión de red.

Bibliografía

Aguado, J. y Nivon, C. (n.d.). *VPN de Capa tres para PYMES – Propuesta de mejora para el canal 22. Recuperado el 31 de marzo de 2013 de* *http://admin.udla.mx/mrs/index.php?option=com_content&view=article&id=127%3Aarticulo-127&catid=15%3Acattec&lang=es*

Alonso, J. (2006). *Redes Privadas Virtuales*. México. Alfaomega RA-MA.

Araya, S., Carvajal, C. y Llico, A. (n.d.). *Utilización y Aplicación de Túneles IPSec en ambiente de VPN Empresarial. Proyecto de Redes, ELO-332*. Recuperado el 07 de abril de 2013 http://profesores.elo.utfsm.cl/~agv/elo322/1s10/project/reports/Utilizacion%20y%20Aplicacion%20de%20Tuneles%20IPsec%20en%20ambiente%20de%20VPN%20empresarial.pdf

Ariganello, E. (2009). *Redes Cisco: Guía de estudio para certificación CCNA640-802*. México. Alfaomega RA-MA.

Briceño, P. (1996). *Administración y Dirección de proyectos*. Chile. McGraw Hill, 2da. Edición

Cabezas, L. y González, L. (2010). *Redes inalámbricas*. México. Anaya multimedia.

Carballar, J. (2004). *Wi-Fi. Cómo construir una red inalámbrica*. Alfaomega RA-MA.

Ford, M. y Kim, L. (1998) *Tecnologías de interconectividad de redes*. Prentice Hall

Forouzan, B. (2002). Transmisión de datos y redes de computadora. Mc Graw Hill, 2da Edición.

García, A. (2008). *Redes Wi-Fi.* México. Anaya multimedia.

Glifer, N. y Olifer, V. (2009). *Redes de Computadoras*. McGraw Hill, 1era. Edición.

Gómez, J. (2008).*Guía de Campo Wi-Fi.* Alfaomega. 1era edición.

Huidobro, J. y Roldan, D. (2004). *Redes y servicios de banda ancha*. McGraw Hill.

López, A. y Novo, A. (2000). *Protocolo de Internet: Diseño e implementación en sistemas Unix.* Alfaomega.

Raya, J. y Raya, C. (1997).*Redes locales y TCP/IP*. Alfaomega.

Reid, N. y Seide, R. (2005).*Manual de Redes Inalámbricas*. McGrawl Hill

Rodriguez, J., García, J. y Lamarca, I. (2007). *Gestión de proyectos informáticos métodos, herramientas y casos.* UOC, 1ra. Edición

Roldán, D. (2004). *Comunicaciones inalámbricas. Un enfoque aplicado*. Ra-Ma.

Schawartz, M (1994) *Redes de telecomunicaciones. Protocolos, Modelado y análisis*. Addison Wesley.

ST-Pierre, A. y Stephano, W. (2005*). Redes Locales e Internet. Introducción a la comunicación de datos.* Trillas, 2da edición.

Stalling, W. (2000) *Comunicación y redes de computadora*. Pearson Educación.

Stallings, W. (2005). *Fundamentos de seguridad en redes: Aplicaciones y estándares*. Prentice Hall, 2da Edición.

Tanenbaum, A. (1997) *Redes de computadora*. Pearson Educación.

Tittel,E.(2004). *Redes de Computadora. McGraw Hill*, 1da. Edición

Trujillo, E. (2006) *Diseño e implementación de una VPN en una empresa comercializadora utilizando IPSec*. Quito. Recuperado el 13 febrero de 2013 de http://bibdigital.epn.edu.ec/bitstream/15000/214/1/CD-0210.pdf