OBJETIVO

OBJETIVO

Objetivo General

Con base en los conocimientos adquiridos, diseñar un servidor VPN en el Laboratorio de Redes y Seguridad.

Objetivos Particulares

- Una vez diseñado, implementar mecanismos de seguridad en dicho servidor.
- Además, contar con una herramienta de seguridad para el laboratorio, que permita una mayor protección lógica de los equipos.
- Que el alumno tenga conocimientos de cómo proteger un servidor VPN, que alimente más sus conocimientos de seguridad informática, que sepa qué requerimientos se necesitan para poder proteger un conjunto de equipos de cómputo en un área específica.

INTRODUCCIÓN

INTRODUCCIÓN

Hace algunos años, poder comunicarse con otra persona era un hecho muy difícil de lograr, ¿Qué se podría decir de comunicarse desde una empresa a cualquier lugar?, eso era imposible para esos tiempos. Hoy en día los avances tecnológicos están dando pasos agigantados y la comunicación entre computadoras se ha hecho cada vez más fácil y rápida.

Mencionando un poco de historia, con la llegada del internet se facilitaron algunas actividades para las empresas, sin embargo, existía la problemática que no cualquiera podía tener acceso a ella. Las empresas necesitaban tener comunicación con otras corporaciones y para poder tener acceso a sus datos les era indispensable comprar costosos equipos para tener una conexión. A medida que ha pasado el tiempo, las corporaciones han requerido que las redes de área local trasciendan más allá de la cobertura local para incluir al personal y a los centros de información ubicados en otros edificios, ciudades, estados e incluso también otros países.

Una VPN (Virtual Private Network) es una estructura de red corporativa implantada sobre una red de transmisión y comunicación ante el público en general que tenga permisos de uso del servicio, básicamente es una red remota que se conecta en forma segura para evitar una conexión insegura como puede ser el Internet. Se usan algoritmos de cifrado y claves, ya que ofrecen seguridad sobre los datos que se transmiten en la red, pues se crea un túnel cifrado entre los puntos que participan en la comunicación y sólo los clientes autorizados pueden acceder a él.

Las ventajas que tiene el usuario al contar con una VPN son la seguridad, la integridad, el menor costo, mejor administración y la facilidad de transferencia

de archivos de un equipo a otro sin necesidad de estar en la misma empresa y con la garantía de contar con un respaldo íntegro de información.

La seguridad brinda un mejor cifrado y encapsulación de datos que viajan codificados a través de un túnel. Los costos de una VPN son muy bajos en su implementación y diseño, no se necesitan grandes sumas de dinero para comprar líneas dedicadas o enlaces físicos de muy altos costos. Las VPN's principalmente brindan autenticidad, autorización, integridad y confidencialidad.

Para contar con estas ventajas se configuran los mecanismos de seguridad de un servidor VPN en Linux en el laboratorio de redes y seguridad, y posteriormente se verifica la identidad de los usuarios para acceder al sistema del servicio de Internet, esto último se hace por medio de las contraseñas para implementar un control de acceso y la autenticación de cada usuario.

Dependiendo del usuario, éste tendrá ciertos permisos para acceder al sistema o servicio de Internet que se esté manejando en el laboratorio de redes y seguridad; la principal idea es contar con un mecanismo de seguridad en el servidor VPN para evitar un sabotaje o robo de información.