UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN

REDES PRIVADAS VIRTUALES EN INSTITUCIONES EDUCATIVAS CASO DE ESTUDIO: "FACULTAD DE MEDICINA-UNAM"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

PRESENTA:
MAURICIO PILAR DÍAZ

MÉXICO, D. F. 2005

AGRADECIMIENTOS

En primer lugar a Dios por darme la oportunidad de vivir y convertir este sueño en realidad.

A mis padres, por su cariño, su compresión, su apoyo y los valores que me han dado.

A mis hermanos, por estar siempre ahí, por su cariño y amistad.

A Yadira, por su apoyo y amor incondicional; por demostrarme que la perseverancia y las ganas de vivir son lo único que nos puede llevar al triunfo sobre las adversidades.

A Gladis, Rodolfo y Francisco por el apoyo en los momentos difíciles y su compañía en eso grandes y gratos momentos, por compartir conmigo sus experiencias y sobre todo, por su amistad.

A la familia Silva López, por el ánimo y apoyo en todo momento, por sus consejos y sus enseñanzas.

A los pocos, pero grandes amigos, gracias por su apoyo y amistad.

La amistad es un alma que habita en dos cuerpos; un corazón que habita en dos almas.

Aristóteles

Todas las batallas en la vida sirven para enseñarnos algo, incluso aquellas que perdemos.

Paulo Coelho

RESUMEN

A continuación se describe de manera general el contenido de cada uno de los cinco capítulos del presente trabajo:

El capítulo número uno tiene como título "Antecedentes"; Describe la misión, visión, recursos tecnológicos e infraestructura de telecomunicaciones de la Facultad de Medicina de la UNAM, además, proporciona un panorama de la estructura organizacional de la Secretaría de Educación Médica ubicada dentro de la misma Facultad y para la cual se ha diseñado este proyecto.

El capítulo número dos tiene como título "Fundamentos de Redes Privadas Virtuales"; éste proporciona una visión general de las Redes Privadas Virtuales, es decir, contiene el concepto, los diferentes tipos existentes, los requerimientos básicos para la implementación y los beneficios de las Redes Privadas Virtuales. También contiene información de túneles y protocolos, seguridad, administración y calidad de servicio de las VPN.

El capítulo número tres tiene como título "Alternativas de implementación para una VPN"; éste refiere información de las actuales condiciones del mercado de los principales proveedores de servicio del país; También, proporciona un panorama general de las diferentes plataformas en donde pueden ser implementadas las VPN.

El capítulo número cuatro tiene como título "Caso de estudio, implementación de la red privada virtual"; éste refiere información del plan de trabajo, situación futura, niveles de servicio, modelo conceptual de la red, ahorros y beneficios obtenidos con la implementación de la VPN.

El capítulo número cinco tiene como título "Monitoreo de la VPN"; proporciona información de diversos aspectos que pueden ser observados y de los cuales se puede recolectar información con la finalidad de saber con anticipación sobre posibles caídas del sistema, tiempos de respuesta y otros elementos que resultan de gran importancia para el administrador; también se menciona en concreto cuales son las funciones del equipo de tecnologías de información de la Secretaría de Educación Médica encargado del monitoreo de la VPN.

Finalmente, se encuentran las conclusiones del presente trabajo.

OBJETIVOS DEL PROYECTO.

- Identificar y evaluar la situación actual de la red de comunicaciones de la Secretaría de Educación Médica (SEM).

- Proponer el modelo conceptual para la Red Privada Virtual de la SEM y los sitios de instituciones hospitalarios.

- Proponer los requisitos mínimos de niveles de servicio que deberán cumplir los proveedores para el adecuado funcionamiento de la red.

- Realizar un análisis comparativo entre una Red Privada Virtual sobre Frame Relay, ATM[1] y una Red Privada Virtual basada en los protocolos IP[2] y MPLS[3] (Conmutación de Etiquetas Multiprotocolo).

- Determinar la viabilidad económica de la implementación de una tecnología u otra.

- Beneficios.

[1] Asyncronous Transfer Mode.
[2] Internet Protocol.
[3] Multiprotocol Label Switching.

INTRODUCCIÓN.

La comunicación ha sido siempre uno de los grandes retos de la humanidad.
La necesidad de intercambiar ideas se ha dado desde tiempos remotos y más recientemente la necesidad de comunicarse ha grandes distancias ha dado paso al nacimiento de las telecomunicaciones.

Desde el inicio del siglo XX la comunicación ha ido en constante evolución debido a lo que esto significa para el hombre. A partir de los años 50's con la introducción de la computadora en el mundo de los negocios, ha habido grandes desarrollos en el campo de las telecomunicaciones.

La introducción de las computadoras personales revolucionó la comunicación tradicional y las redes de computadoras. Conforme el sector de negocios se dio cuenta de la flexibilidad y poder de éstas, se incrementó de manera explosiva su uso. Las redes de computadoras de área local evolucionaron primeramente para disminuir el costo de dispositivos tales como impresoras de alta velocidad o discos duros de gran capacidad de almacenamiento.

Inmediatamente después se reconoció la importancia estratégica de interconectar estas redes, y las corporaciones e instituciones empezaron a interconectar redes de área local antes aisladas. Esto les proporcionó bases para aplicaciones a escala nacional y mundial tales como correo electrónico, transferencia de archivos y acceso remoto a redes corporativas, incrementando de esta manera su productividad y competitividad.

A partir de los años 90's surge el concepto de interconexión e interoperabilidad de redes de computadoras (Internetworking). Esto es, redes de área local, redes públicas de datos, líneas privadas y canales de mainframes, todos siendo usados para lograr una integración y consistencia de intercambio de información de manera transparente sin importar el patrón de tráfico que se esté usando.

La tecnología clave fue la obtención, procesamiento y distribución de la información. Además, hoy día las empresas e instituciones comienzan a darse cuenta de que necesitan sistemas de seguridad en redes o ante ataques de intrusos.
Como podemos observar a medida que los avances en las telecomunicaciones digitales acortan el tiempo y las distancias, se está gestando un nuevo modelo de puesto de trabajo. La oficina moderna ya no esta dentro de una estructura, si no que es móvil y esta geográficamente dispersa, y el puesto de trabajo del siglo XXI será cualquier sitio en el que se pueda trabajar.

Es por esto, que cada vez son más las empresas de negocios e instituciones educativas que necesitan proporcionar acceso a sus servicios de red privados desde diferentes localidades, oficinas remotas y usuarios móviles, así como extender estos servicios a los clientes y colaboradores.

Sin embargo, no todas las empresas e instituciones cuentan con la infraestructura ni con los recursos necesarios para enlazar dichos servicios con lo que ven limitado su crecimiento y desarrollo.

Como ejemplo, actualmente en la Faculta de Medicina de la UNAM, existe la necesidad de proporcionar acceso a servicios de red privados desde diferentes localidades y a usuarios móviles, además, se desea crear nuevos servicios y extender los mismos a colaboradores y alumnos; sin embargo, he aquí un caso en el que no se tienen los recursos e infraestructura necesaria para extender dichos servicios, es por ello y con la finalidad de cubrir dichas necesidades la Secretaría de Educación Médica, ubicada en el tercer piso del edificio B de la Facultad de Medicina, propone como posible solución a las Redes Privadas Virtuales, tema del presente trabajo.

INDICE

CAPÍTULO 1.

ANTECEDENTES.

Este capítulo nos proporciona una descripción general de las necesidades de la Facultad de Medicina, específicamente de la Secretaría de Educación Médica; nos provee de información de las funciones de las áreas que conforman a la Secretaría, y podemos ver en el organigrama de la Secretaría como están ubicadas todas y cada una de ellas.

También nos ofrece información de los servicios que se desean implantar y el por qué y quiénes son los usuarios de dichos servicios.

Además, en éste mismo capítulo podemos observar cuál es la infraestructura actual de telecomunicaciones de la Facultad de Medicina en un esquema que también proporciona información de aspectos importantes como la velocidad, los diferentes medios de transmisión utilizados, los dispositivos de interconexión usados, etc.

ANTECEDENTES.

La educación es parte fundamental en el desarrollo de los países y las exigencias en ella son cada vez mayores debido al mundo globalizado en el que estamos viviendo.

Los modelos educativos dentro de nuestro país no satisfacen las necesidades de nuestra sociedad debido a que estos provienen de países europeos o de los países de América del norte.

Además de estos y muchos otros aspectos que no mencionaré por no ser el tema principal de este trabajo, dentro de la Universidad Nacional Autónoma de México con la finalidad de ofrecer información clara, confiable y oportuna que permita una mejor preparación de estudiantes, académicos, investigadores y demás gente que día a día se está preparando en la institución existe la necesidad y preocupación por aprovechar los constantes cambios y avances tecnológicos que se van presentando.

Tal es el caso particular que se presenta dentro de la Facultad de Medicina, en donde la gente que aquí se forma debe salir preparada para responder a las necesidades de nuestra sociedad.
Tenemos muy claro que no se puede perder esa parte humana que sensibiliza y concientiza a los médicos que de esta facultad egresan, sin embargo, también tenemos la obligación de proporcionar las herramientas que faciliten y mejoren de alguna manera su aprendizaje. Para ello, se ha decidido hacer uso de las tecnologías de información (TI) y servicios de telecomunicaciones con los que actualmente se cuenta.

Muchos de los alumnos de la Facultad de Medicina se encuentran en sedes hospitalarias dentro de la ciudad de México, muchos otros en ciudades de provincia y algunos más en zonas rurales en donde el acceso a la información es mucho más difícil, casi imposible. También, se cuenta con investigadores, académicos y maestros que tratan de generar mayor conocimiento y de la divulgación del mismo. Muchos de ellos se encuentran dentro de la Facultad de Medicina, sin embargo, algunos otros se encuentran en diversas ciudades del país y generalmente se encuentran en constante movimiento.
Con el objetivo de proporcionar y facilitar el acceso a la información que se encuentra dentro de la Facultad de Medicina y de la Universidad misma, en la SEM ubicada

dentro de la Facultad de Medicina se ha diseñado un esquema de comunicación que proporcione y de la posibilidad de contar con información confiable y oportuna desde diferentes puntos de ubicación por parte de alumnos, académicos, investigadores y maestros que así lo requieran.

Iniciaré por mencionar cuales son los principales servicios y aplicaciones tecnológicas que se desean implementar dentro de la SEM.

- ✓ Videoconferencia con diferentes sedes hospitalarias.
- ✓ E-Learning.
- ✓ Consultas a bases de datos.
- ✓ Transferencia de archivos.
- ✓ Impresión remota.
- ✓ Acceso de usuarios móviles a la información.
- ✓ Correo electrónico.

Para poder comprender mejor el funcionamiento y objetivos de la SEM comenzaré por mencionar de forma breve la misión de la Facultad de Medicina y explicaré brevemente como está conformada y las funciones de las diferentes áreas de la Secretaría, además, mostraré el organigrama de la misma.

1.1 MISIÓN Y VISIÓN DE LA FACULTAD DE MEDICINA.

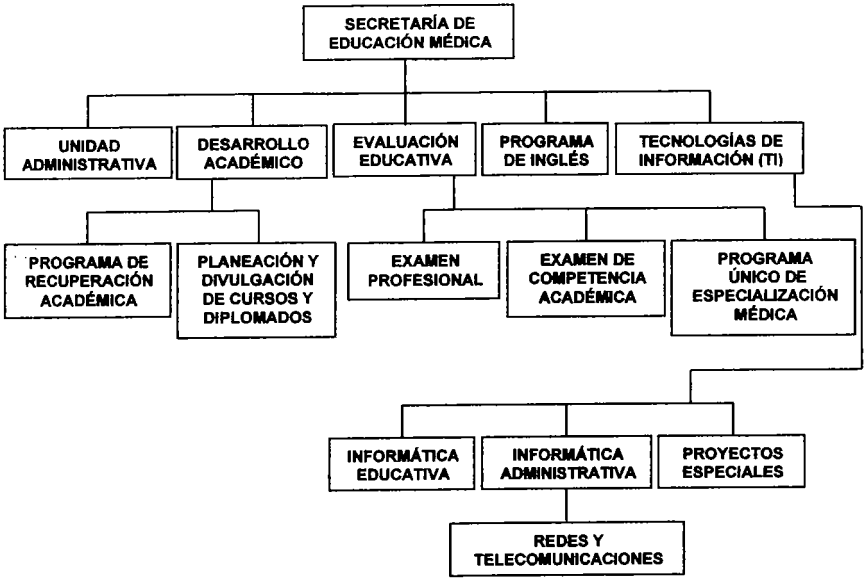
La Facultad de Medicina, en cuanto a institución, aspira a:

Formar a los líderes de las próximas generaciones de médicos mexicanos y contribuir a establecer un sistema de salud capaz de preservar y desarrollar las capacidades físicas y mentales de nuestra población y colaborar en la preparación de investigadores en el campo de las ciencias médicas.
La educación y la formación médica en la Facultad deberán ser factores de cambio e innovación en las instituciones de salud y contribuir a incrementar las aportaciones de la medicina mexicana al conocimiento universal.
La Secretaría de Educación Médica es el órgano encargado de generar cursos, divulgación de los mismos, planes de estudio, estrategias de aprendizaje, exámenes

departamentales, profesionales, de competencia académica, de especialización, etc.; realizar investigaciones en educación médica, métodos de enseñanza, estilos de aprendizaje, métodos de evaluación, etc.; llevar a cabo la evaluación de exámenes, publicación de resultados, planes de recuperación académica, enseñanza del idioma inglés, entre otros; es decir, la SEM es la encargada de apoyar en aspectos de docencia e investigación educativa a todas las áreas de la Facultad de Medicina.

La misión de la Secretaría de Educación Médica, apoyar en aspectos de docencia, investigación, generación de estrategias de evaluación, generación de estrategias que faciliten el proceso enseñanza aprendizaje a las diferentes áreas que conforman a la Facultad de Medicina.

1.2 ORGANIGRAMA DE LA SECRETARÍA DE EDUCACIÓN MÉDICA.



A continuación menciono las actividades de cada una de las áreas observadas en el organigrama y explico cuál es su función principal, todo ello con la finalidad de comprender cuales son las necesidades de cada una de estas.

- Departamento de Desarrollo Académico.

Este departamento se encarga de diseñar, planear, desarrollar y divulgar cursos, talleres y diplomados de actualización y formación docente para alumnos y profesores de la Facultad de Medicina. Algunos de ellos son impartidos fuera de la Facultad por lo que actualmente se esta diseñando un esquema de cursos y diplomados a distancia. También cuenta con un área que se encarga de la recuperación académica y titulación en donde se apoya a alumnos que son suspendidos en el examen profesional. Se encarga de lo que se conoce dentro de la Facultad como Asignaturas de Libre Elección llevando el control de las asignaturas registradas y las asignaturas vigentes. También se lleva a cabo la difusión de la educación médica en diferentes medios impresos y electrónicos.

- Departamento de Evaluación Educativa.

En este departamento se lleva a cabo el diseño y elaboración de los diferentes exámenes realizados por parte de la Facultad de Medicina durante el año; algunos de estos son: examen profesional, examen para los alumnos de primer ingreso, examen de competencia académica y exámenes departamentales del plan único de especializaciones médicas. También se lleva a cabo la evaluación de la enseñanza mediante cuestionarios de opinión a los alumnos. Además se realizan las evaluaciones de los mismos exámenes y la publicación y entrega de resultados para los alumnos. Cuenta con un área encargada del análisis de los resultados de los diferentes exámenes los cuales proporciona al Departamento de Desarrollo Académico para que éste se apoye en ellos en la elaboración de contenidos de sus diferentes cursos, talleres y diplomados ofrecidos a los alumnos de la Facultad. Es importante mencionar que existen diferentes sedes en donde se realizan exámenes además de la misma Facultad como son escuelas en los estados de Veracruz, Tabasco, Querétaro, y otras escuelas incorporadas dentro del Distrito Federal, por lo que también se deben entregar resultados a las diferentes instituciones educativas en tiempo y forma pactados.

- Programa de Inglés.

Permite a los alumnos de pregrado y posgrado de la Facultad de Medicina, la posibilidad de incorporar el idioma inglés a su formación profesional, como herramienta

fundamental en la medicina moderna, logrando la comprensión de la lectura y/o el manejo del idioma en su modalidad de posesión.

- Unidad Administrativa.

La administración se encarga de realizar todas aquellas operaciones que tienen que ver con trámites que como su nombre lo indica son meramente administrativos como la adquisición de recursos tecnológicos, económicos y humanos y la distribución y asignación de los mismos. Es importante resaltar que muchas decisiones no dependen solamente de ésta unidad si no de ella en conjunto con otros órganos de la Facultad.

- Departamento de Tecnologías de Información.

Este departamento tradicionalmente proporcionaba servicios de cómputo básicos, es decir apoyo a usuarios, mantenimiento a equipos de cómputo tanto en software como hardware, apoyo en procesos administrativos y de estadística, etc.
Actualmente esta área ha sufrido una reestructuración que ha modificado la forma de trabajar y las actividades que se deben realizar. Hoy, las actividades de la Secretaría se basan en gran medida en las acciones realizadas por este departamento.
En este momento, se están desarrollando programas y planes de trabajo para satisfacer las necesidades de todas y cada una de las áreas que conforman a la SEM y que se han mencionado con anterioridad.

No explicaré todas y cada una de las acciones que se están realizando dentro del departamento de Tecnologías de Información de la SEM, sin embargo, si mencionaré que para poder implementar algunas de ellas es necesario una plataforma o tecnología de comunicación que permita ofrecer todos los servicios y aplicaciones mencionados anteriormente con el fin de satisfacer por lo menos las necesidades básicas de cada área.

Hasta el momento, se ha mencionado de forma general algunos servicios que se desean implementar dentro de la SEM y las funciones principales de cada área que la conforman. Ahora, continuaré por explicar con un poco más de detalle dichos servicios y las necesidades básicas de cada área.

- ✓ Videoconferencia con diferentes sedes hospitalarias.

Este servicio se ha propuesto con la finalidad de ofrecer sesiones informativas, clases de diferentes materias médicas, diplomados, discusiones de diversos casos clínicos, entre otros, entre la Facultad de Medicina y sedes hospitalarias con las que se tengan convenios. Básicamente se apoya al departamento de Desarrollo Académico en la impartición de cursos, talleres y diplomados, pero se ha planeado que una vez que se encuentre disponible el servicio se apoyará a otras áreas que tengan necesidades similares.

- ✓ Acceso de usuarios móviles a la información.

La implementación de este servicio se debe básicamente al apoyo solicitado por parte de académicos e investigadores en la parte de acceso y búsqueda de información en bases de datos que se encuentra dentro de la SEM o dentro de la Universidad y que no se puede consultar fuera de las instalaciones.

Además, se ha detectado que será de gran utilidad para médicos que constantemente se encuentran viajando y de los cuales se tiene una alta interoperabilidad e interdependencia por ser en su mayoría jefes de departamento y jefes de Secretarías.

- ✓ E-Learning.

Por la preocupación que se tiene de preparar cada vez mejor a los estudiantes de la Facultad sin importar que estos se encuentren fuera de la misma, se ha diseñado el servicio de educación a distancia.
Con este servicio se apoyará de forma directa en una fase inicial a algunos médicos residentes que se encuentran en el estado de Campeche. Sin embargo se tiene planeado que en fases posteriores apoye al Departamento de Evaluación Educativa en la preparación de alumnos para presentar los diferentes exámenes que ellos diseñan y por otra parte se apoye a los Departamentos de Desarrollo Académico e inglés en sus diversas actividades.

- ✓ Impresión remota.

La impresión remota es un servicio que se proporcionará sólo a jefes de departamento y al jefe de la SEM con la finalidad de apoyarlos en la generación urgente de informes y reportes. En este caso se ha puesto especial atención y preferencia al jefe de la Unidad Administrativa por tener una frecuencia alta en la generación de reportes.

- ✓ Correo electrónico.

El correo electrónico es un servicio que será proporcionado a todos y cada uno de los médicos, académicos e investigadores que conforman a la SEM.

- ✓ Consultas a bases de datos.

Este servicio se ha generado especialmente para satisfacer las necesidades del departamento de Evaluación Académica para que el personal que lo conforma pueda contar con información confiable y oportuna generada de los resultados de los diferentes exámenes aplicados durante el año.

- ✓ Transferencia de archivos.

Con este servicio se busca que tanto las sedes con las que se tengan convenios, usuarios que se encuentren en distintas ubicaciones y usuarios ubicados dentro de la Facultad de Medicina, cuenten si así lo requieren, con la misma información y que constantemente se encuentren en un estado de intercambio de lo misma, además de asegurar confiabilidad y oportunidad.

Es importante mencionar que se requiere de una asegurada calidad en el servicio y que ésta debe de basarse en lo crítica que sea cada una de las aplicaciones que se montaran sobre la red siendo actualmente la videoconferencia la de mayor importancia seguida por el servicio de E-Learning. A continuación se encuentra una lista de las diferentes aplicaciones que se necesita correr siendo la primera la de mayor importancia y la última la menos crítica excluyendo de ella las dos que ya mencionamos:

- ✓ Consulta a bases de datos.
- ✓ Transferencia de archivos.

- ✓ Impresión remota.
- ✓ Acceso de usuarios móviles a la información.
- ✓ Correo electrónico.

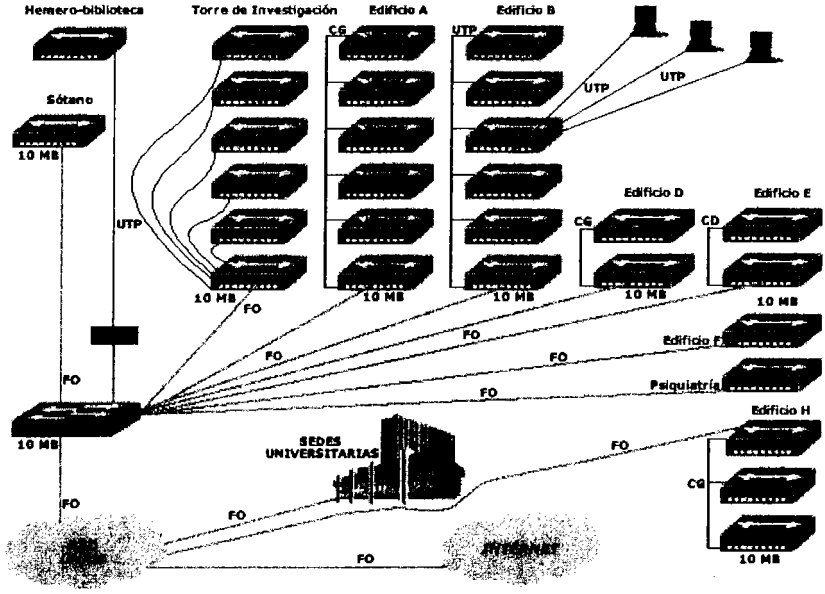
Otro aspecto importante a considerarse en el diseño, planeación e implementación de una solución que cumpla con las necesidades mencionadas por parte de la SEM es el referente a la seguridad. La seguridad es un componente fundamental en cualquier institución, pues todos los usuarios tienen acceso y todos los procesos corren en la red. Toda la infraestructura de red, comenzando por ruteadores, switches, PC's y servidores, deben de estar protegidos auxiliándose por equipos especializados en seguridad como Firewalls, herramientas de detección de intrusos y software para el control de identidad. Por el tipo de aplicaciones que se desean correr sobre la red es primordial asegurar el funcionamiento de la misma y de sus servicios las 24 horas del día los 365 días del año.

1.3 RECURSOS TECNOLÓGICOS E INFRAESTRUCTURA.

Hasta este momento, he mencionado y explicado cuáles son las necesidades de las áreas que conforman a la SEM, cuáles son los servicios que se requieren implementar para satisfacer dichas necesidades, quiénes son los usuarios de dichos servicios y que éstos deben asegurar de alguna forma ciertos parámetros de calidad y seguridad. Ahora es momento entonces de mencionar con que recursos tecnológicos e infraestructura de red se cuenta dentro de la SEM y en general dentro de la Facultad de Medicina.

Iniciaré por mostrar la infraestructura actual de telecomunicaciones de la Facultad de Medicina para tener un panorama muy claro de aspectos tales como velocidad de transmisión, cómo es que tenemos acceso a Internet, cuál es la tecnología usada, cuáles son los diferentes medios de transmisión usados en los diferentes edificios que conforman a la Facultad y en las verticales de los mismos, cuáles son las políticas de seguridad, cuáles son las políticas de calidad de servicio, cuáles son y quién o quiénes proporcionan los diferentes servicios existentes en la actualidad dentro de la Facultad de Medicina.

INFRAESTRUCTURA DE TELECOMUNICACIONES DE LA FACULTAD DE MEDICINA.



En el esquema anterior se puede observar que logramos salir a la red de Internet por medio de RED – UNAM conectándonos a ella a través de un switch que se encuentra ubicado en el área de cómputo de la Facultad de Medicina al cual están conectados los diferentes edificios que conforman a la Facultad utilizando como medio de transmisión fibra óptica.

Sin embargo, observemos que la velocidad de transmisión no es mayor a 10 MB/S debido a que los dispositivos con los que se cuenta no tienen la capacidad de transmitir información a velocidades más altas, además, notemos que las verticales de los diferentes edificios son de diferentes medios de transmisión.

Como ya he mencionado, un aspecto de vital importancia para toda institución es la parte que tiene que ver con la seguridad y en el esquema anterior se puede observar que actualmente dentro de la infraestructura de telecomunicaciones de la Facultad de

Medicina no se cuenta con ningún firewall ni con ningún otro dispositivo o medio que pueda proporcionar algún tipo de seguridad.

Otros hallazgos encontrados de la actual situación son:

- ✓ Obsolescencia del equipo existente.
- ✓ No se cuenta con contratos de mantenimiento preventivo para la infraestructura de la red.
- ✓ El equipo de soporte técnico es insuficiente.
- ✓ Existe fuerte saturación de la red.
- ✓ Existe riesgo de degradación del servicio de las Redes LAN[1].
- ✓ No se cuenta con mecanismos de seguridad de acceso adecuados en los sitios centrales de comunicación.

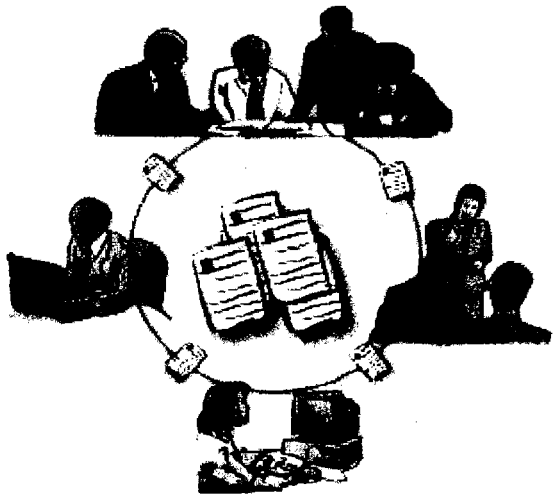
La SEM se encuentra ubicada en el edificio B en el tercer piso. Se puede observar en el esquema anterior que el medio de transmisión de la vertical del edificio es cable par trenzado sin blindaje (UTP)[2], en dicho esquema no se especifica pero se nos informó que el cable es de categoría 5 y también se sabe que los dispositivos de interconexión que aquí se encuentran son básicamente hubs.

Una vez que se han mencionado las necesidades de la SEM, los usuarios de dichos servicios y la infraestructura tecnológica con que se cuenta es momento de mencionar que es necesario una plataforma o tecnología de comunicación que se adapte a la infraestructura ya existente que permita ofrecer todos los servicios y aplicaciones mencionados anteriormente para ello tenemos a las Redes Privadas Virtuales.

[1] Local Area Network.
[2] Unshielded Twisted Pair.

CAPÍTULO 2.

FUNDAMENTOS DE REDES PRIVADAS VIRTUALES (VPN)[3].



[3] Virtual Private Network.

Este capítulo define las VPN y describe los diferentes tipos de VPN existentes. Además nos proporciona una clara descripción sobre cuales son los requerimientos básicos para la implementación de una VPN y cuales son las ventajas que se pueden tener al elegir una VPN como solución a nuestros problemas de comunicación. También nos ayuda a conocer aspectos de seguridad, calidad de servicio, compatibilidad y administración de las VPN.

Este capítulo aborda los siguientes temas:

- ✓ Definición y visión general de las VPN.
- ✓ Tipos de VPN.
- ✓ Requerimientos básicos de una VPN.
- ✓ Beneficios de las VPN.
- ✓ Aspectos básicos de túnel.
- ✓ Tipos de túnel.
- ✓ Algoritmos y protocolos de cifrado.
- ✓ Métodos y protocolos de autenticación.
- ✓ Seguridad del protocolo Internet (IPSec)[4].
- ✓ Firewalls.
- ✓ Concepto y aspectos básicos de la administración de redes de computadoras.
- ✓ Modelo de administración de red de la ISO[5].
- ✓ Administración de las VPN.
- ✓ Concepto y aspectos básicos de la calidad de servicio.
- ✓ Tipos de tecnologías que brindan calidad de servicio.
- ✓ Limitaciones dentro de la calidad de servicio.

[4] Internet Protocol Security.
[5] International Standard Organization.

2.1 VISIÓN GENERAL DE LAS VPN Y LAS TECNOLOGÍAS VPN.

Las VPN proporcionan un canal de comunicaciones seguro entre computadoras que utilizan una red pública como red intermedia. Las VPN permiten a los usuarios u organizaciones conectarse a servidores remotos, redes y servidores de otras sucursales y redes de otras compañías sobre una red pública, mientras mantienen la seguridad de sus comunicaciones. El usuario percibe una comunicación segura como la que existe en una red privada sin tener en cuenta el hecho de que la comunicación está teniendo lugar a través de una red pública.

Las VPN emplean mecanismos de encriptación y autenticación que han demostrado gran robustez desde hace algunos años. Además, la VPN tiene la capacidad de crear un túnel entre dos puntos finales, brindando protección a los paquetes que están atravesando Internet.

Cabe señalar, que una VPN no sólo sirve como medio de acceso remoto, si no también, como un sistema de control para definir grupos de trabajo y controlar el acceso a datos confidenciales.

Actualmente, las VPN tienen gran aceptación y están ampliamente implementadas entre compañías que ofrecen a sus usuarios una conexión segura a sus servidores a través de Internet. Al establecer este tipo de soluciones, las VPN permiten que las compañías cambien la inversión que realizaban en la compra de sistemas de acceso remoto que utilizaban para soportar el acceso directo de usuarios vía modem.

2.1.1 ¿Qué es una VPN?

Una VPN es un servicio que ofrece conectividad segura y fiable sobre una infraestructura de red pública compartida, como Internet.

Las VPN pueden tener muchas definiciones, pero básicamente se enfocan al transporte de datos privados de un corporativo o de un usuario, a través de una red pública.[6]

[6] Ing. Ricardo Domínguez, Nortel Networks de México.

Una VPN conecta una máquina de una red a una máquina de una red remota utilizando otra red intermedia como un conducto, como por ejemplo Internet, entre ellas. Este conducto se denomina canal punto a punto, o túnel, y se implementa como un circuito virtual seguro a través de la red intermedia, la cual puede no ser segura (ver figura 2.1).

El canal forma una conexión punto a punto sobre la que se envían datos cifrados.

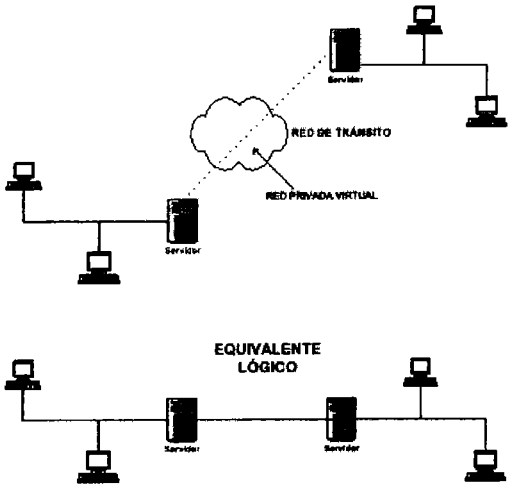


Figura 2.1

Una VPN permite a los usuarios conectarse a una red corporativa utilizando una red como Internet. Internet se convierte en una red conducto que se utiliza como un enlace punto a punto seguro entre el usuario remoto y la red corporativa. Las VPN también se pueden utilizar para configurar canales seguros a través de Internet, que permiten conectar de forma segura varias sucursales de una misma empresa.
El uso de Internet para construir VPN entre sucursales es un método muy efectivo en coste para que una compañía cree una red de área extensa. Otra alternativa es utilizar dispositivos dedicados y enlaces para construir una VPN.

En una VPN todos los usuarios parecen estar en el mismo segmento de Red de Área Local (LAN), pero en realidad están a varias redes (generalmente públicas) de distancia. Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas: primero, deben ser capaces de pasar paquetes IP a través de un

túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública; segundo, la solución debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado; y por último, la solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación, de modo que un adversario no pueda acceder a los recursos del sistema.

La tecnología de la VPN está diseñada para tratar temas relacionados con la tendencia actual de negocios hacia mayores telecomunicaciones, operaciones globales altamente distribuidas y operaciones con una alta interdependencia de socios, sin embargo, actualmente se ha encontrado una gran utilidad de ellas en instituciones educativas.

2.1.2 Tipos de VPN.

Hay tres tipos principales de VPN:

VPN de acceso. Proporciona acceso remoto a la intranet o extranet de una empresa cliente sobre una infraestructura compartida. Las VPN de acceso utilizan tecnologías analógicas, de acceso telefónico, RDSI[7], ADSL[8], IP móvil y de cable para conectar de forma segura usuarios móviles, trabajadores y sucursales.

La figura 2.2 muestra la forma en que un usuario puede conectarse a Internet mediante un ISP[9]. Internet se utiliza para crear la VPN que conecta la computadora del usuario remoto a la red corporativa.

Esta solución ahorra costes, debido a que la conexión entre el usuario y el ISP local se realiza mediante una llamada telefónica local, en lugar de una llamada de larga distancia al servidor de la red corporativa.

[7] Red Digital de Servicios Integrados.
[8] Asymetric Digital Suscriber Line.
[9] Internet Service Provider.

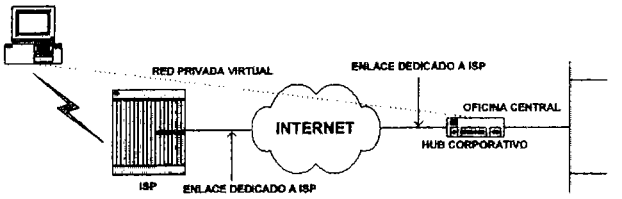


Figura 2.2

VPN de intranet. Enlazan la sede actual de una empresa, las oficinas remotas y las sucursales a una red interna sobre una infraestructura compartida usando conexiones dedicadas. Las VPN de intranet se diferencian de las VPN de extranet en que permiten el acceso sólo a los empleados de la empresa cliente.

La figura 2.3 muestra la forma de usar una VPN entre computadoras en una intranet.

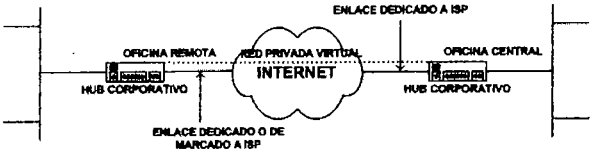


Figura 2.3

VPN de extranet. Enlazan clientes exteriores, proveedores, socios o comunidades de interés a una red de una empresa cliente sobre una infraestructura compartida usando conexiones dedicadas. Las VPN de extranet se diferencian de las VPN de intranet en que permiten el acceso a los usuarios de fuera de la empresa.

La figura 2.4 muestra como se conectan dos redes corporativas utilizando un enlace VPN.

Los servidores de las redes corporativas pueden tener enlaces dedicados a una red pública (como Internet). De forma alternativa, también pueden utilizarse los circuitos dedicados de gran capacidad, como líneas T1 o líneas contratadas.

Una ventaja de utilizar líneas dedicadas punto a punto es que aseguran calidad de servicio.

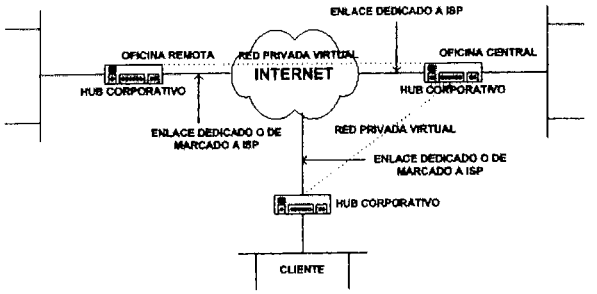


Figura 2.4

El software de la VPN que se ejecuta en los servidores de las sucursales utiliza el ISP local para crear un circuito virtual entre los servidores de las dos sucursales.
También es posible terminar una VPN en el enrutador de una de las sucursales en lugar de en los servidores. El empleo de dispositivos dedicados, como por ejemplo enrutadores, para crear VPN libera a los servidores del trabajo de cifrado y procesamiento. En este caso, los enrutadores actúan como servidores VPN para formar los dos puntos finales del canal.

Es importante tener en cuenta que los servidores de una VPN no actúan como enrutadores entre las redes corporativas. Un enrutador conecta dos redes y enruta los paquetes entre ellas. La VPN forma un circuito lógico que transmite datos cifrados entre dos puntos finales de comunicación.

La seguridad que ofrece el uso de una VPN normalmente es adecuada para la mayoría de las aplicaciones. Si los datos son tan importantes que no se pueden enviar a través de una VPN sobre Internet, se tendrá que construir una red física separada utilizando una tecnología como Frame Relay, ATM u otra parecida. Aunque una red físicamente separada puede incrementar la seguridad, pueden no estar disponibles para usuarios remotos que viajan a diferentes lugares. Además, el coste de la infraestructura es bastante elevado en comparación con una VPN.

2.1.3 Requerimientos básicos de las VPN.

Por lo general, al implementar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la misma.

La solución deberá permitir la libertad para que los clientes roaming o remotos autorizados se conecten con facilidad a los recursos corporativos de la red de área local, así como que las oficinas remotas se conecten entre sí para compartir recursos e información (conexiones de LAN a LAN).

Por último, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet público. Lo mismo se aplica en el caso de datos sensibles que viajan a través de una red corporativa. Por tanto, como mínimo, una solución de VPN debe proporcionar lo siguiente:

- ✓ **Autenticación del usuario.** La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados.

La autenticación de los usuarios es necesaria para asegurar que sólo los usuarios autorizados tienen acceso a la VPN.
Además, deberá proporcionar registros de auditoria y contables para mostrar quién accedió a qué información y cuando.

- ✓ **Administración de dirección.** La solución deberá asignar una dirección al cliente en la red privada, y asegurarse de que las direcciones privadas se mantengan así.
- ✓ **Encriptación de datos.** El cifrado de los datos es esencial para evitar que los datos que viajan por la VPN sean leídos por usuarios no autorizados. Sólo se cifran los datos, no las cabeceras de los protocolos.
- ✓ **Administración de llaves.** La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.
- ✓ **Soporte de protocolo múltiple.** La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen protocolos de Internet (IP), intercambio del paquete de la red (IPX)[10], etc.

Una solución de VPN de Internet basada en un protocolo de túnel de punto a punto (PPTP)[11] o un protocolo de túnel de nivel 2 (L2TP)[12] cumple con todos estos

[10] Internetwork Packet Exchange.
[11] Point to Point Tunneling Protocol.

requerimientos básicos, y aprovecha la amplia disponibilidad de Internet a nivel mundial.

Otras soluciones, incluido el protocolo de seguridad IP, cumplen con algunos de estos requerimientos, y siguen siendo útiles para situaciones específicas.

2.1.4 Aplicaciones que se pueden correr.

- ✓ Intercambio de información en tiempo real.
- ✓ Correo electrónico corporativo.
- ✓ Acceso remoto a la información corporativa sin importar la ubicación geográfica.
- ✓ Impresión remota.
- ✓ Transmisión encriptada de la información a través de Internet.
- ✓ Acceso mediante nombre y contraseña.

2.1.5 Beneficios de las VPN.

- ✓ Se estima que una solución de VPN puede disminuir sus costos entre 20 y 40 por ciento, en comparación con las conexiones punto a punto.
- ✓ La forma en que las VPN logran reducir costos es porque ya no existen enlaces dedicados y porque sobre la misma infraestructura se pueden ofrecer diferentes tipos de servicios; además, es totalmente compartida porque no está basada en circuitos.
- ✓ El costo de una VPN, contando su retorno de inversión, variará de acuerdo con el tipo que se quiera implementar y de lo que se tenga contemplado transportar, pero es un hecho que la alternativa de VPN es mucho más eficiente -en términos de retorno de inversión- que las redes privadas normales.
- ✓ Reducen el número de líneas de acceso en un sitio corporativo.
- ✓ No requiere inversiones en infraestructura.(en el caso de contratar el servicio a un proveedor).
- ✓ El usuario tiene la posibilidad de conectarse desde cualquier lugar.

[12] Layer 2 Tunneling Protocol.

- ✓ Se puede extender la red de comunicaciones privadas a sitios donde la infraestructura dedicada no está disponible.
- ✓ Proporciona la posibilidad de que los usuarios remotos se conecten a través de tecnologías de banda ancha, como cable módems o ADSL.

2.2 TÚNELES Y PROTOCOLOS.

A continuación se explica que es un túnel y veremos cuáles son algunos de los protocolos usados en la creación de túneles.

2.2.1 Aspectos básicos.

El enrutamiento punto a punto, o tunneling, es un método que permite enviar datos a una red utilizando una red intermedia. Los datos que se transfieren se denominan carga y los dos extremos del túnel se denominan extremos finales del túnel o del canal. El paquete que se envía se encapsula utilizando la cabecera del protocolo de enrutamiento punto a punto. Los enrutadores de las redes intermedias utilizan la cabecera del protocolo de enrutamiento punto a punto para enrutar el paquete al punto de destino final del túnel.

Los enrutadores de la red intermedia no saben que están enrutando un paquete de protocolo de enrutamiento punto a punto. Éstos tratan el paquete como uno más en la red. El paquete se origina en uno de los extremos del túnel y alcanza el otro extremo.
En el extremo final del túnel, las cabeceras de los paquetes son extraídas y el paquete es enrutado a continuación a su destino final (ver la figura 2.5).

Hay que observar que este sistema de túnel incluye todo este proceso (encapsulamiento, transmisión y desencapsulamiento de paquetes).

Aunque la red de transito en la figura 2.5 puede ser cualquier red, Internet es la solución más económica y la más utilizada como red de tránsito.

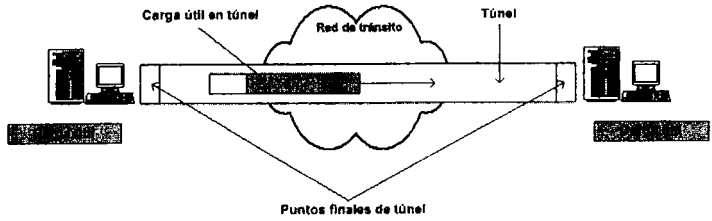


Figura 2.5

Existen muchos otros ejemplos de túneles que pueden realizarse sobre intranets corporativas. Y aunque la Internet proporciona una de las intranets más penetrantes y económicas, las referencias a Internet en este trabajo de Tesis se pueden remplazar por cualquier otra intranet pública o privada que actúe como de tránsito.

Las tecnologías de túnel existen desde hace tiempo; algunos ejemplos de tecnologías maduras incluyen:

- ✓ Túneles SNA[13] sobre intranets IP. Cuando se envía tráfico de la arquitectura de la red el sistema SNA a través de una intranet IP corporativa, la trama SNA se encapsula en un encabezado UPN[14] e IP.

- ✓ Túneles IPX para Novell NetWare sobre intranets IP. Cuando un paquete IPX se envía a un servidor NetWare o ruteador IPX, el servidor o ruteador envuelve el paquete IPX en un encabezado UDP[15] e IP, y luego lo envía a través de una Intranet IP.

El ruteador IP a IPX de destino elimina el encabezado UDP e IP, y transmite el paquete al destino IPX.

Además, se han introducido en los últimos años nuevas tecnologías de sistemas de túneles, mismas que son el enfoque principal de esta sección y que incluyen:

[13] Systems Networks Architecture.
[14] User Principal Name.
[15] User Datagram Protocol.

- ✓ Protocolo de Túnel de Punto a Punto. Permite que se encripte el tráfico IP, IPX, o NetBEUI[16], y luego se encapsule en un encabezado IP para enviase a través de una red corporativa IP o una red pública IP, como Internet.

- ✓ Protocolo de Túnel de Nivel 2. Permite que se encripte el tráfico IP, IPX, o NetBEUI, y luego se envíe sobre cualquier medio que de soporte a la entrega de datagramas punto a punto, como IP, X.25, Frame Relay o ATM.

- ✓ Modo de Túnel de Seguridad IP. Deja que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP, para enviarse a través de una red corporativa IP o una red pública IP como Internet.

2.2.2 Protocolos de túneles.

Para que se establezca un túnel, tanto el cliente de éste como el servidor deberán utilizar el mismo protocolo de túnel.

Un protocolo es un conjunto de reglas que gobiernan el formato y el significado de las tramas, paquetes o mensajes que se intercambian entre capas homólogas.

La tecnología de túnel se puede basar en el protocolo del túnel del nivel 2 o de nivel 3; estos niveles corresponden al modelo de referencia de interconexión de sistemas abiertos.

Los protocolos de nivel 2 corresponden al nivel de enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP y el envío de nivel 2 (L2F)[17] son protocolos de túnel de nivel 2; ambos encapsulan la carga útil en una trama de protocolo de punto a punto (PPP)[18] que se enviará a través de la red.
Los protocolos de nivel 3 corresponden al nivel de la red y utilizan paquetes. IP sobre IP y el modo de túnel de seguridad IP son ejemplos de los protocolos de túnel de nivel 3;

[16] NetBios Extended User Interface.
[17] Layer - 2 Forwarding.
[18] Point to Point Protocol.

éstos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos a través de una red IP.

2.2.3 Cómo funcionan los túneles.

Para las tecnologías de túnel de nivel 2 como PPTP y L2TP, un túnel es similar a una sesión; los dos puntos finales deben de estar de acuerdo respecto al túnel, y negociar las variables de la configuración, como asignación de dirección o los parámetros de encriptación o de compresión.

En la mayor parte de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas; se utiliza un protocolo para mantenimiento del túnel como el mecanismo para administrar al mismo.

Por lo general, las tecnologías del túnel de nivel 3 suponen que se han manejado fuera de banda todos los temas relacionados con la configuración, normalmente a través de procesos manuales; sin embargo, quizá no exista una fase de mantenimiento de túnel. Para los protocolos de nivel 2 (PPTP y L2TP) se debe crear, mantener y luego concluir el túnel.
Cuando se establece el túnel, es posible enviar los datos a través del mismo. El cliente o el servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para su transferencia.

Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor, primero adjunta un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la que lo enruta al servidor del túnel. Este último acepta los paquetes, elimina el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo.
La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar.

2.2.4 Los protocolos y los requerimientos básicos del túnel.

Puesto que se basan en protocolos PPP bien definidos, los protocolos de nivel 2 (como PPTP y L2TP) heredan un conjunto de funciones útiles. Como se señala más adelante, estas funciones y sus contrapartes de nivel 3 cubren los requerimientos básicos de la VPN.

Autenticación del usuario. Los protocolos de túnel nivel 2 heredan los esquemas de autenticación del usuario de PPP, incluidos los métodos del protocolo de autenticación ampliable (EAP)[19].
Muchos de los esquemas de túnel de nivel 3 suponen que los puntos finales han sido bien conocidos (y autenticados) antes de que se estableciera el túnel. Una excepción es la negociación IPSec ISAKMP[20], que proporciona una autenticación mutua de los puntos finales del túnel. (Hay que notar que la mayor parte de las implementaciones IPSec dan soporte sólo a certificados basados en equipo, más que en certificados de usuarios; como resultado, cualquier usuario con acceso a uno de los equipos de punto final puede utilizar el túnel. Se puede eliminar esta debilidad potencial de seguridad cuando se conjunta IPSec con un protocolo de nivel 2, como el L2TP.)

Soporte de tarjetas de señales. Al utilizar el protocolo de autenticación ampliable, los protocolos de túnel nivel 2 pueden ofrecer soporte a una amplia variedad de métodos de autenticación, incluidas contraseñas de una sola vez, calculadores criptográficos y tarjetas inteligentes. Los protocolos de túnel nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define la autenticación de los certificados de llaves públicas en su negociación ISAKMP/Oakley.

Asignación de dirección dinámica. El túnel de nivel 2 da soporte a la asignación dinámica de direcciones de clientes basados en un mecanismo de negociación de protocolo de control de la red. En general, los esquemas de túnel de nivel 3 suponen que ya se ha asignado una dirección antes de la iniciación del túnel. Cabe mencionar que los esquemas para la asignación de direcciones en el modo de túnel IPSec están actualmente en desarrollo, por lo que aún no están disponibles.

[19] Extended Authentication Protocol.
[20] Internet Security Association Key Management Protocol.

Compresión de datos. Los protocolos de túnel nivel 2 proporcionan soporte a esquemas de compresión basados en PPP. Por ejemplo, las implementaciones de Microsoft tanto de PPTP como L2TP utilizan Microsoft Point-to-Point Compression (MPPC). La Fuerza de Trabajo de ingeniería Internet (IETF)[21] está investigando mecanismos similares (como la compresión IP) para los protocolos de túnel nivel 3.

Encriptación de datos. Los protocolos de túnel nivel 2 dan soporte a mecanismos de encriptación de datos basados en PPP. Por su parte, la implementación de Microsoft de PPTP da soporte al uso opcional de Microsoft Point-to-Point Encription (MPPE), basado en el algoritmo RSA / RC4[22].
Los protocolos de túnel nivel 3 pueden utilizar métodos similares; por ejemplo, IPSec define varios métodos de encriptación opcional de datos que se negocian durante el intercambio ISAKMP/Oakley.

La implementación de Microsoft del protocolo L2TP utiliza la encriptación IPSec para proteger el flujo de datos del cliente al servidor del túnel.

Administración de llaves. MPPE, un protocolo de nivel 2, se basa en las claves iniciales generadas durante la autenticación del usuario y luego la renueva en forma periódica. IPSec negocia explícitamente una llave común durante el intercambio ISAKMP y también las renueva de forma periódica.

Soporte de protocolo múltiple. El sistema de túnel de nivel 2 da soporte a protocolos múltiples de carga útil, lo que facilita a los clientes de túnel tener acceso a sus redes corporativas utilizando IP, IPX, NetBEUI, etc.
En contraste, los protocolos de túnel nivel 3, como el modo de túnel IPSec, por lo común dan soporte sólo a redes objetivo que utilizan el protocolo IP.

2.2.5 Tipos de túnel.

Se pueden crear túneles en diferentes formas.

[21] Internet Engineering Task Force.
[22] Rivest Shamir Alderman / RC4.

- ✓ **Túneles voluntarios:** Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente de éste.

- ✓ **Túneles obligatorios:** Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con uno de éstos, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del mismo.

A la fecha, los túneles voluntarios han probado ser el tipo más popular de túnel. A continuación se describen cada uno de estos tipos con mayor detalle.

Túneles voluntarios.

Un túnel voluntario ocurre cuando una estación de trabajo o un servidor de enrutamiento utilizan el software del cliente del túnel, a fin de crear una conexión virtual al servidor del túnel objetivo; para lograr esto se debe instalar el protocolo apropiado de túnel en la computadora cliente.
Para los protocolos que se analizan en esta sección, los túneles voluntarios requieren una conexión IP (ya sea a través de una LAN o marcación).

En determinadas situaciones, el cliente debe establecer una conexión de marcación con el objeto de conectarse a la red antes de que el cliente pueda establecer un túnel (éste es el caso más común). Un buen ejemplo es el usuario de Internet por marcación, que debe marcar a un ISP y obtener una conexión a Internet antes de que se pueda crear un túnel sobre Internet.
Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un enrutamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este sería el caso para un cliente en una LAN corporativa, que inicia un túnel para alcanzar una sub-red privada u oculta en la misma LAN.

Es falso que las VPN requieran una conexión de marcación, pues sólo requieren de una red IP. Algunos clientes (como las PC del hogar) utilizan conexiones de marcación 1 Internet para establecer transporte IP; esto es un paso preliminar en la preparación para la creación de un túnel, y no es parte del protocolo del túnel mismo.

Túneles obligatorios.

Diversos proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora del cliente es conocida de varias maneras: procesador frontal (FEP) en PPTP, un concentrador de acceso a L2TP en L2TP o un gateway de seguridad IP en el IPSec. En esta sección el término FEP se utilizará para describir esta funcionalidad, sin importar el protocolo de túnel.

Para realizar esta función, el FEP deberá tener instalado el protocolo apropiado de túnel y ser capaz de establecer el túnel cuando se conecte la computadora cliente.

En el ejemplo de Internet, la computadora cliente coloca una llamada de marcación al NAS[23] activado por los túneles en el ISP; puede darse el caso de que una empresa haya contratado un ISP para instalar un conjunto nacional de FEP. Estos FEP pueden establecer túneles a través de Internet hacia un servidor de túnel conectado a la red privada de la empresa, consolidando así las llamadas de diferentes ubicaciones geográficas en una conexión única de Internet en la red corporativa.
Esta configuración se conoce como túnel obligatorio debido a que el cliente esta obligado a utilizar el túnel creado por FEP. Cuando se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel.
En los túneles obligatorios, la computadora cliente realiza una conexión única PPP, y cuando un cliente marca en el NAS se crea un túnel y todo el tráfico se enruta de manera automática a través de éste. Es posible configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel. De manera

[23] Network Access Server.

alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el FEP y servidor puede estar compartido entre varios clientes de marcación. Cuando un segundo cliente marca al servidor de acceso a fin de alcanzar un destino (para el cual ya existe un túnel), no hay necesidad de crear una nueva instancia del túnel entre el FEP y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente.

Dado que posiblemente existan varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario.

2.3 SEGURIDAD EN LAS VPN.

Puesto que Internet facilita la creación de VPN desde cualquier lugar, estas necesitan fuertes funciones de seguridad a fin de evitar el acceso no deseado a las VPN, y proteger los datos privados cuando viajan a través de redes públicas.

Para que las VPN puedan ser un medio efectivo para las aplicaciones de extranet y para correr aplicaciones a través de Internet, deben utilizarse tecnologías de autenticación seguras, las más recientes y sofisticadas, así como criptografía y cifrado en cada extremo del túnel de la VPN. Por lo tanto, ¿qué tipo de medidas componen los criterios de seguridad de las VPN? Es decir, ¿qué tipo de garantías necesita una organización para confiar en las transacciones con el uso de la tecnología VPN? Lo siguiente es imperativo para cualquier configuración de seguridad:

Sólo a las partes autorizadas se les permite el acceso a aplicaciones y servidores corporativos. Este es un aspecto importante de la tecnología VPN, ya que se permite que las personas entren y salgan de Internet o de otras redes públicas y se les ofrece acceso a los servidores.

Cualquiera que pase a través del flujo de datos cifrados de la VPN, no debe estar capacitado para descifrar el mensaje. Los datos de la VPN viajaran a través de una red pública, y cualquiera tendrá la capacidad para interceptarlos. El resguardo de los datos yace en el cifrado, incluyendo su solidez y la implementación específica del

proveedor. Una tecnología nueva llamada esteganografía, añade otro nivel de protección al cifrado. Una organización debe asegurarse de que los datos estén seguros y no puedan ser leídos por otros, pero también debe esperar lo contrario.

Los datos deben permanecer intocables al 100%. Algunos individuos sin duda verán el tráfico cifrado e intentarán leerlo. Sin embargo, otro problema es que intenten modificarlo y enviarlo a su destino original. La integridad es un tema diferente cuando se trata de la tecnología VPN. Existen normas de cifrado que proporcionan autenticación, cifrado e integridad de datos; los datos no deben ser modificados y deben permanecer intactos en su forma original. Si los datos pueden modificarse ¿cómo podría determinarse que en realidad vienen del emisor sin ser tocados? Como explicaremos más adelante en éste capítulo, existen técnicas de cifrado que ayudarán a asegurar que los datos no puedan ser modificados.

Los usuarios deben tener distintos niveles de acceso. Los usuarios individuales deben tener un distinto nivel de acceso cuando entren al sitio desde redes no internas. Se debe distinguir los distintos niveles de acceso cuando entren a la organización. No sólo se trata de la autorización necesaria a servidores específicos, si no a las subredes individuales a las que les esta permitido entrar. Con algunos dispositivos de VPN, es necesario que asigne subredes específicas por túnel a los usuarios; esto tiene la ventaja de restringir el acceso de los extraños a las redes individuales.
Esto también agrega una molestia cuando se quiere dar a los empleados internos acceso sin restricciones, puesto que será necesario habilitarlos en todos los túneles.

Los aspectos de interoperabilidad deben tomarse en consideración. La interoperabilidad es un problema cuando existen diferentes plataformas y sistemas operando en conjunto para lograr una meta común.
Entonces, ¿cómo se relaciona esto con la seguridad, especialmente con la seguridad que concierne a las VPN? Las VPN deben funcionar en todas las plataformas; por ejemplo, si se tienen equipos macintosh en la organización y se requiere que sean capaces de utilizar la VPN, es muy probable que se tenga que añadir algún software para estos sistemas. Hay que analizar cuántas plataformas y sistemas operativos se tienen en la organización, cuántos tipos distintos de transporte, cuántos tipos diferentes de

topologías, etc. Después, se debe determinar cuántos de estos sistemas necesitan acceso a la VPN y cómo se puede lograr esto.

Se debe tener facilidad de administración. El dispositivo de las VPN debe proporcionar una administración fácil, la configuración debe ser directa, y el mantenimiento y la actualización de la VPN deben estar asegurados. Una de estas facilidades de administración debe ser el acceso de los usuarios. En cualquier organización, es probable que haya personas que se van, personas que son contratadas, personas que necesitan acceso a Internet y otras personas que no necesitan el acceso a Internet, entre otros ejemplos que pueden mencionarse. Por lo tanto, debe haber una manera sencilla para agregar / eliminar usuarios sin ocupar al administrador de la red o sin decirle a las personas que se necesitará todo un día para darles el acceso.

2.3.1 Algoritmos y sistemas de cifrado.

¿Qué es la criptología?

Se entiende por criptología al estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor. La criptografía es la parte de la criptología que estudia cómo cifrar o esclarecer efectivamente los mensajes. Etimológicamente la palabra criptografía proviene del griego kryptos (oculto) y grafía (escritura): escritura oculta. La criptografía es pues la ciencia que estudia la escritura secreta, es decir, la forma de escribir ocultando el significado.

Por otro lado, su oponente, el criptoanálisis, es la ciencia que se ocupa de esclarecer el significado de la escritura ininteligible. No hay que confundir el criptoanálisis con el descifrado de la información. El descifrado de la información es por medios lícitos, utilizando la clave y el sistema adecuado, y forma parte de la criptología, mientras que el criptoanálisis pretende descifrar el mensaje sin conocer la clave.

La criptología engloba tanto a la criptografía como a criptoanálisis; el éxito de un criptoanalista supone el fracaso de un criptógrafo y viceversa.

En la práctica, la criptografía se ocupa del cifrado y el descifrado de mensajes. Cifrar información consiste en transformar un mensaje claro en un mensaje cifrado mediante el uso de una clave.
El texto en claro es inteligible (si se conoce el lenguaje utilizado), mientras el texto cifrado es ininteligible, es decir, tiende a parecerse a una sucesión de caracteres aleatorios a los que no es posible otorgar ningún significado.
La operación inversa al cifrado es el descifrado, y consiste en obtener el texto en claro a partir del texto cifrado.

Sistemas de cifrado modernos.

Los sistemas criptográficos modernos se desarrollan con la aparición de las computadoras, y basan su funcionamiento en la utilización de potentes y complejas herramientas de hardware y software. Se utilizan claves secretas de gran longitud para controlar una compleja secuencia de operaciones con la información, que pueden incluir tanto transposiciones como sustituciones. Su posibilidad de uso se basa en la potencia y en la capacidad de las máquinas, que permiten aplicar algoritmos de gran complejidad y costos en tiempos admisibles.

Los criptosistemas modernos pueden dividirse en dos grandes categorías en función del tipo y número de claves que utilizan:

- ✓ Criptosistemas simétricos, también llamados de clave única o de clave privada.
- ✓ Criptosistemas asimétricos, también llamados de clave pública o de dos claves.

Ambos tipos de sistemas suelen combinarse para llevar a cabo distintas acciones y lograr ciertos objetivos de seguridad.

Criptosistemas de clave privada.

En estos sistemas se utiliza la misma clave para el cifrado y para el descifrado. Esta clave se denomina clave privada (secreta o única) debido a que tan sólo es conocida por el emisor y por el receptor del mensaje. Para que este tipo de sistema sea efectivo la clave debe ser mantenida en secreto por ambos componentes de la comunicación.

La seguridad de este tipo de sistemas depende totalmente del nivel de protección de la clave. Cuando se descifra un mensaje usando la clave privada, el hecho de que ésta sea tan sólo conocida por el emisor y el receptor garantiza dos propiedades:

1. Que el mensaje no es inteligible por nadie más, es decir, que es confidencial.
2. Que si el texto descifrado es inteligible, sólo hay un emisor posible, aquel que conoce la clave privada. Esto garantiza la autenticidad del mensaje.

Por lo tanto, en este tipo de sistemas, el secreto (confidencialidad) y la autenticidad se obtienen al mismo tiempo.

En la figura 2.6 que se muestra a continuación, se esquematiza el cifrado de un mensaje, usando un criptosistema de clave privada.

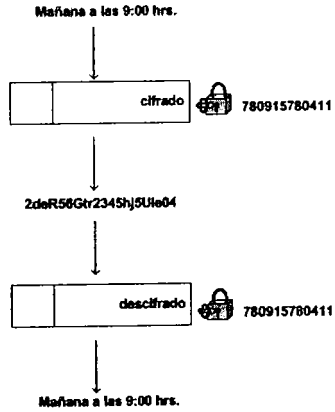


Figura 2.6

Las claves privadas deben intercambiarse de modo totalmente seguro, pues sobre ellas descansan todas las características de seguridad del sistema. Si existe n usuarios, cada usuario necesita n-1 claves distintas para comunicarse con el resto. Todos estos procesos constituyen la denominada gestión de claves.

Criptosistemas de clave pública.

En este tipo de sistemas se utilizan dos claves: una clave pública y una clave privada. En un grupo de usuarios, cada uno de ellos posee dos claves distintas:

- ✓ La clave pública, K', como su propio nombre indica, puede ser conocida por todos los usuarios del sistema.
- ✓ La clave privada, K, tan sólo es conocida por su propietario.

Aunque estas claves están relacionadas matemáticamente, la fortaleza del sistema depende de la imposibilidad computacional de obtener una a partir de la otra.

Este tipo de sistemas se denominan asimétricos por que no es posible usar una misma clave para cifrar y descifrar un mensaje. Ambas claves deben usarse en el proceso. Si se cifra un mensaje con una de ellas, se debe descifrar con la otra.

Si un usuario (emisor) quiere enviar un mensaje secreto a otro (receptor), debe cifrarlo utilizando la clave pública del receptor.

El mensaje tan sólo puede descifrarse utilizando la clave privada del receptor, con lo que se garantiza la confidencialidad del mismo. La clave pública del receptor no sirve para descifrar el mensaje, y por tanto tan sólo el receptor (que es el único que conoce su propia clave privada), puede descifrarlo.

El funcionamiento de un sistema de clave pública, se observa en la figura 2.7.

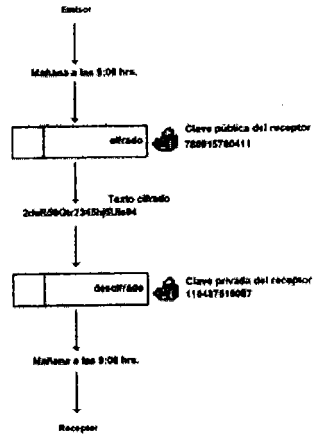


Figura 2.7

Por otra parte, el mensaje no es auténtico. Dado que cualquier usuario puede conocer la clave pública del receptor, cualquier usuario puede ser el emisor del mensaje. La recepción de un mensaje cifrado con la clave pública del receptor no identifica unívocamente al emisor, y por lo tanto no lo autentifica.

Si el emisor quiere garantizar la autenticidad de un mensaje, debe cifrarlo con su clave privada, como se esquematiza en la figura 2.8

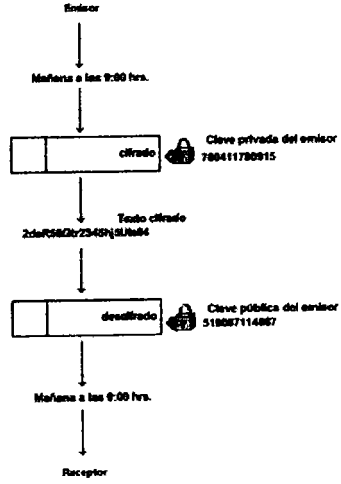


Figura 2.8

El receptor podrá descifrarlo usando la clave pública del emisor. Dado que todo el mundo puede conocer la clave pública del emisor, no se garantiza la confidencialidad del mensaje. Cualquiera puede descifrarlo. Sin embargo, dado que tan sólo el emisor conoce su propia clave privada, tan sólo el puede ser el origen del mensaje, con lo que se garantiza la autenticidad del mismo.

En este tipo de sistemas, el secreto y la autenticidad del mensaje se obtienen por separado. Para lograr las dos características de seguridad es necesario combinar ambas claves y realizar un doble proceso de cifrado y descifrado.

Criptosistemas híbridos.

Tanto la criptografía de clave pública como la de clave privada tienen sus ventajas y sus inconvenientes. Debido a ello se suelen utilizar para distintos fines, y por tanto los criptosistemas de clave pública no son un sustituto de los de clave privada.
Existen dos razones que hacen que la criptografía de clave pública sea poco adecuada para la transferencia de información cifrada:

1. Los algoritmos de clave pública son lentos. Normalmente son unas 1000 veces más lentos que los de clave privada.
2. Los algoritmos de clave pública son vulnerables a ataques mediante elección de mensaje. Dado que la clave pública es de dominio público, cualquiera puede tratar de cifrar todos los mensajes posibles y comparar los resultados con los textos cifrados. Esto es especialmente posible cuando la cantidad de mensajes posibles es limitada o se tiene alguna información adicional sobre su estructura o contenido.

Debido a las razones anteriores, la transferencia de información cifrada se suele realizar mediante criptosistemas de clave privada, mientras los de clave pública se reservan para funciones tales como la transferencia de claves. Lo ideal es combinar ambos tipos de criptosistemas para lograr una transmisión segura.

Norma de cifrado de datos (DES)[24].

La norma de cifrado de datos DES, también conocida como algoritmo de cifrado de datos es uno de los sistemas de cifrado de uso más extendido, dado que se ha convertido en un estándar reconocido por las agencias americanas y que se trata de un sistema de gran fortaleza.

El origen del DES se debe a una petición realizada en 1973 por el NBS (Nacional Bureau of Standards) a distintos fabricantes para someter criptosistemas que pudieran servir como base a un estándar de cifrado de textos reservados no clasificados.

IBM disponía de un sistema altamente seguro denominado LUCIFER basado en una clave de 128 bits. Este sistema fue sometido al examen de la NBS y, tras ser analizados por expertos de la NSA (Nacional Security Agency), y ser reducido a 56 bits, fue aceptado y denominado DES.

Funcionamiento del DES.

El DES se basa en la permutación de combinaciones y sustituciones realizadas sobre bloques de 64 bits de datos usando una clave de 56 bits.
La información a cifrar se divide en bloques de 64 bits, y sobre cada uno de ellos se repite el mismo proceso. Inicialmente se divide cada bloque en dos de 32 bits, L0 y R0, y se permutan estos. Posteriormente se aplican 16 etapas en las que se combina cada bloque LI (aplicando la función XOR), producido en la etapa anterior, con el resultado de aplicar una función al bloque RI en base a 48 bits de la clave inicial, KI+1, dando lugar al bloque RI+1.

En una última etapa, se deshace la permutación inicial reuniendo los dos bloques resultantes para dar lugar a la salida cifrada.

Por lo tanto, el DES es reversible, es decir, puede aplicarse el mismo proceso para el cifrado como para el descifrado. Además puede utilizarse la misma clave para realizar

[24] Data Encryption Standard.

ambos procesos, lo que lo convierte en un proceso simétrico. La clave K da lugar a 16 claves de 48 bits que se utilizan en cada una de las 16 etapas del método. Si para el proceso de cifrado estas claves se utilizan en un orden, para el descifrado deben utilizarse en el orden contrario.

Con el fin de reforzar la seguridad de este sistema se han propuesto diversas modificaciones del mismo, entre las que se puede destacar su aplicación reiterada (3DES), o la ampliación de la longitud de sus claves.

El criptosistema DES puede utilizarse en cuatro modos distintos en función de que se quieran obtener ciertas características, tales como poder transmitir a través de canales con ruido, autentificar el mensaje resultante, poder descifrar sólo una parte del mismo, etc.

Los cuatro modos de operación del DES son:

- ✓ ECB (Electronic Code Book).
- ✓ CBC (Cipher Block Chiang).
- ✓ CFB (Cipher Feedback).
- ✓ OFB (Output Feedback).

Algoritmo de clave pública RSA.

El algoritmo de cifrado RSA, es el criptosistema de clave pública más extendido. Su nombre proviene de sus creadores Rivest, Shamir y Alderman, quienes lo desarrollaron en 1978.

Este sistema usa dos claves y cualquiera de las dos puede ser pública o privada. Las dos claves se generan matemáticamente basándose en parte en la combinación de grandes números con factores primos.

Desde su aparición, el sistema de llave pública RSA ha ganado gran popularidad, por una parte, por la gran seguridad que ofrece al basar esta en un problema matemático difícil de resolver que había dejado interés en la comunidad mundial, como lo es el

Problema de la Factorización Entera (PFE), y a causa del sistema RSA, se ha retomado e incrementado su investigación. La seguridad del sistema depende de que las claves sean de enorme longitud y de que una no pueda deducirse de la otra en un tiempo admisible.

Dado que las claves se generan a partir del producto de dos números primos, la única forma de atacarla sería factorizándolas en dicho números. Lo cual es demasiado costoso y complicado, ya que los números producto de dos primos, son de los más difíciles de factorizar.

El sistema RSA, ha sido uno de las más estudiados hasta el momento y por lo tanto se considera que es uno de los más seguros, ya que ha podido superar algunas controversias; así, actualmente es uno de los sistemas criptográficos de llave pública más usados en la industria, en el comercio, en los gobiernos, en la milicia y en general en toda actividad que requiera que la información tenga un alto grado de seguridad criptográfica.
Es importante mencionar que hasta ahora se han desarrollado una gran cantidad de sistemas de llave pública con el fin de sustituir, generalizar o simplemente competir con RSA, sólo que no han tenido éxito, ya que en principio deben de pasar un riguroso criptoanálisis por parte de la comunidad criptográfica y después se someten a la competencia comercial, la prueba es en general proporcionar al menos la misma seguridad de los sistemas existentes con al menos la misma facilidad de implementación y después que basen su seguridad en problemas muy duros. Hasta ahora, sólo los sistemas basados en el Problema del Logaritmo Discreto Elíptico (PLDE) han podido competir exitosamente con el sistema RSA, incluso son más prometedores que RSA, ya que con sólo llaves de 160 bits proporcionen la misma seguridad. Existe otro tipo de sistemas que basan su seguridad en el PFE, sin embargo, se ha demostrado que son equivalentes a RSA, por lo que se desechan, ya que necesitan la misma o mayor longitud de las llaves.

Algoritmo internacional de cifrado de datos (IDEA).

El algoritmo IDEA es una cifra de bloque que se creó en 1990 por una compañía suiza. Utiliza 64 bits con 8 ciclos. El descifrado es el mismo proceso que el cifrado una vez

que todas las subclaves de descifrado se calcularon a partir de las claves de cifrado. Este cifrado se diseñó para una implementación fácil en hardware y software. La seguridad de IDEA se basa en la utilización de tres tipos incompatibles de operaciones aritméticas en palabras de 16 bits. En este algoritmo, las operaciones de tres grupos algebraicos diferentes se mezclan (XOR, modulo de adición 216 y modulo de multiplicación 216+1). IDEA utiliza 52 subclaves, cada una comienza con una longitud de 16 bits. La generación de subclaves es como sigue:

La clave de 128 bits de IDEA se utiliza como las primeras 8 subclaves K1 a K8. Las 8 siguientes se obtienen de la misma manera, después de una rotación circular a la izquierda de 25 bits. Este proceso se repite hasta que todas las subclaves de cifrado se hayan calculado.
IDEA es un cifrado sólido que ha enfrentado muchos retos en su contra. Se considera inmune al criptoanálisis diferencial y no se han reportado ataques criptoanalíticos lineales.
De cualquier modo, existe una gran clase de claves débiles, 2^{51}, que en proceso de cifrado podrían permitir que se recuperara la clave. Sin embargo, IDEA todavía tiene 2^{128} claves posibles, lo cual hace que sea seguro.

RC5.

RC5 es diferente a los otros algoritmos RC debido a que utiliza un tamaño de bloque variable, un tamaño de clave diferente y un número de ciclos distinto.
RC5 utiliza tamaños de bloque de 32, 64 y 128 bits. La clave variable abarca de 0 a 2048 bits y el número de ciclos puede ir de 0 a 255. Es una cifra de bloque rápida y puede utilizarse con un tamaño de bloque de 64 bits que puede ser un reemplazo para DES. Esta flexibilidad de tamaño le da al RC5 una gran seguridad. La generación de subclaves se calcula con la clave definida por el usuario y el número total de subclaves depende del número de ciclos implementados. Después, la tabla se utiliza para cifrado y descifrado. La rutina de cifrado consiste en tres operaciones algebraicas: adición de enteros, modo en bits OR exclusivo y rotación variable. Estas operaciones hacen que el RC5 sea fácil de probar e implementar. RC5 se ha probado contra ataques de criptoanálisis diferencial y lineal.

Message Digest 2 (MD2), 4 (MD4), 5 (MD5).

Ron Rivest de los laboratorios RSA creó Message Digest 2, 4, 5. Son todas las funciones de transformación de código que toman una cadena de una longitud arbitraria y producen una salida de longitud fija de 128 bits.
MD2 se diseño en 1989 y se mejoró para las maquinas microprocesadores de 8 bits. Se han descubierto algunos puntos débiles en el campo de mensaje de MD2 si algunos cálculos se dejaron incompletos durante la transformación del código. Por consiguiente, la implementación de MD2 ya no es recomendable.

MD4 se diseñó en los noventa y utiliza un bloque de 512 bits con el mensaje. Esta función de transformación del código utiliza tres ciclos en su implementación. Lamentablemente, los ataques a MD4 ocurrieron muy pronto cuando terminaban el primer o tercer ciclo. Además MD4 no se recomienda para uso general.
MD5 se desarrolló en 1992 y aunque es más lento que MD4 se considera más seguro. Este algoritmo consiste en cuatro ciclos. Algunas personas reportaron puntos débiles en él, pero aún así se considera seguro y se usa ampliamente.

Algoritmo de clave pública Diffie-Hellman.

En 1976, whitfield Diffie y Martin Hellman publicaron un artículo titulado Nuevas Tendencias en Criptografía. Desde entonces se ha empleado su algoritmo de clave pública en todo el mundo. El protocolo de acuerdo de claves Diffie-Hellman es una generación de claves negociada.
Su fortaleza radica en el campo matemático finito de exponenciación de los logaritmos. El protocolo permite que dos usuarios intercambien una clave secreta en un medio inseguro sin secreto previo alguno. El algoritmo Diffie-Hellman también ha establecido la función de seguridad de un acuerdo de claves secretas, por lo tanto aunque sea un algoritmo asimétrico, tanto el emisor como el receptor pueden utilizar un algoritmo de cifrado simétrico. Diffie-Hellman fue el primer algoritmo de clave pública desarrollado y continúa siendo muy popular.

Pretty Good Privacy (PGP).

Pretty Good Privacy (PGP) de Philip Zimmermann se ha empleado por todo el mundo. PGP es un criptosistema híbrido, con todas las ventajas. Combina un algoritmo de clave privada con uno de clave pública. Esto le da tanto rapidez de un sistema simétrico como las ventajas de un sistema asimétrico. Por lo que concierne a los usuarios, PGP actúa como cualquier otro criptosistema de clave pública; utiliza el algoritmo de clave pública RSA e IDEA para el cifrado. Se emplea una sola clave IDEA para cifrar el mensaje, y se utiliza la misma clave para descifrarlo (cifrado simétrico). Después se utiliza RSA para cifrar la clave IDEA usada para el cifrado con la clave pública del emisor (asimétrico). El receptor emplea su clave privada para descifrar la clave IDEA cifrada con RSA, posteriormente esta clave IDEA descifrada se emplea para descifrar el resto del mensaje. Junto con PGP, Zimmernmann creó un conjunto de utilerías para administrar un anillo de claves públicas donde los usuarios pueden manejar distintas claves públicas.
PGP se ha desarrollado con una aplicación de interfaz amigable que existe actualmente en muchos equipos de escritorio con todo tipo de aplicaciones. Su popularidad y facilidad de uso, junto con la solidez de la seguridad RSA, la convierten en una herramienta de seguridad muy valiosa.

2.3.2 Protocolos de autenticación.

La autenticación es el segundo factor más importante en la configuración de una VPN. Existen dos aspectos: la autenticación (¿quién tiene el permiso?) y la autorización (¿a qué tiene acceso?).
En cualquier infraestructura de comunicaciones en red existe la necesidad de un proceso de autenticación que permita que el usuario acceda a los servicios de red y que impida, al mismo tiempo, el acceso no garantizado de los usuarios sin autorización. Esto requiere de una configuración de confianza de dos sentidos: el sistema debe confiar en el usuario y el usuario debe confiar en otros usuarios del sistema (por ejemplo, al emplear alguna clave pública). Para que el sistema gane la confianza del usuario, el usuario deberá ser capaz de probar que es quien dice ser. Esto requiere algún tipo de proceso de autenticación.

El sistema que permite que estas comunicaciones se realicen utiliza los protocolos de autenticación, muchos de los cuales ya están disponibles actualmente. Podrá encontrarlos al iniciar una sesión en su computadora, en una red, utilizar un cajero automático para retirar dinero, etc. Estos protocolos son de distintos tipos, pero muchos utilizan el viejo principio de verificación con una o varias contraseñas. Lo que es distinto es quién tiene la contraseña y cómo se transfiere la información del cliente al servidor. En los sistemas de contraseñas normales, tanto el sistema como el usuario conocen la contraseña. Generalmente, si alguien se registra en el sistema de la computadora, ésta tiene almacenada la contraseña de la persona junto con su identidad dentro de una base de datos. La persona proporciona su contraseña y, si coincide con la contraseña que se encuentra en la base de datos de la computadora, se inicia la sesión.

Sin embargo, esto obliga a que las contraseñas se almacenen en algún lugar, en este caso, en un archivo del servidor. Ahora no sólo tiene que preocuparse por la seguridad del servidor, sino también por el archivo en ese servidor. En los sistemas más recientes se utiliza una función de transformación del código de un sentido, en lugar de un archivo. Una función de transformación del código de un sentido es un algoritmo criptográfico que permite crear un valor de transformación del código en una dirección, pero ir en la dirección inversa (por ejemplo, al encontrar la contraseña de texto sencillo a partir del valor de transformación del código) es imposible en términos de computación.
Por desgracia, incluso estas funciones de transformación del código de un sentido no tienen garantía de ser 100% invulnerables.
Al ejecutar un programa que compute miles de valores de transformación del código basados en las contraseñas y al comparar estos valores, es posible adivinar cuales son algunos de esos valores. Las contraseñas no son cadenas muy extensas, por lo que no se necesita un sistema de computadoras muy poderoso para lograrlo.

Después de las contraseñas, los servicios de autenticación se orientan hacia el modelo cliente/servidor de autenticación empleando un Servidor de Acceso a Red (NAS)[25]. Este NAS es el ejecutor (intermediario) de la autenticación y de la autorización del cliente; el servidor de seguridad sólo se encarga de la configuración de los usuarios. Por

[25] Network Access Server.

consiguiente, debe haber un conjunto de reglas que indiquen la forma en que el NAS y el servidor de seguridad pueden comunicarse entre sí, en beneficio del cliente. Por lo general, este conjunto de reglas de comunicación se llama protocolo de autenticación y, como se verá más adelante, existen muchos protocolos de autenticación de distintos tipos de proveedores.
Los servidores de red y los servidores de seguridad son diferentes; por lo tanto, las elecciones que se hagan dependerán de los aspectos de interoperabilidad y del compromiso con las normas abiertas.

Contraseñas del sistema operativo.

Las contraseñas continúan siendo la forma más común en los procesos de autenticación de usuarios en la actualidad. Se emplean para controlar el acceso a la información, desde sencillos registros de red hasta Números de Identificación Personal (NIP) que se usan en los cajeros automáticos. Estas se emplean mucho por que su instalación y su implementación son sencillas y económicas.
Al mismo tiempo, las contraseñas son famosas por que se trata de una forma de protección sumamente pobre. Las fallas de la seguridad de las contraseñas son muy peligrosas debido a que una sola computadora puede tener cientos o miles de cuentas protegidas con contraseñas. En las redes interconectadas de la actualidad, las consecuencias pueden ser devastadoras.

S/KEY.

S/KEY es un algoritmo de software que fue desarrollado por Bellcore Laboratories, este es un sistema de contraseñas descartables, donde cada contraseña utilizada en el sistema se emplea para una sola autenticación. Las contraseñas no se pueden volver a utilizar; por lo tanto, no pueden interceptarse ni usarse como una forma de predecir las contraseñas futuras. El conocimiento de las contraseñas ya usadas en una secuencia de contraseñas de S/KEY no ofrece información sobre las contraseñas futuras. El esquema de contraseñas descartables de S/KEY proporciona una autenticación segura en redes que están sujetas a intrusiones. S/KEY evita que la contraseña secreta del usuario sea interceptada en la red durante la autenticación.

Debido a que es fácil de integrar, muchas redes sensibles a la seguridad utilizan S/KEY como su sistema de seguridad de contraseñas. El sistema S/KEY involucra tres partes clave: el cliente, el servidor y un calculador de contraseñas. El cliente es el responsable de proporcionar el proceso de registro al usuario final. El servidor es responsable de procesar la solicitud de registro del usuario además de que almacena en un archivo la contraseña descartable actual y el número de secuencia del registro. Además, le proporciona al cliente un valor semilla. El controlador de contraseñas es una función de transformación del código de un sentido (irreversible). Esto se define como una función que pierde información cada vez que se aplica y hace un conteo regresivo cada vez que la contraseña se utiliza. Además, el servidor S/KEY no almacena las contraseñas de los usuarios.

Un ejemplo de una función de transformación del código lo podemos observar en la figura 2.9.

La figura 2.9 ilustra un proceso S/KEY típico, un esquema de contraseña descartable basado en transformación del código criptográfico irreversible de una cadena secreta de valores proporcionada por el usuario. Éste pasa la frase en el programa de transformación del código, y en cada iteración se crea un pequeño grupo de bits. S/KEY aplica la función de transformación del código varias veces a la frase de la contraseña, y el usuario proporciona estas funciones de transformación del código como contraseñas en un orden inverso al que se generaron. Se trata de algo seguro, puesto que cada vez que se aplica una transformación de código a la frase de la contraseña hacia delante, se pierde una parte de la información interna, lo cual dificulta revertir el proceso para obtener la frase de la contraseña original. Debido a que el usuario es la única persona que conoce la frase secreta, sólo él puede regresar de manera efectiva al comenzar con su frase secreta y continuar el proceso. Cada valor de transformación del código se utiliza como contraseña de autenticación una sola vez; después de esto, nunca es válida de nuevo, por lo tanto, es inútil para los analizadores de redes y para los intrusos.

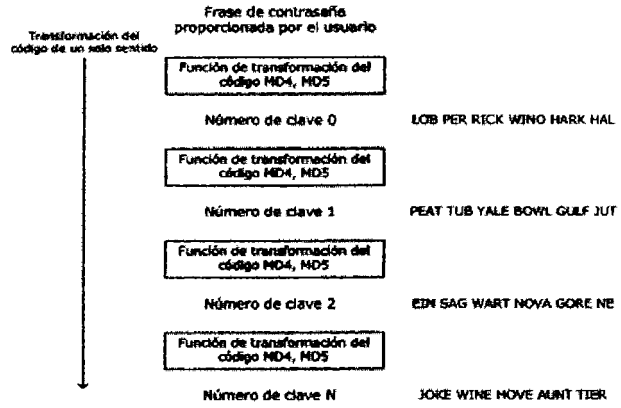


Figura 2.9

Servicio de marcación para autenticación de usuarios remotos (RADIUS).

El servicio de marcación para autenticación de usuarios remotos, o RADIUS, es un sistema de seguridad distribuida que garantiza el acceso remoto a redes y servicios de redes frente al acceso no autorizado, al emplear el protocolo UDP. La autenticación RADIUS incluye dos componentes: un servidor de autenticación y protocolos de cliente. El servidor se instala en una máquina en el sitio del cliente. Toda la información sobre la autenticación de usuarios y el acceso a los servicios de la red se localiza en el servidor RADIUS.

RADIUS permite distintos formatos que pueden adaptarse a los requisitos de un cliente individual. Un servidor RADIUS autenticará a los usuarios utilizando un archivo de contraseñas UNIX, el Servicio de Información de Red de SUN Microsystems o una base de datos RADIUS administrada en forma independiente. El modelo RADIUS trabaja en el cliente enviando solicitudes de autenticación al servidor RADIUS, además de que actúa en los reconocimientos que envía el servidor.

RADIUS autentica a los usuarios a través de una serie de comunicaciones entre el cliente y el servidor. A continuación se muestran los pasos involucrados en una comunicación RADIUS típica que emplea un servidor de comunicación RADIUS:

1. Desde su equipo portátil, un usuario marca a un modem conectado al servidor RADIUS de comunicaciones por marcación. Una vez que se completa la configuración de la conexión, la marcación le solicita al usuario su nombre y su contraseña.
2. El servidor de marcación crea un paquete de datos a partir de esta información, conocido como solicitud de autenticación. Los datos incluyen información para identificar la marcación específica que envía la solicitud de autenticación, el puerto de donde proviene la comunicación, el nombre del usuario y su contraseña. Para ofrecer seguridad adicional, el servidor de marcación, que actúa como un cliente RADIUS, cifra la contraseña antes de enviarla al servidor RADIUS.
3. La solicitud de autenticación se envía desde el cliente RADIUS hasta el servidor RADIUS. RADIUS permite varios servidores y, dependiendo de la topología de la red, los clientes pueden enlutar sus solicitudes a distintos servidores.
4. Cuando el servidor RADIUS recibe la solicitud, el servidor valida y descifra el paquete de datos para tener acceso a la información del nombre de usuario y de la contraseña. Esta información se pasa a los sistemas apropiados que manejan la seguridad, como puede ser una base de datos de usuarios controlada localmente.
5. Una vez que se verifican el nombre de usuario y la contraseña, el servidor envía un reconocimiento (llamado reconocimiento de autenticación) que incluye información sobre el sistema de red del usuario y los requisitos del servicio. Esto quiere decir que el servidor RADIUS puede decirle al servidor de marcación que el usuario sólo tiene permiso para acceder a un anfitrión específico de la red.
6. Si el nombre de usuario y la contraseña son incorrectos, el servidor RADIUS le envía un rechazo de autenticación al dispositivo de marcación, por lo que se le niega el acceso a la red a ese usuario.
7. Para protegerse contra intrusos, especialmente del ataque de intermediario, el servidor RADIUS envía una clave de autenticación, o firma, que los identifica con el cliente RADIUS.
8. Con esta información, el servidor de marcación le permitirá o rechazará los servicios de red al cliente.

El servicio RADIUS no está limitado a servicios de marcación. Muchos proveedores de Firewalls soportan el uso de servidores RADIUS. Por lo tanto, se puede tener a los usuarios de marcación y a los usuarios de VPN autenticados en el servidor RADIUS.

Sistema de control de acceso al controlador de acceso para las terminales (TACACS/XTACACS).

Los servidores habilitados para TACACS envían la información de contraseña/usuario a un servidor TACACS centralizado. El servidor TACACS puede ser una base de datos TACACS o una base de datos, como un archivo de contraseñas de UNIX con soporte para TACACS. Por ejemplo, un enrutador habilitado para TACACS pasa la solicitud del usuario a un servidor TACACS, el cual puede consultar una base de datos UNIX para permitir la autorización. TACACS fue desarrollado originalmente por BBN Planet Corp., un proveedor de Internet. Tiempo después, Cisco Systems lo adoptó y lo reenvió a la IETF para darle el estado de RFC.

En el modo de autenticación de TACACS, un usuario solicita privilegios de acceso a un servidor terminal, un anfitrión UNIX, un enrutador, etc. El dispositivo pedirá un nombre y una contraseña, y reenviará esta solicitud al servidor TACACS en su configuración para validación. El servidor validará el par de inicio de sesión y de contraseña con un archivo de contraseñas TACACS. Si el nombre y la contraseña se validan, el usuario tiene permiso para iniciar una sesión.

Posteriormente TACACS evolucionó en un protocolo extendido, XTACACS, el cual incluye soporte para características de contabilidad y funciones adicionales en el servidor. Los servidores XTACACS proporcionan información para dar seguimiento a auditorias, al número de registros de un usuario y a registros de anfitrión, los cuales regulan el tiempo que un anfitrión debe permanecer conectado a la red.

La última generación de la línea TACACS es el TACACS+, desarrollado por Cisco Systems, el cual incorpora funciones de seguridad adicionales, como una comunicación segura sobre la red y un mejor control de acceso.

Sistema de control de acceso al controlador de acceso para las terminales plus (TACACS+).

A pesar de su nombre, TACACS+ es muy distinto a TACACS y XTACACS. Se trata de un protocolo de control de acceso basado en TCP que emplea el puerto 49 reservado. TACACS+ tiene más ventajas que TACACS y XTACACS como las que a continuación se mencionan:

- ✓ Separa las funciones de autenticación, autorización y creación de cuentas.
- ✓ Cifra todo el tráfico entre el NAS y el daemon.
- ✓ Permite extensiones arbitrarias e intercambio de autenticación de contenidos, gracias a lo cual se puede emplear cualquier mecanismo de autenticación con los clientes TACACS+.
- ✓ Es extensible.
- ✓ Utiliza TCP para asegurar entregas confiables.

Cuando el usuario intente registrarse, el servidor de acceso a la red le preguntará al servidor de seguridad qué debe hacer en lugar de sólo reenviar el nombre/contraseña a un servidor central. El servidor de seguridad le dirá al servidor de acceso a la red que inicie un comando, el cual indicará el nombre de usuario y contraseña. Una vez que estos datos sean introducidos, le enviará un paquete de permiso o de rechazo al NAS. TACACS+ tiene un sistema de atributos que se transmiten entre el NAS y el servidor de seguridad. Estos atributos son un conjunto de configuraciones que se aplican a un usuario individual. Cuando el usuario se registre, para cada comando que introduzca, el NAS enviará una solicitud de autorización al servidor de seguridad. En este momento, el NAS puede sugerir que se aplique un conjunto de atributos al usuario. Con base en la información de la solicitud, el servidor de seguridad le permitirá o rechazará y enviará la respuesta de regreso al NAS. Si es una respuesta de permiso, el servidor de seguridad puede decirle al NAS que aplique atributos adicionales al usuario. Algunos ejemplos de atributos son el direccionamiento IP, los filtros, las restricciones en la hora y fecha, y los valores de expiración de tiempo.

Los atributos que el NAS envía pueden ser opcionales u obligatorios. Si son opcionales, el servidor de seguridad puede proponer atributos alternativos.

Sin embargo, si los atributos del NAS son obligatorios, el servidor de seguridad no podrá cambiarlos. Incluso, si el servidor de seguridad no concuerda con los atributos, sólo puede rechazar la solicitud del usuario. Cada uno de los atributos que regresan al servidor de seguridad también pueden ser opcionales u obligatorios. Si son opcionales, el NAS puede optar por ignorarlos. Si son obligatorios el NAS debe utilizarlos. Si el NAS no puede ejecutar los atributos enviados por el servidor de seguridad, de nuevo debe rechazar la solicitud del usuario.

El NAS también puede enviar registros de contabilidad al servidor de seguridad para indicarle el inicio de una sesión de gestión, y registros de fin de gestión para indicarle que la sesión ha terminado. En el registro de finalización, habrá información sobre el tiempo y la cantidad de datos enviados y recibidos durante la sesión. Estos mensajes de autorizaciones, autenticaciones y cuentas, por lo general se activan en el NAS.

Kerberos.

Kerberos V5 es un protocolo de autenticación confiable fabricado por un tercero que permite que un proceso se ejecute en un cliente para demostrar su identidad frente a un servidor Kerberos, sin tener que enviar los datos a través de la red, lo cual permitiría que un atacante o un verificador se hicieran pasar por un director. Se desarrolló a mediados de la década de los 80 como parte del proyecto Athena del MIT. El protocolo Kerberos se basa en el protocolo de autenticación de Nedham y Schroeder, pero se modificó para soportar distintas funciones en entornos diferentes.

Kerberos es un sistema de cifrado DES simétrico. Utiliza una función de clave privada centralizada y en el núcleo del sistema se encuentra el centro de distribución de claves (KDC). El sistema de autenticación Kerberos utiliza una serie de mensajes cifrados para demostrarle a un verificador que el cliente se ejecuta en beneficio de un usuario. KDC maneja centralmente a los usuarios y los servicios, y es el administrador de las claves secretas que se emplean con los usuarios y los servicios, los cuales se llaman directores. Kerberos no utiliza contraseñas en el sentido normal; en lugar de eso, emplea credenciales y claves de sesión. Los directores contactan al KDC para conseguir credenciales de manera que puedan tener acceso a los servicios de red.

Kerberos es sumamente flexible. Gracias a que cuenta con funciones de seguridad adicionales, hace que las aplicaciones estén protegidas y ofrece una sola firma sin contraseñas que fluye a través de la red. Además, permite que el administrador de la red divida la red en distintas regiones de seguridad, con seguridad diferenciada aplicada a cada región. Pero Kerberos también tiene algunas limitaciones. No es muy efectivo contra ataques de suposición de contraseñas; si un usuario elige una contraseña muy fácil, entonces el atacante que adivina la contraseña puede hacerse pasar por el usuario. En forma similar, Kerberos requiere que la aplicación en la que se introducen las contraseñas sea confiable.

Kerberos tiene que integrarse con otras partes del sistema ya que no protege todos los mensajes enviados entre dos computadoras, sólo protege los mensajes del software escrito o modificado para usar Kerberos. Además, Kerberos necesita que las máquinas estén sincronizadas en el tiempo. Los boletos contienen un sello; si los relojes de las distintas máquinas están desactivados, los boletos serán inútiles. Por lo tanto, un protocolo como el protocolo de hora de red (NTP)[26] debe utilizarse con Kerberos.

Certificados.

Los certificados son simples estructuras de datos que contienen información. En los certificados no sólo nos preocupa la información, sino el hecho de identificar positivamente algo, ya sea un usuario o un dispositivo. Cuando se habla de identificar positivamente algo, se hace referencia al concepto de sin rechazos y, en este contexto, también al concepto de relacionar una clave pública con un sujeto. Se puede pensar en los certificados digitales como un pasaporte que se emplea para comprobar una identidad.

El contenido de los certificados digitales es el siguiente:

- ✓ La identidad de quien ostenta el certificado.
- ✓ El número de serie del certificado.
- ✓ Una fecha válida e inamovible para la transacción.

[26] Network Time Protocol.

- ✓ La fecha de expiración del certificado.
- ✓ Una copia de la clave pública de quien ostenta el certificado para cifrar y/o firmar.
- ✓ La identidad de la autoridad emisora de certificados y su firma digital.
- ✓ Nombre del grupo.
- ✓ Estado, ciudad.

Protocolo ligero para acceso a directorio (LDAP).

El protocolo ligero para acceso a directorio (LDAP) es un protocolo de red extensible que sirve para acceder a la información dentro de un directorio. Sin embargo, la estructura del directorio dentro de LDAP no es la misma que la de un directorio normal. En un directorio normal, por lo general se tiene una vista estática del contenido del directorio, donde el contenido se crea, modifica y elimina con el tiempo.
Al comparar esto con un directorio LDAP (donde es posible almacenar fotos, certificados, URL y cosas por el estilo) se puede ver que la estructura de LDAP esta viva con todo tipo de datos que pueden almacenarse dentro de ella. LDAP puede definirse para grupos de personas, por lo tanto es posible tener un punto de acceso para los distintos tipos de datos. Algunas de las normas de LDAP definen:

- ✓ El protocolo de red para tener acceso a esta información.
- ✓ Un espacio de nombre, que determina cómo se hace referencia a esta información.
- ✓ Cómo esta organizada la información dentro del directorio.
- ✓ Un modelo distribuido (en LDAPv3)

LDAP nació del protocolo para acceso a directorio (DAP) de X.500, que comenzó en 1988.
El DAP de X.500 definía un conjunto de protocolos en un sistema abierto que le proporcionaba a los usuarios y a las máquinas acceso a los servicios de directorio en toda la organización.

LDAPv3 utiliza un modelo de seguridad que se basa en el nivel de seguridad y autenticación simple (SASL). Esto permite cifrado y comunicaciones seguras entre el

servidor y el cliente. SASL es un sistema, mientras que el nivel de conexión segura (SSL) y Kerberos pueden utilizarse como servicios de seguridad.

LDAP permite el uso de certificados con la norma X.509 y se continúa trabajando en él para soportar a LDAP con la última norma de certificado X.509v3.

LDAPv3 ha mejorado el desempeño de su predecesor, LDAPv2. En LDAPv3 un cliente puede solicitar búsquedas al servidor LDAPv3 sin enlazarse primero con él. Esto representa una mejora, puesto que muchas de las solicitudes eran anónimas y primero debían ser permitidas. Si la base de datos X.500 debe establecer la seguridad, el LDAPv3 rechazará la solicitud del cliente, publicará un error de enlace y el cliente intentará de nuevo, pero esta vez enlazándose primero al servidor LDAP.

LDAP viene de la comunidad de Internet y tiene un amplio soporte por parte de los principales proveedores que emplean a X.500. Al igual que el World Wide Web, LDAP le proporciona al usuario una gran flexibilidad. Con LDAPv3 y su soporte para X.509v3, es posible que continúe su crecimiento como otros servicios que existen en Internet. Los navegadores web, los clientes de correo, las aplicaciones basadas en LDAP y las Redes Privadas Virtuales aprovecharán las ventajas de LDAP.

Protocolo de seguridad en Internet (IPSec).

La IETF tiene un grupo de trabajo llamado seguridad de IP (IPSec), el cual es responsable de definir las normas y los protocolos relacionados con la seguridad en Internet. Las Redes Privadas Virtuales utilizan estas normas como parte de las medidas de seguridad. El grupo IPSec trabaja en la definición de la estructura del paquete IP mismo y en la implementación de una asociación de seguridad que se utilizará en comunicaciones de Red Privada Virtual.

IPSec es un marco de estándares abiertos que proporciona confidencialidad de datos, integridad de datos y autenticación de datos entre iguales participantes en la capa IP. IPSec establece que antes de que ocurra cualquier comunicación, se negociará una asociación de seguridad (SA) entre los nodos o compuertas de la Red Privada Virtual.

La asociación de seguridad establece toda la información necesaria para asegurar las comunicaciones entre los dos dispositivos. Aspectos como el transporte y los servicios a nivel de aplicación, autenticación y carga cifrada se determinan durante esta comunicación de asociación de seguridad. La asociación de seguridad es responsable de ajustar los distintos elementos que establecen la comunicación segura entre anfitriones terminales, incluyendo que el paquete esté cifrado, autenticado o las dos cosas. Además, especifica el cifrado de punto terminal y los protocolos de autenticación, por ejemplo, DES para cifrado y MD5 para autenticación. Asimismo determina las claves utilizadas en estos algoritmos y otros tipos de datos.

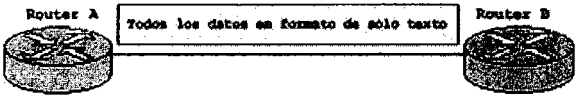
La SA específica se identifica por un número de 32 bits llamado índice de parámetros de seguridad. Este número sólo es un identificador empleado por los mismos anfitriones de comunicación terminal y no tiene ningún significado fuera de esta comunicación. La dirección IP del anfitrión y un índice de parámetros se seguridad indican una SA única. La autoridad Internet para asignación de números asigna números de índice de parámetros de seguridad menores a 256.

IPSec se subdivide posteriormente en dos tipos de transformaciones de datos para la seguridad de los paquetes IP: el Encabezado de Autenticación (AH) y la Carga de Seguridad Encapsulada (ESP).

Encabezado de Autenticación (AH).

La cabecera de autenticación proporciona autenticación e integridad a los datagramas pasados entre dos sistemas.
Esto se logra aplicando una función tipo hash unidireccional con clave al datagrama para crear un boletín de mensajes. Si alguna parte del datagrama es modificada durante el tránsito, será detectada por el receptor cuando realice la misma función tipo hash unidireccional sobre el datagrama y compare el valor del boletín de mensajes que el emisor ha proporcionado. La operación hash unidireccional también implica el uso de un secreto compartido entre los dos sistemas, lo que significa que la autenticidad puede ser garantizada.

La AH puede también reforzar la protección antireproducción al requerir que un host receptor defina el bit de reproducción en la cabecera para indicar que el paquete ha sido visto. Sin esta protección, un atacante podría ser capaz de reenviar el mismo paquete muchas veces: por ejemplo, enviar un paquete que contenga "retirar 100 dólares de la cuenta X". La figura 2.10 muestra dos routers y confirma que los datos entre ellos se envían en formato de sólo texto.



- **Asegura la integridad de los datos**
- **Proporciona autenticación de origen; asegura que los paquetes vinieron definitivamente del vecino.**
- **Utiliza un mecanismo hash con clave.**
- **NO proporciona confidencialidad (sin cifrado).**
- **Proporciona protección oficial de reproducción.**

Figura 2.10

La función AH se aplica a todo el datagrama, exceptuando aquellos campos de la cabecera de IP mutables que cambien en tránsito, como por ejemplo, los campos Tiempo de Vida (TTL) que son modificados por los routers a lo largo de la ruta de transmisión.

La AH funciona como sigue:

Paso 1. Se aplica la función tipo hash a la cabecera de IP y la sobrecarga de datos.

Paso 2. La función tipo hash se utiliza para construir una nueva cabecera AH, que se añade al paquete original.

Paso 3. El nuevo paquete se transmite al vecino IPSec.

Paso 4. El vecino aplica una función tipo hash a la cabecera de IP y la sobrecarga de datos, extrae el resultado de la función tipo hash transmitida desde la cabecera AH, y compara el resultado de las dos funciones hash. Los resultados de las funciones tipo hash deben coincidir con exactitud. Incluso si un bit es cambiado en el paquete transmitido, la salida de la función tipo hash en el paquete recibido cambiará y la cabecera AH no coincidirá.

El RFC-2402 del Encabezado de Autenticación describe como autenticar paquetes de datagramas IP (autenticación de datos) y proporciona integridad sin conexión y, si esta implementada, protección contra ataques repetitivos.

IPSec brinda servicios opcionales contra dichos ataques al utilizar un número de secuencia combinado con el uso de la autenticación; es un servicio de seguridad en el que el receptor puede rechazar paquetes viejos o duplicados para protegerse a sí mismo contra ataques repetitivos. El emisor en el AH incrementará un número de secuencia en la asociación de seguridad para protegerse, pero el receptor no esta obligado a revisar este número. AH no es un mecanismo de seguridad completo, como lo declara el RFC:

AH proporciona autenticación en el encabezado IP en la medida de lo posible, al igual que en los datos de protocolos de nivel superior. Sin embargo, algunos campos de los encabezados IP pueden cambiar en el trayecto y los valores de estos campos, cuando el paquete llegue al receptor, podrían no ser predecibles por el emisor. Los valores de tales campos no pueden protegerse con AH. Por lo tanto, la protección que AH proporciona al encabezado IP se degrada en cierta forma.

AH puede utilizarse en los modos de túnel y transporte. En el modo de transporte, se inserta después del encabezado IP original y protege a los protocolos de nivel superior. En el modo de túnel, se inserta antes del encabezado original y se introduce un nuevo encabezado IP. Además, AH se diseñó para IPv6; en este protocolo AH se considera una carga de extremo a extremo y, de acuerdo con el RFC, aparecerá después de los encabezados de enrutamiento. La figura 2.11 muestra varios modos para AH.

AH proporciona autenticación de datos al calcular un Valor de verificación de integridad (ICV). De acuerdo con el RFC-2402, las funciones de transformación del código MAC (HMAC con MD5 y HMAC con SHA-1) deberían proporcionarlo y soportarlo. Se puede instalar una implementación adicional de algoritmos de autenticación, pero éstos dos son obligatorios.

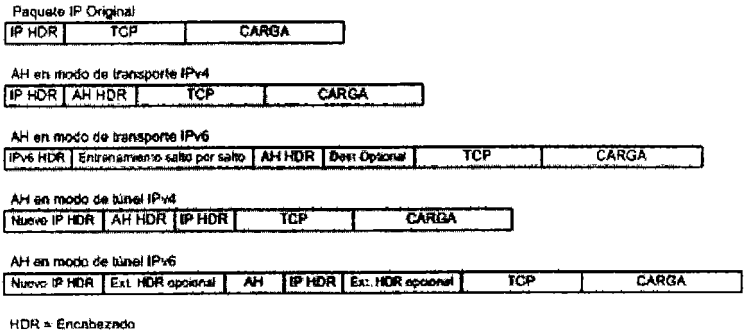
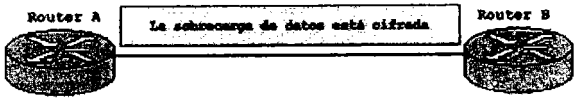


Figura 2.11

Carga con Seguridad de Encapsulamiento (ESP).

La sobrecarga de seguridad del encapsulamiento es un protocolo de seguridad usado para proporcionar confidencialidad (cifrado), autenticación del origen de los datos, integridad, servicio antirreproducción opcional y confidencialidad del flujo de tráfico limitado anulando el análisis del flujo de tráfico. La figura 2.12 muestra que la sobrecarga de datos está cifrada con ESP.



- **Confidencialidad de datos.**
- **Confidencialidad del flujo de tráfico limitado.**
- **Integridad de los datos.**
- **Autenticación opcional del origen de datos.**
- **Protección antireproducción.**
- **No protege la cabecera de IP.**

Figura 2.12

ESP proporciona confidencialidad realizando un cifrado en la capa del paquete IP. Soporta varios algoritmos de cifrado simétrico. El algoritmo predeterminado para IPSec es DES de 56 bits. Este código debe ser implementado para garantizar la interoperabilidad entre los productos IPSec.

La norma de Carga con Seguridad de Encapsulamiento (ESP) proporciona confianza, autenticación, integridad sin conexión y servicios contra repeticiones. Este conjunto de

servicios en ESP se instala durante el establecimiento de la asociación de seguridad. Si sólo se decide instalar la confidencialidad del datagrama, el RFC-2406 que es el que corresponde a ESP, advierte de un problema potencial de seguridad. El RFC dice lo siguiente:

La confidencialidad puede ser independiente de todos los otros servicios. Sin embargo, el uso de la confidencialidad sin integridad/autenticación (ya sea en ESP o separadamente en AH) puede someter al tráfico a ciertas formas de ataques activos que podrían destruir el servicio de confidencialidad.
Como en AH, ESP puede emplearse en dos modos, de transporte y de túnel, tanto para IPv4 como para IPv6.

Al igual que en AH, ESP en modo de transporte protege a los protocolos de niveles superiores la figura 2.13 muestra distintos modos de ESP.

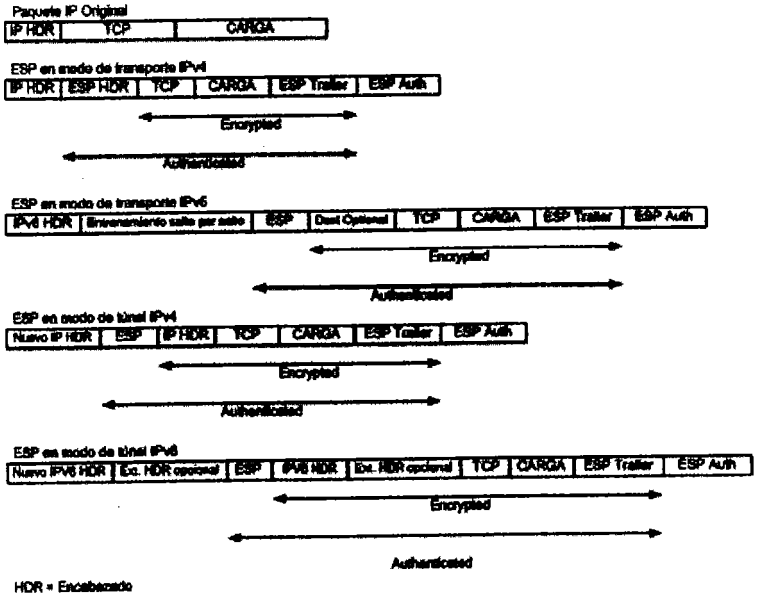


Figura 2.13

2.3.3 Cortafuegos (firewalls).

Además de la criptografía y la autenticación el mecanismo más utilizado para proporcionar seguridad en redes son los cortafuegos (firewalls).

Cabe señalar que los cortafuegos no proporcionan seguridad absoluta, si no que son un mecanismo más, y deben combinarse con otras medidas de seguridad como la criptografía, autenticación de usuarios, etc.

Definición y funciones.

Existen múltiples concepciones posibles para un cortafuego, las cuales pueden ser abarcadas por la siguiente definición:

Un cortafuegos es un mecanismo que combina hardware y software para aislar una red local de Internet, ya que es el qué decide que servicios pueden ser accedidos desde el exterior de una red privada, por quiénes pueden ser ejecutados estos servicios y también qué servicios pueden ejecutar los usuarios de la red interna hacia el exterior. Para realizar esta tarea, todo el tráfico entre las dos redes tiene que pasar a través de él.

Se trata de colocar algún dispositivo o conjunto de dispositivos y programas entre la red local y la red exterior (Internet), con el fin de proteger a la primera de los posibles peligros involucrados por la segunda.

Es importante no confundir un firewall con un enrutador, ya que el primero no direcciona información, función que si realiza el enrutador, además de que el firewall solamente filtra información.

En la figura 2.14 se esquematiza el funcionamiento de un cortafuego:

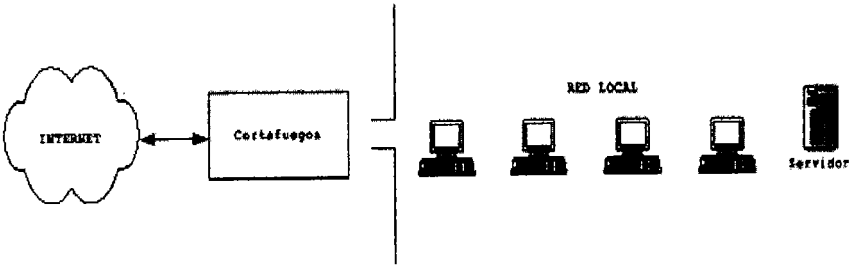


Figura 2.14

Así pues, el objetivo fundamental de un cortafuego es restringir el flujo de información entre las dos redes, la local e Internet. Se trata de prevenir que cualquier ataque desde el exterior afecte a la red local. Por lo tanto, un cortafuego no previene los ataques desde el interior, o aquellos que se llevan a cabo mediante la colaboración de usuarios interiores y exteriores.

Todo el tráfico hacia el interior y desde el interior pasa a través del cortafuego, lo que permite establecer un punto de control donde se implementen toda una serie de medidas de seguridad. Es en los cortafuegos, donde se concreta la política de seguridad relativa al tráfico de la institución propietaria de la red local.
Existen dos políticas generales para el uso de los cortafuegos que coinciden con las establecidas en el control de acceso a sistemas operativos:

- ✓ Permitir por defecto. Siguiendo esta política todos los paquetes cuya circulación no se prohíbe explícitamente pueden circular a través del cortafuego. Cuando el administrador considera que los paquetes de algún origen o relacionados con algún servicio son peligrosos, bloquea su paso. Este tipo de política es más sencillo de aplicar, pero puede ser más peligroso. En este caso si algún servicio desconocido o no controlado es peligroso puede causar problemas en la red local.
- ✓ Denegar por defecto. Siguiendo esta política los paquetes cuya circulación no esté explícitamente permitida quedan bloqueados en el cortafuego. En este caso el administrador del cortafuego debe estudiar qué paquetes quiere dejar pasar y cuáles son sus implicaciones de seguridad. Esto hace que sea una política más costosa de implementar, pero mucho más segura.

Las principales funciones de los cortafuegos son las siguientes:

- ✓ Bloquear el acceso a determinados lugares en Internet (redes, subredes, nodos específicos), o prevenir que ciertos usuarios o máquinas puedan acceder a ciertos servidores o servicios.
- ✓ Filtrar los paquetes que circulan entre la red local e Internet, de modo que sólo aquellos correspondientes a servicios permitidos puedan pasar (telnet, e-mail, ftp, www, etc.).
- ✓ Monitorear el tráfico, supervisar el destino, origen y cantidad de información enviados o recibidos.
- ✓ Almacenar total o selectivamente los paquetes que circulan en el cortafuego con el fin de analizarlos en caso de problemas.
- ✓ Establecer un punto de cifrado de la información si se pretenden comunicar dos redes locales a través de Internet.

Componentes.

Los cortafuegos se construyen a partir de dos componentes fundamentales: filtros y nodos bastión.

Los filtros son dispositivos que permiten bloquear selectivamente determinados tipos de paquetes. Normalmente se utilizan para este propósito encaminadores o máquinas con esta función específica. En la figura siguiente podemos observar el esquema de un dispositivo de éste tipo.

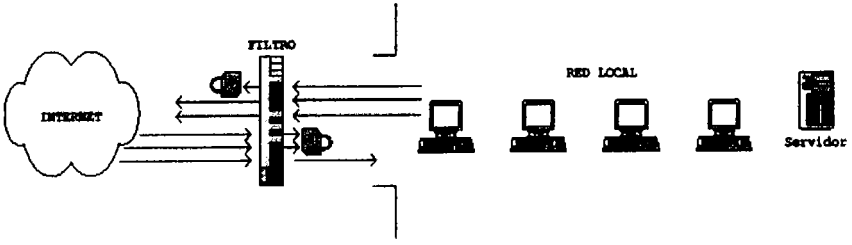


Figura 2.15

Los nodos bastión son computadoras altamente seguras que sirven como punto de contacto principal entre Internet y la red local. Se trata de máquinas muy vulnerables al encontrarse expuestas directamente a Internet. En la siguiente figura podemos observar el esquema de un nodo bastión.

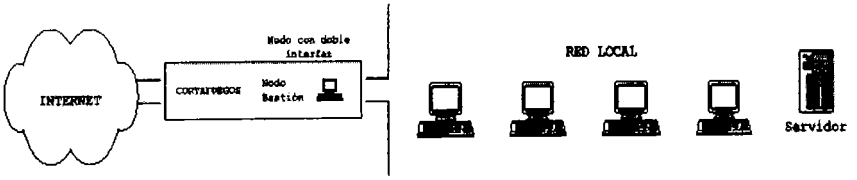


Figura 2.16

Los nodos bastión suelen ser máquinas UNIX en las que se han extremado las medidas de seguridad. Para ello el sistema debe reducirse al máximo y tan sólo deben instalarse los servicios que sean absolutamente imprescindibles. Algunas de las medidas de seguridad a tomar en estos nodos son las siguientes:

- ✓ Intensificar la monitorización y auditación de acciones.
- ✓ No permitir las cuentas de usuario normales.
- ✓ Borrar:

    1. Todos los comandos innecesarios para su funcionamiento.
    2. Todos los compiladores y las librerías innecesarias.
    3. Todos los intérpretes de órdenes.

- ✓ Extremar la rigurosidad en los permisos sobre archivos y directorios.
- ✓ Eliminar todos los servicios de red innecesarios.
- ✓ Sustituir las versiones estándar de los servidores de red por otras versiones más seguras.

Los distintos tipos de cortafuegos existentes se basan en la combinación adecuada de uno o varios de los siguientes componentes:

- ✓ Un enrutador que sirva única y exclusivamente de filtro de paquetes.

- ✓ Un servidor proxy o gateway a nivel de aplicación.
- ✓ El gateway a nivel de circuito.

Técnicas de uso.

El funcionamiento de los cortafuegos se basa en el uso de dos tipos de técnicas básicas sobre los filtros y nodos bastión:

1. El filtrado de paquetes.
2. La delegación (proxying).

Filtrado de paquetes.

El filtrado de paquetes consiste en controlar selectivamente que paquetes circulan entre la red local e Internet. Para llevar a cabo este control se definen una serie de reglas que especifican que tipo de paquetes pueden circular en cada sentido y cuales deben bloquearse. El filtrado de paquetes se desarrolla en un filtro, que como se comento anteriormente, puede ser un router o una máquina a la que se le ha asignado esta función.

Las reglas para permitir los paquetes permitidos y bloqueados se basan en las cabeceras de los paquetes, y fundamentalmente en los siguientes datos incluidos en las mismas:

- ✓ Dirección IP de la fuente.
- ✓ Dirección IP del destino.
- ✓ Tipo de protocolo (TCP, UDP, ICMP, etc.)
- ✓ Puerto TCP o UDP de la fuente.
- ✓ Puesto TCP o UDP del destino.
- ✓ Algunas de las banderas u opciones de las cabeceras.

El hecho de que los programas servidores para determinados servicios Internet, tales como ftp, telnet, correo electrónico, etc., residan en ciertos puertos, permite al filtro aceptarlos o bloquearlos, simplemente especificando el puerto correspondiente. Así,

sería posible bloquear los conexiones telnet desde el exterior sin más que impedir el paso de todos los paquetes cuyo puerto destino sea el puerto TCP 23.

Algunos ejemplos de uso del filtrado de paquetes podrían ser los siguientes:

- ✓ Bloquear todas las conexiones desde el exterior excepto aquellas correspondientes a paquetes SMTP, es decir, aquellas que van destinadas al puerto 25 y que permiten la recepción de correo electrónico.
- ✓ Bloquear todas las conexiones desde o hacia ciertos sistemas (redes, subredes o nodos) en los que no confiamos.
- ✓ Permitir ciertos servicios básicos como correo electrónico o ftp, pero bloquear otros "peligrosos" que pueden permitir acceso al servidor remotamente y sin identificación continua del usuario.

Mediante el uso del filtrado de paquetes, es posible discriminar entre determinados tipos de paquetes, permitir o denegar determinados servicios, pero no es posible protegerse de operaciones elementales dentro de los servicios que pueden resultar inseguras, es decir, no se puede personalizar el funcionamiento de los mismos. Con el fin de lograr este último tipo de control se suele utilizar la delegación (proxying).

Servicios delegados (proxy services).

Los servicios delegados son aplicaciones especializadas que funcionan en un cortafuego (normalmente en el nodo bastión) y que sirven de intermediarios entre los servidores y clientes reales. Estas aplicaciones reciben las peticiones de servicios por parte de los usuarios, los analizan y en su caso modifican, y los transmiten a los servidores reales.

En un servicio delegado se distinguen tres componentes:

1. El servicio real.
2. El servidor delegado (proxy server).
3. el cliente delegado (proxy client).

El servidor real funciona en un nodo externo en Internet y proporciona algún servicio tal como conexión telnet, correo electrónico, conexión http, etc. Se trata de alguno de los programas servidores propios del sistema operativo, tales como el telnetd, ftpd, sendmail, entre otros., que se encuentra activos en los puertos del nodo servidor remoto.

El cliente delegado (proxy client) es una versión especial del programa cliente estándar del sistema operativo (telnet, ftp, netscape, etc.). Este programa funciona en los nodos de la red local y es utilizado por los usuarios para acceder al servicio.
El programa se ha preparado para que cuando el usuario solicite algún servicio se conecte al servidor delegado, y no al servidor real en Internet. Como se ejemplifica en la figura 2.17.

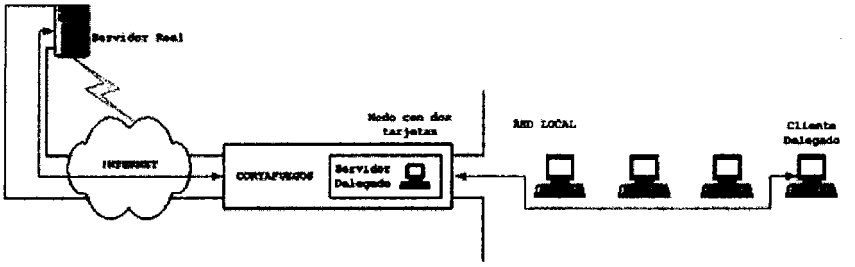


Figura 2.17

El servidor delegado (proxy server) es un programa especial que funciona sobre el cortafuego (normalmente sobre el nodo bastión). Este programa actúa como intermediario entre el cliente delegado y el servidor real. Su funcionamiento es totalmente transparente a ambas partes, es decir, al servidor real y al usuario que utiliza el programa cliente. Cuando el usuario intenta obtener un servicio lo hace a través del servidor delegado, pero cree estar conectado directamente con el servidor real en Internet. En cuanto al servidor externo, cuando recibe o envía paquetes al servidor delegado, cree estar conectado directamente con el nodo local en el que se origina la petición y no con el programa cliente funcionando sobre el nodo bastión.

Las conexiones se efectúan como se muestra en la figura 2.18.

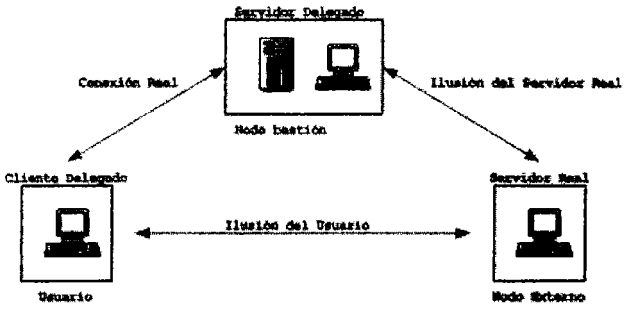


Figura 2.18

La función del servidor delegado es analizar los paquetes que circulan a través de él, estudiar su contenido y, en función de la política de seguridad de la organización, permitir o denegar su acceso o modificar su contenido o cabeceras.
También pueden usarse estos programas para monitorear el tráfico y almacenar datos sobre el mismo, tales como los destinos u orígenes más comunes, los servicios más solicitados, etc.

Algunos ejemplos de uso de los servicios delegados son los siguientes:

- ✓ Cifrado de la información enviada y descifrado de la recibida. Especialmente útil cuando se requiere conectar dos redes locales a través de Internet.
- ✓ Modificación de las cabeceras de los correos electrónicos con el fin de ocultar información sobre la red local.
- ✓ Autenticación mediante un sistema más potente que el de contraseña simple. Por ejemplo puede utilizarse un mecanismo de contraseñas de un solo uso para acceder a la red local desde Internet, mientras que las máquinas locales tan sólo utilizan un mecanismo de contraseña simple.

Arquitecturas de cortafuegos.

La combinación de los dos componentes básicos de los cortafuegos (filtros y nodos bastión), y la utilización de las dos principales funciones (filtrado y delegación) sobre ellos, permite definir múltiples tipos de arquitecturas para los cortafuegos. Las cuatro más comunes de menor a mayor grado de sofisticación y seguridad proporcionada son:

1. **Filtro de paquetes (screening router).**

Esta arquitectura se basa en el uso de un simple filtro de paquetes que se encuentra entre Internet y la red local. Este filtro de paquetes suele ser un encaminador (router) que implementa las reglas de filtrado de la red local.

El problema de este tipo de cortafuegos es que toda la seguridad del sistema con respecto Internet se concentra en el router. Adicionalmente el simple filtrado de paquetes no permite una gran flexibilidad a la hora de controlar la seguridad de los diferentes servicios que incluyen.

2. **Nodo con doble interfaz.**

El nodo con doble interfaz (dual-homed host architecture) se construye sobre una máquina que actúa como nodo bastión y que incorpora dos tarjetas o interfaces de red. Una tarjeta tan sólo permite la comunicación con el exterior (Internet), mientras la otra tan sólo permite la comunicación con la red local. Cualquier tipo de comunicación entre las dos tarjetas se encuentra bloqueada.
Usando este tipo de cortafuegos la comunicación directa entre la red local e Internet esta prohibida. Cualquier servicio que se quiera proporcionar a los nodos locales debe implementarse mediante un servidor delegado ejecutado sobre el nodo con doble bastión.

Otra solución consiste en permitir a los usuarios conectarse al nodo bastión para que éstos accedan a los servicios de Internet. Sin embargo esta opción es bastante peligrosa puesto que puede dejar desprotegido al nodo bastión.

3. **Nodo pantalla.**

En esta arquitectura, el cortafuegos se construye combinando un filtro y un nodo bastión; el primer nivel de seguridad descansa sobre el filtro y sobre el modo en que éste realice la función del filtrado de paquetes. El nodo bastión se sitúa en la red local y se encarga de ejecutar los distintos servidores que conectan a la red local con Internet.

El filtrado de paquetes de diseña de modo que no se permita el tráfico directo entre los nodos locales e Internet. Todo el tráfico, tanto de salida como de entrada, debe circular a través del nodo bastión y del filtro. Cuando el filtro recibe paquetes desde el interior, sólo debe dejar pasar aquellos que provengan del nodo bastión. Asimismo, cuando el filtro recibe paquetes desde el exterior, tan sólo debe dejar pasar aquellos que vayan dirigidos al nodo bastión.

De este modo, el único nodo que realmente puede recibir y enviar correo, abrir conexiones telnet, enviar o recibir ficheros por ftp, etc., es el nodo bastión. La seguridad en los distintos tipos de servicios pueden conseguirse directamente a través del filtrado de paquetes, o bien combinando este con un servidor delegado. En el segundo caso, cuando un usuario quiere acceder a alguno de estos servicios, si están permitidos, utiliza el cliente delegado en su nodo local, este programa contacta con el servidor delegado en ejecución en el nodo bastión, y es el servidor delegado el que realmente interactúa con los servidores de Internet pasando a través del filtro.
Dado que el nodo bastión es la única máquina de la red local expuesta a Internet (siempre a través del filtro), se deben tomar especiales medidas de protección sobre el mismo.
El principal problema de este tipo de arquitecturas se produce cuando se compromete el nodo bastión. En este caso toda la red local queda expuesta a cualquier tipo de ataque desde el exterior.

4. Red pantalla.

Se trata de una arquitectura más sofisticada y al mismo tiempo más segura que las anteriores, por lo que cada vez es más utilizada. Este tipo de cortafuegos consta de dos filtros y de un nodo bastión.

Los dos filtros, uno interior y uno exterior, definen entre ellos una red de perímetro (que actúa como red pantalla). En esta red de perímetro se encuentra situado el nodo bastión. Con este tipo de configuración, si el nodo bastión es comprometido, el atacante tan sólo tendrá acceso a la red de perímetro, y no podrá acceder directamente a los nodos de la red local.

La red perímetro actúa como un nivel más de seguridad del sistema. Todo el tráfico confidencial entre los nodos locales, incluyendo las contraseñas de usuario, circula tan sólo a través de la red local. El único tráfico permitido en la red de perímetro debe ser el destinado o proveniente de Internet.
Las técnicas de protección utilizadas con este tipo de arquitectura son similares a las de la arquitectura de nodo pantalla. Los servicios pueden controlarse directamente mediante los dos filtros, o bien pueden implementarse mediante un servidor delegado en ejecución en el nodo bastión.

En ocasiones la red de perímetro contiene más de un nodo bastión. Cada nodo en esta red puede encargarse de algunos de los servicios. Por ejemplo, uno podría encargarse del ftp y www, mientras otro podría encargarse del correo electrónico y el servicio de nombres por dominio.

Beneficios y limitaciones de un cortafuego.

Beneficios.

Los cortafuegos manejan el acceso entre dos redes, si no existiera, todos los hosts de la intranet estarían expuestos a ataques desde hosts remotos en Internet. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada máquina interna.

El cortafuegos es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador de la red tendrá el poder de decidir si revisar éstas alarmas o no, la decisión tomada por éste, no cambiará la manera de operar del cortafuegos.

Otra causa que ha hecho que el uso de los cortafuegos se halla convertido en casi imperativo, es el hecho de que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones CIRD (o direcciones sin clase), las cuales salen a Internet por medio de un

NAT[27], y efectivamente el lugar ideal y seguro para alojar el NAT ha sido el cortafuegos.

Los cortafuegos también han sido importantes desde el punto de vista de llevar las estadísticas del ancho de banda usado por el tráfico de la red, y qué procesos han influido más en ese tráfico, de esta manera el administrador de la red, puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda.

Finalmente, los cortafuegos también son usados para albergar los servicios www y ftp de la intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables.

Limitaciones.

La limitación más grande que tiene un cortafuego, es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, actúan de acuerdo a parámetros introducidos por el diseñador, por lo tanto, si un paquete de información no se encuentra dentro de esos parámetros como una amenaza de peligro, simplemente lo dejará pasar. Pero esto no es lo más peligroso, si no cuando el intruso deja puertas traseras, es decir, abre un hueco diferente y borra las pruebas o indicios del ataque original.

Otra limitación es que el cortafuego no es contra humanos, es decir, que si un intruso logra entrar a la organización y descubrir passswords o se entera de los huecos del cortafuego y difunde la información, éste no será capaz de detectarlo.

[27] Network Address Traslator.

Tipo de Cortafuegos	Ventajas	Desventajas	Recomendación
Filtrado de Paquetes	- Bajo costo. - Rápidos, flexibles y transparentes. - Puede bloquear todas las conexiones desde o hacia ciertos sistemas en los que no confiamos. - Se puede permitir o denegar determinados servicios.	- Baja seguridad. - Difícil mantenimiento de reglas de filtrado. - No protegen contra engaño de direcciones DNS o IP. - Proporcionan poca o nula información útil de registro.	Buena opción para entornos de bajo riesgo
Servicios Delegados	- Puede configurarse como la única dirección de computadora que es visible para la red externa. - Puede proporcionar registro detallado. - La autenticación fuerte de usuario puede ser obligada.	-Alto costo. - Son más seguros pero más lentos.	Buena opción para entornos de riesgo medio.

Cuadro 1

2.4 ADMINISTRACIÓN Y CALIDAD DE SERVICIO DE LAS VPN.

En la actualidad los sistemas informáticos se basan en una red de datos, la cual debe ser capaz de soportar una cada vez más amplia gama de aplicaciones. El protocolo de Internet, que ha sido utilizado en estas redes durante las tres últimas décadas para el intercambio de información entre los diferentes ordenadores, ha terminado imponiéndose como el protocolo más usado.

Actualmente el desarrollo de estas redes de datos se está enfocando hacia la provisión de Calidad de Servicio (QoS)[28], la cual se requiere para permitir asegurar determinadas características de calidad en la transmisión de información. El objetivo es evitar que la congestión de determinados nodos de la red afecte a algunas aplicaciones que requieran un especial caudal o retardo, como pueden ser aplicaciones de videoconferencia. Para solucionar este problema existen dos tendencias muy distintas:

Sobredimensionar adecuadamente la red de transporte, esto implica aumentar cuando resulte necesario los equipos de conmutación así como el ancho de banda disponible en los canales. Este método se basa en el abaratamiento de los sistemas de conmutación y transporte, si bien provoca una gestión ineficiente por definición de los recursos disponibles.

[28] Quality of Service.

Gestionar de forma inteligente los recursos disponibles, compartiéndolo de manera desigual entre los diferentes flujos de tráfico.

Sin embargo, las actuales redes de datos no distinguen entre las diferentes aplicaciones que transportan: no pueden diferenciar entre una videoconferencia con determinados requisitos de ancho de banda y la navegación Web de características completamente diferentes. Esto requiere que primero se lleve a cabo una adecuada administración y segundo que de alguna manera las funciones de calidad de servicio sean capaces de reconocer las aplicaciones para reservarles unos determinados recursos en la red.

2.4.1 Administración de redes.

A continuación podemos ver algunos conceptos y aspectos básicos.

La administración de redes significa diferentes cosas para diferentes personas. En algunos casos, implica a un consultor de redes solitario que supervisa la actividad de la red con un analizador anticuado de protocolos.

En otros, la administración de redes involucra una base de datos distribuida, un autosondeo de dispositivos de red y estaciones de trabajo, que generan vistas gráficas en tiempo real de los cambios de la topología de la red y del tráfico.

La administración de redes es el proceso de gestión de fallos, control de configuraciones, supervisión de rendimiento, aseguramiento de la seguridad y contabilidad de actividades en una red de datos. Es necesario que todas estas tareas tengan un control absoluto sobre algún entorno de la red de datos, que es uno de los componentes esenciales de cualquier organización. El ISO Network Management Forum ha definido la administración de redes como la suma de todas las actividades necesarias para realizar la administración de los fallos, la configuración, el rendimiento, la seguridad y la contabilidad de una red de datos.

El objetivo principal de la administración de red es en mantener operativa la red satisfaciendo las necesidades de los usuarios. La utilización de herramientas adecuadas

permite realizar de forma centralizada la administración de múltiples redes de gran tamaño compuestos de cientos de servidores, puestos de trabajo y periféricos.

Normalmente las herramientas de administración de red forman un conjunto muy heterogéneo de aplicaciones provenientes de, por ejemplo, el sistema de gestión de red, el Help Desk, herramientas de los fabricantes de los dispositivos, herramientas autónomas e independientes. Además muchas de estas herramientas suelen tener APIs (Application Program Interface) que permiten el acceso por programación.

Hoy en día estas herramientas corren sobre diferentes sistemas operativos y suelen tener la característica de disponer de un interfase gráfico de usuario basado en ventanas.

Algunos ejemplos de plataformas de administración de redes son:

Hewlett–Packard OpenView, Cabletron Spectrum, Sun Solstice, enterprise Manager, IBM NetView/AIX y CiscoWorks2000. Estas plataformas proporcionan la arquitectura de software para las aplicaciones de administración de redes que realizan una gran variedad de tareas.

No se pueden agrupar en una sola categoría. Algunas presentan un mapa de la red y comprueban el estado de todos los dispositivos de la red, lo que proporciona una función de administración de fallos. Algunas herramientas de administración del rendimiento diseñan la utilización de los enlaces de la red y envían advertencias si se producen errores en alguna interfaz de LAN. Sin embargo, otras vigilan la seguridad de la red y envían advertencias a través del correo electrónico o de buscapersonas.

Ahora, conozcamos los componentes de la administración de redes.

Agentes y consolas.

Los agentes y consolas son los conceptos claves en la administración de redes.

- ✓ Consola: es una estación de trabajo convenientemente configurada para visualizar la información recogida por los agentes.

- ✓ Agentes: son programas especiales que están diseñados para recoger información específica de la red.

Entre las características de los agentes cabe destacar:

- ✓ Están basados en software frente a monitores y analizadores basados en hardware.
- ✓ Son transparentes a los usuarios. Se ejecutan en los puestos de trabajo sin afectar al rendimiento de los mismos.
- ✓ La información que recogen la almacenan en bases de datos relacionales que después son explotadas a través de las consolas.
- ✓ Los agentes son configurados de forma remota a través de la consola para su correcta operación.
- ✓ Al ser software pueden realizar las mismas tareas que los analizadores y hacen un mayor procesamiento de la información que obtienen.

Las funciones que soportan los agentes son entre otras:

- ✓ Visualizar y manipular información de la red.
- ✓ Automatizar la distribución de ficheros.
- ✓ Mantener el inventario del hardware.
- ✓ Gestión y configuración del software remoto.
- ✓ Recibir notificación de alarmas de red.
- ✓ Soportar y gestionar la impresión en red.
- ✓ Automatizar tareas como copias de seguridad y detección de virus.
- ✓ Monitorizar la utilización de discos y de ficheros.
- ✓ Establecer y gestionar la seguridad en la red.
- ✓ Procesar scripts.

Gestión de usuarios.

La gestión de usuarios es la actividad referida a la creación y mantenimiento de cuentas de usuarios, así como la de asignación de recursos y mantenimiento de la seguridad en los accesos a la red.

Las tareas principales en la gestión de usuarios son:

1. Altas, bajas y modificaciones de usuarios en la red.
2. Establecimiento de políticas de passwords como su longitud, tiempo de vida, seguridad de la base de datos de passwords, etc.
3. Asignación de permisos para la utilización de recursos de red.
4. Monitorización de la actividad de los usuarios.
5. Establecimiento de políticas generales y de grupo que faciliten la configuración de usuarios.

Gestión del hardware.

La gestión del hardware es una actividad esencial para el control del equipamiento y sus costes asociados así como para asegurar que los usuarios disponen del equipamiento suficiente para cubrir sus necesidades.

Para evitar visita física a los equipos, se utilizan agentes que se ejecutan en los puestos de trabajo y que realizan el inventario del hardware de forma autónoma y remota.

Una vez que la información de inventario es recogida, la administración de red puede hacer las siguientes funciones:

1. Añadir información relativa a puestos de trabajo no instalados en red.
2. Añadir información sobre otros aspectos como la localización física, condiciones en que se encuentra, etc.
3. Establecimiento de parámetros de configuración en los ficheros de configuración del sistema operativo.
4. Realizar el seguimiento de averías de los componentes de las estaciones de trabajo.
5. Anotar información al inventario referente a los componentes que forman la estación de trabajo (tarjetas, discos, etc.).

El inventario se realiza periódicamente bien cada vez que se ponen en marcha los puestos o bien durante su tiempo de funcionamiento. Normalmente los datos que se recogen son variados:

- ✓ BIOS del sistema.
- ✓ Ficheros de configuración del sistema operativo.

- ✓ Parámetros del sistema operativo.
- ✓ Características de los discos duros.
- ✓ Drivers cargados en memoria durante el funcionamiento de la estación.
- ✓ Otras características establecidas por el administrador.

En los servidores, además se suelen realizar un seguimiento de los parámetros de funcionamiento como pueden ser actividad del CPU, de los discos, espacios disponibles, número de conexiones, etc.

Este seguimiento permite analizar el comportamiento y, en su caso, detectar nuevas necesidades y adaptar las características hardware de los servidores.

Gestión del software.

Las actividades relativas a la gestión de software permiten a la administración de red determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red.

De igual forma que en el hardware, se utilizan agentes que realizan la función de obtener toda la información acerca del software en la red. Sus características particulares son:

- ✓ Obtienen su información chequeando todos los discos de los puestos de trabajo en la red.
- ✓ Normalmente son capaces de identificar cientos de paquetes comerciales y se les puede añadir nuevos paquetes particulares de la empresa.
- ✓ Realizan mediciones del número de copias de un paquete que se están usando en la red de forma simultánea con objeto de comprobar su adecuación al número de licencias adquiridas.

Las tareas que normalmente realiza la administración de red en esta área son:

- ✓ Creación y mantenimiento del inventario de software instalado.
- ✓ Especificación y requerimiento del número de copias disponibles de los distintos paquetes.

- ✓ Seguimiento de la instalación no autorizada de software y de otros ficheros en prevención de introducción de virus.
- ✓ Autorización a los usuarios para la utilización de los paquetes de software.

La información que se suele extraer es la siguiente:

- ✓ Información general del paquete: fabricante, versión, nº de licencias, etc.
- ✓ Disponibilidad: quién usa el software, quién lo puede usar, etc.
- ✓ Ficheros que componen el paquete.
- ✓ Información adicional establecida por el administrador.

Distribución de ficheros.

Debido a la enorme dispersión de puestos en red, la distribución de software y otros ficheros se realiza mediante la utilización de agentes de distribución de ficheros.

Las características de los agentes de distribución de ficheros son:

- ✓ Las funciones que realizan son instalación y actualización de software, descargas y eliminación de ficheros.
- ✓ Pueden aplicarse a puestos individuales o a grupos de estaciones simultáneamente.
- ✓ Recoger información sobre el estado de la distribución presentando la información en la consola de administración.
- ✓ Tienen en cuenta los permisos de accesos de los usuarios a más de una máquina para instalar el software en cada una de las máquinas a las que se accede.

En la mayoría de los casos se utilizan lenguajes de scripts para realizar las tareas de distribución de software.

Otros paquetes más sofisticados disponen de herramientas que guían el proceso de creación de scripts generando paquetes completos que contienen scripts, ficheros y reglas de dependencias para su correcta distribución.

Normalmente estos paquetes se comprimen para ahorrar tráfico de red.

Los momentos de distribución suelen ser cuando los puestos inician su funcionamiento aunque los usuarios a veces puedan posponer la instalación de paquetes.

Monitorización de la actividad de red.

Las funciones de la monitorización de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas al personal responsable del buen funcionamiento de la red.

Los eventos típicos que son monitorizados suelen ser:

- ✓ Ejecución de tareas como pueden ser realización de copias de seguridad o búsqueda de virus.
- ✓ Registro del estado de finalización de los procesos que se ejecutan en la red.
- ✓ Registro de los cambios que se producen en el inventario de hardware.
- ✓ Registro de las entradas y salidas de los usuarios en la red.
- ✓ Registro del arranque de determinadas aplicaciones.
- ✓ Errores en el arranque de las aplicaciones.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención se pueden utilizar diferentes métodos de notificación como son:

- ✓ Mensajes en la consola: se suelen codificar con colores en función de su importancia.
- ✓ Mensajes por correo electrónico: conteniendo el nivel de prioridad y el nombre e información del evento.
- ✓ Mensajes a móviles: cuando el evento necesita intervención inmediata se suele comunicar a los técnicos de guardia a través de este método.

Además de los eventos, otra característica importante es la monitorización del tráfico de red:

- ✓ Se toman nuevas medidas sobre aspectos de los protocolos, colisiones, fallos, paquetes, etc.
- ✓ Se almacenan en bases de datos para su posterior análisis.

- ✓ Del análisis se obtienen conclusiones, bien para resolver problemas concretos o bien para optimizar la utilización de la red.

Planificación de procesos.

En vez de tener que recordar y realizar trabajos periódicos o en horas no laborables, el administrador puede programar un agente que realiza las tareas programadas en los momentos previstos.

Además, estos agentes recogen información sobre el estado de finalización de los procesos para un posterior análisis por el administrador.

Los procesos típicos que se suelen planificar son: copias de seguridad, búsqueda de virus, distribución de software, impresiones masivas, etc.

La planificación de procesos permite también aprovechar los períodos en que la red esta más libre como las noches y los fines de semana.

Los planificadores como AT de Windows NT y CRON de UNIX permiten procesos especificando un momento determinado y una frecuencia.

Normalmente también se suelen usar scripts para programar a los agentes planificadores.

Protección contra virus.

La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en los puestos de trabajo.

La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador, comunicación con otros servidores distribuidos en la red con software antivirus, protección de los discos y ficheros de los propios servidores, etc.

Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

Soporte de impresoras.

La gestión centralizada de impresoras en la red permite reducir el tiempo y el esfuerzo que necesitan los usuarios para configurar la impresión desde unos puestos de trabajo y también permiten al administrador realizar una gestión unificada de todas las impresoras de la red.

Las actividades relacionadas con el soporte de impresoras son dos:

1. Las relacionadas con el manejo de las impresoras por parte del administrador.
2. Las relacionadas con la selección de impresoras e impresión por parte de los usuarios.

El modo de operar suele ser el siguiente:

1. El administrador da de alta las impresoras en la red seleccionando los servidores que actuarán de spoolers, identificándolos con un nombre y asociando el driver correspondiente para su utilización.
2. Posteriormente el administrador, establece las condiciones de acceso como permisos a los usuarios, horario de acceso a las impresoras, etc.
3. El usuario después selecciona las impresoras de las que tiene acceso permitido y las instala en un puerto de trabajo de forma remota y transparente.
4. Cuando el usuario imprime también tiene acceso a las colas de impresión de forma que puede añadir o eliminar trabajos de su propiedad.
5. El administrador a través de la consola y los agentes de impresión monitoriza la actividad de las impresoras y soluciona problemas que puedan surgir.

Gestión del espacio de almacenamiento.

La utilización masiva de servidores de ficheros y bases de datos en las redes actuales han hecho del espacio de almacenamiento un recurso común a los usuarios y un elemento escaso que hay que optimizar.

El administrador utiliza agentes que recolectan información sobre el grado de ocupación de los discos con objeto de tomar decisiones al respecto de la redistribución de ficheros y de la adquisición de nuevos discos.

La extracción de información que realiza el agente suele ser a nivel de:

- ✓ Partición: utilización del espacio de la partición (poco nivel de detalle).
- ✓ Directorios: grado de utilización del espacio para los directorios.
- ✓ Ficheros: tamaño que ocupan los ficheros.

Al igual que con otras actividades de administración se suelen programar una serie de eventos consistente en ciertos límites que cuando son sobrepasados elevan una alarma que es comunicada al administrador a través de un mensaje en la consola, un correo electrónico o un mensaje a un móvil por ejemplo.

La tarea de recopilación de información normalmente se puede hacer en background sin afectar a los procesos en ejecución aunque también pueden ser planificados para su posterior ejecución.

Seguridad.

La seguridad es un aspecto que afecta a todas las áreas de administración que se han comentado anteriormente.

Para cada recurso en la red, el administrador dispone de los mecanismos para establecer permisos de utilización, así como monitorizar el uso que se hace de los recursos.

Todas estas tareas son muy complejas por lo que se utilizan actualmente políticas de seguridad. Las políticas de seguridad permiten establecer aspectos de seguridad en forma de perfiles que afectan a grupos de usuarios. Una vez definidas las políticas, el administrador sólo tiene que añadir los usuarios a los grupos establecidos con lo que adquieren los perfiles de seguridad. De esta forma la actualización de medidas de seguridad se hace sobre las políticas y no sobre los usuarios directamente.

Otro aspecto a considerar es el de la monitorización y registro de las actividades de los usuarios pudiendo denegar el acceso de los usuarios en función de que intenten realizar actividades para los que no tienen permiso.

Arquitectura de la administración de la red.

La mayoría de las arquitecturas de administración de la red utilizan el mismo conjunto de relaciones y estructura básicas.
Las estaciones terminales (dispositivos administrados), como sistemas de computación y otros dispositivos de red, corren software que les permite enviar señales de alerta cuando descubren que hay problemas (por ejemplo, cuando se excede uno o más de los niveles de umbral fijados por el usuario).

En el momento en que reciben estas señales de alerta, las entidades de administración se programan para reaccionar ejecutando una, varias o un grupo de acciones, incluyendo la notificación del operador, el registro de eventos, el corte del sistema y los intentos automáticos de reparación del sistema.

Las entidades de administración también pueden sondear a las estaciones terminales para verificar los valores de determinadas variables.
El sondeo puede ser automático o iniciado por el usuario, pero los agentes en los dispositivos que se están administrando responden a todos los sondeos.
Los agentes, como ya mencionamos anteriormente, son módulos de software que, en primer lugar, compilan información acerca de los dispositivos administrados en los que residen, después almacenan esta información en una base de datos de administración y, por último, la ponen a disposición (de manera proactiva o reactiva) de las entidades de administración que forman parte de los NMSs (Sistemas de Administración de la Red) vía un protocolo de administración de red.

Entre los protocolos más conocidos de administración de redes están SNMP y CMIP (Protocolo de Información de Administración común).

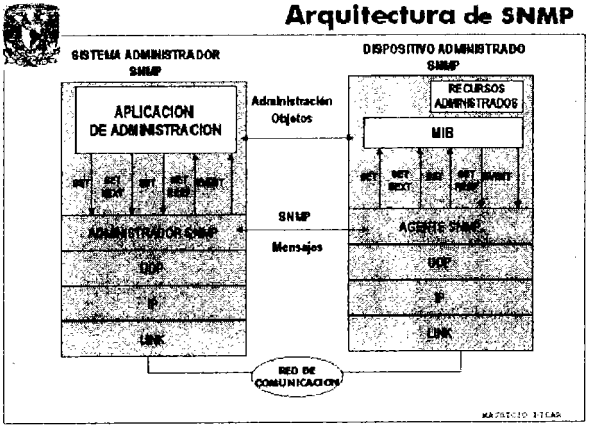


Figura 2.19

Modelo de administración de red de la ISO.

La ISO ha contribuido en gran medida a la estandarización de las redes. Su modelo de administración de redes es el medio que más puede ayudar al lector a comprender las funciones principales de los sistemas de administración de redes. Este modelo consta de 5 áreas conceptuales:

- ✓ Administración del desempeño.
- ✓ Administración de la configuración.
- ✓ Administración de la contabilidad.
- ✓ Administración de fallas.
- ✓ Administración de la seguridad.

Administración del desempeño.

El objetivo de la administración del desempeño es medir y hacer disponibles diferentes aspectos del desempeño de la red para que el desempeño total de la interred se pueda mantener a un nivel aceptable.

Como ejemplos de las variables de funcionamiento que se pueden proporcionar están el rendimiento eficiente total de la red, los tiempos de respuesta del usuario y la utilización de la línea.

La administración del desempeño implica tres pasos principales. Primero, se reúnen los datos del funcionamiento con respecto a las variables de interés para los administradores de la red.

Segundo, se analizan los datos para determinar los niveles normales (niveles base). Por último, se determinan umbrales de desempeño adecuados para cada variable importante, de modo que excederlos indique un problema en la red al cual valga la pena prestar atención.

Las entidades de administración supervisan de manera continua las variables del desempeño. Cuando se excede un umbral del desempeño, se genera una señal de alerta y se envía al sistema de administración de la red.

Cada uno de los pasos que se acaban de describir son parte del proceso de establecimiento de un sistema reactivo. Cuando el desempeño de la red se hace inaceptable por haberse excedido un umbral definido por el usuario, el sistema reacciona enviando un mensaje.

La administración del desempeño también permite el uso de métodos proactivos; por ejemplo, se puede utilizar una simulación de la red para hacer una proyección de cómo se verán afectados los parámetros por el desempeño del crecimiento de la red.
Dicha simulación puede poner en alerta a los administradores de la red para que traten de retrazar la aparición de problemas y tomen medidas tendientes a eliminarlos.

Administración de la configuración.

El objetivo de la administración de la configuración es supervisar la red, así como la información referente a la configuración del sistema, para que se pueda registrar y administrar los efectos de las diferentes versiones de los elementos de software y hardware sobre la operación de la red. Cada dispositivo de red tiene una amplia gama de

información respecto a la versión asociada con él. Una estación de trabajo de ingeniería, por ejemplo, puede configurarse de la manera siguiente:

- ✓ Sistemas operativos, versión 3.2
- ✓ Interfaz de Ethernet, versión 5.4
- ✓ Software TCP / IP versión 2.0
- ✓ Software NetWare, versión 4.1
- ✓ Controlador de comunicaciones seriales, versión 1.1
- ✓ Software X25, versión1.0
- ✓ Software SNMP, versión 3.1

Los subsistemas de administración de la configuración almacenan esta información en una base de datos para tener fácil acceso a ella.
Cuado se presenta un problema, se puede buscar esta base de datos para tratar de encontrar claves que ayuden a resolver el problema.

Administración de la contabilidad.

El objetivo de la administración de la contabilidad es medir los parámetros de la utilización de la red, para que el uso de la misma, tanto individual como de grupo, pueda regularse de manera adecuada.

Con dicha regulación se reducen los problemas de la red (ya que los recursos de la misma pueden dividirse en cantidades iguales dependiendo de las capacidades de los recursos) y se hace más justo el acceso a la red para todos los usuarios.

Tal como sucede con la administración del desempeño, el primer paso hacia una administración adecuada de la confiabilidad es medir la utilización de todos los recursos importantes de la red. El análisis de los resultados permite hacerse una idea de los patrones de uso actuales y en este punto, establecer cuotas de uso.

Por supuesto, será necesario hacer correcciones para alcanzar las prácticas de acceso óptimo. A partir de este punto, la medición del uso del recurso puede proporcionar

información de facturación, así como información que servirá para analizar continuamente la utilización óptima y justa de los recursos.

Administración de fallas.

El objetivo de la administración de fallas es detectar, registrar, notificar a los usuarios y (en la medida de lo posible) arreglar automáticamente los problemas de la red para mantenerla en operación de manera eficiente.
Como las fallas pueden dejar fuera a la red o causar una degradación inaceptable de la misma, la administración de fallas es quizás uno de los elementos de la administración de redes ISO de mayor implementación.

La administración de fallas implica, en primera instancia, la determinación de los síntomas y el aislamiento del problema. Entonces se repara el problema y se prueba la solución en todos los subsistemas importantes. Por último, se registran la detección y la solución del problema.

Administración de la seguridad.

El objetivo de la administración de la seguridad es controlar el acceso a los recursos de la red de acuerdo con los lineamientos locales, para que la red no pueda ser saboteada (intencional o no intencionalmente) y que personal sin autorización no tenga acceso a información de alta seguridad.
Por ejemplo, un subsistema de administración de la seguridad puede supervisar el acceso a un recurso de la red, y niega el acceso a usuarios que no ingresen los códigos de acceso correctos.

Los subsistemas de administración de la seguridad funcionan dividiendo los recursos de la red en áreas autorizadas y no autorizadas. Para algunos usuarios, el acceso a cualquier recurso de la red esta prohibido, principalmente por que dichos usuarios son, en general, gente ajena a la compañía. A otros usuarios (internos) de la red, se les puede rehusar el acceso a la información que se origina desde un departamento en particular. El acceso a los archivos de recursos humanos, por ejemplo, puede ser denegado a los usuarios que no pertenezcan al departamento de recursos humanos.

Los subsistemas de la administración de la seguridad llevan a cabo varias funciones. Identifican los recursos de alta seguridad dentro de la red (incluyendo sistemas, archivos y otras entidades) y determina los mapeos entre los recursos de alta seguridad de la red y los grupos de usuarios. También supervisan los puntos de acceso de los recursos de alta seguridad de la red y registran el acceso no autorizado a los mismos.

2.4.2 Administración de las VPN.

Es claro que una adecuada gestión de la red de datos, además de proporcionar un funcionamiento lo más cercano al óptimo deseado y planeado, evita muchos problemas que van desde el funcionamiento excesivamente lento de la misma, ya sea por el tráfico generado, por el retrazo de los paquetes de datos, etc., hasta la pérdida total del funcionamiento de la red.
Por esta razón es importante considerar que una VPN, al igual que otros modelos de redes, debe ser administrada de forma adecuada para garantizar el buen funcionamiento de la misma y así asegurar al máximo la operación de aquellas aplicaciones que se ejecutan sobre el enlace de conexión.

Es obvio que alguien tendrá que responsabilizarse de la supervisión, del mantenimiento y de la administración de la VPN, ya sea el personal de la empresa o el proveedor de servicio. Si el proveedor proporciona un servicio administrado, entonces éste se incluye en la tarifa por el servicio. En la mayoría de los casos, las actualizaciones normales y las actualizaciones de correcciones pueden manejarse vía telefónica si el dispositivo VPN es un dispositivo de sistema operativo como UNIX o un tipo de enrutador. Con los dispositivos de hardware generalmente existe un disco flexible que se carga en el dispositivo, de tal forma que al encender el hardware se instalará la nueva revisión. En cualquier caso, sólo se requiere un poco de coordinación ya que probablemente se necesitará reiniciar el dispositivo.
Si el personal de la empresa es el que está manejando las tareas administrativas debe disponer de los procedimientos de administración para este nuevo hardware.
Si dicho personal está instalando estos dispositivos en varias ubicaciones, necesitará administrarlos en forma remota.

Los dos tipos de acceso que requerirá son los siguientes:

- ✓ En banda. Aquí es donde el personal puede crear un túnel de administración cerrado entre los dispositivos VPN de tal forma que pueda administrarlos remotamente a través de Internet.

- ✓ Fuera de banda. Esta configuración coloca un módem de cifrado en los puertos de consola de los dispositivos VPN en diferentes ubicaciones. Se necesita tener esta configuración en caso de que no se pueda tener acceso en banda a su dispositivo VPN. Si, por ejemplo, se instala este dispositivo en forma remota y de manera inadvertida se establece un parámetro denegando el acceso en banda, con esto se habrá perdido la conectividad a ese dispositivo, así que se necesitará otra forma de llegar a él. Además, hay que asegurarse de utilizar módems de cifrado. Estos sólo se comunicarán con los módems de cifrado que se hayan instalado, bloqueando así cualquier llamada entrante desde otros módems.

2.4.3 Calidad de Servicio (QoS).

La calidad de servicio consiste en la capacidad de la red para reservar algunos de los recursos disponibles para un tráfico concreto con la intención de proporcionar un determinado servicio. Debemos tener en cuenta que en la red se pueden utilizar diferentes tecnologías de transporte (como pueden ser Frame Relay, X.25, ATM, etc.) de manera que la gestión de calidad de servicio implica la interacción con estas tecnologías y con los equipos de conmutación, que son los que finalmente determinarán el nivel de calidad de servicio alcanzado.

La calidad de servicio es fundamental para afrontar y dar eficiencia a diferentes tipos de aplicaciones: voz, datos y video, el control de redes complejas y un servicio predecible de aplicaciones en red y de tipos de tráfico. El ancho de banda necesario, la priorización por tipo de trafico (http, ftp, smtp, udp etc.), el retardo, la fluctuación de fase y la pérdida de paquetes pueden controlarse de una manera eficaz. Al garantizar los resultados deseados, las características de calidad de servicio hacen posible servicios eficientes y previsibles para su organización.

La calidad de servicio debe estar garantizada para aplicaciones que requieren baja pérdida, bajo retrazo y baja variación de retrazo para así poder garantizar el servicio, es decir garantizar un porcentaje de ancho de banda, aún en caso de embotellamiento.

Las siguientes definiciones son importantes para comprender cuando se habla de calidad de servicio:

- ✓ La clase de servicio (CS), define un conjunto preciso de parámetros cuando se ofrece un servicio.
- ✓ El nivel acordado de servicios (SLA)[29] establece la calidad de servicio pactada mediante un contrato.

El concepto de calidad de servicio se originó en las técnicas y estándares de redes, pero también puede extenderse al Web, las aplicaciones y los servidores de contenido para administrar las clases de servicio a lo largo de todos los recursos de transmisión y procesamiento que forman la infraestructura de Internet. Las computadoras locales y remotas también pueden administrarse con calidad de servicio para optimizar las tareas de procesamiento de aplicaciones en Internet (siguiendo el nivel acordado de servicios bajo una verdadera arquitectura distribuida). Deben establecerse protocolos de calidad de servicio eficientes entre las redes y los servidores para administrar la red y las computadoras, según lo establece el nivel acordado de servicios, adaptándose a las condiciones reales de la red y los servidores, que cambian a cada momento.

Las redes pueden introducir retardos, pérdida de paquetes o errores debido a problemas de multiplexaje, conmutación o transmisión en nodos congestionados, impactando entonces la calidad del servicio. Cuando se maneja asignación de recursos de voz, datos y video, las condiciones de la red se tensan al máximo para poder garantizar el desempeño de los servicios múltiples. La calidad de servicio se definió inicialmente en los protocolos de comunicaciones ATM y luego evolucionó al protocolo IP para disponer de las herramientas para manejar la infraestructura de las redes de nueva generación.

[29] Service Level Agreement.

Las computadoras existentes en Internet pueden presentar problemas de sobrecarga en el procesador, la memoria y los dispositivos de E/S, lo cual disminuye la calidad de servicio. Las aplicaciones deben considerar redundancia, balanceo de cargas y prioridades de asignación de recursos a lo largo de todos los elementos de cómputo disponibles. Las tecnologías de calidad de servicio son bastante nuevas en la industria de las computadoras, especialmente cuando se establecen protocolos entre redes y procesadores distribuidos.

El acceso y la seguridad son dos componentes centrales de las tecnologías aplicadas a los servicios corporativos distribuidos mediante Internet, así como dos tecnologías paralelas incluidas en una solución de calidad de servicio. De hecho, el acceso, la seguridad y los protocolos de calidad de servicio deben interoperar en forma natural con los entornos privados virtuales para conformar aplicaciones tipo calidad de servicio a lo largo de la red y los servidores. Los recursos de las computadoras y la red pueden programarse para diferenciar los servicios por usuario y por aplicación. Se pueden definir clases de servicio para cada usuario y aplicación que se ejecute en Internet (hasta llegar al nivel de las funciones específicas o los componentes de cada aplicación). Promediando los parámetros de la clase de servicio empleados por los usuarios y sus aplicaciones, cada paquete IP puede ser procesado en forma diferente, de modo tal que se puede disponer de los recursos de la infraestructura de acuerdo con el nivel de servicios pactado.

Aun cuando los costos del ancho de banda se reducen en algunos países, las aplicaciones de nueva generación requieren cada vez más recursos de Internet. A medida que la infraestructura cambia con rapidez en todo el mundo, las empresas e instituciones requieren la calidad de servicio no sólo para garantizar la entrega eficiente y económica de las aplicaciones en Internet, sino también para programar la asignación de los recursos de cómputo y red y aplicar las políticas corporativas e institucionales. Internet se ha hecho tan grande que requiere de mejores herramientas para administrarla.
Las tecnologías de calidad de servicio permiten recuperar el mismo control que existía en los entornos centrados en las aplicaciones, como en los mainframes (como si todo se estuviera procesando en una sola computadora).

En detalle, las características de calidad de servicio proporcionan un servicio de red mejor y más fiable.

- ✓ Utilizando ancho de banda dedicado.
- ✓ Mejorando las características de pérdida.
- ✓ Evitando y administrando la congestión de la red.
- ✓ Fijando prioridades del tráfico a través de la red.

Tipos de tecnologías que brindan calidad de servicio.

En este momento existen principalmente dos tipos de tecnologías que proporcionan calidad de servicio.

La primera se basa en la **reserva**, y asigna recursos basándose en flujos de tráfico. Alternativamente, un segundo tipo de calidad de servicio se caracteriza por la **priorización** de determinado tipo de tráfico.

Veremos más adelante que los flujos de datos individuales se van agrupando en grandes agregados de tráfico de acuerdo a la "clase de servicio" a la que pertenezcan, y dependiendo de esa clase de servicio recibirán un distinto trato en los diferentes elementos de la red.

En comunicaciones IP se traduce en dos modelos de trabajo:

Modelo Intserv: basado en la utilización de algún protocolo de reserva como RSVP[30], que permite la reserva de recursos a lo largo de los routers implicados en la comunicación. El principal problema de este modelo es la necesidad de mantener información sobre cada flujo en todos los routers de la red, lo cual lleva a problemas de escalabilidad.

Modelo Diffserv: se basa en la división del tráfico en diferentes clases y en la asignación de prioridades a estos agregados. Utiliza diferente información de la

[30] ReSerVation Protocol.

cabecera de los paquetes, por ejemplo, DSCP[31] para distinguir y clasificar los paquetes y conocer el tratamiento que debe recibir el tráfico en los nodos de la red Diffserv.

Calidad de servicio: Diffserv

Los servicios diferenciados Diffserv proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio.
Los paquetes que pertenecen a una determinada clase se marcan con un código específico DSCP. Este código es todo lo que necesitamos para identificar una clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, hecho conocido como PHB[32].

De esta manera a través de Diffserv planteamos asignar prioridades a los diferentes paquetes que son enviados a la red.
Los nodos intermedios (routers) tendrán que analizar estos paquetes y tratarlos según sus necesidades. Esta es la razón principal por la que Diffserv ofrece mejores características de escalabilidad que Intserv. Dentro de Diffserv se define en el campo DS[33] donde se especificarán las prioridades de los paquetes. En el subcampo DSCP se especifica la prioridad de cada paquete. Estos campos son validos tanto para IPv4 como IPv6.

En la arquitectura definida por Diffserv aparece nodos extremos DS de entrada y salida, así como nodos DS internos. Este conjunto de nodos definen el dominio Diffserv y presenta un tipo de políticas y grupos de comportamiento por salto PHB que determinarán el tratamiento de los paquetes en la red.

[31] Diffserv Code Point.
[32] Per Hop Behavior.
[33] Differentiated Services.

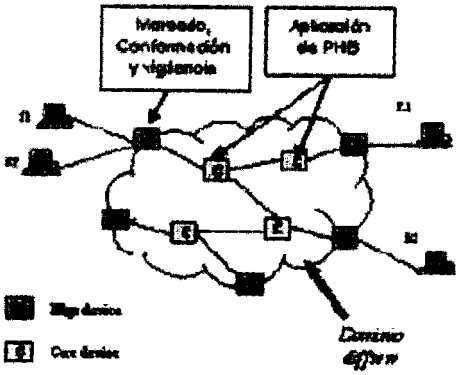


Figura 2.22
Arquitectura Diffserv

Veamos a continuación las diferentes funciones que deben realizar los nodos DS:

Nodos extremos DS: será necesario realizar diferentes funciones como el acondicionamiento de tráfico entre los dominios Diffserv interconectados. De esta manera debe clasificar y establecer las condiciones de ingreso de los flujos de tráfico en función de: dirección IP y puerto (origen y destino), protocolo de transporte y DSCP, este clasificador se conoce como MF[34].

Una vez que los paquetes han sido marcados adecuadamente, los nodos internos deberán seleccionar el PHB definido para cada flujo de datos.

Los nodos DS de entrada serán responsables de asegurar que el tráfico de entrada cumple los requisitos de algún TCA[35], que es un derivado del SLA, entre los dominios interconectados.

Por otro lado los nodos DS de salida deberán realizar funciones de acondicionamiento de tráfico o de conformación de tráfico sobre el tráfico transferido al otro dominio DS conectado.

Nodos internos DS: podrá realizar limitadas funciones de conformación de tráfico, tales como, remarcado de DSCP. Los nodos DS internos solo se conectan a nodos internos o a nodos externos de su propio dominio. A diferencia de los nodos externos

[34] Multi-Field Classifier.
[35] Traffic Conditioning Agreement.

para la selección del PHB solo se tendrá en cuenta el campo DSCP, conocido como clasificador BA[36].

Protocolo de gestión de políticas (COPS)[37].

Dentro de este escenario que define Diffserv necesitamos algún modo de comunicación para distribuir las políticas de calidad de servicio entre los elementos de red que las necesiten. Existe un protocolo creado para tal efecto que nos permitirá resolver este problema de comunicación, el protocolo COPS.

Este define un modelo sencillo de cliente/servidor que proporciona control de políticas para protocolos con señalización de calidad de servicio. El modelo descrito no hace ninguna suposición acerca de los procedimientos utilizados en el servidor de políticas, sino que se basa en un servidor que devuelve decisiones a las peticiones realizadas por los clientes. La definición del protocolo es bastante abierta para que sea extensible y poder soportar los distintos tipos de clientes que pudieran aparecer en el futuro.

El protocolo COPS se basa en sencillos mensajes de petición y respuesta utilizados para intercambiar información acerca de políticas de tráfico entre un servidor de políticas PDP[38] y distintos tipos de clientes PEP[39]. Un ejemplo de cliente COPS podría ser un router RSVP o Diffserv que deba realizar funciones de control de admisión en base a determinada política.
Por otro lado, el modelo supone que existe al menos un servidor de políticas en cada dominio administrativo.
Uno de los objetivos principales del protocolo es proporcionar un modelo sencillo pero fácilmente extensible.

Las características principales del protocolo COPS son las siguientes:

[36] Behavior Aggregate Classifier.
[37] Common Open Policy Service.
[38] Policy Decision Point.
[39] Policy Enforcement Points.

- ✓ El protocolo emplea un modelo cliente/servidor en el que el PEP envía peticiones y actualizaciones al PDP, y el PDP responde con las decisiones tomadas.
- ✓ El protocolo utiliza TCP como protocolo de transporte para asegurar así fiabilidad en el intercambio de mensajes entre los clientes y el servidor.
- ✓ El protocolo es extensible en el sentido de que está diseñado para permitir el uso de objetos autoidentificativos y soporta distintos tipos de información específica de clientes, sin tener que realizar ningún tipo de modificación sobre el protocolo.
- ✓ COPS se creó para la administración general, configuración y aplicación de políticas en una red.
- ✓ COPS proporciona seguridad a nivel de mensaje mediante autenticación, protección frente al reenvío (replay) e integridad de mensaje. COPS permite además reutilizar otros protocolos de seguridad existentes para proporcionar autenticación y proteger el canal entre el PEP y el PDP.

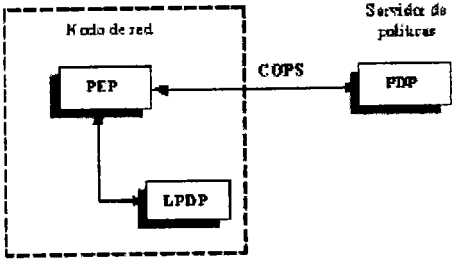


Figura 2.24
El modelo COPS

La figura anterior muestra la disposición de diferentes componentes en un ejemplo COPS típico. En este modelo, el protocolo COPS se utiliza para comunicar la información sobre las políticas de la red entre los puntos de aplicación de políticas y un servidor de políticas remoto. Dentro del nodo de red puede existir un PDP local que puede ser utilizado para tomar decisiones locales en ausencia de un PDP.

El PEP puede tener también la capacidad de tomar decisiones de política localmente, a través de su LPDP[40], aunque el PDP sigue manteniendo la autoridad en cuanto a las decisiones. Esto quiere decir que cualquier decisión local relevante debe enviarse al

[40] Local Policy Decision Point.

PDP. Asimismo, el PDP debe tener acceso a toda la información para poder tomar una decisión final. Para ello, el PEP debe enviar las decisiones locales al PDP a través de un objeto LPDP Decisión, y posteriormente atenerse a la decisión que tome el PDP.

Limitaciones.

Tras haber estudiado como Diffserv puede implementarse para alcanzar la tan deseada calidad de servicio en comunicaciones dentro de Internet, debemos comentar la existencia de ciertas limitaciones inherentes al modelo Diffserv, las cuales impiden en cierta manera la implementación a gran escala de este sistema. Directamente relacionado con este tema se encuentra el estudio del modelo de negocio que presenta Diffserv en la actualidad.

A continuación analizaremos los problemas de implantación de Diffserv gracias a un estudio del modelo de negocio:
Dentro del modelo Diffserv es necesario indicar que este no asegura de manera determinista que los flujos de tráfico consigan determinados parámetros de calidad de servicio, como pueda hacer ATM a través de circuitos. Diffserv permite la creación de agregaciones de tráfico, lo que nos ofrece cierta probabilidad de calidad de servicio, de manera que un proveedor puede integrar las conexiones pertenecientes a diferentes VPN dentro de un mismo agregado, recibiendo todas ellas las mismas prestaciones a nivel de red. De esta manera el tratamiento que recibieran podría ser diferente del que consiguen usuarios con acceso gratuito a Internet.

Resulta especialmente curioso que en Diffserv el principal beneficiario de la reserva de calidad de servicio será el destino, siendo el origen el que debe pagar por conseguir ese trato diferenciado de su tráfico. De esta forma surgen conflictos por ejemplo en la descarga de audio-streaming, donde el que pagaría sería el servidor en lugar del usuario receptor.
Analizando el modelo Diffserv parece lógico que alcanzar un destino más lejano resulte más caro que otro más cercano donde se necesiten atravesar menos ISP. En consecuencia el coste de enviar un paquete será diferente en función del camino que deba atravesar. Esto puede suponer una complicación a la hora de ofrecer el servicio y tarificarlo. Sin embargo, este mismo problema aparecía en el nacimiento de Internet,

donde también resultaba más caro enviar un paquete cuantos más ISP tuviese que atravesar, y sin embargo, por el momento los proveedores de acceso han decidido ofrecer una tarifa fija independientemente del destino de los paquetes. Parece lógico entonces pensar que de alguna manera nuestro proveedor de acceso a Internet nos tarificará adecuadamente teniendo en cuenta que los mensajes deberán ser tratados adecuadamente en los diferentes ISP.

A partir del estudio de estas limitaciones que presenta el modelo Diffserv podemos distinguir algunas aplicaciones como las más interesantes para este modelo.

En primer lugar los servicios basados en suscripción cobran especial importancia. Debido al hecho de ser el origen el encargado de realizar la reserva, servicios como VoD, canales de radio, canales de televisión, etc. podrían aparecer en el modelo de negocio de redes Diffserv. En este caso el proveedor de contenidos recibiría cierto ingreso por cada evento distribuido. Y sería el mismo el encargado de seleccionar la calidad de servicio que recibirían los usuarios.

Siguiendo el mismo razonamiento, vemos que el principal problema es poner de acuerdo a origen y destino para alcanzar un acuerdo en la calidad de servicio deseada. Este problema desaparece en el caso de VPN donde el origen y el destino pertenecen a la misma organización, de manera que comparten los mismos criterios sobre calidad de servicio.

De esta manera, el desarrollo de Diffserv presenta un especial interés de cara a la creación de VPN sobre una red IP.

Por otro lado, existen una serie de aplicaciones con determinados requisitos de calidad de servicio donde el desarrollo e implementación de alguna tecnología de calidad de servicio en la actual Internet podría suponer su despegue.
A continuación podemos ver algunos ejemplos:

Resulta de especial interés en las videoconferencias, donde incluimos cualquier tipo de escenario VoIP. El desarrollo de este tipo de comunicaciones no había tenido éxito por

la falta de algún tipo de provisión de calidad de servicio, pero la llegada de Diffserv permitió el despegue definitivo de este servicio.

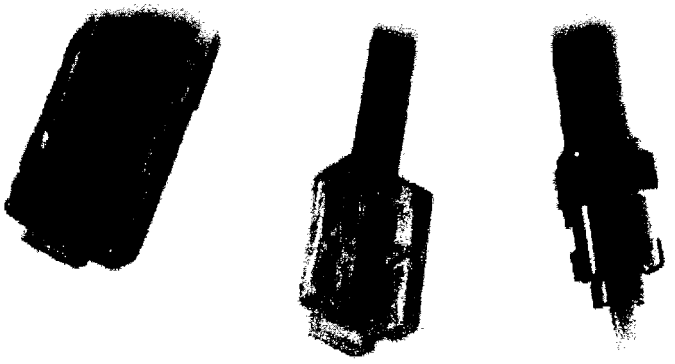
2.4.4 Calidad de servicio dentro de las VPN.

En las VPN como en cualquier otra red de datos se tienen la posibilidad de proporcionar calidad de servicio, esto se logra mediante las tecnologías que ya explicamos anteriormente. Debido a esto, las VPN se convierten, se fortalecen y por ende se ratifican como una buena opción para aquellas empresas e instituciones que requieren de la ejecución de aplicaciones críticas para su negocio o actividades principales además de tener muchas otras necesidades de comunicación como las que se describieron anteriormente.

En la actualidad muchas de las empresas e instituciones que habían considerado como una buena solución a las VPN no se habían atrevido a la implantación de la misma debido a que era casi imposible asegurar calidad de servicio dentro de las mismas pero con los modelos que se han explicado en este capítulo y algunos otros que están en desarrollo la tendencia de crecimiento en la implantación de VPN indica que el problema ha sido resuelto de manera exitosa.

CAPÍTULO 3.

ALTERNATIVAS DE IMPLEMENTACIÓN PARA UNA VPN.



En este capítulo se analizan las soluciones ofrecidas por los diferentes proveedores de servicios consultados.

Podemos ver las características principales de las mismas, las ventajas que nos ofrecen y los beneficios obtenidos una vez implementadas.

Además, se muestra un cuadro comparativo de tecnologías donde pueden ser implementadas las VPN.

ALTERNATIVAS DE IMPLEMENTACIÓN.

La actual demanda de aplicaciones relacionadas con información multimedia, como son la videoconferencia, audio - conferencia, video bajo demanda (VoD)[41] o sistemas colaborativos (pizarras compartidas, teletrabajo, telemedicina , etc.) y su coexistencia con aplicaciones más clásicas (bases de datos, transferencia de ficheros, www, etc.), requieren tecnologías de comunicaciones capaces de ofrecer elevadas prestaciones.

Estas elevadas prestaciones están directamente relacionadas con la calidad de servicio, y concretamente con conceptos claramente parametrizables como el ancho de banda y la velocidad de transmisión, el retardo de las transferencias, la variabilidad en el retardo, la fiabilidad de las transmisiones; las características de multidifusión a grupos dispersos de usuarios y la posibilidad de gestionar múltiples clases de servicio o flujos de información en redes multiclass.

Para que las nuevas tecnologías en comunicaciones puedan ofrecer estas características es necesario revisar, potenciar y ampliar las actuales arquitecturas, servicios y protocolos de comunicaciones.

3.1 Condiciones de mercado.

Se emitió un documento de Solicitud de Información a tres proveedores nacionales que ofrecen servicios de VPN, incluyendo:

[41] Video over Demand.

- ✓ Telmex.
- ✓ Avantel.
- ✓ Alestra.

A continuación mencionaré en forma general el contenido de los documentos obtenidos por parte de todos y cada uno de los proveedores encargados de proporcionar el servicio.

Telmex.

VPN Multiservicios.

VPN Multiservicios proporciona el transporte de cualquier tipo de información en una plataforma única y convergente, donde se pueda transmitir voz, video o datos con una calidad de servicio diferenciada, asignándole mayor prioridad de las comunicaciones de voz o videoconferencia, las cuales son aplicaciones que no pueden sufrir retardos.

Es una red privada construida dentro de una infraestructura IP para el transporte diferenciado de datos, datos de misión crítica, voz y video, con la consecuente reducción en costos operativos y de inversión, flexibilidad y escalabilidad de la infraestructura de comunicaciones, altos niveles de seguridad, desempeño y confiabilidad.

VPN Multiservicios se compone de:

- ✓ Puerto VPN: Es el puerto de acceso de ruteador de la red VPN Multiservicios al cual se va a conectar.
- ✓ Calidad de Servicio: Tipo de tráfico contratados, se manejan 3 calidades de servicio:

    1. Datos: Transporte de datos no prioritarios, como puede ser correo electrónico, transferencia de archivos, respaldos, consultas a bases de datos, etc.
    2. Datos críticos: Transporte de datos de misión crítica.

3. Voz / video: Transporte de aplicaciones sensibles a retardos, como puede ser el transporte de voz y del video.

Beneficios.

- ✓ Reducción de costos.
- ✓ Una sola red convergente, una administración y operación (antes redes separadas de telefonía, datos o videoconferencia).
- ✓ Conectividad sencilla.
- ✓ Fácil implantación de conexiones hacia usuarios móviles, socios, proveedores y clientes.

Seguridad.

- ✓ Toda la información que se transporta en esta red permanece totalmente confidencial y privada.

Aplicaciones.

Plataforma flexible para la creación de futuros servicios.

Las aplicaciones que se pueden implementar sobre este servicio de transporte son muy variadas y siguen creciendo, principalmente este servicio se utiliza para aplicaciones que son sensibles a protocolo IP, como ejemplos tenemos:

- ✓ Voz sobre IP (es muy diferente a voz sobre Internet, ya que esta aplicación tiene calidad de servicio en el transporte).
- ✓ Telefonía sobre IP (todas las funcionalidades del conmutador tradicional de voz dentro de este servicio).
- ✓ Transmisión de datos.
- ✓ Intranets, Extranets y accesos remotos.
- ✓ Educación a distancia IP.
- ✓ Video sobre demanda.

Alestra.

El servicio AT&T Solución Integral de Túneles de VPN ofrece un acceso seguro a la red corporativa de su empresa utilizando la tecnología de encriptación IPSec.

Adicionalmente, incluye métodos de autentificación de red, encriptación de datos y análisis de integridad. Todo lo anterior ayuda a prevenir que los datos sean interferidos y asegura la confiabilidad de la información que viaja a través de una red pública como lo es Internet.
El servicio AT&T Solución Integral de Túneles de VPN se ofrece utilizando IPSec ya que provee una mayor protección y autentificación de datos que otros protocolos y porque es un sistema estándar no propietario. Lo cual significa que IPSec, puede convivir con los sistemas de autentificación y políticas de seguridad existentes en la infraestructura de su empresa.

Independientemente de quién sea su proveedor de servicios de Internet, AT&T Solución Integral de Túneles de VPN opera con accesos de cualquier velocidad y cualquier aplicación que utilice el protocolo de red TCP/IP.

Con el servicio de Solución Integral de Túneles de VPN, su empresa se beneficia del mejor protocolo de seguridad entre sus usuarios remotos y de la Red AT&T. Además de:

- ✓ Incrementar la confiabilidad y seguridad limitando el acceso a redes locales autorizadas.
- ✓ Obtener la compatibilidad con sus sistemas de seguridad y de autentificación existentes.
- ✓ Proveer de conexión a Internet para sus usuarios remotos.
- ✓ Lograr la escalabilidad que permite que su negocio crezca.

Características.

AT&T ha desarrollado una solución totalmente administrada que sea rápida y se incorpora fácilmente a su negocio. Esta solución tiene poderosas características como:

- ✓ Escalabilidad para las pequeñas oficinas.
- ✓ Encriptación que fortalezca la seguridad interna y se añada a la seguridad del túnel.
- ✓ Métodos de autentificación flexibles.
- ✓ Flexibilidad de acceso a través de la conectividad a Internet y mayor seguridad para accesar a la red corporativa en la misma sesión de "dial" además de poder bloquear el acceso a Internet a aquellos empleados que usted seleccione.
- ✓ Administración, monitoreo y soporte a la medida.
- ✓ Administración total de su equipo de ruteo lo que incluye instalación, configuración y actualizaciones.

Avantel.

Avantel VPN – Multimedia.

Avantel VPN Multimedia combina redes privadas virtuales de voz y datos que utilizan el protocolo de Internet que le permiten establecer comunicación entre sus localidades mediante un plan de marcación privado, el cual podrá ser utilizado para realizar llamadas dentro de su red, así como también fuera de la misma. Adicionalmente, le permiten crear una red privada virtual de datos para comunicar diferentes localidades del cliente y conectarse a otras redes privadas.

Este nuevo servicio constituye la evolución natural de la única red 100% IP de alto desempeño en México. La red de Avantel le ofrece servicios con Calidad de Servicio para la transmisión de voz y datos.

Características.

- ✓ Con Avantel VPN Multimedia, se establece un plan de marcación privado entre sus oficinas en localidades distantes. Usted elige los 3 primeros dígitos para identificar a sus diferentes oficinas; usted ahorrará tiempo simplificando y distribuyendo el plan de numeración interno de acuerdo a lógica que más le convenga a su empresa.

- ✓ Adicionalmente a la red privada de voz, con Avantel VPN Multimedia puede establecer comunicación de datos (aplicaciones) entre sus oficinas, en un mismo enlace.
- ✓ Reducirá significativamente sus gastos de operación, ya que aprovechará la capacidad de un sólo enlace hacia la red IP de Avantel, que le permitirá tener varios canales de voz y ancho de banda para envío de datos, controlados por el protocolo IP. A través del pago de una renta fija, se pueden realizar todas las llamadas que sean necesarias entre sus oficinas.
- ✓ Al contar con este servicio, usted puede canalizar todo su tráfico de voz en una red interna de voz. Adicionalmente, puede realizar llamadas telefónicas hacia cualquier parte de México y el mundo, con cargos por minuto.
- ✓ A partir de la comunicación establecida con protocolo de Internet se le proporciona una Calidad en el Servicio, misma que sólo Avantel puede proporcionar debido al compromiso con sus clientes.
- ✓ Es un servicio donde la voz es bajo el estándar H.323.
- ✓ Facilidad de conectar su Conmutador al ruteador que soporte Voz por IP.
- ✓ Avantel VPN Multimedia le permite crear una red interna (intranet) de sitio a sitio para la comunicación entre sus oficinas y conectarse a otras redes (extranets) que le permiten establecer comunicación con clientes y /o proveedores.
- ✓ Avantel VPN Multimedia tiene mecanismos de calidad de servicio donde se asignan prioridades a las aplicaciones más sensibles al retraso como son la voz y el video.
- ✓ Con Avantel VPN Multimedia su empresa tiene la facilidad de crear redes de topologías malla, estrella o combinadas sin la necesidad de utilizar una circuito privado virtual, para la transmisión de datos..
- ✓ Puede realizar el monitoreo de su enlace dedicado a través de Internet.
- ✓ Con este servicio, todas sus aplicaciones son transportadas por una red segura y de alto desempeño.

Ventajas y Beneficios.

- ✓ Con Avantel VPN Multimedia usted ahorrará en gastos de operación ya que solo requerirá de un solo equipo y una sola conexión para tener comunicación privada de voz y datos en su red.
- ✓ Con el servicio de Avantel VPN Multimedia puede realizar videoconferencias y llamadas dentro de su propia red, por lo que el gasto de larga distancia o líneas privadas se elimina.
- ✓ Las llamadas que realicen entre sus localidades son ilimitadas, sólo paga una renta fija por el servicio.
- ✓ Avantel VPN Multimedia es una solución flexible, ya que no requiere de circuitos privados virtuales y esto le permite tener una mejor comunicación de datos dentro de su empresa.
- ✓ Con Avantel VPN Multimedia usted cuenta con privacidad y seguridad, debido a que sólo existe comunicación sobre las localidades que usted designe y sume a su propia red, además de soportar cualquier direccionamiento IP de carácter privado.
- ✓ Diversas opciones de acceso y conexión a la red de Avantel.

A continuación presento un cuadro donde se muestran de manera resumida las características de las soluciones ya mencionadas, esto con el objetivo de visualizar de forma rápida y sencilla los puntos más importantes de las mismas.

CARACTERISTICAS	AVANTEL	TELMEX / UNINET	ALESTRA
Nombre del servicio	Avantel VPN Multimedia	VPN Multiservicios	AT&T VPN QoS
Cobertura a nivel nacional (ciudades)	58	No se mencionó de manera escrita (150)*	34
Servicios soportados	Video, voz y datos	Video, voz y datos	Video, voz y datos
Cobertura de servicios	24x7	24x7	24x7
Tecnología de la red del proveedor	MPLS	MPLS	MPLS
Disponibilidad (extremo a extremo)	99.95% en el Backbone como mínimo	99.97% en el Backbone como mínimo	99.80% mínimo
Latencia (RTT)**	45 mseg. O menor	100/150/200 mseg.	80 mseg. o menor
Eficiencia en la entrega de paquetes (PDR)***	99.95% (datos críticos)		99% mínimo
MTTR****			< 4.5 hrs.
Servicios de seguridad informática	Dentro de la red y a través de mecanismos de encriptado y autenticación.	Dentro de la red y a través de mecanismos de encriptado y autenticación.	Dentro de la red y a través de mecanismos de encriptado y autenticación.
Gestión de la red	24x7	24x7	24x7
Otros servicios opcionales	Consultoría, implantación, auditoria, renta de equipo y centro de llamadas.	Consultoría, implantación, auditoria, renta de equipo y centro de llamadas.	Consultoría, implantación, auditoria, renta de equipo y centro de llamadas.

Cuadro 2

* Aproximadamente
** Round Trip Time (latencia de viaje redondo)
*** Packet Delivery Rate (eficiencia en la entrega de paquetes)
****Packet Delay Variation (variabilidad en la latencia de los paquetes)

3.2 Tecnologías en donde se puede implementar una VPN.

Una de las características de las VPN es que éstas pueden ser implementadas en diferentes plataformas, cada una de ellas con sus ventajas y beneficios.

A continuación se puede observar un cuadro comparativo de tecnologías de VPN.

	FR / ATM	VPN MPLS	VPN IPSec
Aplicaciones y protocolos	Múltiples protocolos. Transferencia de archivos, correo electrónico, intranet, telefonía.	IP (puede encapsular) transferencia de archivos, correo electrónico, intranets, aplicaciones sensibles al retardo (video, voz)	IP (puede encapsular) transferencia de archivos, correo electrónico, intranets.
Escalabilidad y topología	Altamente escalable para topología de red tipo estrella.	Altamente escalable para topologías de red estrella y malla completa.	Para configuraciones tipo estrella y malla parcial. Problemas de escalabilidad y seguridad para la distribución de llaves.
Cobertura	Nacional e Internacional.	Nacional e Internacional.	Internet y en donde IPSec sea soportado y permitido.
Seguridad		Se puede manejar diferentes clase de servicio, permitiendo tener diferentes prioridades a diferentes servicios (datos críticos, video, voz)	IPSec a través de la red pública de Internet.
Desempeño	Alta, basada en las etiquetas (tramas / celdas) específicas de cada cliente.	Alta basada en etiquetas MPLS específicas de cada cliente (IP - Sec).	Variable. No existe reservación en la capa central de las redes de muchos proveedores.
Requerimientos de habilidades del cliente	Adaptable, ancho de banda reservable en el acceso y la capa central.	Predecible y adaptable a los requerimientos del cliente (SLA), por prioridad en el acceso y la capa central.	Baja / media en IP y planeación de ancho de banda.
administración, supervisión y control de la red	Alta para conectividad con IP, media para planeación de capacidades.	Baja / media en IP y planeación de ancho de banda.	

Cuadro 3

La decisión de elegir sobre que tecnología se montará la VPN variará en función de las necesidades de cada institución y de los recursos con los que ésta cuente.

CAPÍTULO 4.

IMPLEMENTACIÓN DE LA VPN.

Este capítulo nos describe cuál es el modelo conceptual propuesto para la VPN de la SEM y las 5 sedes hospitalarias con las que se desea enlazar actualmente.

También nos muestra un esquema general de conexión de los usuarios móviles a la VPN y nos dice de las necesidades de hardware y software de los clientes.

Además, en este capítulo podemos conocer el plan de trabajo y tiempos de implementación, cuáles son los requerimientos de nuestros usuarios, el esquema de operación de la VPN y los alcances y las obligaciones del departamento TI y sus límites.

IMPLEMENTACIÓN DE LA VPN.

Como se ha mencionado en el capítulo anterior el proveedor de servicios elegido por parte de la SEM ha sido Avantel y una vez que se comunique la decisión al proveedor se llevará a cabo la firma del contrato; Avantel por su parte, se compromete a que en un lapso de 2 a 3 semanas máximo entregar a la SEM la solución completamente instalada y en funcionamiento.
Además cabe mencionar que los requerimientos básicos solicitados por Avantel son equipo de hardware y software compatible con el protocolo IP y que soporte voz sobre IP y el protocolo H.323.

A continuación se presenta el plan de trabajo realizado de manera conjunta tanto por la SEM como por Avantel.

4.1 Plan de Trabajo.

A continuación se describen de forma general las actividades que se realizarán en cada una de las etapas que conforman nuestro plan de trabajo.

Primera Etapa.

En esta etapa Avantel iniciará con la recomendación y acondicionamiento de las instalaciones donde serán ubicados los dispositivos de interconexión para posteriormente ser colocados dentro de la Facultad de Medicina. Posteriormente, se procederá a realizar la misma acción dentro de las demás sedes hospitalarias.
Se deberán obtener los permisos necesarios por parte de las instituciones para la remodelación y cambios en la infraestructura física de los sitios elegidos, esto variará dependiendo de cada caso. Además de la ubicación física de los dispositivos, en esta etapa se deberá de iniciar con el cableado necesario por parte de cada institución.
Se ha informado a las SEM que las operaciones para cumplir con esta etapa serán realizadas de manera paralela en dos sitios hasta terminar con las cinco sedes y el punto principal, el cual será el primero en el que se finalice la primera etapa.
También, en esta primera etapa se ha de informar a los usuarios móviles cuales son los requisitos mínimos que deberán cumplir sus equipos para poder conectarse a la VPN.
La seguridad física de los sitios elegidos para la ubicación de los dispositivos de interconexión será responsabilidad del personal de TI de cada sede.
La seguridad y el cumplimiento de los requisitos para el acceso a la VPN por parte de usuarios móviles es responsabilidad del usuario o de la institución que proporciona el equipo y el servicio.
El tiempo estimado para la finalización de esta primera etapa es de aproximadamente de 7 a 10 días.

Segunda Etapa.

En esta etapa se tiene planeado la configuración de todos y cada uno de los dispositivos de interconexión colocados en la etapa número uno además de la configuración de los dispositivos ubicados dentro de la red de Avantel para proporcionar el acceso a la misma. También, se instalará el software necesario para el acceso a la VPN a las computadoras portátiles de los usuarios con acceso remoto. En esta segunda etapa se realizarán pruebas de comunicación entre los dispositivos de interconexión ubicados en la Facultad de Medicina y los dispositivos ubicados dentro de la red de Avantel, posteriormente se harán las mismas pruebas entre las sedes y el proveedor y finalmente se probará el acceso por parte de los equipos móviles.

Además, se tiene contemplado que en esta etapa se realicen las primeras pruebas de comunicación entre las sedes hospitalarias y la SEM y los usuarios móviles prueben su acceso a los servicios de la SEM.
El tiempo estimado para la finalización de esta segunda etapa es de aproximadamente de 3 a 4 días.

Tercera Etapa.

En ésta etapa básicamente se tienen planeadas pruebas de conexión y comunicación entre las sedes hospitalarias y los usuarios con acceso remoto hacia la red y servicios de la SEM con aplicaciones reales y que serán utilizadas constantemente con la finalidad de observar el correcto funcionamiento de la solución.
Además, se tienen planeado que en este momento personal de Avantel proporcione las herramientas necesarias para el monitoreo de la VPN al personal de TI de la SEM encargado de dicha función. También se ha acordado que el personal especializado de Avantel entrenará de forma rápida y precisa al personal de TI de la SEM para el uso de las herramientas de monitoreo y administración de la VPN.
El tiempo estimado para la finalización de esta tercera etapa es de aproximadamente de 2 a 3 días.

Se recomienda contar con una oficina de administración de proyectos, independiente al proveedor de la VPN, durante el proceso de implantación con el fin de administrar el proyecto, asegurar el cumplimiento de los tiempos y calidad contratados, asegurar la continuidad de la operación durante la transición, entre otros.

Si al finalizar la tercera etapa la solución VPN trabaja de forma correcta sin contratiempo alguno y cumpliendo con las necesidades de comunicación de la SEM, de las sedes hospitalarias y de los usuarios móviles, la solución será liberada y entregada de manera formal a la SEM. De aquí en adelante las actividades y responsabilidades para el mantenimiento y funcionamiento de la VPN se llevarán a cabo de acuerdo a políticas de seguridad, administración y monitoreo acordadas por la SEM y Avantel y las cuales menciono un poco más adelante en éste mismo capítulo.

4.1.1 Situación futura.

Topología de la red expandida VPN (propuesta).

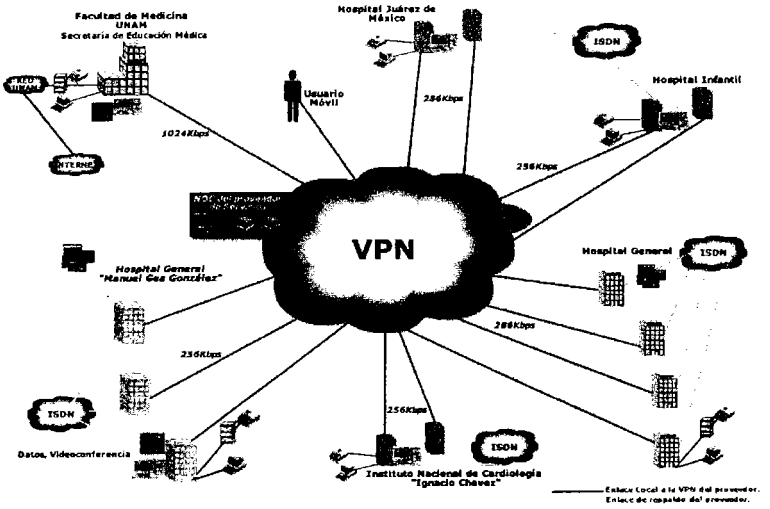


Figura 4.1

El modelo de operación de la Red está basado en que la Secretaría tercerizará las funciones de Mesa de Ayuda, Seguridad Informática y de la operación de la Red como se muestra a continuación. Este modelo deberá estar basado en una adecuada definición y administración de los niveles de servicio establecidos con el proveedor y en la coordinación y administración con el proveedor.

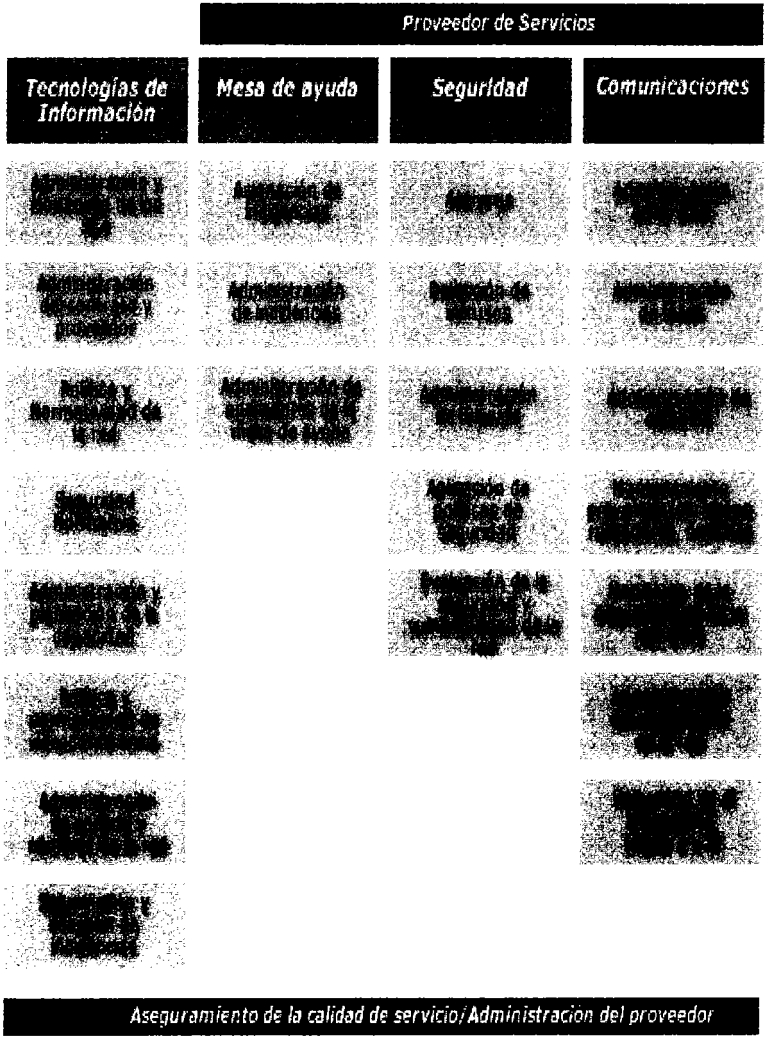

Proveedor de Servicios
Tecnologías de Información
Mesa de ayuda
Seguridad
Comunicaciones
Aseguramiento de la calidad de servicio/Administración del proveedor

Figura 4.2

4.1.2 Niveles de Servicio de la VPN.

Tipo de criticidad del nodo	Disponibilidad (%)	Interrupción máxima por mes (minutos.)	Latencia MTT (mseg.)	PDR (%)	PDV (mseg.)
Muy alta	99.96%	17.2	<50	>99.97	<30
Alta	99.85%	64.8	<50	>99.80	<30
Media	99.60%	172.8	<100	>99.60	<30
Baja	99.50%	216	<120	>99.50	<30

Cuadro 4

A continuación se muestra la definición de niveles de criticidad.

Nodo 1.

Nivel de criticidad. 1.

Tiempo máximo de atención (en minutos). Inmediata.

Impacto. Interrupción completa del servicio (Carencia de disponibilidad de todos los usuarios y funciones, aquí llega toda la información de la SEM)

Problema atendido con el más alto nivel de prioridad hasta que la solución sea encontrada, a través de la solución del problema o con otro curso de acción acordado con la Secretaría. Deberá trabajarse durante las 24 hrs. del día hasta encontrar una solución al problema.

Nodo 2.

Nivel de criticidad. 2.

Tiempo máximo de atención (en minutos). Inmediata.

Impacto. Degradación significativa del servicio (Alto número de usuarios sin servicio o funciones críticas afectadas, aquí se incluyen todos los Centros Hospitalarios.

Nodo 3.

Nivel de criticidad. 3.

Tiempo máximo de atención (en minutos). 10 minutos.

Impacto. Degradación media del servicio (limitado número de usuarios o funciones afectadas, los procesos de la Secretaría pueden continuar).

Nodo 4.

Nivel de criticidad. 4.

Tiempo máximo de atención (en minutos). 15 minutos.

Impacto. Poca degradación del servicio (Los procesos de la Secretaría pueden continuar. Un grupo reducido de usuarios afectados).

Propuesta de clasificación de nodos por disponibilidad.

Nivel 1. Muy alta.

Facultad de Medicina (SEM).
Hospital General "Manuel Gea González".

Nivel 2. Alta.

Cuatro centros hospitalarios.
Unidades centrales administrativas.

Nivel 3. Media.

Instituciones universitarias.

Nivel 4. Baja.

Usuarios móviles.

4.1.3 Modelo conceptual de la red.

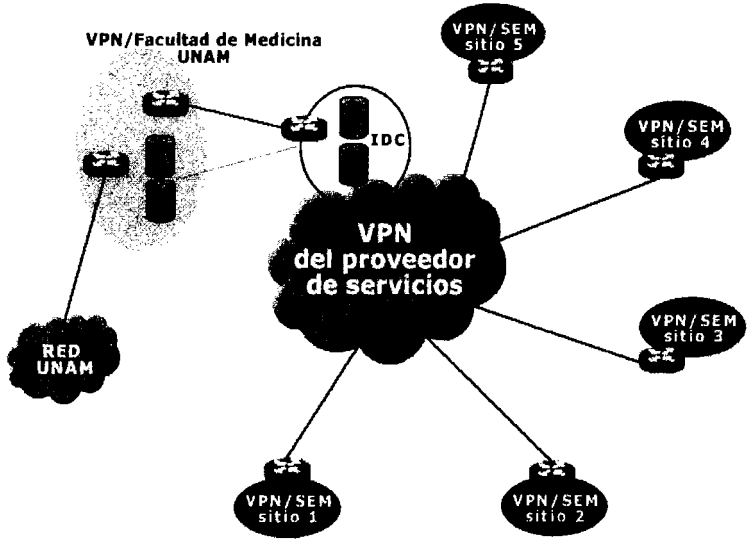


Figura 4.3

Variables críticas para el desarrollo del modelo.

- ✓ A través de un análisis de sensibilidad se encontró que las variables críticas que impactan al resultado del estudio son las siguientes dos:
    1. Ahorros Directos.
    2. Ingresos Potenciales.
- ✓ Si el monto pronosticado de los ahorros e ingresos no son alcanzados, se deberá disminuir la expansión de la red de comunicaciones de la SEM.

4.1.4 Ahorros y Beneficios.

Escenarios	Premisa	Posibles Beneficios
Aumento de ancho de banda.	Con el ancho de banda actual no es posible introducir nuevas aplicaciones debido a que la red se encuentra ya saturada.	Disminución de horas perdidas por caídas en los sistemas. Disminución del costo de larga y servicios medidos de distancia. Ahorro en los enlaces privados.
Aumento en el número de sitios + ancho de banda.	La Secretaría requiere crecer la red actual para ofrecer mayor cobertura de los nuevos servicios y aplicaciones entre las áreas centrales, los sitos remotos y los usuarios móviles.	Mejora de productividad a través del uso de nuevas aplicaciones. Información oportuna y veraz para toma de decisiones. Más y mejores servicios a alumnos, médicos, investigadores y docentes. Incremento en el beneficio social al poder prestar los servicios de mejor manera en más lugares.

Cuadro 5

4.2 Conclusiones.

Estrategia.

- ✓ Es necesario alinear y priorizar los diferentes proyectos de sistemas de la SEM con el fin de tener una estrategia integrada a mediano y largo plazo.
- ✓ Se recomienda tener una estrategia de tercerización de la red lo que implica un cambio de funciones en el equipo actual de trabajo.

Operaciones e Infraestructura.

- ✓ Se debe fortalecer la infraestructura de comunicaciones existente con el fin de soportar tanto las necesidades de crecimiento como las iniciativas planeadas.
- ✓ Se requiere contar con herramientas de monitoreo, control y planeación de la red con la finalidad de asegurar el cumplimiento y la calidad de los servicios.
- ✓ Se requiere establecer e implementar los procesos operativos, de soporte (a la infraestructura y a la seguridad informática) y de planeación para una eficiente operación y explotación de la red.

Organización.

- ✓ Se requiere establecer un área que sea responsable de administrar los niveles de servicio contratados con el proveedor, así mismo, ésta área deberá tener elementos para planear y administrar el crecimiento de la red.
- ✓ Se requiere establecer un área de seguridad informática que establezca, implemente y supervise el cumplimiento de las políticas de seguridad informática.

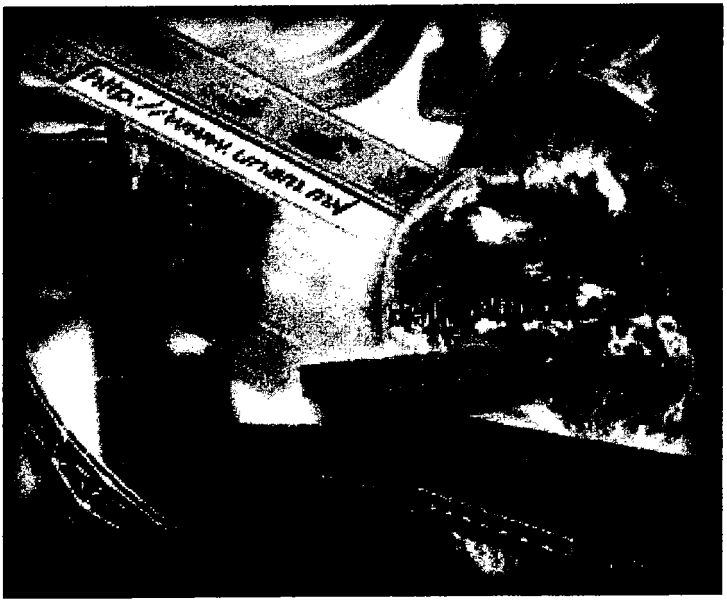
Financiero.

- ✓ Mediante el estudio realizado se determinó que migrar la red actual a una VPN es económicamente viable.
- ✓ A mayor duración en los plazos de contratación de la VPN, disminuyen los costos de la misma.
- ✓ El costo total de propiedad de la red es más bajo arrendando el equipo que realizando una inversión presupuestal (tercerización).
- ✓ El costo total de la red a través del modelo de Red Privada Virtual IP es más bajo en todos los escenarios, sin embargo, en algunos de ellos no existe una diferencia significativa entre el costo de los dos modelos.
- ✓ El aumento de los anchos de banda y de número de sitios de la red actual, se justifica como una inversión estratégica que permitirá la puesta en marcha de nuevas aplicaciones, lo que permitirá la mejora en la productividad y eficiencia de la Secretaría siempre y cuando la red sea explotada de una forma eficiente y sí se realicen los proyectos de reingeniería e implantación de sistemas.
- ✓ Las condiciones necesarias para que se den los beneficios potenciales son (lista no exhaustiva):

    1. Implantación de nuevas aplicaciones.
    2. Reingeniería de las aplicaciones actuales.
    3. Reingeniería de los procesos.
    4. Aplicación de las políticas de reducción de costos.

CAPÍTULO 5.

MONITOREO DE LA VPN.



Este capítulo nos describe la forma en que se llevará a cabo el monitoreo de la VPN por parte del personal de la SEM con la finalidad de confirmar que efectivamente se está cumpliendo por parte del proveedor de servicios con los parámetros acordados en el contrato.

Además, otro de los objetivos de monitorear la red es recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, los cuales se detallaran más adelante.

MONITOREO DE LA VPN.

Como he mencionado en capítulos anteriores la administración de redes se está convirtiendo en una creciente y compleja tarea debido a la variedad de tipos de red y a la integración de diferentes medios de comunicación. A medida que las redes se vuelven más grandes, más complejas y más heterogéneas, el costo de su administración aumenta. En tal situación, son necesarias herramientas automáticas para dar el soporte requerido por el personal encargado de la administración, recolectando información del estatus y el comportamiento de los elementos y aplicaciones de la red.

Para recolectar la información de diversos parámetros de la red para su posterior análisis, es necesario monitorear; es decir, supervisar el tráfico que viaja por la misma.

Para esto, al igual que se crean políticas de seguridad y de administración, se deben crear políticas para monitorear la red y procedimientos que especifiquen acciones a realizar una vez analizada la información obtenida del monitoreo, dependiendo de los resultados de los mismos.

El monitoreo, es una etapa que forma parte de la administración del rendimiento que tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

- ✓ Utilización de enlaces

Se refiere a las cantidades de ancho de banda utilizado por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc.), ya sea por elemento o de la red en su conjunto.

- ✓ Caracterización de tráfico.

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

- ✓ Porcentaje de transmisión y recepción de información.

Encontrar los elementos de la red que mas solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

- ✓ Utilización de procesamiento

Es importante conocer la cantidad de procesador que un servidor esta consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

- ✓ Utilización elevada.

Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

- ✓ Tráfico inusual.

El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

- ✓ Elementos principales de la red.

Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con mas actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

- ✓ Calidad de servicio.

Otro aspecto, es la Calidad de servicio, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP, el video sobre IP mediante H.323, etc.

- ✓ Control de tráfico.

El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

Dentro del área de TI de la SEM se ha decidido integrar un equipo que se encargue del monitoreo de la red, en concreto éste equipo se encargará de:

- ✓ Administración y monitoreo de los SLA.
- ✓ Administración del contrato y proveedor.
- ✓ Política y normatividad de la red.
- ✓ Administración y planeación de la capacidad.
- ✓ Política y normatividad de videoconferencia.
- ✓ Administración de control y cambios de la red.
- ✓ Seguimiento y solución de incidencias.

Como podemos observar, éste equipo se encargará prácticamente de todas las actividades relacionadas con la red privada virtual de la SEM especificadas anteriormente como tareas del área de TI. Sin embargo, hasta este momento no se han cubierto todas las funciones descritas en dicho cuadro por lo que a continuación describiré cuál será la relación del área de TI con las diferentes áreas dependientes del proveedor para cubrir dichas funciones.

Como ya mencioné, el monitoreo forma parte de la administración del rendimiento y éste se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la

administración de la seguridad, cuando se detecta tráfico que es generado hacia un sólo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

Una breve descripción de las tareas de algunas de las áreas se presenta a continuación.
La administración de fallas tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases:

- ✓ Monitoreo de alarmas. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.

- ✓ Localización de fallas. Determinar el origen de una falla.

- ✓ Pruebas de diagnóstico. Diseñar y realizar pruebas que apoyen la localización de una falla.

- ✓ Corrección de fallas. Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.

- ✓ Administración de reportes. Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

La administración de la seguridad tiene como objetivo ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

Es importante mencionar que aunque el monitoreo será llevado a cabo por el área de TI de la SEM las tareas de corrección de fallas, seguridad, configuración, etc. dependerán del proveedor de servicios por lo que no se describen de manera extensa todas las actividades de la mesa de ayuda, seguridad y comunicaciones.

CONCLUSIONES.

Los enlaces dedicados continuarán siendo una solución adecuada para redes de tráfico intenso, o para empresas o instituciones que aprovechan la capacidad del enlace para también cursar tráfico de voz además de contar con la infraestructura y los recursos suficientes para la contratación. Sin embargo, con las VPN basadas en Internet se desvanecen los problemas de cobertura geográfica y justificación económica de los enlaces dedicados. El acceso ubicuo a Internet permitirá a cualquier empresa o institución reducir costos y optimizar sus operaciones. Las VPN son una excelente opción debido a su gran flexibilidad, robustez, administración y calidad de servicio que nos proporcionan. Sin embargo, hay que hacer nuevamente hincapié que el tipo de empresa o institución y sus aplicaciones dictarán en buena medida el nivel de seguridad, confiabilidad y calidad de la conexión que debe exigirse de la VPN.
Las soluciones de seguridad para las VPN han hecho de éstas una opción igual de confiable que una red privada.

Actualmente, los proveedores han desarrollado un portafolio de servicios para VPN; anteriormente el problema consistía en que los proveedores no tenían la capacidad de proporcionar VPN sobre Internet y por eso los corporativos e instituciones crearon sus propias redes privadas, pero hoy, con las nuevas tecnologías, el proveedor puede ofrecer este tipo de servicios de una forma bastante flexible y escalable.
El contar con un sistema de VPN flexibiliza el trabajo, ya que el usuario (sin ser el dueño de la infraestructura) puede montar diferentes tipos de servicios y, en el momento en que no los ocupe, puede dejar de rentarlos y pedir nuevos servicios. Posiblemente la complejidad pudiera presentarse con el proveedor de servicios, el cual finalmente ofrece diferentes opciones, pero en realidad, en cuestión de flexibilidad, ninguno tiene problemas; la flexibilidad es por excelencia la virtud de las VPN, ya que se puede montar cualquier tipo de servicio.

En cuanto al acceso, la parte de ubicuidad es una de las características fundamentales de las VPN, pues en cualquier lugar se puede accesar independientemente del esquema que se utilice.
En cuanto al desempeño, éste variará según el tipo de VPN que se haya seleccionado y del servicio que el proveedor brinde. En el esquema iniciado por el cliente, pudiera

haber una sobrecarga en la plataforma de cómputo que se utilice, pero cuando el proveedor inicia la VPN, entonces ahí se produciría la sobrecarga (aunque es difícil que exista pues normalmente cuenta con equipos muy robustos).

Como ya se vio, las VPN se pueden implementar en diferentes tecnologías, pero esto resulta transparente para el usuario final pues continuará recibiendo su servicio. La diferencia entre usar una tecnología u otra dependerá del proveedor de servicios.

Definitivamente la oportunidad que brinda ésta tecnología es bastante óptima, ya que en cuanto a costos es muy accesible y en países con economías emergentes, donde el gasto en infraestructura es limitado, ofrece una opción bastante sencilla para hacerla llegar a un número mayor de personas a precios bastante competitivos.

Finalmente, para el caso específico de la Secretaría de Educación Médica, se ha determinado que una solución de VPN rentada a un ISP es una opción bastante adecuada para satisfacer las necesidades inmediatas con la posibilidad de incluir más adelante nuevos servicios y usuarios en caso de ser requeridos. Algunos de los aspectos que se tomaron en cuenta para determinar la viabilidad de contratar el servicio son:

- ✓ No contar con la infraestructura necesaria para implementar y manejar al 100% la VPN
- ✓ Reducción de costos de implementación y de operación
- ✓ Pronto retorno de inversión
- ✓ Fácil administración del servicio
- ✓ Escalabilidad y robustez por parte de la solución
- ✓ Contratos específicos de soporte y asistencia técnica

Sin embargo, para la implementación de la VPN y el óptimo funcionamiento de la misma la Secretaría de Educación Médica deberá sustituir algunos equipos existentes por ser demasiado obsoletos, definir políticas de seguridad y asignar tareas específicas a cada área de Tecnologías de Información o cómputo existentes, de ser necesario, dentro de toda la Facultad de Medicina.

BIBLIOGRAFÍA.

1. G. Mazon, A; "Redes Privadas Virtuales de Cisco Secure". Pearson Educación. Madrid 2002.

2. Brown, S; "Implementación de Redes Privadas Virtuales". McGraw–Hill Interamericana Editores.

3. Karanjit Siyan, PH.D; "Redes Privadas Virtuales. Edición Especial Microsoft Windows 2000 TCP/IP". Pearson Educación. Madrid 2001.

4. Comer, DE; "Redes Globales de información con Internet y TCP / IP". Prentice Hall Hispanoamericana.

5. Ford, M; Lew, HK; "Tecnología de Interconectividad de Redes". Prentice Hall Hispanoamericana.

6. Wang, HH; "Telecommunications Network Management". McGraw-Hill. 1999.

7. Hegering, HG. "Integrated Network and System Management Network Management". Addison-Wesley. 1994.

8. Russel, C; Crawford, S; "Running Microsoft Windows NT Server 4.0". McGraw–Hill.

9. Raya, JL; "Redes locales y TCP / IP". Alfa Omega Grupo Editor.

10. Parker, T; "Aprendiendo TCP / IP en 14 días". Prentice Hall Hispanoamericana.

11. Fúster Sabater, A; Hernández Encinas, L; Otros; "Técnicas criptográficas de protección de datos". Alfa Omega Grupo Editor.

12. Black, UD. "Network management standards: SNMP, CMIP, TMN, MIBs, and object libraries". Segunda Edición. McGraw-Hill. New York 1995.

13. Kauffels, F; "Network Management: Problems, Standards and Strategies". Addison-Wesley. 1992.

REFERENCIAS CORRESPONDIENTES A ARTÍCULOS DE REVISTAS.

1. Red. Enero 2001 VPN: túneles cómodos y seguros para proteger su información.

2. PC Magazine en español. Volumen 11 número 5. Artículo: Redes Privadas Virtuales.

3. Smart Business. Año 7 numero 8 Proyecto: Redes Privadas Virtuales.

SITIOS DE INTERNET.

http://www.avantel.net.mx

http://www.att.net.mx

http://www.telmex.com.mx

http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml

http://www.red.com.mx/scripts/redArticulo.php3?idNumero=46&articuloID=7294

http://biblioteca.dgsca.unam.mx/cu/productos/boletines/msg00004.html

http://www.logiclinux.com/soluciones/vpn/

http://www.entarasys.com/la

http://www.itu.int