ESCUELA SUPERIOR POLITÈCNICA DEL LITORAL

FACULTAD DE INGENIERÌA EN ELECTRICIDAD Y COMPUTACIÒN

SEGURIDAD EN EL COMERCIO ELECTRÒNICO A TRAVÈS DE VPN

TESIS DE GRADO

PREVIO A LA OBTENCIÒN DEL TÌTULO DE

INGENIERO EN ELECTRICIDAD

ESPECIALIZACIÒN ELECTRÒNICA

PRESENTADO POR:

RITA CABRERA SARMIENTO

LENIN LEMOS PONCE

RICARDO MORÀN VERA

GUAYAQUIL – ECUADOR

2.006

AGRADECIMIENTO

A todas las personas
que de uno u otro modo
proporcionaron
información para la
realización de este
trabajo, especialmente
a todos nuestros
familiares y amigos
por su invaluable ayuda.

DEDICATORIA

Dedico este trabajo a mis padres, que supieron apoyarme siempre, a mi esposo y a mis hijos que me dieron la fuerza para continuar.

Rita

A Dios, a mi madre, a mis hermanos y a toda mi familia que nunca me dejò desfallecer y en todo momento supo brindarme su apoyo y comprensión.

Lenin

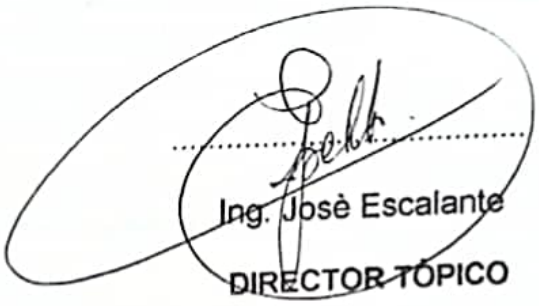
Dedico este proyecto a mis padres, a mis hermanos, a mis abuelos y a mi novia, que en todo momento me brindaron su comprensión y apoyo.

Ricardo

TRIBUNAL DE GRADUACIÒN

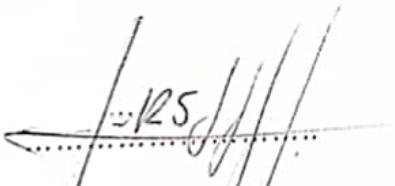
Ing. Miguel Yapur

SUBDECANO FIEC



Ing. Josè Escalante

DIRECTOR TÓPICO



Ing. Servio Lima

VOCAL

Ing. Washington Medina

VOCAL

DECLARACIÒN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestos en esta tesis, nos corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÈCNICA DEL LITORAL".

(Reglamento de Exàmenes y Tìtulos profesionales de la ESPOL.)

Rita Cabrera Sarmiento

Lenin Lemos Ponce

Ricardo Morán Vera

ÌNDICE GENERAL

INDICE DE FIGURAS

ÌNDICE DE TABLAS

INTRODUCCIÓN

Las nuevas prácticas de negocios están provocando grandes cambios en las redes empresariales. Los empleados en las sedes corporativas y en las oficinas de todo el mundo, así como las personas que trabajan en sus casas, necesitan acceso inmediato a los datos, sin importar si los datos se encuentran en servidores centralizados o departamentales.

Las organizaciones como empresas, agencias, universidades, etc., necesitan información en forma inmediata, y es precisamente el Internet el proveedor de toda la información, en cualquier lugar que nos encontremos, sea en la computadora personal de la oficina o de la universidad, o una computadora portátil, o una computadora casera o de un cyber, obtendremos la información deseada.

Hay personas que no desean hacer largas filas para realizar sus pagos o una compra. Hoy la tecnología está muy avanzada y podemos realizar todo tipo de transacciones

desde el lugar que estemos, sólo oprimiendo unas cuantas teclas.

Pero en las empresas siempre habrá el miedo de que se roben información confidencial, por lo que se creó las VPN (Virtual Private Network) o en español Redes Privadas Virtuales, como su nombre lo indica, redes privadas, es decir, que cualquier transacción que se lleve a efecto será entre las personas que se están comunicando sin la intrusión de un tercero.

Las VPN fueron creadas para dar mayor agilidad al comercio electrónico pero junto a ella aparece la parte legal que debe valorar lo que se envía a través de la VPN, es decir, lo que llamamos la firma electrónica, que es la única que puede certificar la transacción electrónica que se realice a través del enlace entre dos computadoras y que trabajan con Virtual Private Network por medio de Internet.

Las VPN junto a Internet son una herramienta poderosa que puede ampliar nuestras puertas al mundo del Comercio Global, gracias a ella podremos realizar cualquier tipo de transacción

electrónica con todas las garantías de seguridad sin necesidad de trasladarnos desde nuestros hogares o empresas.

CAPITULO I

COMERCIO ELECTRÓNICO

1.1 ANTECEDENTES.

¿Cree Usted que el Comercio Electrónico, cambiará la forma de hacer negocios en el mundo?

¿Qué impacto tiene este fenómeno sobre los flujos financieros, la legislación comercial, las estrategias empresariales y la producción de artículos?

¿Qué habilidades y conocimientos se espera que tengan los EMPRESARIOS y los PROFESIONALES para operar en un contexto de la RUPTURA DEL PARADIGMA?

Si asumimos que "Comercio Electrónico" es cualquier negocio desarrollado con la intervención de medios o intermediación tecnológica, prácticamente TODO entra en esta categoría, desde la invención del telégrafo, el teléfono y luego el fax;

TODO SE HACE CON INTERVENCION DE ALGUN APARATO.

Pero "Electronic Commerce" no es solo un negocio con intervención tecnológica, en consecuencia, debemos ajustar la definición para que se comprenda que la importancia actualmente es la consolidación de los MEDIOS DE PAGO y la TRANSNACIONALIZACION DE LAS LEGISLACIONES INVOLUCRADAS, obteniéndose de esta forma la RUPTURA DEL PARADIGMA.

En efecto, si el tema del E-Commerce adquiere trascendencia es porque representa en el mediano plazo el derribo de las últimas barreras de la tan mencionada GLOBALIZACION.

Siempre ha existido el COMERCIO ENTRE NACIONES, incluso antes de que estuviesen definidas como tales.

Para que exista un NEGOCIO debe existir:

VENDEDOR,
COMPRADOR,
PRODUCTO o SERVICIO a transferir,

PAGO y

ENTREGA del Producto o Servicio.

Además como etapa previa se requiere la PROMOCION o PUBLICIDAD de los productos y servicios y de la oferta de sus precios. Esto constituye la esencia de los negocios. Antiguamente, los comerciantes viajaban llevando consigo los productos, promocionándolos y cobrando de contado en oro, esclavos, especias o alfombras. Estos comerciantes cumplían la doble función de compra y venta, es decir importación y exportación.

La creación y desarrollo de la Letra de Cambio permitió un primitivo pero eficaz medio de pago internacional que completa su evolución con las Cartas de Crédito.

Desde la invención del telégrafo y posteriormente el teléfono, estos medios de acreditar fondos internacionalmente se fueron perfeccionando sin cambiar su esencia y naturaleza.

Otro tanto ocurrió con la posibilidad de remitir presupuestos, requerir ofertas o enviar catálogos de productos. Las

facilidades de transportación a su vez, permitieron la "mundialización" de las antiguas Ferias de Pueblo para convertirlas en "Ferias Internacionales", facilitando la promoción y contacto de compradores y vendedores.

En la última y previa etapa a la ruptura del paradigma, los sistemas financieros y comerciales perfeccionaron los procedimientos del INTERCAMBIO ELECTRONICO DE DOCUMENTOS, reconocido en su sigla inglesa como EDI (Electronic Document Interchange), estos procedimientos son formas estándares, bastante seguras y sumamente rápidas para transferir fondos entre Instituciones Financieras.

Mucho antes de que se consolide el EDI, las comunicaciones de masas (periódicos, cine, radio y televisión) permitieron el desarrollo de MARCAS GLOBALES y una ESTANDARIZACION DE LAS PAUTAS DE CONSUMO como Nike, Marlboro o Coca Cola representan lo mismo para toda la humanidad.

¿Por qué decimos que el E-Commerce representa la ruptura del paradigma?

Porque lo que ha cambiado y va a cambiar aún más es el contacto MASIVO entre oferta y demanda sin importar dónde está radicada la demanda. Y en ello confluyeron DOS FACTORES FUNDAMENTALES que hoy están presentes:

- Comunicación Global Real de Doble Vía
- Moneda Universal

Cuando a principios de los 90' se habilitó el uso COMERCIAL DE INTERNET ni aún los más entusiastas previeron que en menos de CINCO AÑOS cerca de 100 millones de usuarios estarían en contacto unos con otros. Pero además, ese contacto es un contacto NO REGULADO. El intercambio de información es ABSOLUTAMENTE LIBRE y CASI IMPOSIBLE de ser limitado, regulado, controlado o interrumpido por los gobiernos locales. Además, tiene rango amplio (imágenes, texto, voz) y a diferencia de la televisión, es de DOBLE VIA, es decir, recibo y envío de información).

¿Tiene idea dónde queda Amazon? en tres años se convirtió en el TERCER MAYOR VENDEDOR DE LIBROS EN LOS EE.UU., sabemos que queda en EE.UU., pero, no tiene local a la calle y

además podría estar radicado en Tanganica, Bulgaria o Zimbawe sudoccidental que sería exactamente lo mismo.

¿Quiere un Informe de la Comisión Internacional del Azúcar? PAGUE CON SU TARJETA y BAJELO DIRECTAMENTE CON SU COMPUTADORA en formato de archivo para Excel, en estos casos ni los buenos DHL pueden cobrar su tajada por entregarle el documento en su casa.

Entonces, ¿qué falta para completar el circuito? Aún varias cosas importantes:

1. Mayor seguridad en la transferencia de datos para evitar el "robo" de la información.

2. Ajustes en las legislaciones comerciales internacionales para hacer extensivo los derechos del comprador, como por ejemplo: garantías del producto.

3. Un leve retoque en la optimización de la distribución, aunque DHL llega casi en 48 horas a cualquier lugar del mundo.

4. El punto más complejo y que más tiempo tomará, es la ESTANDARIZACION de los DERECHOS ADUANEROS y ARANCELARIOS.

¡El mundo está en el umbral de un Transfer interrupted!

HE AQUÍ LA RUPTURA DEL PARADIGMA.

- Los mercados SON GLOBALES.
- Las Principales MARCAS son GLOBALES.
- Existen medios de pago GLOBALES.
- Las reglas de PROMOCION Y PUBLICIDAD deberán ser GLOBALES.
- Las empresas TENDRAN QUE SER GLOBALES.
- Los profesionales DEBERAN GLOBALIZARSE.

1.2 ¿ QUE ES EL COMERCIO ELECTRONICO?

Es cualquier forma de transacción comercial basada en la **transmisión de datos sobre redes de comunicación** como

Internet en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo.

El comercio electrónico es el nuevo marco de negocios en el que se desarrollan cada vez más operaciones mercantiles. Cada vez son más numerosas las empresas que realizan todas sus operaciones comerciales utilizando tecnologías de la comunicación, aunque solo lo utilicen para algunas funciones especificas.

No se limita a comprar y vender, sino a todos los aspectos mercantiles como publicidad, relaciones con los trabajadores, contabilidad, búsqueda de información sobre productos o proveedores, trámites administrativos,etc.Las empresas, aunque estén físicamente alejadas de sus clientes y proveedores, pueden tener una mejor comunicación y accesibilidad a todas las acciones

En Ecuador el uso del comercio electrónico es todavía incipiente pero se espera que sea una práctica generalizada dentro de pocos años. Aquellas personas y empresas que desconozcan estas técnicas se quedarán desplazadas en sus

actividades profesionales y, por lo tanto, perderán competitividad.

El comercio electrónico, de carácter mundial por su propia naturaleza, abarca una amplia gama de actividades, algunas de ellas conocidas, la mayoría totalmente nuevas.

Impulsado por la revolución de Internet se expande aceleradamente y experimenta cambios radicales. Bajo la denominación de comercio electrónico se incluye tanto el comercio electrónico indirecto, como por ejemplo, el pedido electrónico de bienes tangibles; y el directo, como la entrega en línea de bienes intangibles.

No cabe duda que la aparición del comercio electrónico obliga claramente a replantear procedimientos del comercio tradicional, surgiendo nuevos problemas, e incluso agudizando algunos de los existentes. En ese catálogo de problemas, se plantean preguntas que van, desde:

La validez legal de las transacciones y contratos sin papel, el control de las transacciones internacionales, incluido el cobro

de impuestos; la protección de los derechos de propiedad intelectual, el fraude, y el uso abusivo de datos personales. Hasta otros provocados por:

La falta de seguridad de las transacciones y medios de pago electrónicos, la falta de estándares consolidados, la congestión de Internet, la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles.

1.3 TIPOS DE COMERCIO ELECTRONICO SEGÚN AGENTES QUE INTERVENGAN.

- Comercio entre empresas “business to business” (B2B).
- Venta de productos fiables a un consumidor o “business to consumer” (B2C).
- Consumer to Consumer” (C2C) subastas en la que usuarios particulares venden productos.
- A2B/C/A “administration to business/consumer o administration”.
- “Peer to peer” (P2P), o de amigo a amigo.
- “Business to employee” (B2E), comunicaciones entre empresas y trabajadores.

- “Goverment to Consumer” (G2C).
- “Goverment to Goverment” (G2G).

1.4 VENTAJAS Y DESVENTAJAS EN COMPARACIÓN CON EL SISTEMA TRADICIONAL.

Los negocios en Internet no son tan diferentes de los negocios clásicos. Erróneamente se piensa que lo importante es la tecnología. Ventajas son el ahorro de tiempo y los costos asociados a la compra.

Además debemos considerar también:

LAS 5 REGLAS DE LA NUEVA ECONOMIA.-

- Los costos de interacción y transformación actualmente no son tan elevados.
- Los activos no desempeñan un papel tan fundamental en la generación de la oferta.
- El tamaño de la empresa no condiciona los beneficios.
- El acceso a la información ha dejado de ser caro y restringido.

- No se necesitan varios años ni grandes capitales para establecer un negocio a escala mundial.

1.5 ASPECTOS CLAVES DEL COMERCIO ELECTRONICO.

- Personalización.
- Medios de pagos en tiempo real.
- Barreras tecnológicas.
- Seguridad y confianza.

1.6 SISTEMAS DE PAGO DIGITALES.

1.6.1 Historia de las tarjetas de crédito.

Las compañías petroleras fueron pioneras en el uso de tarjetas de crédito a principios de los años veinte. Llamadas tarjetas de cortesía, en realidad estaban hechas de papel y se emitían cada 3 a 6 meses. Aunque las compañías petroleras perdían dinero en las tarjetas, las veían como una forma de atraer y retener clientes.

(Club de los comensales) que apareció en el año 49 con la finalidad de que vendedores cubrieran sus gastos de viaje, hoteles y restaurantes.

En 1958, American Express y Carte Blanche entraron al negocio de las tarjetas de viaje y entretenimiento. En ese mismo año el Bank of America y el Chase Manhattan, el primero y el segundo bancos más grandes de Estados Unidos introdujeron sus propias tarjetas. La tarjeta del Bank of América se llamo BankAmericard, nombre que se cambió por Visa en 1976. La tarjeta del Chase Manhattan se llamó MasterChase; la división de tarjeta de crédito se vendió en 1962 y se le cambió el nombre a MasterCard en 1980.

1.6.2 Concepto de crédito.

El crédito es creencia, fe y confianza. Es el reconocimiento de pago cuando se hace un asiento en una cuenta. Es una cantidad de dinero a disposición de una persona en los libros de un banco. El crédito es confianza en la habilidad y deseo de una persona de pagar, en un momento futuro, bienes o servicios que se le entregan en este momento.

1.6.3 Transacción de pagos interbancarios de tarjetas.

En la actualidad la transacción de pagos interbancarios de tarjetas ha evolucionado a una danza compleja entre muchos participantes. Una transacción común de tarjeta con crédito involucra hasta a 5 partes:

1. El cliente.
2. El comerciante.
3. El banco del cliente, el cual emite la tarjeta de crédito del cliente.
4. El banco del comerciante (también conocido como banco adquiriente).
5. La red interbancaria.

Una transacción ordinaria con tarjetas de crédito consta de 10 pasos:

1. El cliente entrega su tarjeta de crédito al comerciante.
2. El comerciante pide certificación al banco adquiriente.
3. La red interbancaria envía un mensaje del banco adquiriente al banco del consumidor pidiendo la certificación.
4. El banco del cliente envía una respuesta al banco adquiriente mediante la red interbancaria (el banco del consumidor puede también

detener parte de la línea de crédito del cliente, quedando pendiente del cierre de la transacción).

5. El banco adquiriente notifica al comerciante que el cargo ha sido aprobado.

6. El comerciante llena la orden del cliente.

7. En algún momento posterior el comerciante presenta cierta cantidad de cargos al banco adquiriente.

8. El banco adquiriente envía la solicitud de pago al banco del cliente mediante la red interbancaria.

9. El banco del cliente debita de la cuenta del cliente y coloca el dinero en una cuenta de pagos interbancarios, deduciendo un cargo de servicio.

10. El banco adquiriente hace un crédito a la cuenta del comerciante y retira una suma similar de dinero de la cuenta de pagos interbancarios.

En el pasado muchas transacciones de punto de venta no eran autorizadas por cuanto tomaban mucho tiempo y los bancos se preocupaban de que perderían más dinero debido a ventas perdidas de lo que pudieran perder por fraude.

En años recientes el tiempo que demora una autorización de cargo con tarjeta de crédito ha disminuído de casi un minuto a menos de 5 segundos, esto hace que en la actualidad casi todas las transacciones son autorizadas, especialmente las de valor alto.

1.6.4 El algoritmo verificador de las tarjetas de crédito.

El último dígito de un número de tarjeta de crédito es un digito verificador utilizado para detectar errores al digitar al introducir un número de tarjeta en una computadora. El algoritmo es el siguiente:

1.- Multiplique cada digito de la tarjeta por su “peso”. Si una tarjeta de crédito tiene un número par de dígitos, el primero tiene un peso de 2, de otra forma, tiene un peso de 1. Los pesos de los siguientes dígitos se alternan de

forma 1, 2, 1, 2....

2.- Si cualquier digito tiene un valor pesado mayor a nueve, restar 9.

3.- Sumar los pesos de todos los dígitos, módulo 10.

4.- El resultado debe ser cero.

Este algoritmo está diseñado para detectar dígitos transpuestos u otros errores de tecleo, como un mecanismo de seguridad de propósito general. Supongamos que el número de tarjeta de crédito de Rita es el siguiente 3728 024906 54059.

La tarjeta tiene 15 dígitos. El numero 15 es impar, por lo que el primer digito tiene un peso de 1.

Para calcular el digito verificador, multiplicamos:

(3x1) , (7x2) , (2x1) , (8x2) , (0x1) , (2x2) , (4x1) , (9x2) , (0x1) , (6x2) , (5x1) , (4x2) , (0x1) , (5x2) , (9x1).

al realizar las operaciones obtenemos:

(3) , (14) , (2) , (16) , (0) , (4) , (4)

(18) , (0) , (12) , (5) , (8) , (0) , (10)

(9).

Restamos 9 de todos los valores mayores a 9, y los sumamos:

(3) + (5) + (2) + (7) + (0) + (4) + (4)+(9) + (0) + (3) + (5) + (8) + (0) + (1)+ (9) = 60 .

Esto nos dara un digito verificador de 0, debido a que:

60 mod 10 = 0 .

1.6.5 El comprobante del cargo o voucher

El comprobante del cargo o voucher registra las transacciones de la tarjeta de crédito. Para finales de los 70 los clientes de visa y mastercard recibían estados de cuentas mensuales que resumían sus cargos, en vez de los comprobantes originales. En los 80, American Express comenzó a digitalizar los comprobantes y entregar a sus clientes impresiones digitales de sus comprobantes. Hoy los clientes simplemente reciben informes impresos que listan todos los cargos relevantes.

Con el tiempo, la cantidad de información que contiene el comprobante se ha incrementado. En la actualidad contiene una gran cantidad de información, incluyendo:

- Nombre del cliente.
- Número de tarjeta de crédito del cliente.
- Dirección del cliente.
- Número de cliente.
- Fecha de la transacción.
- Monto de la transacción.
- Descripción de la mercancía o servicio.
- Número de referencia.
- Código de autorización.
- Nombre del comerciante.

Muchos sistemas computarizados aún utilizan la palabra “voucher”. Otros se refieren al “registro” o “giro” del pago.

1.6.6 **Usos de tarjetas de crédito en Internet.**

Transacciones con tarjeta de crédito en forma telefónica, tales

tarjetas fueron una opción obvia para los primeros sistemas de pago basados en Internet.

No obstante las tarjetas de crédito presentan también un problema para los comerciantes, debido a que los números de las tarjetas son claves de acceso invariables que pueden utilizarse para cargar pagos repetidamente a la cuenta del consumidor. Por ello los números de la tarjeta de crédito deben protegerse para no ser ¡escuchados! y adivinados. Existen 3 técnicas distintas para aceptar números de tarjetas de crédito junto con transacciones iniciadas a través del Web:

Fuera de línea (Off line)-

Una vez puesta la orden a través del Web, el cliente llama por teléfono al comerciante y le recita el número de su tarjeta. Esta técnica es tan segura como cualquier otra compra realizada por correo o por teléfono. Aunque los números de tarjetas de crédito pueden ser escuchados si se interviene el teléfono o se reprograma el conmutador, parece ser un riesgo que los comerciantes, consumidores y bancos están dispuestos a correr.

En línea con encriptación (On line with encription).-

El consumidor envía el número de su tarjeta al comerciante a través de Internet mediante una transacción encriptada.

En línea sin encriptación (On line without encription).-

El consumidor simplemente envía el número de su tarjeta, mediante un mensaje de correo electrónico o en un comando POST o GET de http. Esta técnica es vulnerable a la intersección.

1.6.7 Sistemas de pago basados en Internet.

A pesar de que la mayoría de las compras hechas en Internet se realizan con tarjetas de crédito. Los comerciantes y consumidores están prestando cada vez mas atención a otros sistemas de pagos basados en Internet.

Ventajas.

A diferencia de las tarjetas de crédito, estos nuevos sistemas

tienen varias ventajas:

Costos reducidos de transacción.-

Los costos por transacción de sistemas de pagos basados en Internet son menos elevados que los costos de las tarjetas de crédito tradicionales.

Anonimidad.-

Con los sistemas de tarjeta de crédito actuales, el comerciante debe saber el nombre, y el número de cuenta del cliente, y con frecuencia también su dirección. Al no pedir tanta información los comerciantes incrementarían sus ventas.

Mayor mercado.-

Hoy en día, existen muchos individuos en el mundo que utilizan efectivos por no ser elegibles para recibir tarjetas de crédito.

Los sistemas de pago que no se basan en el crédito podrían ser útiles para muchas más personas.

Tipos.

Existen varios tipos de sistemas de pago:

Anónimos.-

Los sistemas de pago pueden ser anónimos: es matemáticamente imposible que un comerciante o banco averigüen la identidad del consumidor que hace una compra si no desea revelar información.

Privados.-

El comerciante no conoce la identidad del consumidor, pero le es posible averiguarla a través de la organización que opera el sistema de pagos.

Identificatorios.-

Los sistemas de pago pueden identificar al consumidor ante el comerciante en todos los casos. Las tarjetas de crédito convencionales y los cheques son ejemplos de los sistemas de

pago identificatorios.En esta sección describiremos diversos sistemas de pagos utilizados hoy en día en Internet.

DigiCash.

DigiCash (¨DigiEfectivo¨) es un sistema de pagos electrónicos también conocido como E-cash. DigiCash se basa en un sistema de prendas (tokens) digitales llamadas ¨monedas digitales¨. El consumidor crea cada moneda y la firma digitalmente la casa de monedas de DigiCash, la cual, se presume, opera un banco o el gobierno. Los usuarios del sistema pueden intercambiar las monedas o convertirlas en efectivo en la casa de moneda, proceso similar al de un jugador de póker que convierte sus fichas en efectivo al final del día.

Suscripción.-

Para suscribirse al sistema DigiCash, un consumidor debe descargar el software de DigiCash y establecer una cuenta con una organización capaz tanto de emitir como de recibir las monedas electrónicas de DigiCash. Las cuentas de DigiCash constan de dos partes: Una cuenta de depósito en la institución financiera y una billetera electrónica que se mantiene en la

computadora del usuario. Para obtener dinero Digital, el software del usuario crea cierto número de monedas electrónicas, es decir, bloques de datos.

Parte de estas monedas son entonces marcadas, es decir se les hace una operación binaria SHORT con una cadena aleatoria. Las monedas se envían entonces a la casa de monedas para que las firme. Por cada dólar de moneda que firma la casa de moneda se retira una cantidad igual de la cuenta del usuario. Las monedas se devuelven después a la computadora del usuario, donde se les vuelve a aplicar la operación SHORT. De esta forma, es imposible que la institución emisora rastree las monedas gastadas por el usuario que las emitió.

Compra.-

Para realizar una compra con dinero de DigiCash, el consumidor debe ejecutar un pequeño programa llamado billetera DigiCash

El programa se comunica mediante un protocolo que le permite intercambiar monedas con el sistema del comerciante y con sus

billeteras.Las monedas también pueden enviarse por correo electrónico o imprimirse y enviarse por cualquier otro medio.

Seguridad y privacía.

Este sistema de efecto electrónico ofrece ser anónimo incondicional, así como ser anónimo condicional: el cliente siempre conoce la identidad del comerciante, y este puede conocer la del cliente si este intenta hacer un doble gasto del dinero.

Virtual PIN.

Virtual PIN se distingue de los demás sistemas de pagos electrónicos porque no necesita de un programa especial para que el consumidor pueda realizar compras. En vez de ello, los pagos son autorizados mediante correo electrónico.

PIN virtuales típicos son ¨COMPRA-VIRTUAL¨, ¨SU-PIN-VIRTUAL¨, ¨SMITH-SAUNDERS¨ y ¨GASTA-MI-DINERO¨.

No se utiliza encriptación al enviar información de o al consumidor. En vez de ello, el PIN virtual obtiene su seguridad confiando en la dificultad de interceptar el correo electrónico y manteniendo toda la información de las tarjetas de crédito de los clientes fuera de Internet. Proporciona seguridad adicional por el hecho de que los cargos a la tarjeta de crédito pueden revertirse hasta 60 días después de ser realizados.

Virtual PIN utiliza firmas digitales para autenticar los mensajes de autorización que intercambian con los comerciantes que entregan mercancías físicas. También permite a los grandes comerciantes encriptar sus transacciones.

Suscripción.-

Para suscribirse, el consumidor llena y envía una forma de suscripción de Virtual PIN. Esta forma se la proporciona en un sitio web y mediante correo electrónico, que incluye el nombre y la dirección de la persona y el PIN virtual que desea utilizar, pero no su número de tarjeta de crédito.

Una vez recibida la forma, se envía al usuario un mensaje de correo electrónico que contiene su número de solicitud y un número telefónico gratuito para que llame. El suscriptor llama al número, marca su número de solicitud mediante un teléfono de tonos e introduce los números de su tarjeta de crédito.

Compra.-

El ciclo de compra mediante PIN virtual consta de 5 partes:

1.- El consumidor entrega al comerciante su PIN virtual.

2.- El comerciante transmite su PIN a Virtual PIN y el monto de la transacción para que la autorice.

3.- Virtual PIN envía al consumidor un mensaje de correo electrónico en el que le pregunta si el cargo del comerciante es legítimo.

4.- El consumidor responde al mensaje de Virtual PIN con las palabras ¨Yes¨ (Si) o ¨Fraud¨ (Fraude).

5.- Si el consumidor responde ¨Yes¨, Virtual PIN informa al comerciante que el cargo ha sido aceptado.

Seguridad y privacía.-

Los PIN virtuales no encriptan al viajar a través de Internet. Por ello un espía puede interceptarlos e intentar utilizarlos para realizar una transacción fraudulenta. Sin embargo también tendría que ser capaz de interceptar el mensaje de confirmación que se envía al consumidor. Por ello la seguridad del sistema de PIN virtual se basa en la dificultad de interceptar mensajes de correo electrónico.

CyberCash/CyberCoin.-

CyberCash (¨ciber efectivo¨) es un sistema basado en tecnología de llave pública que permite usar tarjetas de crédito convencionales a través del World Wide Web.

CyberCoin (¨ciber moneda¨) es una adaptación de la misma tecnología para realizar transacciones de pequeño monto.

Más que parecerse a las tarjetas de crédito el servicio de CyberCash puede equipararse a una tarjeta de débito.

Suscripción.-

Antes de utilizar CyberCash, el consumidor debe descargar un programa especial del sitio web de CyberCash. Al programa se le llama billetera CyberCash, y mantiene una base de datos de las tarjetas de crédito y otros instrumentos de pago del usuario.

Cuando se ejecuta por primera vez, el software de billetera crea una combina ción de llaves pública y privada. La llave privada, el número de tarjeta de crédito y bitácoras de transacción se almacenan en el disco duro del usuario encriptada mediante una frase de acceso, con un respaldo encriptado en un disket.

Para utilizar una tarjeta de crédito con el sistema CyberCash, esta primero debe suscribirse. Para crear una cuenta CyberCoin, el usuario debe llenar una forma de suscripción en línea. La implementación actual de CyberCash permite transferir dinero de una tarjeta de crédito o cuenta de cheques a una cuenta de CyberCoin mediante el sistema de transferencia electrónica de fondos Automated Clearing House(ACH). El dinero transferido a la cuenta de CyberCoin desde una cuenta de cheques puede transferirse de vuelta a la misma, mientras el dinero transferido

desde una tarjeta de crédito debe ser gastado. CyberCash permite al usuario cancelar su cuenta de CyberCoin y recibir un cheque por los fondos restantes.

Compra.-

La billetera CyberCash se registra como aplicación auxiliar para Navigator de Nestcape e Internet Explorer. Después las compras, pueden iniciarse descargando archivos con un tipo de MIME específico.

Al iniciar una compra, la billetera CyberCash muestra el monto de la transacción y el nombre del comerciante. El usuario decide entonces que tarjeta de crédito utilizar y si aprobar o rechazar la transacción. El software también puede programarse para aprobar de forma automática transacciones con un monto menor a 5 dólares, lo cual crea el peligro de que los comerciantes creen páginas web que roben pequeñas cantidades de dinero a los usuarios sin su conocimiento.

Si el usuario aprueba la transacción, se envía al comerciante una orden de pago encriptada. El comerciante puede

desencriptar parte de la información contenida en la orden de pago, pero no toda. Además, agrega su propia información de pago a la orden, la firma digitalmente y la envía al servidor de CyberCash.

El servidor de CyberCash recibe la información de pago y la desencripta. Verifica que no sea una solicitud duplicada y compara la copia de la factura del usuario con la del comerciante para asegurarse que todo sea legal.

Luego envía la información de pago de la tarjeta de crédito al banco adquiriente, quien autoriza la transacción y envía la respuesta a CyberCash, que a su vez envía una respuesta encriptada al comerciante. Por último, el comerciante transmite la confirmación de pago de CyberCash de vuelta al consumidor.

Las compras mediante CyberCoin son similares a las realizadas con CyberCash, excepto que el dinero simplemente se debita de la cuenta del usuario en CyberCoin y se acredita a la del comerciante.

Seguridad y privacía.-

El pago mediante CyberCash está diseñado para proteger a los consumidores, comerciantes y bancos contra el fraude. Hace esto, utilizando la criptografía para proteger la información de pagos mientras está en tránsito.

Toda la información de pago se encripta antes de ser enviada a través de Internet. Además, CyberCash protege al consumidor contra fraudes del comerciante: este nunca tiene acceso al número de tarjeta de crédito del cliente.

SET.-

SET es el protocolo para Transacciones Electrónicas Seguras (Secure Electronics Transaction) para enviar información de pagos hechos con tarjetas a través de Internet.

Se diseñó para encriptar tipos específicos de mensajes relacionados con pagos.MasterCard, Visa y varias compañías de computadoras desarrollan en forma conjunta el SET estándar.

De acuerdo con la documentación de SET algunas de sus metas son:

- Permitir la transmisión confidencial.
- Autenticar a las partes involucradas.
- Asegurar la integridad de las instrucciones de pago por bienes y servicios.
- Autentificar la identidad del tarjeta habiente y del comerciante entre si.

SET utiliza encriptación para brindar confidencialidad en la comunicación, y firmas digitales para autenticación. Con SET, se pide a los comerciantes certificados digitales emitidos por sus bancos adquirientes. Los consumidores pueden tener, de manera opcional, certificados digitales emitidos por sus bancos. Durante las pruebas de SET, MasterCard obligaba a los consumidores a tener certificados digitales; en cambio Visa no lo pide.

En una transacción con SET ordinaria, existe información privada entre el consumidor y el comerciante (digamos los productos que se ordenan) e información privada entre el

consumidor y el banco (el número de cuenta por decir algo). SET permite incluír ambos tipos de información privada en una sola transacción firmada mediante una estructura criptográfica conocida como firma dual.

Un solo mensaje de solicitud de compra de SET consta de 2 campos, uno para el comerciante y otro para el banco adquiriente.

El campo del comerciante sé encripta con la llave pública del comerciante; de la misma forma, el campo del banco sé encripta con la llave pública del banco. El SET estándar no proporciona directamente al comerciante el número de tarjeta de crédito del consumidor, pero el banco adquiriente puede, a discreción, proporcionárselo al enviar su confirmación.

Además de estos bloques de encriptación, la solicitud de compra contiene compendios de mensaje* de cada uno de estos 2 campos y una firma. Dicha firma se obtiene concatenando ambos compendios, tomando el compendio de los compendios y firmando el compendio resultante.

La firma dual permite tanto al comerciante como al banco leer y validar su firma en la mitad de la solicitud de compra sin tener que desencriptar el campo de la otra parte.

Tarjetas inteligentes.-

Las tarjetas inteligentes son idénticas a las de crédito, excepto que almacenan información en chips de microprocesadores en vez de bandas magnéticas. Difieren respecto de las tarjetas convencionales en varias formas importantes:

- Las tarjetas inteligentes pueden almacenar una cantidad de información mucho mayor que las tarjetas de banda magnéticas. Las bandas magnéticas pueden almacenar algunos cientos de bytes de información; los chips de las tarjetas inteligentes, muchos kilobytes. Además, la cantidad de información que puede almacenarse en una tarjeta inteligente va en constante incremento conforme aumentan las densidades de los chips. Debido a esta mayor capacidad de almacenamiento, una sola tarjeta inteligente puede servir para múltiples propósitos.

- Las tarjetas inteligentes pueden protegerse mediante una clave de acceso. Toda la información almacenada en una banda magnética puede ser leída cada vez que se inserte en una unidad lectora; la información contenida en una tarjeta inteligente puede estar protegida con una clave de acceso y ser revelada en forma selectiva.

- Las tarjetas inteligentes pueden ejecutar motores de encriptación RSA. Una tarjeta inteligente puede servir para crear una pareja de llaves pública/privada. La tarjeta puede diseñarse de forma que la llave pública sea legible libremente, pero la privada no. Así, al desencriptar un mensaje, el usuario debe tener posesión física de la tarjeta, lo que le brinda gran confianza en que su llave secreta no ha sido copiada.

Mondex.-

Mondex no es un sistema de pagos basado en Internet, pero es uno de los sistemas de pagos digitales de propósito general más grandes hoy en día.

Mondex es un sistema cerrado que se basa en una pequeña tarjeta inteligente del tamaño de una tarjeta de crédito, en teoría, no puede hacérsele una ingeniería inversa. Utiliza un protocolo secreto. Por ello, lo que se diga de mondex se basa casi en su totalidad en declaraciones de la empresa.

Cada tarjeta mondex puede programarse para contener cierta cantidad de dinero. El valor de la tarjeta puede leerse colocándola en un dispositivo conocido como billetera mondex se puede transferir dinero entre 2 billeteras mediante un rayo infrarrojo. A los comerciantes se les proporciona, además, una billetera especial para ellos. Mondex puede utilizarse también para realizar compras telefónicas utilizando un teléfono propietario. La tarjeta puede ser vuelta a ¨llenar¨ mediante un cajero automático con equipo especial.

1.7 SEGURIDAD

1.7.1 ¿Que es la Criptografia?

La criptografía es un conjunto de técnicas empleadas para conservar segura la información. Con ella es posible transformar

palabras escritas y otros tipos de mensajes de forma que sean incomprensibles para receptores no autorizados. Los sistemas de encriptación (codificación) modernos constan de dos procesos complementarios:

Encriptación.-

Proceso mediante el cual el mensaje llano se transforma en un segundo mensaje cifrado mediante un algoritmo de encriptación y una llave de encriptación especial.

Desencriptación.-

Proceso inverso, en el que el texto cifrado se convierte nuevamente en el texto llano original mediante una segunda función compleja y una llave de desencriptación. En algunos sistemas de codificación, las llaves de encriptación y de desencriptación son iguales; en otros, son distintas.

La figura 1-1 que se muestra a continuación nos enseña como se acoplan ambos procesos.

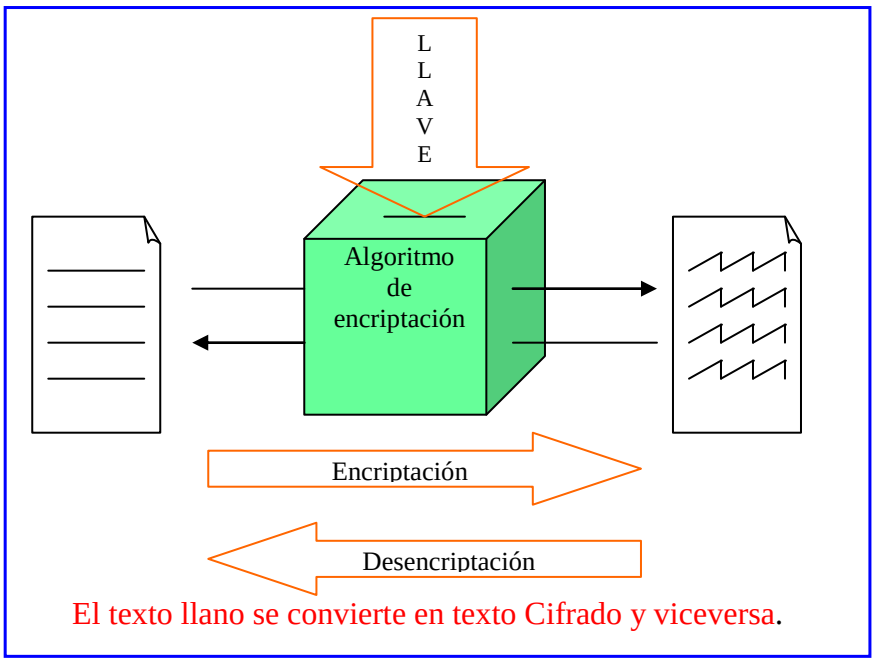


FIG. 1.1 Proceso de encriptación y desencriptación.

1.7.2 Firewall.

Un cortafuego es un medio que sirve para regular el acceso a la red de computadoras de una organización.

Para la red de computadoras de una organización un cortafuegos tiene como funciones: controlar el acceso y registrar los intentos de acceso. Para ello, consulta la información identificada asociada a la comunicación procedente del exterior. Esta información consta de datos sobre la dirección del host origen, sobre la dirección del host destino e

información acerca del servicio solicitado. El cortafuegos decide entonces permitir o no la comunicación de acuerdo con la política de seguridad configurada por el administrador del cortafuegos. Además la mayoría de cortafuegos anota los intentos de acceso en un registro electrónico.

1.7.3 VPN.

Una red privada virtual es la creación de una conexión punto a punto segura a través de una red privada o una red pública tal como la internet. Un cliente de red privada virtual (cliente VPN) usa protocolos especiales basados en TCP/ IP llamados protocolos “Tunneling” para hacer una llamada virtual a un puerto virtual en un servidor VPN. El mejor ejemplo de redes privadas virtuales es aquel en el que un cliente VPN que hace una conexión de red privada virtual a un servidor de acceso remoto que está conectado a Internet.

El servidor de acceso remoto responde la llamada virtual, autentifica a la persona que hace la llamada, y transfiere datos entre el cliente de la red privada virtual y la red de la empresa.

Una red privada virtual es siempre una conexión lógica e indirecta entre el cliente de la red privada virtual y el servidor de la red privada virtual. Para asegurar privacía, usted debe encriptar los datos enviados sobre la conexión.

1.8 PROBLEMAS QUE SE SUSCITAN CON EL E-COMERCE.

A.- Problemas legales de las direcciones IP y DNS.

Las direcciones IP son el sistema numérico básico de intercomunicación en la red, que asigna direcciones de origen y destino, es decir, identifican los distintos ordenadores conectados a la red.

Para facilitar el uso de estos números, aparecen los nombres de Dominio (DNS Domain Name Server), que son nombres asociados a direcciones IP y que constituyen su domicilio.

Estas direcciones son identificables desde cualquier ordenador conectado a la red, las cuales son únicas para cada agente. Tener un nombre de dominio deducible es vital para las

compañías que quieran realizar su actividad en Internet. Así conocidas instituciones, tanto comerciales como no comerciales, se presentan en la red con el nombre que utilizan en otros ámbitos.

Ejemplos de esta utilización de la marca con la que se conocen como nombre de dominio son los siguientes: el diario " EL PAIS " tiene la dirección " el ais.es", "TELEFONICA" tiene el dominio "telefónica. es".

Desde un punto de vista legal, la institución de los DNS plantea distintos problemas. Por un lado pueden surgir disputas entre particulares respecto a un DNS concreto. Por otro lado, un DNS pueden entrar en conflicto con una marca registrada o suponer una práctica de competencia desleal, al producir confusión en el mercado, como es el caso McDonalds en USA.

Por otra parte el uso indiscriminado de las direcciones IP puede ocasionar graves perjuicios debido a una utilización fraudulenta. Un claro ejemplo fue el ocurrido en una gran superficie que realizaba sus ventas a través de la red. La utilización indebida por parte de un tercero del número IP le

ocasionó grandes pérdidas. Independientemente de las actividades técnicas de prevención, será necesario adoptar las soluciones jurídicas y llevar acabo las acciones legales pertinentes.

B.- Propiedad intelectual e industrial.

Gran parte de los productos que se van a comercializar por medios electrónicos tales como vídeo, sonido, fotografías, bases de datos, programas de ordenador, texto, animaciones, etc. pueden ser considerados creaciones intelectuales.

Esta misma protección sería de aplicación a las creaciones intelectuales que puedan ser desarrolladas por la propia entidad financiera o por un tercero por encargo de ésta en la implantación y desarrollo de sus sistemas de comercio electrónico.

Un supuesto muy común es la necesidad de regular los términos de la licencia de uso del software que el cliente necesita para poder operar en sistemas de banca en casa.

C.- Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.

La proliferación del comercio electrónico conlleva la necesidad de creación de grandes bases de datos con información relativa a datos personales de personas físicas e interconexión de unas bases e datos con otras, con la consecuente cesión de datos. Por este motivo, será necesario analizar, al menos, el tipo de dato recogido, estructura del fichero, tratamiento y almacenamiento de los datos, con la finalidad de cumplir con las obligaciones impuestas.

Las redes informáticas abiertas, tales como Internet, serán con toda probabilidad el medio clave para la comercialización a distancia de productos y servicios.

Como muestra de esta nueva realidad pueden señalarse proyectos de teletrabajo, tiendas virtuales ("virtual malls"), relaciones proveedores-empresas vía EDI, sistemas de pago electrónico, compras de obras audiovisuales, música, fotografías, libros o programas de ordenador a través de medios telemáticos. Esto hará que ciertas personas o

empresas manejen obligadamente datos personales de sus clientes. Pero estas personas deberán manejar esta información con la mayor confidencialidad posible, porque de lo contrario podrían tener problemas con la ley de comercio electrónico, específicamente con el Artículo 58 al final del cual se estipula:

"Sobre la obtención y utilización no autorizada de información .- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionados con pena de prisión de 2 meses a 2 años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."

D.- Dinero Electrónico.

Uno de los servicios que comienzan a prestar las entidades financieras a través de las Redes, es la posibilidad que se ofrece al usuario de realizar compras en la Red utilizando dinero virtual o dinero electrónico.

Para ello, el usuario debe instalar un software en su PC, generalmente denominado Wallet, que le permite acceder a un tercero que actúa como broker y cambiar dinero de curso legal de su cuenta bancaria por dinero electrónico.

Las ventajas de este sistema consisten en que los datos de tipo económico del comprador no circulan constantemente por la red, permitiendo una mayor seguridad de su intimidad.

Para la utilización de este sistema deben concertarse distintos negocios jurídicos al menos, entre el usuario e intermediario y entidad financiera e intermediario, regulando las obligaciones y entre ellos.

Una vez en activo, aparecen relaciones jurídicas entre comprador y vendedor, surgiendo preguntas jurídicas de muy variada índole, como legislación aplicable, obligaciones derivadas de la legislación de ventas a distancia, responsabilidad del vendedor o medios de prueba de las operaciones realizadas, que deben ser objeto de análisis desde un punto de vista legal.

E.- Derecho de Las Telecomunicaciones.

Partiendo de la premisa de que para realizar negocios vía telemática es necesario poseer o contratar líneas de telecomunicaciones, surgen relaciones jurídicas con diferentes agentes, tales como operadores de telecomunicaciones, proveedores de servicios y de contenidos, que afectan tanto a la entidad financiera como al usuario final.

Estas relaciones jurídicas deberán ser objeto de un análisis que prevea situaciones de conflicto como responsabilidad de proveedores, difusión de contenidos ilícitos en la red, calidad de servicio o cumplimiento de la legislación aplicable y sus posibles soluciones.

Una vez definidas, será conveniente plasmarlas en un contrato por las partes que intervienen.

Por el momento no poseemos ningún marco regulatorio sobre el uso de las VPN, sin embargo sugerimos que se revise primero la ley de comercio electrónico antes de la elaboración de cualquier contrato que incluya la utilización de VPNs.

F.- Efecto Aldea Global.

La denominada “Aldea Global” surge al utilizar inmensas redes en las que actúan innumerables agentes de procedencias y características distintas, que al relacionarse constituyen una nueva estructura que va más allá de las conocidas. Produciendo que las implementaciones que se hacen en este entorno se encuentren cada vez con nuevos problemas.

G.- Seguridad y Valor Probatorio del Documento Electrónico.

Uno de los problemas que se plantean a la hora de dar una solución de comercio electrónico es la seguridad. Esta afecta a la autenticidad de las partes, confidencialidad e integridad y no repudio del documento. Las soluciones en materia de seguridad son necesarias tanto para conseguir la confianza del usuario como para cumplir con la legislación que en materia de protección de datos pueda desarrollarse.

Relacionado con lo anterior, aparecen grandes problemas relativos a la prueba de las transacciones electrónicas en las

posibles reclamaciones por los usuarios u organizaciones de consumidores, derivadas de la ejecución de los servicios contratados a través de medios telemáticos.

En este sentido, han comenzado a crearse empresas que realizan funciones de certificación de documentos, utilizando las últimas técnicas de criptografía. La contratación con una autoridad de certificación o notario electrónico podría ser una solución alternativa, si bien será conveniente analizar los procedimientos seguidos por dichas entidades, así como cuestiones de atribución de competencia o valor público o privado del documento generado.

En nuestro país la Ley de Comercio Electrónico en su Artículo 56 especifica lo siguiente:

“La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejan la técnica y la tecnología. En todo caso la valoración

de la prueba se someterá al libre criterio judicial según las circunstancias en que hayan sido producidos.

1.9 CONSIDERACIONES LEGALES: CIVILES

Al operar una computadora, existen preocupaciones adicionales de las interrupciones y desastres físicos. También es necesario preocuparse de que las acciones de algunos de los usuarios o del mismo administrador u operador puedan resultar en violaciones a la ley o en demanda civil.

La ley está cambiando rápidamente en las áreas del uso y abuso computacional. También respecto a las redes y la comunicación a través de ellas. Conforme se incrementa el número de personas que utilizan computadoras y redes, y al irse atando cada vez más interés comercial al cómputo, podemos esperar que vaya en aumento el ritmo de nuevas legislaciones, decisiones legales y otras acciones.

Así como el mundo legal es confuso para las personas que trabajan en informática, el mundo de la computación, también

lo es para muchas personas que trabajan en leyes. Por ello, es responsable acudir a un abogado especializado en la materia.

a. Propiedad Intelectual.

La web es una creación del intelecto, talento, trabajo duro y persistencia. No existen artefactos físicos que puedan designarse como “Internet”, todo existe como efímeros bits almacenados en discos y desplegados en monitores. Las palabras, algoritmos, programas, imágenes y diseños que se encuentran en la red, son productos de trabajo esforzado, y representan un activo para quienes han hecho o contratado el trabajo.

La sociedad etiqueta tal trabajo como “propiedad intelectual”. La ley reconoce ciertas formas de protección a la propiedad intelectual para proteger los activos y fomentar su desarrollo y uso. Las tres formas de protección que más se aplican al material el Web son las de derechos de autor(copyright), de patente y de marca registrada. Cada una ampara un tipo de material ligeramente diferente y en forma distinta.

b. La Ley de Derechos de Autor.

La finalidad de los derechos de autor es amparar la expresión de las ideas, no las ideas en sí. Los derechos de autor abarcan el texto, fotografías, tipos de letra y combinaciones de ellos una vez ensamblados en alguna forma fija.

Los derechos de autor también abarcan ejecuciones musicales, obras teatrales y películas. De acuerdo con las leyes actuales, no hay necesidad de marcarlo con un símbolo de derechos reservados o de registrar los derechos para que quede protegido; sin embargo, el registro y marcaje de los derechos pueden aumentar las penas impuestas si ocurre una infracción.

c. Infracción de derecho de autor.

La práctica estándar en Internet ha sido que algo que se exporta desde un servidor de acceso público es para uso público, a menos que se indique lo contrario. No obstante, esta práctica no está de acuerdo con la forma en que está escrita la ley de derechos de autor. Además, se puede haber eliminado la

información de propiedad y de derechos de algunos elementos obtenidos de alguna parte intermedia.

Esto no absuelve al que los utilice de ninguna responsabilidad legal por derechos de autor.

Los tipos de infracciones incluyen:

- Poner fotografía, dibujos e imágenes en sitios FTP y web sin obtener permiso adecuado, aún si los elementos originales no están claramente identificados en cuanto al propietario, tema o derechos de autor.

- Distribuír fotografías, extractos de libros, informes y otros materiales con derechos de autor, mediante correo, el Web, FTP o mensajes en Usenet.

- Distribuír fragmentos de sonido de películas, programas de televisión u otros medios grabados sin aprobación del propietario de los derechos de autor. Esto incluye el agregar tales sonidos a las páginas web en cualquier forma.

- Distribuír caricaturas digitalizadas de periódicos o revistas.

- Redistribuír artículos de noticias de fuentes con derechos de autor. reenviar mensajes de correo electrónico. Al igual que con el correo de papel, el autor de mensajes de correo electrónico adquiere derechos de autor tan pronto como se pone el correo en forma tangible. El acto de enviar el correo a alguien no otorga al receptor interés de derechos de autor sobre su contenido. La práctica estándar en la red no está de acuerdo a la forma en que fue escrita la ley. Por ello, el reenvío de correo electrónico puede ser técnicamente una violación de la ley de derechos de autor

d. Piratería de Software y la SPA.

La asociación de Editores de software (SPA, software publishers association) es una entre varias organizaciones fundadas por los principales editores de software. Una de sus metas principales es disminuir la gran cantidad de piratería de software que existe en el medio.

Aunque existen sanciones penales para copia no autorizada, se imponen en contra de las organizaciones de piratería de software organizada. A diferencia de esto, la SPA y otras organizaciones se basan en la ley civil. En particular, la SPA puede obtener una orden de la corte para examinar cualquier sistema de cómputo en busca de evidencias de copias de programas sin licencia.

e. Warez

Existe un peligro adicional en el caso de los ISP. Los warez son programas o códigos de activación que se ponen a disposición de otros ”piratas” de software para descargarlos sin licencias ni pago al poseedor legítimo de los derechos de autor.

Si algún usuario opera un servidor de warez de un sitio FTP o web, la SPA o los propietarios de los derechos, pueden buscar retribución financiera por parte de quien opera la máquina para ayudarles a reponer la perdida, aun si el ISP no tiene conocimiento del contenido pirata y, además no tolera al comportamiento. La SPA ha impuesto demandas contra ISP

que han aparentando responder inmediatamente a las quejas sobre servidores de warez operados por sus clientes.

f. La Ley de Patentes

Las patentes son un tipo de licencia otorgada a un inventor para proteger inventos novedosos, útiles y no obvios. En sus orígenes, su intención fue otorgar a un inventor un tiempo fijo para obtener beneficios de algún nuevo invento o descubrimiento, motivando a que el inventor divulgara el desarrollo que había detrás de la patente. En años recientes, ha habido un cambio en cuanto a l otorgamiento de patentes en la informática. Las empresas e individuos están solicitando y obteniendo patentes sobre software y algoritmos a una velocidad sorprendente.

En la actualidad, muchas empresas están intentando construir grandes bibliotecas de patentes para utilizarlas como palanca en los mercados. En efecto, solicitan patentes sobre todo lo que se desarrolla. Esta práctica es triste, por ello, ha tenido efectos negativos. Por ejemplo, las patentes sobre la encriptación de llave pública en realidad han perjudicado el desarrollo de

seguridad de la información en años recientes. ¿Que significan estas patentes para quien se dedica al desarrollo del web, ISP o comerciante? La preocupación principal es el licenciamiento. Si usted realiza alguna actividad utilizando cualquiera de los sistemas de comercio en Internet basados en criptografía de llave pública, debe estar seguro de utilizar software con licencia apropiada. Debe hacer lo mismo si emplea cualquier tipo de firma de llave pública sobre applets, programas, plug.ins u otros aspectos de construcción web.

g. La Ley De Marcas Registradas.

Las marcas registradas están definidas como cualquier palabra, nombre, símbolo, color, sonido, forma de producto o dispositivo o cualquier combinación de las anteriores, adoptadas y utilizadas por un fabricante o comerciante para identificar bienes y distinguirlos de aquellos fabricados o vendidos por alguien más. Las marcas de servicio son un concepto relacionado que se aplica a los servicios en vez de los productos.

1.10 FUNDAMENTOS DE REDES LAN Y REDES WAN.

1.10.1 EL MODELO OSI3

I. Modelo de red dividido en capas

Las nuevas prácticas de negocios están provocando grandes cambios en las redes empresariales. Los empleados en las sedes corporativas y en las oficinas de todo el mundo, así como las personas que trabajan en sus casas, necesitan acceso inmediato a los datos, sin importar si los datos se encuentran en servidores centralizados o departamentales. Las organizaciones como empresas, agencias, escuelas, etc., que unen entre sí sus servidores de archivos, informática y comunicación de datos, necesitan:

- LAN interconectadas que brinden acceso a los computadores o servidores de archivo en otras ubicaciones.

- Ancho de banda mayor en las LAN para satisfacer las necesidades de los usuarios finales.
- Tecnologías que se puedan aplicar para el servicio de las WAN.

Para mejorar la comunicación con sus asociados, empleados y clientes, las empresas están implementando nuevas aplicaciones, tales como el comercio electrónico, videoconferencia, voz sobre IP y aprendizaje a distancia. Las empresas están fusionando sus redes de voz, vídeo y datos en redes empresariales mundiales. Estas redes son fundamentales para el éxito comercial de la organización.

Las redes empresariales se encuentran diseñadas y desarrolladas para servir de apoyo a las aplicaciones actuales y futuras. Para adaptarse a los crecientes requisitos de ancho de banda, escalabilidad y confiabilidad, los fabricantes y las organizaciones de normalización presentan nuevos protocolos y tecnologías casi constantemente. Los diseñadores de redes se ven obligados a desarrollar redes de tecnología avanzada.

Al dividir y organizar las tareas de networking en capas/funciones separadas, se pueden manejar las nuevas aplicaciones sin problemas. El modelo de referencia OSI organiza las funciones de red en siete categorías, denominadas capas. Los datos fluyen desde las aplicaciones del usuario de los niveles superiores hasta los bits de nivel inferior que se transmiten a través de los medios de red. La tarea de la mayoría de los administradores de redes de área amplia es configurar las tres capas inferiores. Las funciones de par a par usan el encapsulamiento y el desencapsulamiento como interfaz para las capas.

Como vemos en la figura 1.2, el modelo de referencia OSI se divide en siete capas, cada una de las cuales poseen funciones distintas. Las funciones del modelo del Protocolo de Control de Transmisión / Protocolo Internet (TCP/IP) caben en cinco capas. Esta separación de las funciones de networking se denomina división en capas. Sin embargo, más allá de la cantidad de capas, entre las razones de la división de las funciones de red se incluyen las siguientes:

- Dividir los aspectos interrelacionados de las operaciones de red en elementos menos complejos.

- Definir interfaces estándar para compatibilidad plug-and-play y para la integración de elementos de múltiples proveedores.
- Permitir que los ingenieros concentren sus esfuerzos de diseño y de desarrollo en las funciones de una capa específica.
- Promover la simetría de las diferentes funciones modulares de la internetwork con fines de interoperabilidad.
- Evitar que los cambios en un área afecten otras áreas de forma significativa, de manera que cada área pueda evolucionar más rápidamente.

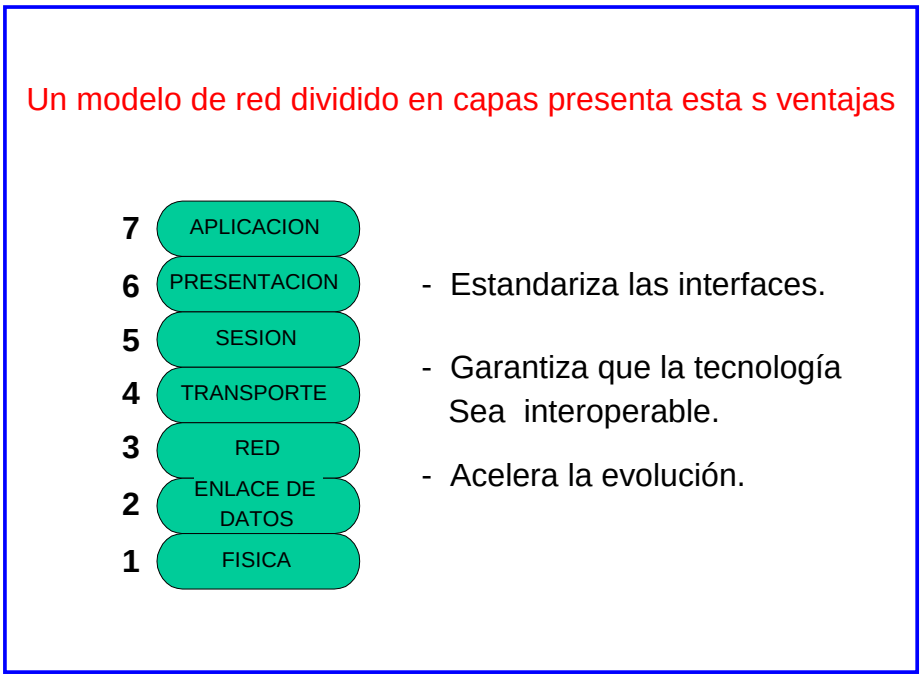


FIG. 1.2 Un modelo de red dividido en capas

II. Funciones de las capas del modelo OSI.

Cada una de las siete capas del modelo de referencia OSI sirve para una función específica. El modelo OSI define las funciones que pueden ser utilizadas por cualquier proveedor de productos de red.

Las capas son:

Aplicación: La capa de aplicación proporciona servicios de red a las aplicaciones del usuario. Por ejemplo, los servicios de transferencia de archivos prestan servicios a una aplicación de procesamiento de texto en esta capa.

Presentación: Esta capa proporciona representación de datos y formateo de códigos. Garantiza que los datos que llegan desde la red puedan ser utilizados por la aplicación y que la información enviada por la aplicación se pueda transmitir a través de la red.

Sesión: Esta capa establece, mantiene y administra las sesiones entre aplicaciones.

Transporte : Esta capa divide en segmentos y recompone los datos en una corriente de datos. TCP es uno de los protocolos de la capa de transporte que se usan con IP.

Red: Esta capa determina la mejor manera de desplazar los datos de un lugar a otro. Los routers operan en esta capa. También se encuentran en esta capa el esquema de direccionamiento IP

Enlace de datos: Esta capa prepara un datagrama o paquete para su transmisión física a través del medio. Maneja la notificación de errores, topología de la red y control de flujo.

Esta capa utiliza direcciones de Control de Acceso al Medio (MAC).

Física : Esta capa proporciona los medios eléctricos, mecánicos, de procedimiento y funcionales para activar y mantener el enlace físico entre los sistemas. Esta capa usa medios físicos como cables de par trenzado, coaxial y de fibra óptica.

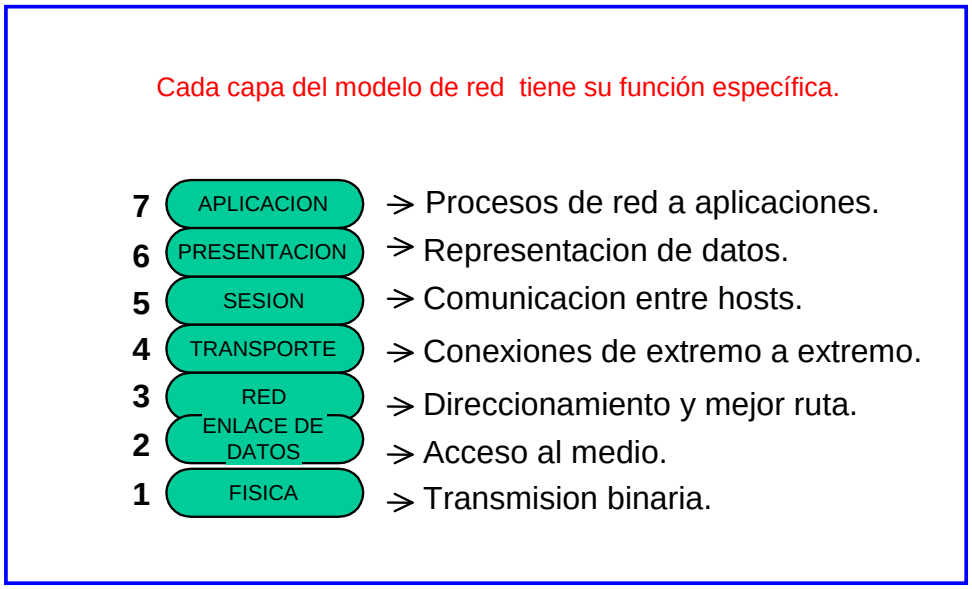
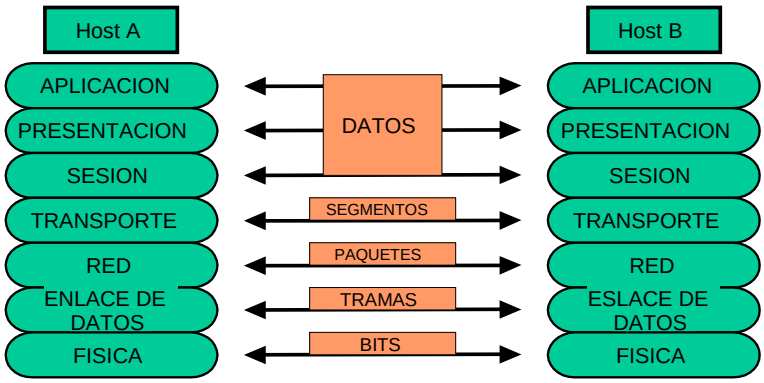


FIG. 1.3 Funciones de las capas

III. Comunicaciones de par a par.

Cada capa usa su propio protocolo de capa para comunicarse con su capa equivalente en otros sistemas. El protocolo de cada capa intercambia información, denominada unidades de datos de protocolo (PDU), con su capa par. Una capa puede usar un nombre más específico para su PDU. Por ejemplo, en TCP/IP la capa de transporte de TCP se comunica con su función TCP par mediante segmentos. Cada una usa los servicios de la inmediata inferior para comunicarse con su capa par. El servicio de la capa inferior usa la información de

las superiores como parte de las PDU que intercambia con su par. FIG. 1.4.



La información desciende en el modelo pero finalmente la comunicación es entre cada capa y su contraparte.

FIG. 1.4 Comunicaciones par a par

Los segmentos de TCP pasan a formar parte de los paquetes de la capa de red (datagramas) que se intercambian entre pares IP. Por su parte, los paquetes de IP pasan a formar parte de las tramas de enlace de datos que se intercambian entre dispositivos directamente conectados. Por último, estas tramas se transforman en bits a medida que los datos son transmitidos finalmente por el hardware utilizado por el protocolo de la capa física Cada capa depende de los

servicios de la capa del modelo de referencia OSI inmediatamente inferior. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la unidad de datos de protocolo (PDU) de la capa superior en su campo de datos; entonces puede agregar los encabezados e información final que la capa necesite para cumplir su función.

Por ejemplo, la capa de red presta un servicio a la capa de transporte, y la capa de transporte presenta datos al subsistema de internetwork. La capa de red tiene la tarea de desplazar estos datos a través de la internetwork. Realiza esta tarea encapsulando los datos dentro de un paquete.

Este paquete incluye un encabezado que contiene la información necesaria para completar la transferencia, por ejemplo, las direcciones lógicas origen y destino.

La capa de enlace de datos por su parte presta un servicio a la capa de red. Encapsula el paquete de la capa de red en una trama. El encabezado de trama contiene la información necesaria para completar las funciones de enlace de datos, por ejemplo direcciones físicas. Finalmente, la capa física

proporciona un servicio a la capa de enlace de datos, codifica la trama de enlace de datos en un patrón de unos y ceros para su transmisión a través del medio.

IV. Los cinco pasos del encapsulamiento de datos. A medida que las redes prestan servicios a los usuarios, el flujo y la organización en paquetes de la información original del usuario pasan por diversos cambios. En este ejemplo de internetworking, se pueden distinguir cinco pasos de conversión.

Paso 1

Un computador convierte un mensaje de correo electrónico en caracteres alfanuméricos que pueden ser utilizados por el sistema de internetworking.

Paso 2

Los datos del mensaje son segmentados para su transporte en el sistema de internetworking por la capa de transporte. ,que garantiza que los hosts del sistema de correo electrónico que

intercambian mensajes desde ambos extremos de la red se puedan comunicar de manera confiable.

Paso 3

Los datos entonces son convertidos en un paquete, o datagrama, por la capa de red. El paquete también contiene un encabezado de red que incluye una dirección lógica origen y destino. La dirección ayuda a los dispositivos de red a enviar el paquete a través de la red por una ruta seleccionada.

Paso 4

Cada dispositivo de la capa de enlace de datos coloca el paquete en una trama. La trama permite que el dispositivo se conecte al siguiente dispositivo de red directamente conectado con el enlace.

Paso 5

La trama se transforma en un patrón de unos y ceros para su transmisión en el medio. Una función de temporización permite

que los dispositivos distingan los bits a medida que se desplazan por el medio.

El medio en la internetworking física puede variar a lo largo de la ruta. Por ejemplo, un mensaje de correo electrónico se puede originar en una LAN, atravesar el backbone de un campus, y continuar a lo largo de un enlace WAN hasta llegar a su destino en otra LAN remota.

1.10.2 LAN

I. Dispositivos y tecnologías LAN

Las características principales de las LAN son las siguientes:

- La red opera dentro de un edificio o piso de un edificio.
- Las LAN se componen de múltiples dispositivos de escritorio conectados, con acceso a medios de ancho de banda elevados.
- Por definición, la LAN conecta computadores y servicios a un medio común de Capa 1. Los dispositivos LAN incluyen:

- Puentes que conectan los segmentos LAN y ayudan a filtrar el tráfico.
- Hubs que concentran las conexiones LAN y permiten el uso de medios de cobre de par trenzado.
- Switches Ethernet que brindan ancho de banda dedicado full duplex a tráfico proveniente de estaciones de trabajo o segmentos.
- Routers que ofrecen varios servicios, incluyendo internetworking y control de tráfico broadcast.

Prácticamente todas las LAN instaladas pertenecen a una de las siguientes tres tecnologías LAN como se observa en la figura 1.5.

Ethernet: La tecnología más común de las LAN.

Token-Ring: Desarrollada por IBM, apareció después de Ethernet y hoy en día se usa en una gran cantidad de redes.

FDD*I*: También utiliza tokens, y actualmente es una LAN que se usa ampliamente en los campus.

En una LAN, la capa física proporciona acceso a los medios de red.

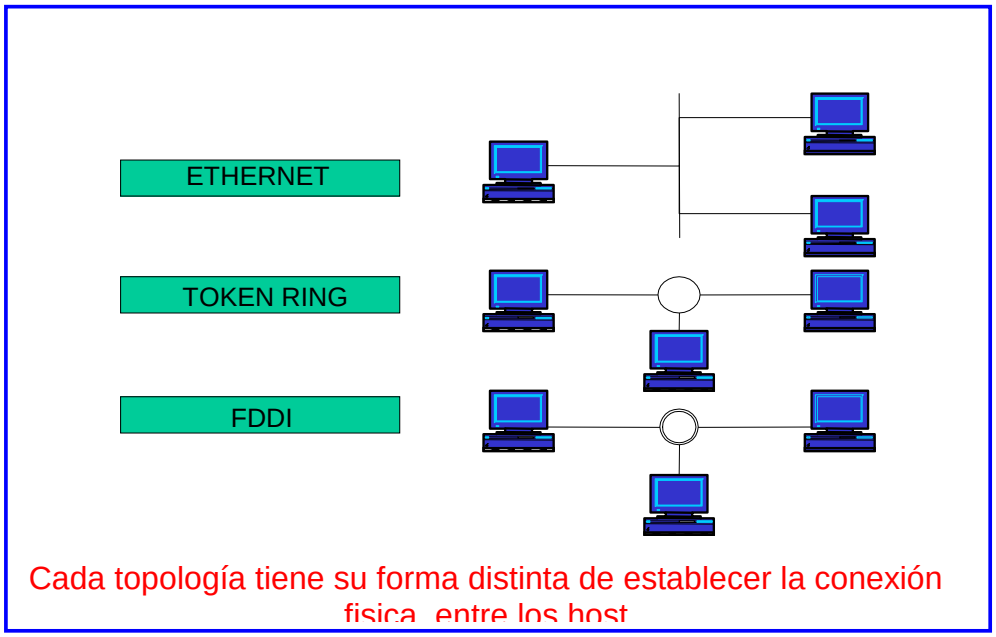


FIG. 1.5 Descripción general de la tecnología LAN.

La capa de enlace de datos brinda soporte para las comunicaciones a través de diferentes tipos de enlaces de datos, tales como los medios Ethernet/IEEE 802.3.

Los esquemas de direccionamiento como el Control de Acceso al Medio (MAC) y el Protocolo Internet ofrecen un método muy estructurado para buscar y entregar datos a computadores u otros hosts en una red.

II. Estándares de Ethernet e IEEE 802.3

Los estándares Ethernet e IEEE 802.3 definen una LAN con topología de bus que opera a una velocidad de señalización de banda base de 10 Mbps. Los tres estándares de cableado definidos son:

- *10BASE2* (Ethernet de cable fino): Permite segmentos de red en cable coaxial de hasta 185 m de longitud.
- *10BASE5* (Ethernet estándar): Permite segmentos de red en cable coaxial de hasta 500 m de longitud.
- *10BASE-T* Transporta tramas Ethernet en económicos cables de par trenzado.

Los estándares 10BASE5 y 10BASE2 brindan acceso para varias estaciones al mismo segmento LAN. Las estaciones se conectan al segmento mediante un cable tendido desde una interfaz de unidad de conexión (AUI) en la estación hasta un transceiver directamente conectado al cable coaxial ethernet.
Debido a que 10BASE-T brinda acceso a una sola estación, las estaciones conectadas a una LAN Ethernet mediante 10BASE-T casi siempre están conectadas a un hub o switch LAN. En

esta disposición, el hub o switch LAN es igual a un segmento de Ethernet.

Los enlaces de datos Ethernet y 802.3 preparan los datos para su transporte a través del enlace físico que une dos dispositivos. En el ejemplo que aparece en la figura 1.6, tres dispositivos se pueden conectar entre sí directamente a través de la LAN Ethernet. La Macintosh a la izquierda y el PC basado en Intel del medio tienen direcciones MAC utilizadas por la capa de enlace de datos. El router a la derecha también usa direcciones MAC para cada una de las interfaces LAN. La interfaz Ethernet/802.3 del router usa la abreviatura "E" especificada para este tipo de interfaz por Cisco IOS, seguida por un número de interfaz, por ejemplo "0".

Los broadcasts son herramientas poderosas que pueden enviar una sola trama a varias estaciones al mismo tiempo.

Los broadcasts usan una dirección destino a nivel de enlace de datos compuesta exclusivamente por unos FFFF.FFFF.FFFF en numeración hexadecimal.

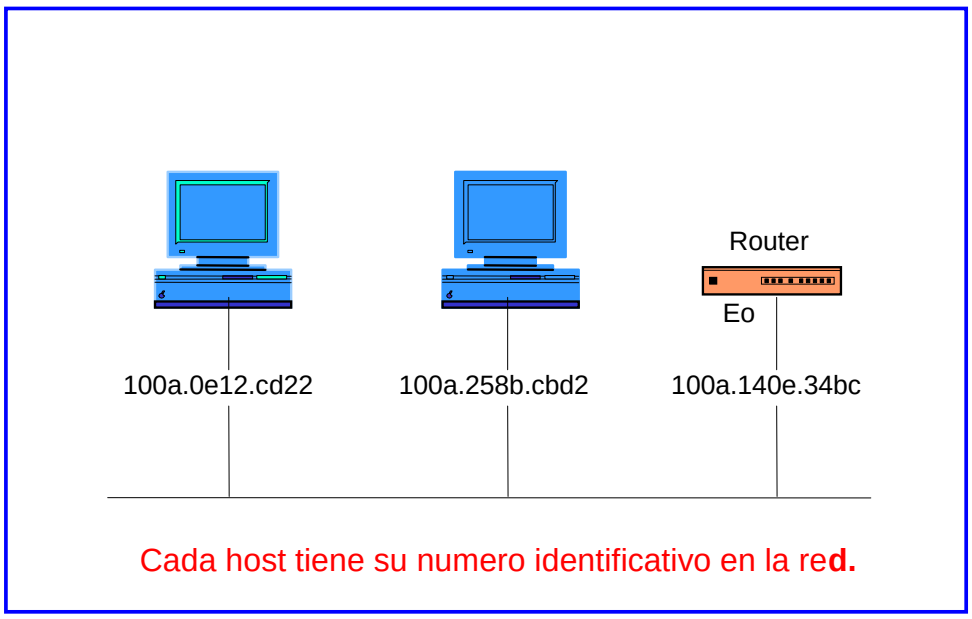


FIG. 1.6 Interfaz Ethernet/802.3.

Observamos en la figura 1.7, si la estación A transmite una trama con una dirección destino compuesta exclusivamente por unos, las estaciones B, C y D recibirán y pasarán la trama a sus capas superiores para su procesamiento.

Cuando se usan de manera incorrecta, los broadcasts pueden afectar seriamente el rendimiento de las estaciones, porque las interrumpe de manera innecesaria. Los broadcasts, por lo tanto, deben usarse sólo si la dirección MAC destino es desconocida, o cuando el destino son todas las estaciones.

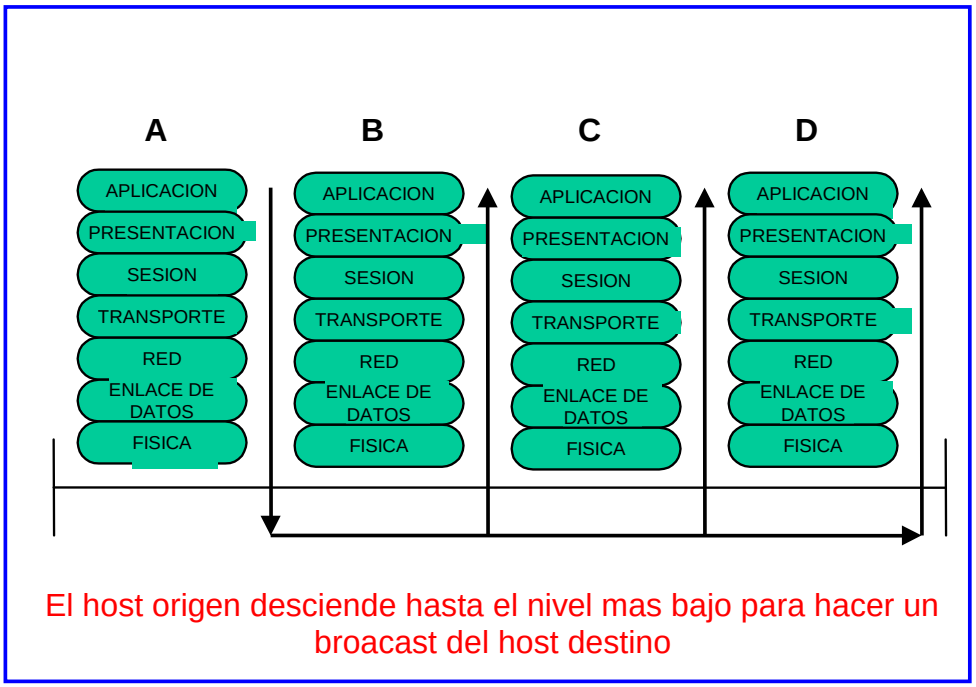


FIG. 1.7 Broadcast Ethernet/802.3

III. Acceso múltiple con detección de portadora y detección de colisiones

En una LAN Ethernet, sólo se permite una transmisión por vez en un momento determinado. Una LAN Ethernet se denomina red de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD).

Esto significa que la transmisión de un nodo atraviesa toda la red y es recibida y examinada por cada nodo. Cuando la señal alcanza el final de un segmento, los terminadores la absorben para evitar que vuelva al segmento. FIG. 1.8.

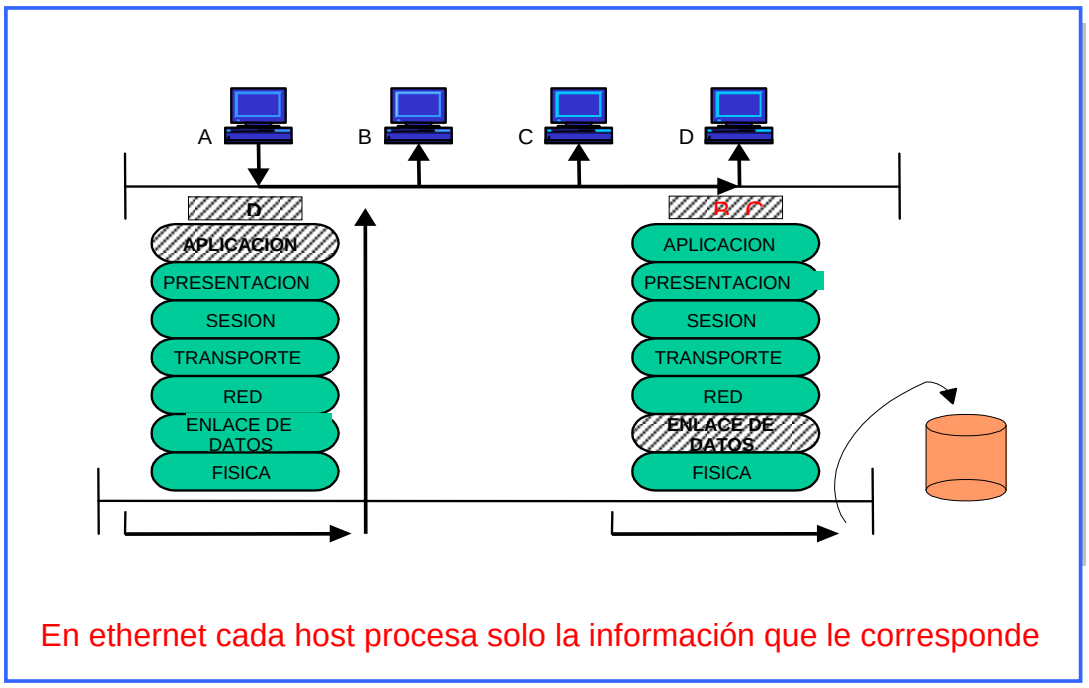


FIG. 1.8 Operación de Ethernet/802.3

Cuando una estación desea transmitir una señal, verifica la red para determinar si alguna otra estación se encuentra transmitiendo, como se ilustra en la FIG. 1.9. Si la red no está en uso, la estación comienza la transmisión. Mientras manda la señal, la estación monitorea la red para asegurarse de que ninguna otra estación esté transmitiendo en ese momento. Es

posible que dos estaciones determinen que la red se encuentra disponible y comiencen a transmitir de forma simultánea. Si esto ocurriera, se produciría una colisión como vemos en la parte superior del gráfico.

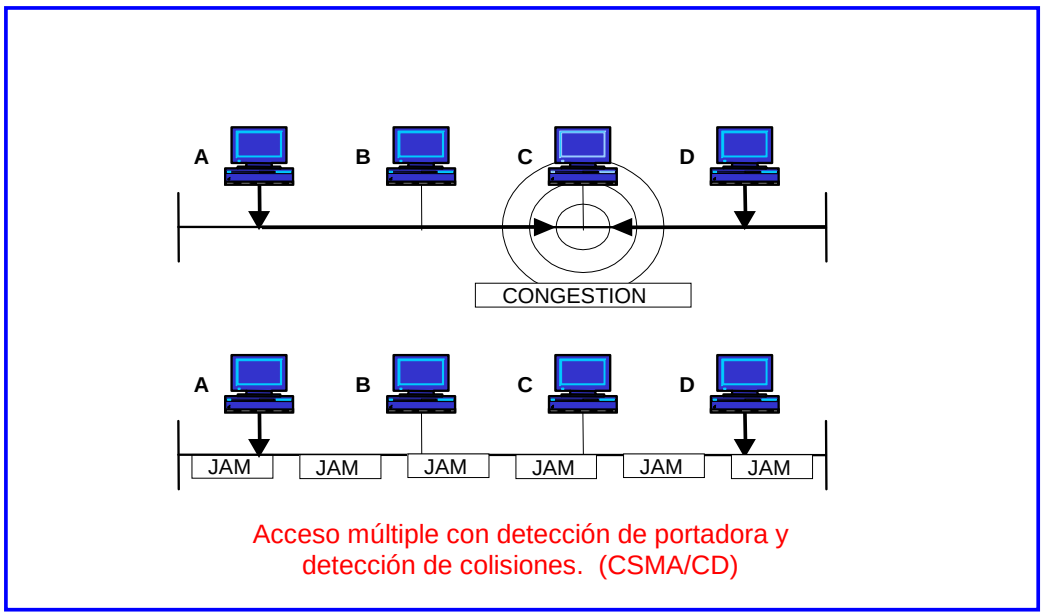


FIG. 1.9 Confiabilidad de Ethernet/802.3.

Cuando un nodo que transmite reconoce una colisión, transmite una señal de congestión que hace que la colisión dure lo suficiente como para que todos los demás nodos la reconozcan. Todos los nodos transmisores entonces dejan de enviar tramas durante un período de tiempo seleccionado al azar antes de intentar retransmitir. Si los intentos posteriores también producen colisiones, el nodo intenta retransmitir hasta quince veces antes de abandonar el intento.

Los relojes indican diversos temporizadores de postergación. Si los dos temporizadores son suficientemente diferentes, una de las estaciones tendrá éxito la próxima vez.

IV. Direccionamiento lógico.

Un componente fundamental en cualquier sistema de redes es el proceso que permite que la información localice sistemas informáticos específicos en una red. Se utilizan diversos esquemas de direccionamiento con este fin, según el conjunto de protocolos que se utilice. Por ejemplo, el direccionamiento AppleTalk es diferente del direccionamiento TCP/IP, que a su vez es diferente del direccionamiento IPX. Las direcciones de la capa de enlace de datos también denominadas direcciones físicas de hardware o direcciones MAC, ver FIG.1.10, son normalmente únicas para cada conexión de red. De hecho, en la mayoría de las LAN las direcciones de la capa de datos se encuentran localizadas en la NIC (tarjeta de interfaz de red). Debido a que un computador típico tiene una conexión de red física, tiene sólo una dirección de capa de enlace de datos. Tal como lo dice su nombre, las direcciones de la capa de enlace

de datos existen en la Capa 2 del modelo de referencia OSI.Las direcciones de capa de red o direcciones IP existen en la Capa 3 del modelo de referencia OSI. Al contrario de lo que ocurre con las direcciones de la capa de enlace de datos, que normalmente existen dentro de un espacio de direccionamiento plano, las direcciones de la capa de red normalmente son jerárquicas.

En otras palabras, son como las direcciones postales, que describen la ubicación de una persona indicando el país, estado/provincia, código postal, ciudad, calle, número y nombre. Ver FIG. 1.10.

Un ejemplo de dirección plana es el número de seguridad social de los EE.UU. Cada persona tiene un número de seguridad social exclusivo. Las personas pueden mudarse a cualquier lugar del país y obtener nuevas direcciones lógicas, según la ciudad, calle o código postal, pero sus números de seguridad social permanecen inmodificados.

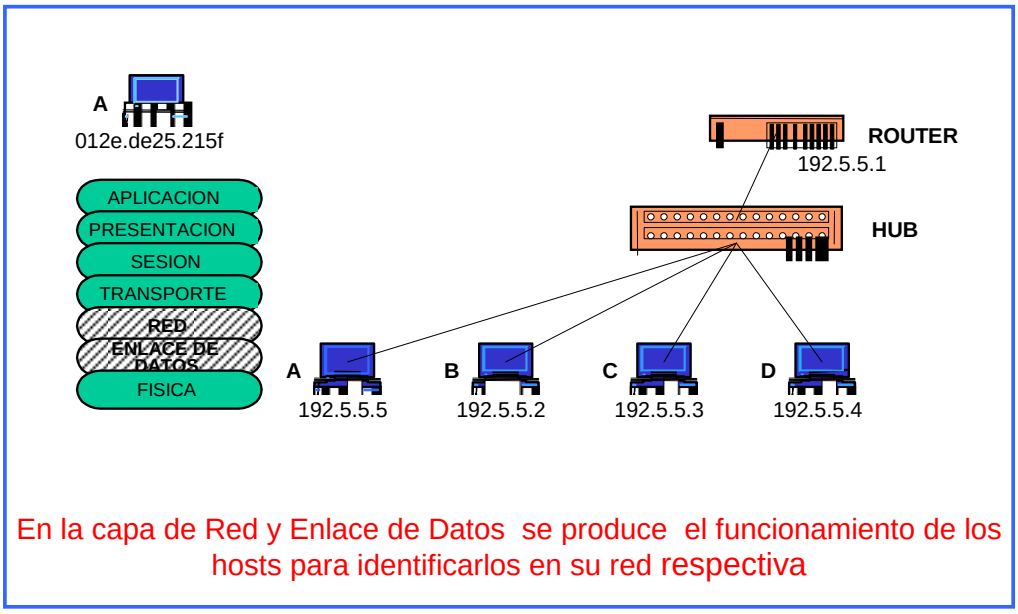


FIG. 1.10 Direccionamiento Físico y Lógico.

V. Direccionamiento MAC.

Para que múltiples estaciones puedan compartir los mismos medios y aún así identificarse entre sí, las subcapas MAC definen las direcciones de hardware o de enlace de datos, denominadas direcciones MAC. Cada interfaz LAN posee una dirección MAC exclusiva. En la mayoría de las NIC, la dirección MAC está grabada en la ROM.

Cuando se inicia la NIC, esta dirección se copia en la RAM. Ver FIG. 1.11.

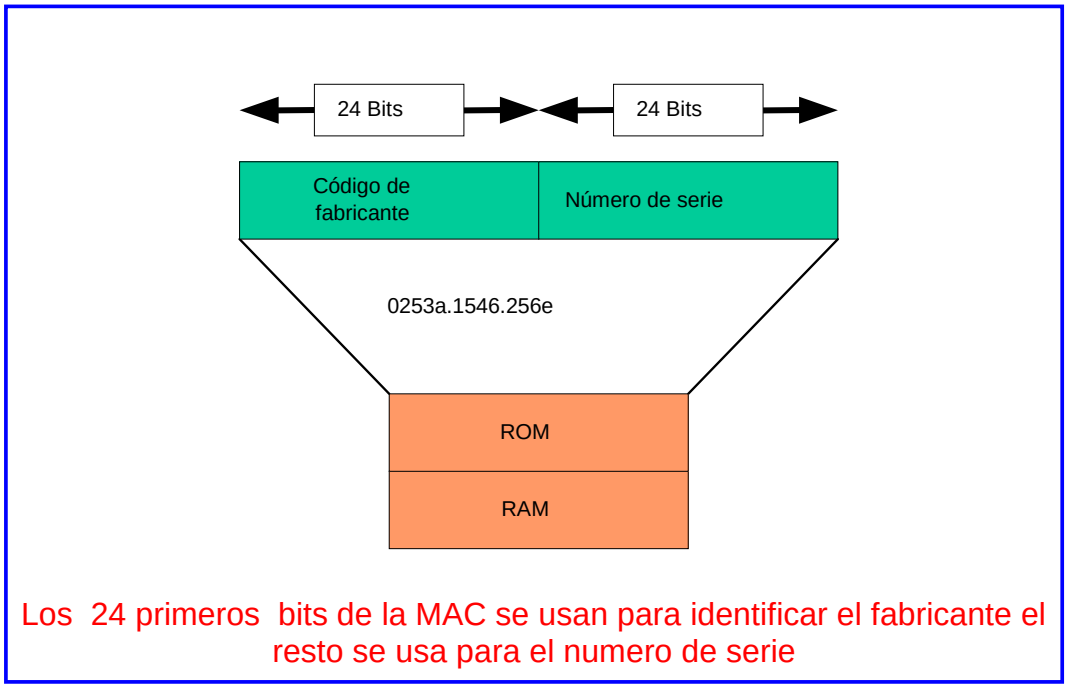


FIG. 1.11 Direccionamiento MAC.

Antes de que los dispositivos directamente conectados en la misma LAN puedan intercambiar una trama de datos, el dispositivo origen debe tener la dirección MAC del dispositivo destino. Una manera de que el emisor pueda asegurarse de que encontrará las direcciones MAC que necesita es utilizar un ARP (Protocolo de Resolución de Direcciones). El gráfico ilustra dos maneras en que se usa ARP para encontrar una dirección MAC en un ejemplo de TCP/IP.

En el primer ejemplo, el Host Y y el Host Z se encuentran en la

misma LAN. El Host Y realiza un broadcast de una petición ARP a la LAN buscando el Host Z. Como el Host Y ha enviado un broadcast, todos los dispositivos, incluyendo el Host Z reciben la petición, pero sólo el Host Z responde con su dirección MAC. El Host Y recibe la respuesta del Host Z y guarda la dirección MAC en la memoria local, a menudo denominada caché ARP. La próxima vez que el Host Y necesite comunicarse directamente con el Host Z, utilizará la dirección MAC almacenada.

En el segundo ejemplo, el Host Y y el Host Z se encuentran en LAN diferentes, pero pueden acceder el uno al otro a través del Router A. Cuando el Host Y realiza un broadcast de su petición ARP, el Router A determina que el Host Z no puede reconocer la petición porque el Router A detecta que la dirección IP del Host Z es de una LAN diferente. Debido a que el Router A también determina que cualquier paquete para el Host Z debe ser retransmitido, el Router A ofrece su propia dirección MAC como una respuesta proxy a la petición ARP. El Host Y recibe la respuesta del Router A y guarda la dirección MAC en su caché de memoria ARP. La próxima vez que el Host

Y necesite comunicarse con el Host Z, utiliza la dirección MAC almacenada del Router A.

1.10.3 Direccionamiento TCP/IP.

II. Entorno TCP/IP.

En un entorno TCP/IP, las estaciones finales se comunican con servidores u otras estaciones finales. Esto puede ocurrir porque cada nodo que utiliza el conjunto de protocolos TCP/IP tiene una dirección lógica de 32 bits exclusiva. Esta dirección se conoce como dirección IP.

Cada empresa u organización conectada a la internetwork aparece como una sola red que debe ser alcanzada antes de que se pueda contactar un host en particular dentro de esa empresa. Cada red de una empresa tiene una dirección; los hosts que residen en esa red comparten la misma dirección de red, pero cada host se identifica por medio de la dirección exclusiva de host en la red. Ver FIG. 1.12.

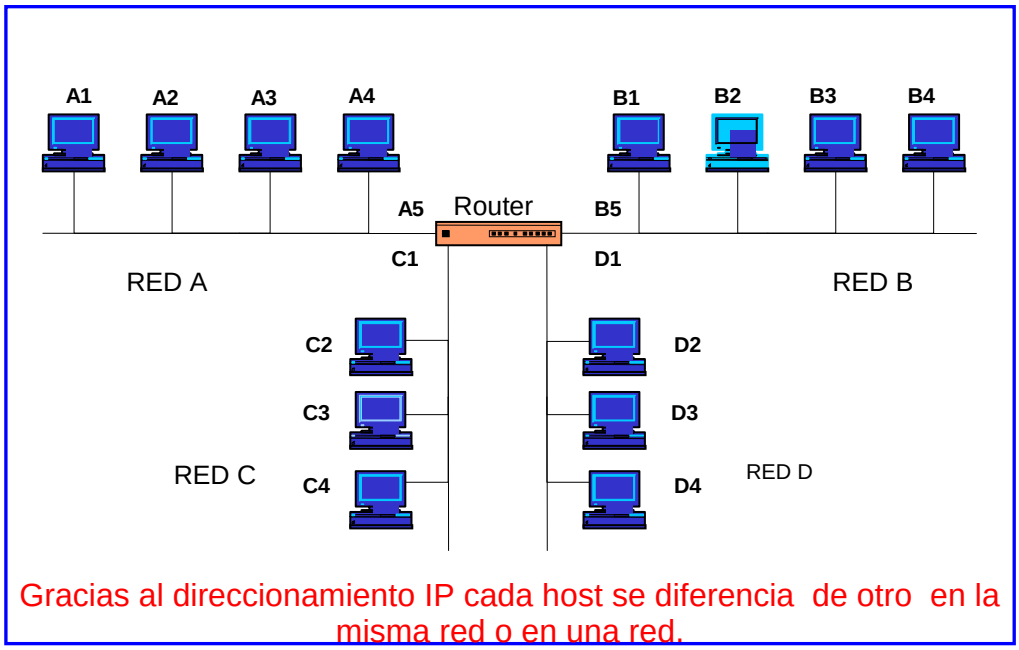


FIG. 1.12.- Direccionamiento IP.

II. Subredes.

Las subredes mejoran la eficiencia del direccionamiento de la red. La adición de subredes no cambia la manera en que el mundo exterior visualiza la red, pero hace que dentro de la organización exista una estructura adicional. En la figura 1.13, la red 172.16.0.0 se subdivide en cuatro subredes: 172.16.1.0, 172.16.2.0, 172.16.3.0 y 172.16.4.0. Los routers determinan la red destino utilizando la dirección de subred, que limita la cantidad de tráfico en los demás segmentos de la red.

Desde el punto de vista del direccionamiento, las subredes son una extensión del número de una red. Los administradores de red determinan el tamaño de las subredes según las necesidades de expansión de sus organizaciones. Los dispositivos de red usan máscaras de subred para identificar qué parte de la dirección le corresponde a la red y qué parte representa el direccionamiento del host.

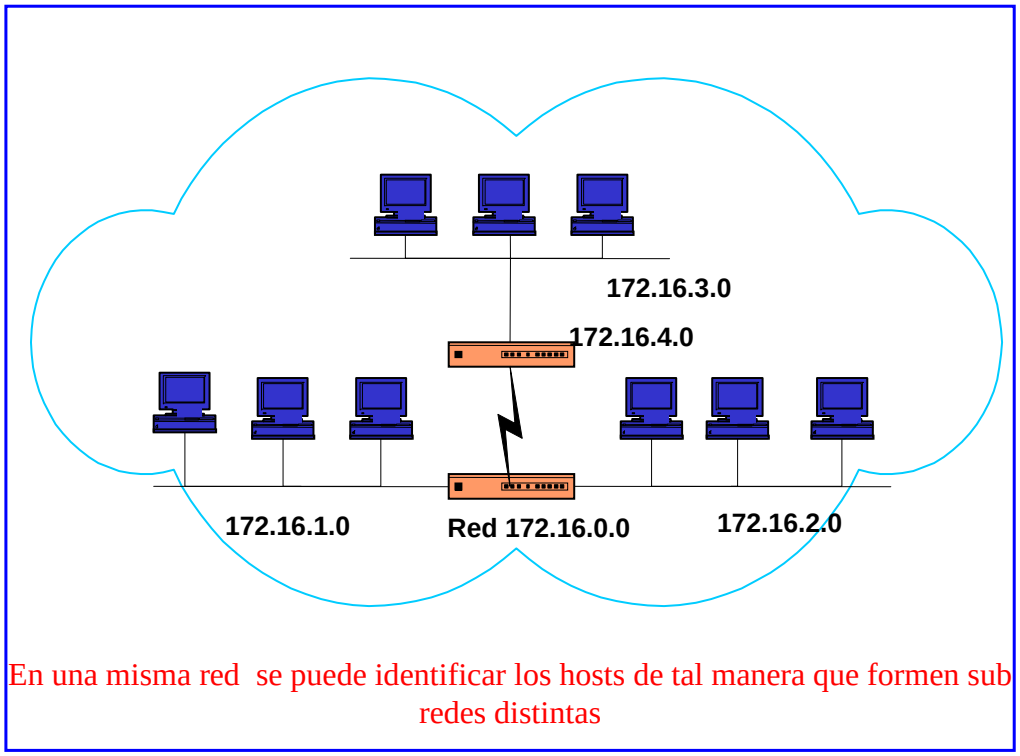


FIG. 1.13.- Direccionamiento con subredes.

1.10.4 LAS 4 CAPAS SUPERIORES DEL MODELO OSI.

I. Capas de aplicación, presentación y sesión.

CAPA DE APLICACIÓN.

En el contexto del modelo de referencia OSI, la capa de aplicación (Capa 7) brinda soporte al componente de comunicación de una aplicación. No proporciona servicios a ninguna otra capa del modelo OSI. Por otra parte, sí brinda servicios a los procesos de aplicación que no se encuentran cubiertos por el modelo OSI, por ejemplo: programas de hoja de cálculo, Telnet, WWW, etc.. Una aplicación informática puede funcionar a pleno utilizando sólo la información que reside en su computador. Sin embargo, una aplicación también puede tener un componente de comunicaciones que se conecta con una o más aplicaciones de red.

Un ejemplo de una aplicación de este tipo puede ser un procesador de texto que incorpore un componente de transferencia de archivos que permita que un documento se transfiera electrónicamente a través de una red. El

componente de transferencia de archivos hace que el procesador de texto se pueda calificar como una aplicación en el contexto del modelo OSI, y, por lo tanto, pertenece a la Capa 7 del modelo de referencia OSI. Otro ejemplo de aplicación informática con componentes de transferencia de datos es un navegador de la Web como el Netscape Navigator o Internet Explorer. Siempre que usted visita un sitio Web, las páginas se transfieren a su computador.

CAPA DE PRESENTACION.

La capa de presentación (Capa 6) del modelo de referencia OSI es responsable por la presentación de datos en un formato que un dispositivo receptor pueda comprender. Sirve como traductor para dispositivos que necesitan comunicarse a través de una red, brindando formateo y conversión de códigos. La capa de presentación (Capa 6) formatea y convierte los datos de aplicación de red en texto, gráficos, vídeo, audio o el formato que sea necesario para que el dispositivo receptor lo entienda.

La capa de presentación no sólo se ocupa del formato y representación de los datos, sino también de la estructura de los datos que usan los programas. Para comprender cómo funciona, supongamos que hay dos sistemas. Un sistema usa EBCDIC, y el otro usa ASCII para representar los datos. Cuando los dos sistemas necesitan comunicarse, la Capa 6 convierte y traduce los dos formatos diferentes.

Otra función de la Capa 6 es el cifrado de datos. El cifrado se utiliza cuando existe la necesidad de proteger la información transmitida para evitar su recepción por parte de receptores no autorizados. Para ejecutar esta tarea, los procesos y códigos ubicados en la Capa 6 deben convertir los datos. Otras rutinas ubicadas en la capa de presentación comprimen el texto y convierten las imágenes gráficas en corrientes de bits para que se puedan transmitir a través de una red.

Los estándares de la Capa 6 también constituyen una guía para la presentación de imágenes gráficas. A continuación se ofrecen algunos ejemplos:

- **PICT:** Formato de imágenes utilizado para transferir gráficos quickdraw entre programas Macintosh o PowerPc.
- **TIFF:** Formato de archivo de imágenes rotuladas, utilizado para imágenes de alta resolución con mapas de bits.
- **JPEG:** del Grupo Conjunto de Expertos en Fotografía, se utiliza para imágenes de calidad fotográfica

Otros estándares de la Capa 6 regulan la presentación de sonido y películas. Entre estos estándares se encuentran:

- **MIDI:** Interfaz digital de instrumentos musicales para música digitalizada.
- **MPEG:** Estándar de los expertos en películas para la compresión y codificación de vídeo en movimiento utilizado en CDs y almacenamiento digital con velocidades de bits de hasta 1,5 Mbps
- **QUICKTIME:** Estándar que maneja audio y vídeo para programas Macintosh y PowerPC.

CAPA DE SESION.

La capa de sesión (Capa 5) establece, administra y termina las sesiones entre aplicaciones. Coordina las peticiones de servicio y las respuestas que se producen cuando las aplicaciones establecen comunicaciones entre hosts diferentes.

III. Capa de transporte.

La capa de transporte (Capa 4) es responsable por el transporte
y regulación del flujo de información desde el origen hasta el destino de forma confiable y precisa. Sus funciones incluyen:

- sincronización de conexión.
- control de flujo.
- recuperación de errores.
- confiabilidad a través del uso de ventanas

La capa de transporte permite que un dispositivo de usuario divida en segmentos varias aplicaciones de capa superior para

colocarlas en la misma corriente de datos de Capa 4, y permite que un dispositivo receptor pueda recomponer los segmentos de las aplicaciones de las capas superiores. La corriente de datos de Capa 4 es una conexión lógica entre los extremos de una red, y brinda servicios de transporte desde un host hasta un destino. Este servicio a veces se denomina servicio de extremo a extremo.

A medida que la capa de transporte envía sus segmentos de datos, también garantiza la integridad de los datos. Este transporte es una relación orientada a conexión entre sistemas finales que se comunican. Algunas de las razones por las que se debe lograr el transporte confiable son:

- Garantizar que los emisores reciban el acuse de recibo de los segmentos entregados.
- Realizar la retransmisión de cualquier segmento que no genere acuse de recibo.
- Volver a colocar los segmentos en su secuencia correcta en el dispositivo destino.
- Evitar y controlar la congestión.

Uno de los problemas que se pueden producir durante el transporte de datos es el desbordamiento de los búferes en los dispositivos receptores. Los desbordamientos pueden producir serios problemas que tienen como resultado la pérdida de datos. La capa de transporte usa un método denominado control de flujo para resolver este problema.

III. Funciones de la capa de transporte.

Cada una de las capas de nivel superior ejecuta sus propias funciones. Sin embargo, sus funciones dependen de los servicios de las capas inferiores.

Las cuatro capas superiores pueden encapsular datos en segmentos extremo a extremo.

La capa de transporte da por sentado que puede usar la red como una nube para enviar paquetes de datos desde el origen al destino.

a. Segmentación de las aplicaciones de capa superior.

Una de las razones para utilizar un modelo de múltiples capas como el modelo de referencia OSI es que múltiples aplicaciones pueden compartir la misma conexión de transporte. La funcionalidad de transporte se logra segmento por segmento. Esto significa que diferentes segmentos de datos de diferentes aplicaciones que se envían al mismo destino o a varios destinos diferentes se envían según un método "el que llega primero, es atendido primero". FIG. 1.14.

Para comprender cómo funciona, supongamos que se envía un mensaje de correo electrónico y se transfiere un archivo a otro dispositivo en una red. Al enviar el mensaje de correo electrónico, antes de que comience la transmisión en sí, el software en el dispositivo establece el número de puerto SMTP y el número de puerto del programa origen.

A medida que cada aplicación envía un segmento de corriente de datos, utiliza el número de puerto definido previamente.

Cuando el dispositivo destino recibe la corriente de datos, separa y clasifica los segmentos de manera tal que la capa de transporte pueda pasar los datos a la aplicación destino correspondiente.

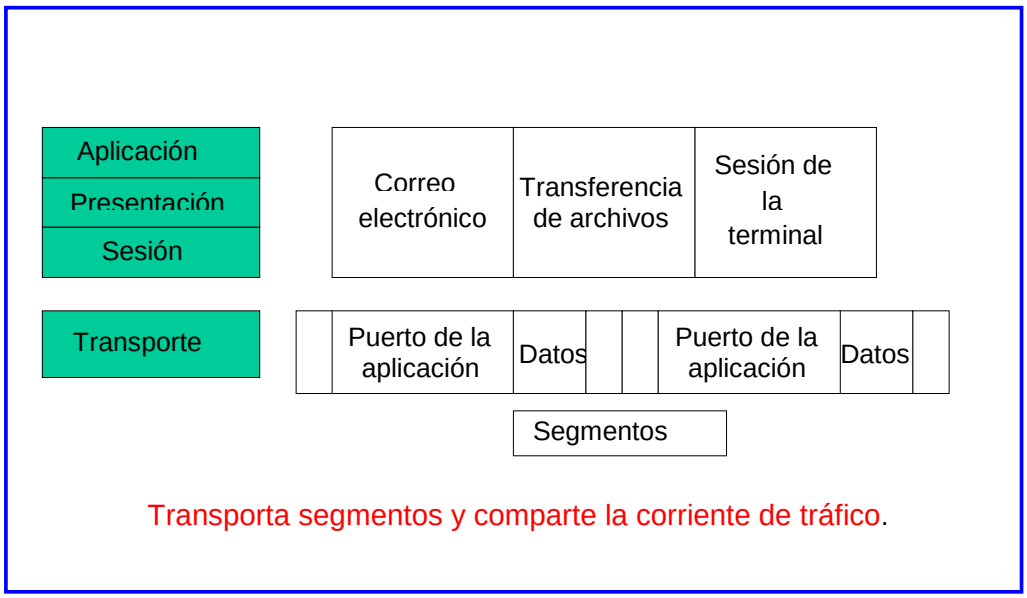


FIG. 1.14.- Segmenta aplicaciones de capa superior.

b. TCP establece una conexión.

Para que comience la transferencia de datos, el usuario de la capa de transporte debe establecer una sesión orientada a conexión con su sistema par. Entonces, los programas de aplicación emisores y receptores deben informar a sus sistemas operativos respectivos que se iniciará una conexión.

El concepto es que un dispositivo realiza una llamada a otro dispositivo, que este último debe aceptar. Los módulos de software de protocolo en los dos sistemas operativos se comunican enviando mensajes a través de la red a fin de verificar que la transferencia esté autorizada y que ambos lados estén preparados. Después de que se haya producido toda la sincronización, se establece una conexión, y comienza la transferencia de datos. Durante la transferencia, los dos dispositivos siguen comunicándose con su software de protocolo para verificar que estén recibiendo los datos correctamente.

El primer saludo solicita la sincronización. El segundo y el tercer saludo acusan recibo de la petición inicial de sincronización, y sincronizan los parámetros de conexión en sentido opuesto.

El segmento final del saludo envía un acuse de recibo al destino y ambos lados aceptan que se ha establecido una conexión. A partir del momento en que se establece la conexión, comienza la transferencia de datos.

c. TCP envía datos con control de flujo.

Mientras la transferencia de datos está en marcha, se puede producir congestión por dos motivos diferentes. En primer lugar, un computador de alta velocidad puede generar tráfico a una velocidad mayor que la capacidad de una red para transferirla.

En segundo lugar, si varios computadores envían datagramas simultáneamente a un solo destino, este destino puede sufrir congestión. Cuando los datagramas llegan demasiado rápido como para que un host o gateway los procese, se almacena temporalmente en la memoria. Si el tráfico continúa, tarde o temprano el host o el gateway agota su memoria y descarta cualquier otro datagrama que llegue. En lugar de permitir que los datos se pierdan, la función de transporte puede emitir un indicador de "no está listo" al emisor. Este indicador funciona como una señal de "pare" e indica al emisor que debe dejar de enviar datos. Cuando el receptor está en condiciones de aceptar más datos, envía un indicador de transporte de "listo", que es como una señal de "siga". Cuando el dispositivo emisor

recibe este indicador, reanuda la transmisión de segmentos.

d. TCP logra la confiabilidad con el uso de ventanas.

Una transferencia confiable de datos orientada a conexión significa que los paquetes de datos llegan en el mismo orden en el que se envían. Ver FIG. 1.15. Los protocolos fallan si algún paquete se pierde, se daña, se duplica o se recibe en el orden incorrecto. Para garantizar la confiabilidad de transferencia, los dispositivos receptores deben mandar un reconocimiento de todos y cada uno de los segmentos de datos.

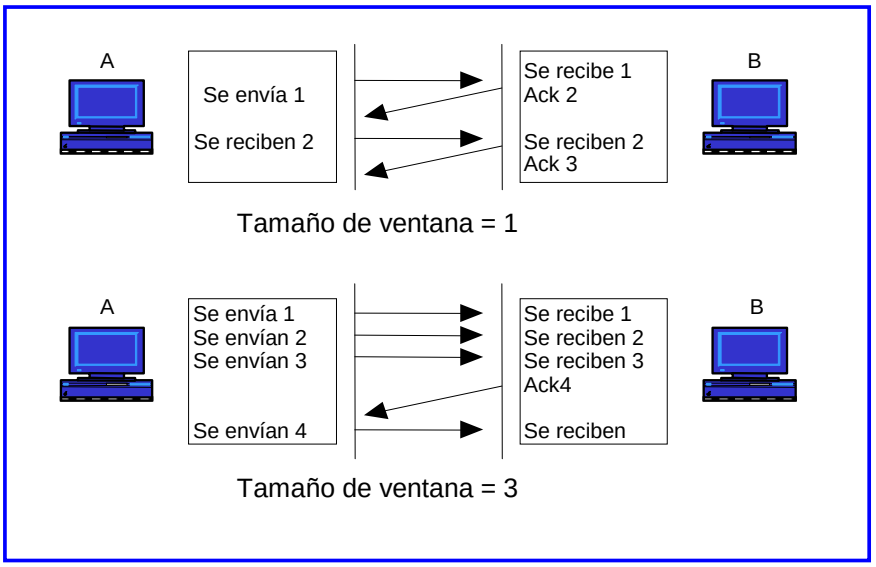


FIG. 1.15.- Confiabilidad con ventanas.

Si un dispositivo emisor debe esperar el reconocimiento de recibo después de enviar cada segmento, es fácil ver que el rendimiento será bastante bajo. Sin embargo, como hay un período de tiempo no utilizado disponible después de cada transmisión de paquetes de datos y antes de procesar cualquier reconocimiento, se puede usar el intervalo para transmitir más datos. La cantidad de paquetes de datos que se permite que un emisor transmita sin recibir un reconocimiento se denomina ventana.

El uso de ventanas es un acuerdo entre el emisor y el receptor. Es un método para controlar la cantidad de información que se puede transferir de un extremo al otro.

Algunos protocolos miden la información en términos de la cantidad de paquetes; TCP/IP mide la información en términos de cantidad de bytes.

Los ejemplos en la figura FIG 1.15 muestran las estaciones de trabajo de un emisor y un receptor. Uno tiene un tamaño de ventana de 1, y el otro un tamaño de ventana de 3. Con un

tamaño de ventana de 1, un emisor debe esperar el reconocimiento de cada paquete de datos que se ha transmitido. Con un tamaño de ventana de 3, un emisor puede transmitir tres paquetes de datos antes de recibir un reconocimiento.

e. Técnica de reconocimiento de TCP.

La entrega confiable garantiza que una corriente de datos enviada desde un dispositivo sea entregada a través de un enlace de datos a otro dispositivo sin que se dupliquen o pierdan los datos.

El reconocimiento positivo con retransmisión es un proceso que garantiza la entrega confiable de corrientes de datos. Exige que un receptor envíe un mensaje de reconocimiento al emisor siempre que reciba datos. El emisor mantiene un registro de cada paquete de datos enviado y luego espera el reconocimiento antes de enviar el siguiente paquete de datos. El emisor también inicia un temporizador cada vez que envía

un segmento y retransmite el segmento si el temporizador expira antes de que llegue el reconocimiento.

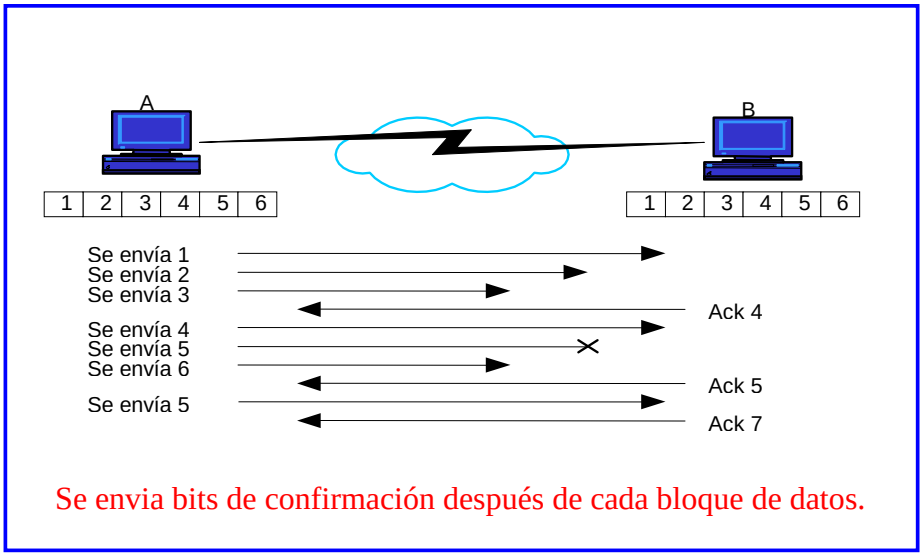


FIG. 1.16.- Técnica de acuse de recibo.

La figura 1.16 muestra un emisor que transmite los Paquetes de Datos 1, 2 y 3. El receptor recibe los paquetes solicitando el Paquete 4. El emisor, al recibir el reconocimiento, envía los Paquetes 4, 5 y 6. Si el Paquete 5 no llega a destino el receptor solicita reenviar el Paquete 5. El emisor vuelve a enviar el Paquete 5 y espera el reconocimiento antes de transmitir el Paquete 7.

CAPITULO II.

SEGURIDAD EN EL WEB.

2.1.- INTRODUCCIÓN A LA CRIPTOGRAFíA.-

La idea de la criptografía tiene miles de años de antigüedad: los generales griegos y romanos la utilizaban para enviar mensajes en clave a los comandantes que están en el campo de batalla. Estos sistemas primitivos se basaban en 2 técnicas: la sustitución y la transposición.

La sustitución se basa en el principio de reemplazar cada letra del mensaje que se desea encriptar con otra. Algunos códigos de sustitución ocupan el mismo esquema de reemplazo para todas las letras del mensaje que se encripta; otros emplean diferentes esquemas para distintas letras.

La transposición se basa en la revoltura de los caracteres del mensaje. Un sistema de transposición implica escribir un mensaje dentro de una tabla, renglón por renglón, y luego leerlo columna por columna. El cifrado de doble transposición implica repr la revoltura otra vez.

Hoy en día, los algoritmos de encriptación, que se ejecutan en computadoras digitales de alta velocidad emplean sustitución y transposición combinada, así como otras funciones matemáticas.

2.1.1.- ¿Que es la Criptografía?

La criptografía es un conjunto de técnicas empleadas para conservar segura la información. Con ella es posible trasformar palabras escritas y otros tipos de mensajes de forma que sean incomprensibles para receptores no autorizados. Un receptor autorizado puede después regresar las palabras o mensajes a un mensaje perfectamente comprensible.

Por ejemplo, he aquí un mensaje que tal vez se desee enviar:

SSL is a cryptographic protocol.

Este podría ser el mensaje una vez encriptado:

***---'¡'¡&($%$#*-¡”°#$%&&//][_:;¨*¡?=)%**

Aún mejor, mediante la criptografía es posible volver a convertir este código en el comprensible mensaje original.

I.- Terminología.

Los sistemas de encriptación modernos constan de dos procesos complementarios:

a.- Encriptación.

Proceso mediante el cual el mensaje llano se transforma en un mensaje cifrado mediante una función compleja y una llave de codificación especial.

b.- Desencriptación.

Proceso inverso, en el cual el texto cifrado se convierte nuevamente en el texto llano original mediante una segunda función compleja y **una llave de desencriptación**.

La figura 2.1 muestra como se acoplan ambos procesos.

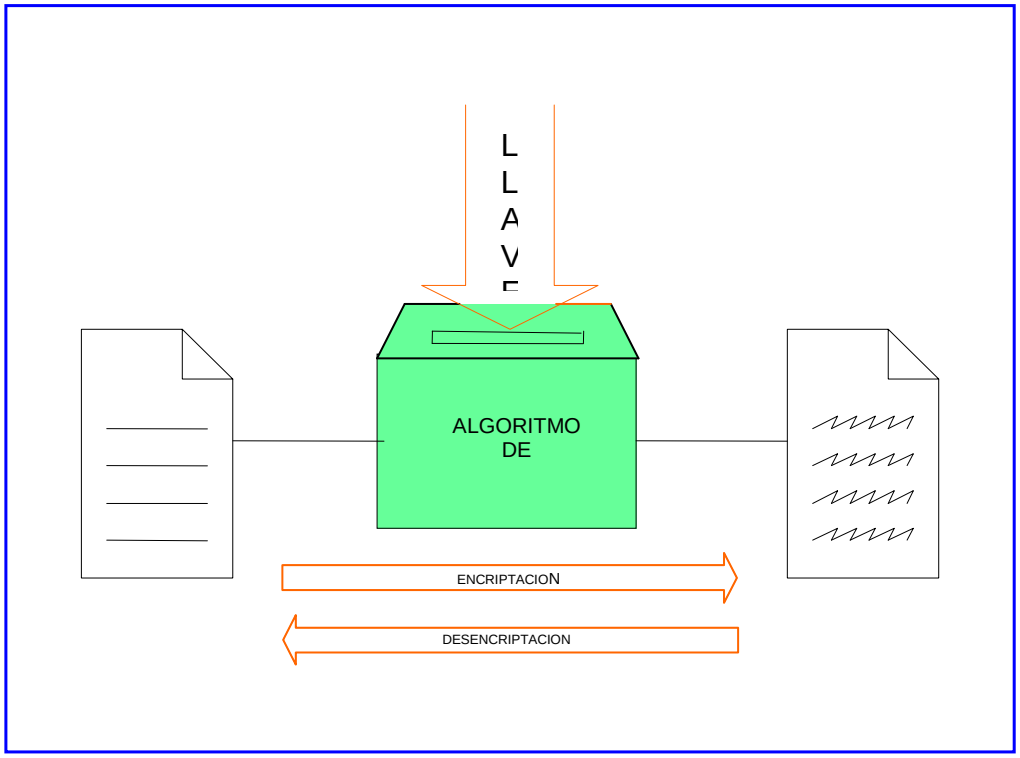


FIG. 2.1 Encriptación y Desencriptación

La meta de la criptografía es hacer imposible tomar el texto cifrado y reproducirlo en su forma original sin la llave correspondiente, y elevar el costo de adivinar la llave más allá de lo práctico.

II.- Algoritmos y funciones criptográficas.

Actualmente se emplean dos tipos básicos de algoritmos criptográficos:

a.- Algoritmos de llaves simétricas.-

En este tipo de algoritmos se utiliza la misma llave para encriptar y desencriptar el mensaje. El algoritmo DES, es un algoritmo de llaves simétricas.

Estos algoritmos se conocen también como algoritmos de llaves secretas y, en ocasiones como algoritmos de llave privada.

b.- Algoritmos de llave pública.-

En este tipo de algoritmos se utiliza una llave para encriptar el mensaje y otra para desencriptarlo. La llave de encriptación por lo general se conoce como llave pública y se puede divulgar públicamente sin poner en peligro la confidencialidad del mensaje ni la llave de desencriptación. Esta última por lo común se conoce como llave privada o llave secreta.

Los algoritmos de llaves simétricas son los caballos de batalla de los sistemas criptográficos modernos, son mucho más rápidos que los de llave pública, además de ser algo más

fáciles de implementar. Cabe indicar que estos algoritmos tienen un problema que limitan su uso en el mundo real: para intercambiar información mediante un algoritmo de llaves simétricas, ambas partes deben primero intercambiar, en forma segura, una llave de encriptación.

Los algoritmos de llave pública resuelven este problema. Las personas que desean comunicarse crean una llave pública y una llave secreta. La llave pública se publica. Si Gisella desea enviar un mensaje confidencial a María, todo lo que debe hacer es obtener una copia de la llave pública de María, usarla para encriptar el mensaje y enviarlo. Nadie, excepto María, puede desencriptar el mensaje, debido a que solo ella posee la llave secreta correspondiente.

La criptografía de llave pública también se ocupa para crear firmas digitales para la información, digamos un mensaje de correo electrónico, a fin de certificar su origen e integridad.

En el caso de las firmas digitales, la llave secreta se utiliza para crear la firma digital y la llave pública para comprobarla. Por ejemplo, María podría escribirle una carta a Gisella y

firmarla con su llave secreta. Cuando Gisella recibe el mensaje, puede verificarlo mediante la llave pública de María.

Los algoritmos de llave pública tienen inherente un problema importante: son increíblemente lentos. La encriptación y desencriptación mediante llave pública se ejecuta entre 10 y 100 veces más lenta que con el algoritmo equivalente de llaves simétricas. Debido a ello, existe un tercer tipo de sistema:

c.- Criptosistemas Híbridos Público/Privado.

En estos sistemas, la criptografía de llave pública, más lenta, se utiliza para intercambiar una llave de sesión aleatoria, que se usa entonces como base para un algoritmo de llaves simétricas (una llave de sesión es la que se utiliza para una sola sesión de encriptación; luego se desecha).

Existe un nuevo tipo de funciones que se utilizan junto con la criptografía de llave pública:

d.- Funciones de compendio de mensajes.

Una función de compendio de mensajes (message digest)

genera un patrón de bits único o casi único para una entrada específica. El valor del compendio se calcula de modo que encontrar una entrada que genere en forma exacta un compendio específico no sea factible computacionalmente.

2.1.2.- Algoritmos de Llaves Simetricas.

Los algoritmos de llaves simétricas sirven para la encriptación en masa de datos o flujo de datos. Están diseñados para ser muy rápidos y tienen un gran número de llaves posibles.

Los mejores algoritmos de llaves simétricas ofrecen confidencialidad casi perfecta: una vez que los datos son encriptados mediante una llave no hay forma de desencriptarlos sin poseer la misma llave.

Pueden dividirse en dos categorías: de bloque y de flujo. Los algoritmos de bloques encriptan los datos un bloque a la vez; los algoritmos de flujo encriptan byte por byte.

La siguiente lista analiza los algoritmos más comunes:

I.- DES.

DES es un algoritmo de bloque que utiliza una llave de 56 bits y tiene varios modos de operación, de acuerdo con el propósito con el que se utilice.

II.- DESX.

DESX consiste en una sencilla modificación al algoritmo DES, construida alrededor de dos pasos de ¨blanqueo¨. Estos pasos mejoran la seguridad del algoritmo, haciendo casi imposible la búsqueda de las llaves.

III.- Triple-DES.

Triple-DES duplica la seguridad del algoritmo DES, mediante el uso del algoritmo DES tres veces con tres diferentes llaves debido a que utilizar simplemente DES dos veces con diferentes llaves no mejora la seguridad al grado que se podría esperar, debido a un tipo teórico de ataque conocido como “encontrarlo a la mitad”, en el cual un atacante intenta, de modo simultáneo, encriptar el texto llano con una sola operación

DES y desencriptar el texto cifrado con otra operación DES, hasta que se encuentre una correspondencia a la mitad.

IV.- Blowfish.

Blowfish (pez globo) es un algoritmo de bloque rápido, compacto y sencillo que permite una llave de longitud variable de hasta 448 bits, está optimado para ejecutarse en procesadores de 32 y 64 bits.

V.-IDEA.

El Algoritmo Internacional de Encriptación de Datos IDEA (International Data Encription Algorithm) utiliza una llave de 128 bits que es bastante segura. IDEA se utiliza dentro del popular programa PGP para encriptar archivos y correo electrónico.

VI.- RC2.

Es un algoritmo de bloque razonablemente seguro que permite llaves de entre 1 y 128 bits.

VII.- RC4.

Es un algoritmo de flujo razonablemente seguro que permite llaves entre 1 y 128 bits.

VIII.-RC5.

Este algoritmo de bloque permite que la longitud de la llave, el tamaño de bloque de datos, y número de pasadas de encriptación las defina el usuario.

2.1.2.1.- Fortaleza Criptográfica.

Algunos sistemas no son muy buenos para la protección de datos, pues permiten desencriptar la información sin conocer la llave correspondiente. Otros son bastantes resistentes aún a los ataques más persistentes. La capacidad de un sistema criptográfico para proteger información contra el ataque se conoce como fortaleza, y depende de muchos factores:

- La confidencialidad de la llave

- La dificultad de adivinar la llave o intentar todas las llaves posibles. Las llaves más largas por lo general son más difíciles de adivinar o encontrar.

- La dificultad de invertir o romper el algoritmo de encriptación sin conocer la llave.

- La existencia de puertas traseras, es decir, formas adicionales de poder desencriptar un archivo encriptado más fácilmente sin conocer la llave.

- La habilidad de desencriptar un mensaje encriptado, se conoce como desencriptar una parte de él, denominado como ataque de texto llano conocido.

- Las propiedades y el conocimiento del texto llano que tenga un atacante, por ejemplo; un sistema criptográfico puede ser vulnerable al ataque si todos los mensajes encriptados con él comienzan o terminan con un fragmento conocido de texto llano.

La fortaleza criptográfica casi nunca puede probarse: sólo puede probarse la debilidad.

2.1.3.- Algoritmos de Llaves Públicas.

Los buenos algoritmos de llaves simétricas simplemente revuelven su entrada con base en la llave de entrada; el desarrollo de un nuevo algoritmo de llaves simétricas solo requiere idear nuevas formas de hacer esa revoltura en forma confiable. Los algoritmos de llave pública por lo general se basan en la teoría numérica. El desarrollo de nuevos algoritmos de llave pública requiere la identificación de nuevos problemas matemáticos con propiedades específicas.

A continuación, resumimos los algoritmos más comunes:

I.- Intercambio de llaves Diffie-Helman.

Sistema para intercambio de llaves criptográficas entre partes activas. No es en realidad un método de encriptación y desencriptacón sino un método para desarrollar e intercambiar una llave privada compartida mediante un canal de comunicación público. A fin de cuentas, ambas partes acuerdan utilizar algunos valores numéricos comunes, y luego cada una de ellas crea una llave. Cada parte puede calcular entonces una tercera llave de sesión la cual no puede ser fácilmente derivada por un atacante que conozca ambos valores intercambiados.

II.- RSA.

RSA puede ocuparse para encriptar información y como fundamento de un sistema de firmas digitales. Las firmas digitales pueden utilizarse para probar la autoría y autenticidad de información digital. La llave puede tener cualquier longitud, dependiendo de la implementación que se utilice.

III.- El Gamal.

Es un sistema de encriptación de llaves públicas basado en el algoritmo de intercambio de llaves Difie-Hellman. En forma similar a RSA,

El Gamal puede emplearse tanto para encriptación como para firmas digitales.

IV.- DSS.

El Estándar de Firmas Digitales (DSS, Digital Signature Stándar) se basa en el Algoritmo de Firmas Digitales (DSA). Permite utilizar llaves de cualquier longitud y puede utilizarse sólo para firmas digitales, aunque es posible utilizar implementaciones de DSA también para encriptación.

2.1.4.- Funciones De Compendio De Mensajes.

Las funciones de compendio de mensajes transforman la información contenida en un archivo que puede ser pequeño o grande, a un sólo número grande, típicamente de entre 128 y 256 bits. Ver figura 2.2.

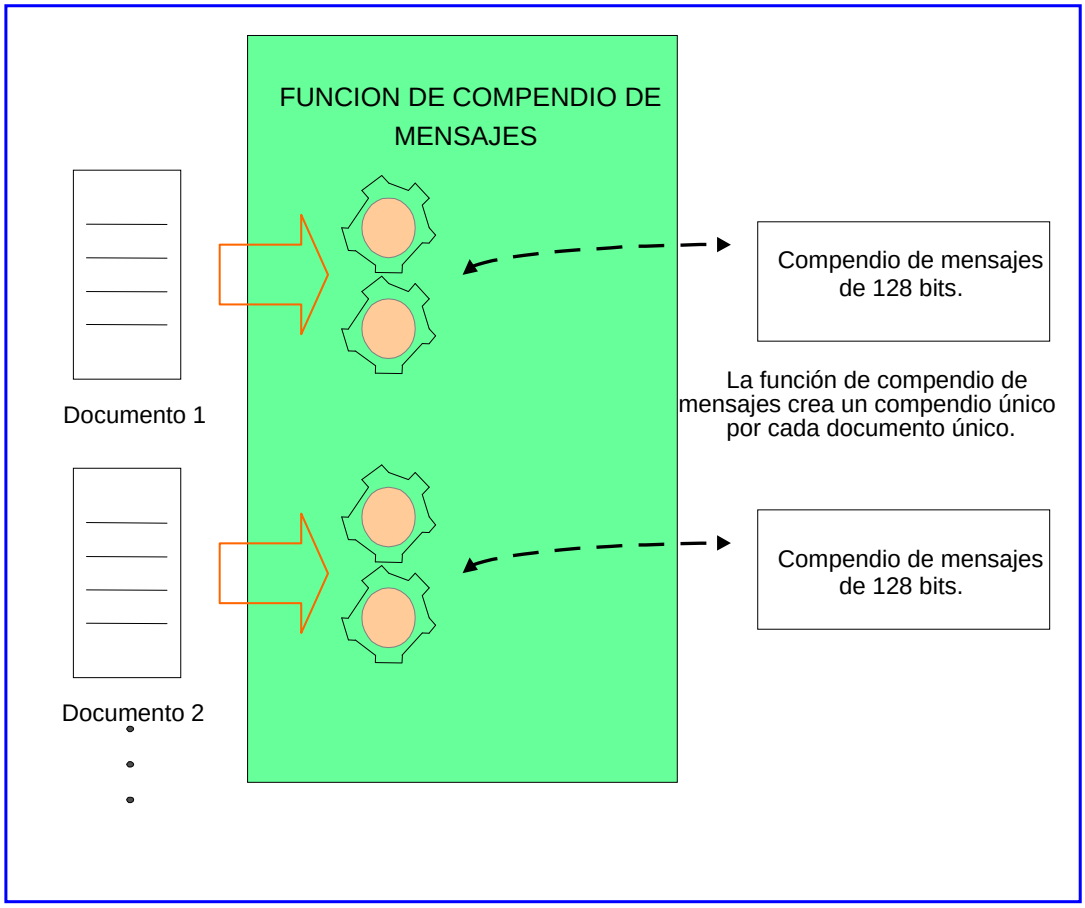


FIG. 2.2 Función de compendio de mensajes.

Las mejores funciones de compendio de mensajes combinan las siguientes propiedades matemáticas:

- Cada bit de la función de compendio de mensajes sufre la influencia de cada bit de la entrada de la misma función.

- Si se modifica cualquier bit de la entrada de la función, cada bit de salida tiene 50% de probabilidad de cambiar.

- Dado un archivo de entrada y su compendio correspondiente, debe ser no factible computacional encontrar otro archivo con el mismo valor de compendio.

Los compendios de mensajes también se conocen como funciones *hash* de un solo sentido, debido a que producen valores difíciles de invertir, resistentes al ataque, en su mayoría única y ampliamente distribuidos.

A continuación analizamos algunas funciones de compendio de mensaje:

I.- HMAC.-

El código de autenticación de mensajes por Hash (HMAC, Hashed Message Autenthication Code) utiliza una llave secreta y una función de compendio de mensajes para crear un código de autenticación secreto para mensajes. El método HMAC fortalece una función de compendio de mensaje existente para hacerla resistente a un ataque externo, aún si la función es violada.

II.- MD2.-

El compendio de mensajes número dos (Message Digest # 2), es una de las funciones de compendio de mensaje más seguras, pero es la que lleva más tiempo calcular. Produce un compendio de 128 bits.

III.-MD4.-

El compendio de mensajes número cuatro (Message Digest # 4), se desarrolló como alternativa a MD2, luego se demostró que MD4 es inseguro, es decir, que es posible encontrar dos archivos que produzcan el mismo código MD4 sin tener que

hacer una búsqueda de fuerza bruta. MD4 produce un compendio de 128 bits.

IV.- MD5.-

El compendio de mensajes número cinco (Message Digest # 5), incluye técnicas diseñadas para hacerlo más seguro. Se le han descubierto fallas que permiten calcular algunos tipos de colisiones. MD5 produce un compendio de 128 bits.

V.- SHA.-

El Algoritmo Seguro de Hash (SHA, Secure Hash Algorithm) diseñado para usarse junto con el Estándar de Firmas digitales del Instituto Nacional de Estándares y Tecnologías (el DSS del NIST). SHA produce un compendio de 160 bits.

VI.- SHA1.-

El Algoritmo Seguro de Hash revisado, empleado en conjunto con DSS. SHA1 produce un compendio de 160 bits.

Además de estas funciones, también es posible utilizar como función de compendio de mensajes sistemas de encriptación simétrica de bloque; por ejemplo, DES. Para utilizar una función de encriptación como función de compendio de mensajes, simplemente debe ejecutar la función de encriptación en modo de retroalimentación de código. Como llave se utiliza una llave elegida al azar y específica a la aplicación. Se encripta todo el archivo y el último bloque de datos encriptados es el compendio.

2.1.4.1.- Como Funcionan los Algoritmos de Compendio de Mensaje.-

Los algoritmos de compendios de mensajes no se emplean para operaciones de encriptación y desencriptación; se utilizan en la creación de firmas digitales, códigos de autenticación de mensajes (MAC, Message Autentication Codes) y llaves de encriptación a partir de frases de acceso.

La forma más fácil de entender las funciones de compendio de mensajes es verlas trabajando. Considere el siguiente ejemplo que utiliza el algoritmo de compendio de mensajes MD5.

```
MD5 (Hay $1500 en la caja azul.)  =  f1348485f7619f3017c641af3268cda
MD5 (la junta de ayer estuvo bien.) = 0500502790abfe19d0t97f4f3f878518
MD5 (Hay $1100 en la caja azul.)  = 4430869e496c75d94328c180c01cfe3f
```

Observe que todos estos mensajes tienen códigos MD5 sumamente distintos. Aún el primer y tercer mensaje, que difieren en un solo carácter (y aún en ese carácter en un solo bit), tienen compendios de mensajes diferentes por completo.

En apariencia, el compendio es del todo aleatorio, pero en realidad no es así.

Veamos algunos compendios mas:

```
MD5 (Hay $1500 en la caja azu  )  d9261e7d6d1ee9c039076ab02cda6629
MD5 (Hay $1500 en la caja azul )  = b8f3aa09ccdec76bce9001f1043ceefa
MD5 (Hay $1500 en la caja azul. )  =  f1348485f7619f3017c641af3268cda
MD5 (Hay $1500 en la caja azul! )  =062dc60d4db7b2fc6130389e8bba6254
MD5 (Hay $1500 en la caja azul: )  = 3159032c79d7f6017c077a87305faaf0
MD5 (Hay $1500 en la caja azul..)  = cf4521537e5df7d6d47d73c6e32230d
```

Considere la tercera línea de código MD5 del ejemplo anterior: puede ver que es idéntica a la primera línea mostrada con anterioridad. Esto se debe a que el mismo texto siempre produce el mismo código MD5.

La función de compendio de mensajes es una herramienta poderosa para detectar cambios muy pequeños en archivos o mensajes muy grandes; se calcula el código MD5 del mensaje y lo guarda en lugar aparte. Si cree que el archivo ha sido modificado a propósito o por accidente, sólo recalcula el código MD5 y lo compara con el MD5 creado originalmente. Si son idénticos, hay una probabilidad muy alta de que el archivo no haya sido modificado.

Dos archivos diferentes pueden tener el mismo valor de compendio. Esto se conoce como una colisión. Para que una función de compendios de mensaje deba ser imposible computacionalmente encontrar o producir tales colisiones.

2.1.4.2.- Usos de las Funciones de Compendios de Mensajes.

Las funciones de compendio de mensajes se utilizan ampliamente hoy en día por varias razones:

- Son mucho más rápidas que las funciones criptográficas tradicionales, pero parecen compartir muchas de sus fuertes propiedades criptográficas.

- Al parecer proporcionan una excelente forma de esparcir el azar o entropía de una entrada entre todos los bits de salida de la función.

- Mediante un compendio de mensajes es posible crear llaves de encriptación para códigos de encriptación simétrica permitiendo a los usuarios introducir frases de acceso. La llave de encriptación se produce calculando el compendio de la frase introducida. PGP utiliza esta técnica para calcular las llaves de encriptación para la encriptación convencional.

- Los compendios de mensajes pueden usarse con facilidad para generar códigos de autenticación de mensajes que utilicen un secreto compartido entre dos partes para comprobar que el mensaje es autentico. Se agregan los códigos de autenticación al final del mensaje que se va a verificar.

- Las funciones de compendios de mensajes también forman parte importante de muchos sistemas de criptografía de llave pública.

- Los compendios de mensajes forman la base de la mayoría de los estándares de firmas digitales. En vez de firmar todo el documento, la mayoría de los estándares de firmas digitales simplemente firman un compendio.

- Los códigos de autenticación de mensajes basados en compendios de mensajes proporcionan la seguridad “criptografía” de la mayoría de los protocolos de enrutamiento de Internet.

- Los programas como PGP emplean compendios de mensajes para transformar una frase de acceso proporcionada por un usuario en una llave de encriptación usada para encriptación simétrica. En el caso de PGP, la encriptación simétrica se utiliza tanto para su función de “encriptación convencional” como para encriptar la llave privada del usuario.

2.1.5.- La Criptografía y la Seguridad en el Web.

Existen cuatro palabras claves que se utilizan para describir

todas las funciones que tiene la encriptación en los sistemas de información modernos. Estas funciones son:

I.- Confidencialidad

La encriptación se utiliza para ocultar la información enviada a través de Internet y almacenarla en servidores, de forma que cualquiera que intente interceptarlas no pueda tener acceso al contenido de los datos.

II.- Autenticación

Las firmas digitales sirven para identificar al autor de un mensaje; las personas que reciben el mensaje pueden comprobar la identidad de quien lo firmó. Pueden emplearse junto con claves de acceso o como alternativas a ellas.

III.- Integridad

Para verificar que un mensaje no ha sido modificado en tránsito se utilizan varios métodos. Con frecuencia se lleva a

cabo mediante códigos de compendio de mensajes firmados digitalmente.

IV.- No repudiación

Mediante la encriptación se crean recibos de forma que el autor de un mensaje no pueda negar falsamente su envío.

En términos estrictos, hay cierto traslape entre estas áreas. Por ejemplo, cuando se utiliza el algoritmo de encriptación DES para brindar confidencialidad, a menudo proporciona integridad de modo colateral. Esto se debe a que si un mensaje es alterado, no será posible desencriptarlo en forma adecuada.

Sin embargo, en la práctica se considera mejor utilizar para este propósito diferentes algoritmos diseñados específicamente para asegurar la integridad en vez de confiar en los beneficios colaterales de otros algoritmos. De este modo, si el usuario decide no incluir un aspecto como por ejemplo, la encriptación, debido a razones legales o de eficiencia, el usuario aún podrá utilizar un algoritmo estándar para los demás requerimientos del sistema.

2.1.6.- LOS SISTEMAS ACTUALES DE ENCRIPTACION

Los sistemas criptográficos que se utilizan en forma más amplia hoy en día pueden dividirse en dos categorías. El primer grupo lo forman los programas y protocolos utilizados para encriptar mensajes de correo electrónico. Estos programas toman un mensaje en texto llano, lo encriptan y almacenan el texto cifrado o lo envían a otro usuario en Internet. También pueden ocuparse para encriptar mensajes de correo electrónico o archivos guardados en las computadoras para darles mayor protección. Algunos de los sistemas populares que caen en esta categoría incluyen:

- **PGP**
- **S/MIME**

La segunda categoría de sistemas criptográficos se compone de protocolos de red utilizados para proporcionar confidencialidad, autenticación, integridad y no repudiación en un ambiente de red. Para funcionar de modo adecuado, estos sistemas requieren interacción en tiempo real entre un cliente y

un servidor. Algunos sistemas populares que caen en esta categoría son:

- **SSL**
- **PCT**
- **S-HTTP**
- **SET y CYBER CASH**
- **DNSSEC**
- **IPSEC e IPV6**
- **KERBEROS**
- **SSH**

***I*.-PGP**

Privacía bastante segura (Pretty Good Privacy), es un sistema completo para la protección de correo electrónico y archivos. También es un conjunto de estándares que describen los formatos de los mensajes encriptados, llaves y firmas digitales.

PGP es un sistema de encriptación híbrido que utiliza encriptación de llave pública RSA para la administración de llaves, y el código simétrico IDEA para la encriptación de los

datos. PGP ofrece confidencialidad mediante el algoritmo de encriptación IDEA; integridad mediante funciones Hash criptográficas MD5; autenticación mediante certificados de llave publica, y no repudiación mediante mensajes firmados criptográficamente.

Un problema con PGP es la administración y certificación de llaves públicas. Las llaves de PGP nunca expiran: en vez de ello, cuando una llave es comprometida, es responsabilidad del poseedor distribuir un certificado especial de revocación de llave PGP a todas las personas con las que se comunica. Los corresponsales que no se enteren de que la llave ha sido comprometida, y la utilicen semanas, meses o años después para enviar un mensaje encriptado lo hacen bajo su propio riesgo. Como efecto colateral, si se crea o distribuye una llave pública PGP, es necesario conservar la llave secreta indefinidamente, debido a que nunca expira.

II.- S/MIME

Las Extensiones Multipropósito de Correo de Internet, MIME *(*Multipurpose Internet Mail Extensions) son un estándar para

enviar mensajes, con archivos binarios anexos a través de Internet. Secure/MIME extiende al estándar MIME para proporcionar correo electrónico firmado.

S/MIME ofrece confidencialidad mediante algoritmos de encriptación especificados por el usuario; integridad mediante una función de Hash especificada por el usuario; autenticación mediante certificados de llave pública X.509v3, y no repudiación mediante mensajes firmados criptográficamente. El sistema puede usarse tanto con encriptación fuerte como débil.

III.- SSL

El Nivel de Conexiones Seguras, SSL (Secure Sockets Layer) es un protocolo criptográfico de propósito general para asegurar canales de comunicación bidireccionales. SSL se utiliza comúnmente junto con el protocolo TCP/IP, y es el sistema de encriptación que usan navegadores como Navigator de Netscape e Internet Explorer de Microsoft, pero puede emplearse con cualquier servicio basado en TCP/IP.

Las conexiones de SSL por lo general las inicia un navegador utilizando un prefijo especial en los URL.

Por ejemplo el prefijo “https” se utiliza para indicar una conexión de HTTP encriptada con SSL, mientras “snews” se usa para indicar una conexión de NNTP encriptada con SSL.

SSL ofrece confidencialidad mediante algoritmos de encriptación especificados por el usuario; integridad, mediante funciones Hash criptográficas especificadas por el usuario, y no repudiación, mediante mensajes firmados criptográficamente.

IV.- PCT.

PCT Private Comunications Technology (Tecnología deComunicaciones Seguras) es un protocolo de seguridad de nivel de transporte similar a SSL.

Fue desarrollado en respuesta a los problemas asociados a SSL 2.0 y que se corrigieron en SSL 3.0.

V.- S-HTTP*. W<*

S-HTTP es un sistema para firmar y encriptar información enviado mediante el protocolo HTTP del Web. S-HTTP se diseñó antes de la liberación pública de SSL. Incluye algunas características interesantes como la capacidad de guardar documentos prefirmados en un servidor Web.

VI.- SET*.*

SET (Transacciones Electrónicas Seguras, Secure Electronic Transactions) es un protocolo criptográfico diseñado para envío de números de tarjetas de crédito por Internet.

El sistema SET consta de tres partes: una "billetera electrónica", que reside en la computadora del usuario; un servidor que se ejecuta en el sitio web del comerciante, y el servidor de pagos SET que se ejecuta en el banco del comerciante.

Para utilizar el sistema SET, el usuario primero debe introducir el número de su tarjeta de crédito en el software de billetera

electrónica. La mayoría de las implementaciones almacenan el número en un archivo encriptado en el disco duro o en una tarjeta inteligente. El software también crea una llave pública y una privada para encriptar la información financiera antes de enviarla a través de Internet.

SET proporciona confidencialidad para los números de tarjetas de crédito, pues se encriptan mediante el algoritmo RSA. Y proporciona, además, integridad, autenticación y no repudiación mediante funciones de compendio de mensajes y firmas digitales.

VII.- Cyber Cash.

Cyber Cash (Ciber efectivo) es un protocolo de pagos electrónicos de propósito similar al de SET. De hecho, algunas partes de SET fueron modeladas concretamente sobre Cyber Cash.

VIII.- DNSSEC.

El estándar de seguridad del Sistema de Nombres de Dominios

(DNSSEC, Domain Name Security) es un sistema diseñado para proporcionar seguridad al Sistema de Nombres de Dominios (DNS, Domain Name Sistem) de Internet. DNSSEC crea una infraestructura paralela de llaves públicas sobre el sistema de DNS. A cada dominio del DNS se le asigna una llave pública. La llave pública de un dominio se puede obtener en forma confiable a partir del dominio padre, o puede ser precargada en un servidor de DNS mediante su archivo “boot”.

DNSSEC permite la actualización segura de la información almacenada en los servidores de DNS, ideal para administración remota.

IX.- IPSEC e IPV6.

IPsec es un protocolo criptográfico diseñado por el Grupo de Ingeniería de Internet IETEF, (Internet Engineering Task Force) para proporcionar confidencialidad de principio a fin. IPsec puede funcionar con IPv4, la versión estándar de IP utilizada actualmente en Internet. IPv6, el IP de “Próxima Generación”, incluye IPsec.

Ipsec no proporciona integridad, autenticación ni, no repudiación, dejando estas características a otros protocolos. Hoy en día el uso principal de Ipsec parece ser como protocolo proveedor para crear redes privadas virtuales (VPN, virtual private networks) a través de Internet, siempre y cuando los proveedores lo implementen ampliamente.

X.- KERBEROS

A diferencia de los demás sistemas mencionados, Kerberos no utiliza tecnologías de llave pública. Más bien kerberos se basa en códigos simétricos y en secretos compartidos entre el servidor de Kerberos y cada usuario, quien tiene su propia clave de acceso. El servidor de Kerberos lo utiliza para encriptar los mensajes enviados a ese usuario de forma que no pueda leerlos nadie más.

El soporte de Kerberos debe agregarse a cada programa que se desee proteger. En la actualidad se encuentran en uso generalizado versiones “Kerberizadas” de Telnet, FTP, POP, y Sun RPC. Para operar un sistema con Kerberos, cada sitio debe tener un servidor de Kerberos que se encuentre

físicamente seguro. El servidor de Kerberos mantiene una copia de la clave de acceso de cada usuario.

XI.- SSH.

SSH (secure shell) es el interprete de comandos seguros. Proporciona operaciones protegidas de terminal virtual (Telnet) y transferencia de archivos (ftp).

2.2.- FIREWALL

2.2.1.- ¿Qué es un Cortafuegos (Firewall)?

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuál de los servicios de red puede ser accesado dentro de la red por los que están fuera, es decir, quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es

parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

I.-Administración de los cortafuegos.

La mayoría de los trabajos administrativos necesarios para un cortafuegos consiste en la instalación inicial y la configuración de la regla de acceso. Por ejemplo, los routers de la red deben configurarse para dirigir el tráfico hacia el cortafuegos, y este debe definirse con dos direcciones IP, una para cada interfaz, y con rutas hacia routers situados en las

proximidades. La mayoría de cortafuegos obligan a utilizar rutas estáticas en lugar de aplicaciones de direccionamiento dinámico. El administrador debe configurar las reglas de acceso así como los registros de actividades y alarmas.

Una vez realizada la configuración inicial, las demás tareas del administrador de un cortafuegos es supervisar y hacer copias de seguridad de los registro de actividades, agregar o modificar reglas de acceso según convenga y añadir nueva información de autentificación de usuarios, siempre y cuando este disponible esta característica.

Asimismo, el administrador debe hacer copias de seguridad de los archivos de configuración junto con cualquier otra función de mantenimiento necesaria por el sistema operativo en el que se esta ejecutando el cortafuegos

Tenga presente que algunos cortafuegos ofrecen también la posibilidad de realizar la administración de forma remota, permitiendo configurar múltiples cortafuegos desde una ubicación central. Esta función es atractiva en el caso de que la red precise múltiples cortafuegos.

II.-Plataforma de Cortafuegos.

Hoy en día la mayoría de Firewalls presentan habitualmente el de un PC normal; de hecho, muchos cortafuegos se ejecutan en un PC estándar. Algunos lo hacen en estaciones de trabajo SUN y otros pocos en estaciones de trabajo HP. Muchos otros cortafuegos se ejecutan en computadoras genéricas Intel, y la mayoría de fabricantes de grandes computadoras, como DEC, IBM y Harris, suministran software para cortafuegos que se ejecutan en sus máquinas. Los routers de cortafuegos utilizan hardware especial, aunque todavía así tienen el aspecto de un PC de sobremesa o de torre.

La capacidad de procesamiento que precisa un cortafuegos depende del tipo de cortafuegos y de la velocidad de la red. A efectos de velocidad y seguridad, la función del cortafuegos debería ser el único servicio soportado por el sistema.

III.- La Seguridad que proporcionan.

Los cortafuegos son una parte importante de un sistema de seguridad equilibrado. No son, sin embargo, la solución de

seguridad definitiva. Actúan como un filtro y, como tal, todavía pueden permitir la entrada de las amenazas en la red. Es conveniente evaluar cuidadosamente los servicios de red que podrán atravesar él cortafuegos. Además, debe proporcionarse seguridad adicional en otras áreas de la red como los controles de acceso basados en un host.

2.2.2.- Tipos de Cortafuegos

I.-Dos Tipos Básicos de Cortafuegos.

Los cortafuegos difieren tanto en las arquitecturas en que se basan como en las características que ofrecen.

Los dos tipos de cortafuegos mas habituales son filtros de paquetes, que funcionan a nivel de paquete IP, y gateways a nivel de aplicación, que funcionan a nivel de aplicación en la computadora.

- Un cortafuegos de filtrado de paquetes ofrecen un control básico de acceso a la red basado en la información de protocolo contenida en los paquetes IP.

Cuando estos llegan al cortafuegos, la información se compara con un conjunto de reglas de filtrado, que especifican las condiciones según las cuales se autoriza o niega a los paquetes su acceso a la red.

- Un cortafuego de gateway a nivel de aplicación interrumpe la ejecución de todas las secciones de red y crea una sesión aparte hacia el destino deseado, siempre y cuando reciba autorización para ello. A continuación trasmite la información desde la conexión original hasta la segunda conexión.

- Ambos actúan como un filtro entre dos redes con el fin de restringir los servicios que se ofrecen en cualquier dirección según una política preestablecida. Sin embargo los tipos de cortafuegos difieren en lo que se refiere al nivel de control que ofrecen. Los cortafuegos de gateway a nivel de aplicación. Ejerce mayor control sobre una sesión, dado que crea y mantiene la conexión actual con el exterior.

a.- Filtros de Paquetes.

La mayoría de cortafuegos actuantes como filtros de paquetes son routers, que por lo general, son conocidos como routers de filtrado. Algunos de los primeros cortafuegos que estuvieron disponibles eran routers estándar de paquetes IP a los que se les había incorporado un conjunto de reglas sencillas. La función normal de un router es aceptar un paquete, identificar su próximo salto de la ruta, por medio del exámen de la información que contiene el paquete IP, y hacerlo pasar o desecharlo en el caso de no poder encontrar una ruta.

La incorporación de la función de filtrado de paquete fue una ampliación lógica dentro de las características de un router normal. Sólo tuvieron que añadir un paso para determinar, en función de la información de las direcciones de origen y destino del paquete, si este podía continuar o no su recorrido.

Los filtros de paquetes aceptan la entrada de paquetes IP en un conjunto de interfaces, tras lo cual los desechan o los hacen pasar según un conjunto de reglas definidas por el administrador. Este proceso se lleva a cabo en la porción del

kernel del sistema operativo. A diferencia de las aplicaciones, el Kernel no está sujeto a ningún programa, por lo que puede procesar la información más rápidamente que aquellas.

Algunos routers de filtrado de alta velocidad realizan este procesamiento en la tarjeta de interfaz de red con el fin de proporcionar un rendimiento total de procesamiento todavía mayor.

Los routers no son los únicos cortafuegos que se usan para filtrar paquetes.

Algunos cortafuegos de hosts, también incorporan la posibilidad de filtrar paquetes

Algunos de ellos representan perfeccionamiento del filtrado de paquetes tradicional realizado por routers al ofrecer un filtrado a nivel de sesión o avanzados mecanismos de auditoria.

Los cortafuegos de paquetes de filtrados se consideran generalmente menos seguros que los gateways que

funcionan a nivel de aplicación, consecuencia, por lo general, de que los filtros de paquetes no acceden a la información situada al nivel, más elevado, de las aplicaciones.

b.- *Gateways a Nivel de* Aplicación.

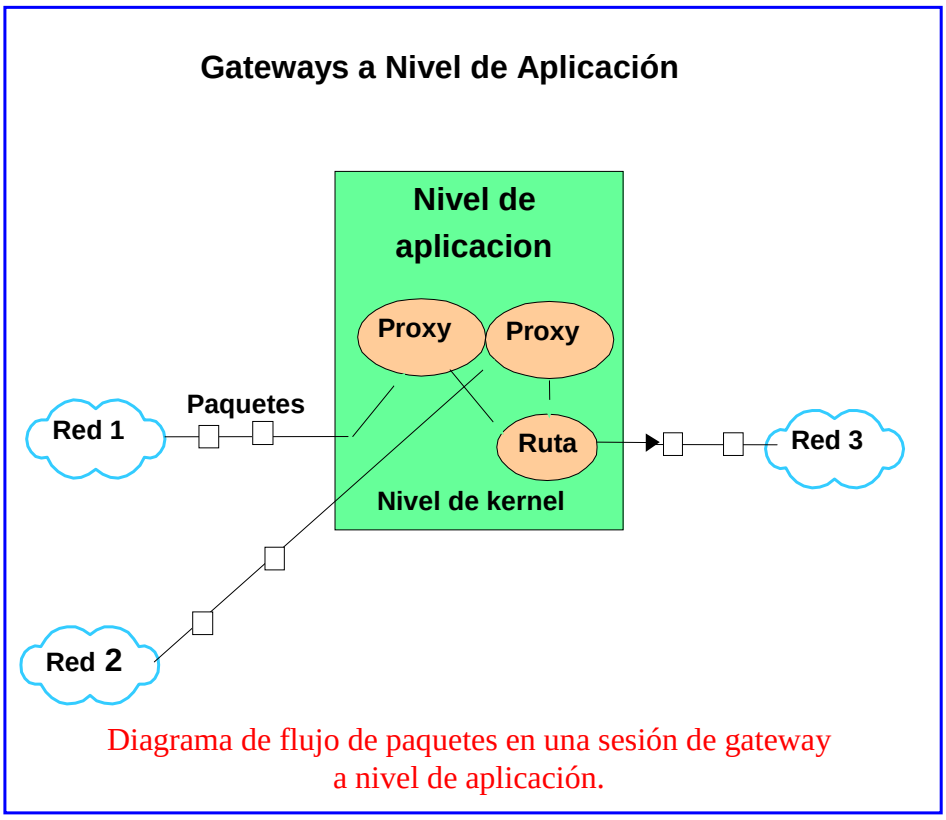


FIG. 2.3 Gateway a Nivel de Aplicación.

Los gateways de nivel de aplicación se implementan en forma de programas de software en una plataforma de sistema host, que puede ser desde un pequeño PC hasta una compleja configuración de múltiples procesadores. La figura 2.3 ilustra el funcionamiento general de un gateway de nivel de aplicación.

Los gateways de nivel de aplicación impiden el paso directo de los paquetes de una red a otra. Más bien, obligan a que la conexión original se haga a una aplicación específica, conocida como proxy, que se encuentra en el cortafuego. Esta aplicación decide si debe o no establecer, en representación del hosts origen, una conexión con el host destino solicitado. Este tipo de retransmisión de paquetes que efectúa el proxy ayuda a impedir algunos ataques de nivel de aplicación como el conocido ataque por sobreflujo de buffer. Naturalmente, esto implica que la aplicación proxy del cortafuego pueda sufrir algún ataque. Una de las limitaciones de un cortafuego basado en un gateway de nivel de aplicación es que precisa de una aplicación individual para cada servicio de red. En otras palabras, un cortafuego de este tipo necesita programas individuales para Telnet, para el correo electrónico, para el

World Wide Web o para cualquier otro servicio que soporte el sistema. Cada vez que el cortafuego soporte un nuevo servicio en Internet y el cortafuego no cuenta con una aplicación proxy para dicho servicio, se niega el acceso a los usuarios al mismo. Además, existe un límite en cuanto al número de aplicaciones activas que puede soportar un computador, lo que restringe el número total de conexiones simultáneas que puede proporcionar el cortafuego. NO obstante, algunos gateways de nivel de aplicación proporcionan una aplicación proxy genérica que permite la retransmisión de cualquier servicio. Pero estos proxys genéricos pierden gran parte de las ventajas de un gateway de nivel de aplicación, debido a que no conocen el protocolo especifico de la aplicación. El resultado es una versión más lenta de la capacidad de filtrado de paquetes.

II.- Tipos de Cortafuegos Adicionales.

Hay dos tipos de arquitectura de cortafuegos alternativas, que son esencialmente una combinación de filtrado de paquetes y de gateway de nivel de aplicación que proporcionan uno o más sistemas.

a.- Cortafuegos Híbridos.

Una variante natural de los tipos de cortafuegos descritos anteriormente es un sistema de cortafuegos híbrido que incluye un filtro de paquetes y un gateway a nivel de aplicación.

El diagrama de la figura 2.4 ilustra esta arquitectura.

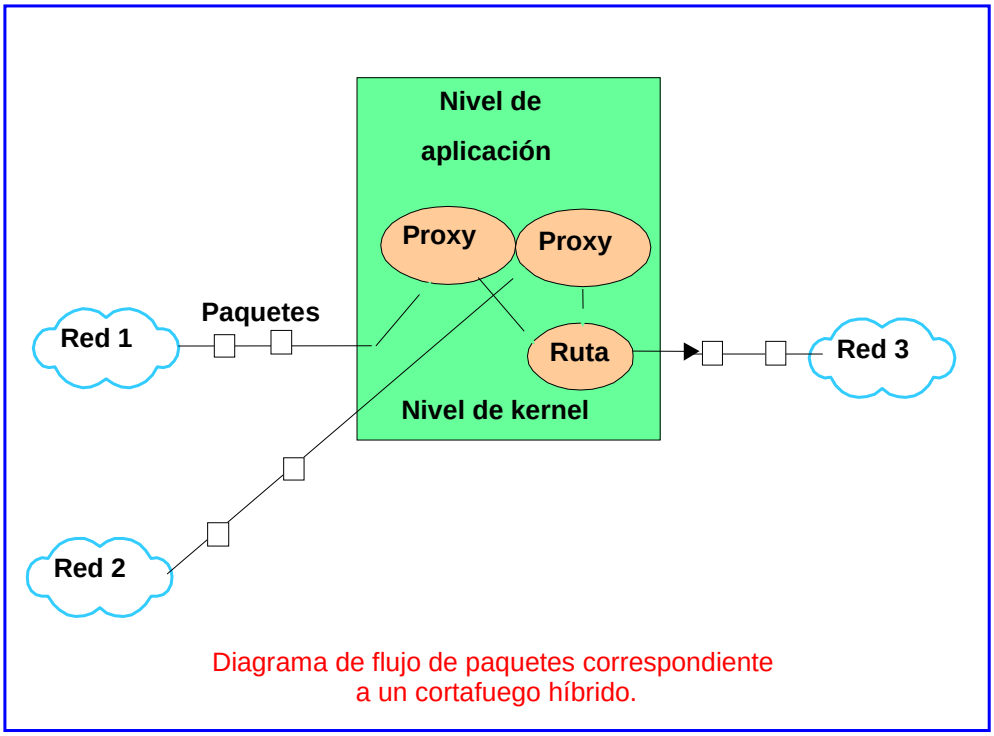


FIG. 2.4 Cortafuegos híbridos.

En una configuración híbrida los paquetes recibidos son sometidos en primer lugar a las decisiones de filtrado de paquetes. Luego los paquetes pueden desecharse, hacerse

pasar a través del Kernel hacia su destino previsto o enviarse a un proxy a fin de ser procesados posteriormente. Un cortafuego híbrido es la mejor solución para una Intranet que necesita la seguridad que ofrece un gateway a nivel de aplicación para ciertos servicios y la velocidad y flexibilidad de un filtro de paquetes para otros tipos de servicios.

b.- Cortafuegos basados en un host Bastión.

La arquitectura basada en host bastión consiste en un host configurado para resistir los ataques procedentes del exterior. El blindaje del host bastión es importante porque este se sitúa normalmente en un lugar expuesto directamente a la Internet.
Existen dos tipos de host bastión:

- Al igual que la mayoría de cortafuegos, el host bastión de residencia dual posee una conexión a la intranet y otra a la red exterior o internet pública. Esta forma temprana de host bastión obligaba a los usuarios del interior a registrarse en el cortafuegos y a efectuar desde el host bastión todas sus acciones con la red exterior. Esta configuración aislaba a los hosts internos del exterior,

pero afectaba considerablemente la capacidad de los usuarios para interaccionar con la red exterior. A medida que evolucionó la tecnología de los bastiones, fueron agregándoseles aplicaciones proxy con el fin de que actuaran en representación del usuario. El resultado de esta evolución es la arquitectura basada en un gateway a nivel de aplicación descrita anteriormente.

- El segundo tipo de cortafuegos basado en un host bastión es un host de residencia única (que significa que solo hay una conexión de red) conectado a lo que se conoce como red de perímetro. La figura 2.5 muestra un ejemplo de una red de perímetro que soporta un host bastión individual.

Observe en el diagrama 2.5, que el servicio de cortafuegos lo proporciona una combinación de los dos routers de filtrado, la red de perímetro y el host bastión. El router exterior filtra los servicios no soportados por la red interna o por el host bastión. El router interno, conocido en ocasiones como router de bloqueo, limita todos los servicios no soportados por la red interna y sirve de protección principal. El host bastión

proporciona a los usuarios externos servicios como un gateway de correo electrónico, FTP anónimo, es decir, un sitio que permite la transferencia de ficheros a clientes remotos, consultas del Domain Name system (DNS) o un servidor Web http. Una red de perímetro puede contener varios hosts bastiones, que proporcionan cada uno de ellos uno o más servicios.

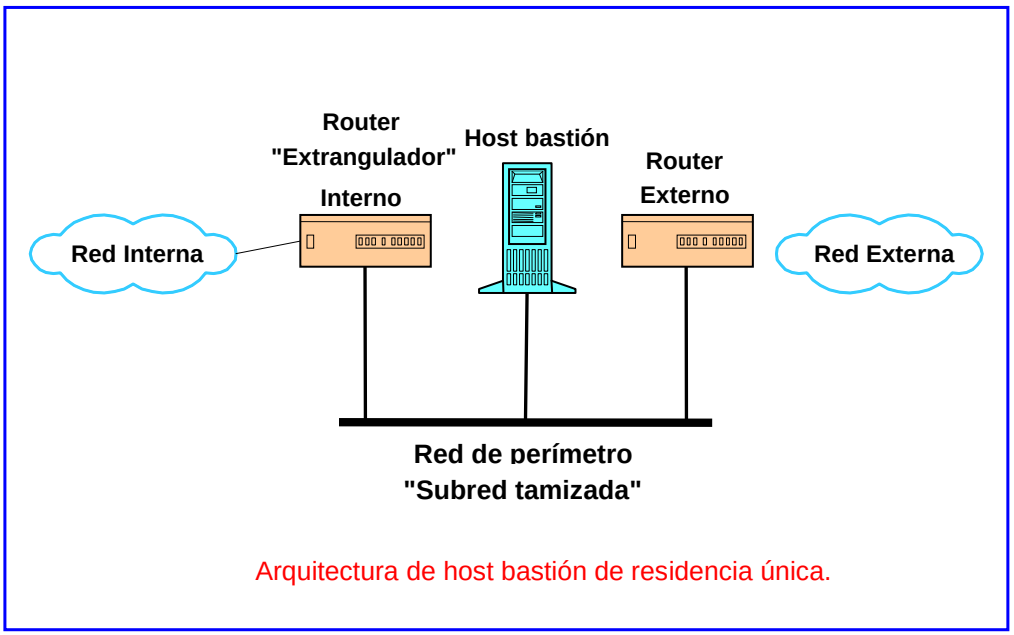


FIG. 2.5 Cortafuegos basados en un host Bastión.

c.- Administración de Cortafuegos.

La interfaz del administrador es una de las principales características de un cortafuegos. Si está bien diseñada puede ayudar a evitar errores de administración que podrían inhabilitar el cortafuegos. Las tres clases de interfaz de administración son:

- Administración basadas en texto.
- Administración basadas en menús de texto.
- Administración basadas en GUI.

La interfaz basada en ficheros de texto es la de uso más extendido en lo que respecta a los routers y a los cortafuegos de cosecha propia. Este tipo de interfaces permite al administrador editar un archivo específico donde puede introducir parámetros de configuración específicos. La desventaja de dicho control a bajo nivel es que resulta mucho más fácil el cometer errores, debido que al editar un fichero, pueden producirse errores de escritura u otros errores técnicos, en un sistema basado en menús, es menos probable que ocurran.

La interfaz de administración basada en menús de texto presenta un menú basado en texto que reduce la probabilidad de producirse errores pero que proporciona menos capacidad de control para el administrador. Sin embargo, la posibilidad de errores no queda totalmente excluída, dado que el administrador no siempre puede ver el efecto de algunos cambios.

La interfaz gráfica de usuario GUI incorpora ventanas, botones menús desplegables y pantallas de ayuda que facilitan el trabajo de configuración. La mayoría de proveedores ha optado por incluir esta interfaz en sus productos, puesto que tiende a ser más fácil de utilizar y no es susceptible a muchos de los errores que pueden producirse en los otros dos tipos de interfaz.

d.- Cortafuegos Basados en Redes

Un cortafuego basado en una red es similar a los cortafuegos basados en premisas. Se diferencia por estar situado en la red de un proveedor de servicios de Internet y por su capacidad para servir a múltiples clientes. Este tipo de cortafuegos

debería superar diversos desafíos antes de convertirse en realidad, como son la exigencia de un mayor rendimiento de procesamiento y la necesidad de impedir el paso. Ver FIG. 2.6.

Como se muestra en la figura 2.6, un cortafuego basado en red está situado en la red del proveedor de servicios de Internet que a su vez está conectado con la organización.

Observe que el cortafuego basado en red deberá contemplar múltiples políticas de seguridad, una para cada cliente, e impedir que estos se mezclen.

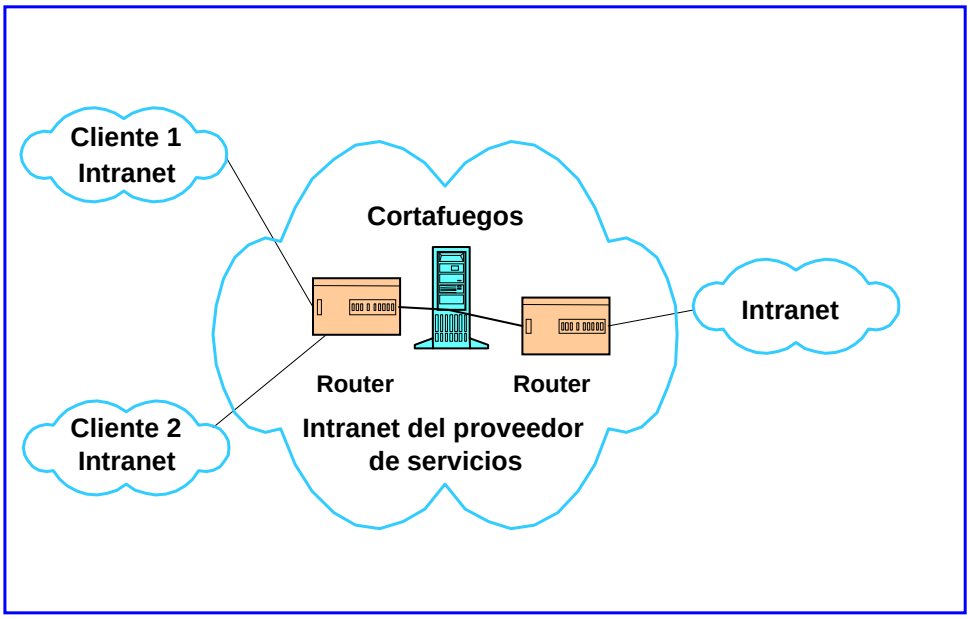


Fig.2.6 Cortafuegos Basados en Redes.

Tendrán que superar dos obstáculos principales antes de hacer realidad. El primero es la velocidad. Debido a que el cortafuego de red habrá de gestionar el trafico de múltiples intranets, deberá soportar un elevado rendimiento total de procesamiento. El segundo es impedir que cualquier router situado entre cliente y el cortafuego pueda evitar y permitir el acceso incontrolado a la intranet de otro cliente.

2.2.3.- ¿ Cómo Funciona Un Cortafuego?

Para saber como funciona un cortafuego hay que entender las tres funciones principales de los cortafuegos que son:

- Control de acceso.
- Autentificación.
- Registro de actividades.

Antes de explicar en detalle cada una de estas funciones principales, conviene considerar primero el recorrido que sigue un paquete a lo largo del cortafuego. Hay tres recorridos habituales según el tipo de cortafuegos instalado. Los paquetes pueden atravesar el cortafuego a nivel de aplicación,

a nivel de Kernel o a nivel de la tarjeta de red. La figura 2.7 muestra los recorridos, además de las ubicaciones del sistema de donde se procesan dichos paquetes.

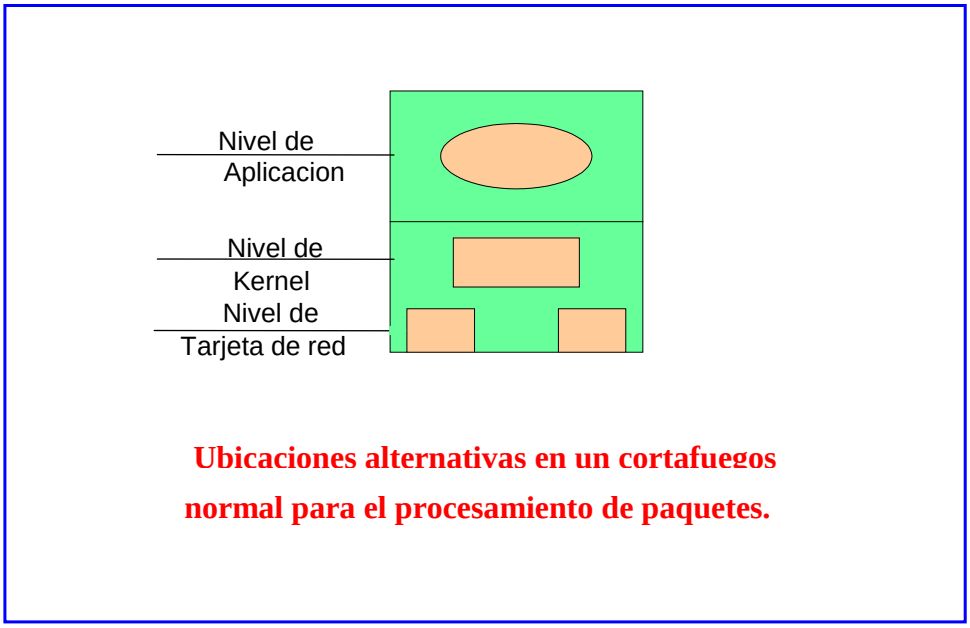


FIG. 2.7 Ubicaciones alternativas.

En el caso de los routers de alta velocidad, el filtrado de paquetes se lleva a cabo en tarjetas de interfaz de red perfeccionadas, provistas de procesadores especializados que optimizan el procesamiento de los paquetes. Para lograr estas velocidades elevadas, los procesadores especializados solamente pueden soportar un procesamiento basado en reglas simples, consistente en comparaciones binarias veloces.

Otros routers y filtros de paquetes basados en hosts procesan los paquetes a nivel del Kernel del sistema operativo en lugar de a nivel de la tarjeta de red. Estos cortafuegos, que se implementan habitualmente en un procesador de propósito general, pueden realizar funciones de filtrado de paquetes y de auditoria más perfeccionadas que las que son posibles a nivel de tarjeta de interfaz de red.

I.- Control de acceso.

Los mecanismos básicos de control de acceso son el filtrado de paquetes y los proxies de aplicaciones. A continuación describimos cada uno de ellos.

a.- Filtrado de paquetes.

El filtrado de paquetes puede llevarse a cabo en cualquiera de las ubicaciones de procesamiento, en general se produce en la tarjeta de red o en el kernel. Un filtro de paquetes examina cada paquete IP y determina, en función de la información de las direcciones de origen y de destino, si dejarlo pasar o desecharlo.

- Reglas de Filtrado

Los filtros de paquetes examinan cinco elementos de información que contiene un paquete IP. Estos elementos de información, conocidos como campos del paquete, se muestran en la tabla 2.2.

CAMPO	PROPOSITO
Dirección IP origen.	Dirección del host del remitente.
Dirección IP destino.	Dirección del host proveedor.
Protocolo de nivel Superior TCP o UDP.	Distintos protocolos ofrecen servicios distintos.
Número de puerto origen TCP o UDP.	Normalmente Un número aleatorio mayor a 1024.
Número de puerto destino TCP o UDP.	Indica un servicio como http.

Tabla 2.2 Campos de interés para el filtrado de paquetes.

En un filtro de paquetes a medida que se reciben los paquetes, los campos específicos en la tabla 2.1 se comparan con un conjunto de reglas especificas de filtrado de paquetes a fin de determinar la acción apropiada que debe llevarse acabo. Una regla de filtrado de paquetes asocia un valor o rango de valores a cada uno de estos campos. Asimismo, especifica la acción autorizar o descartar que debe realizarse cuando todos los campos coinciden.

De este modo, los filtros de paquetes realizan un proceso muy simple y rápido de comparaciones binarias al buscar una coincidencia dentro de una lista de reglas. El Cortafuegos efectúa la acción de la primera coincidencia que encuentra. Por consiguiente, el orden de las reglas tiene gran importancia.

- Filtrado de Sesiones.

Los filtros de sesión son filtros de paquetes especiales que conservan información sobre todas las sesiones activas que atraviesan el cortafuego. El filtro emplea esta información para determinar si los paquetes que fluyen en la dirección opuesta

pertenecen a la conexión aprobada. Asimismo, utilizan dicha información para permitir la auditoria de nivel de sesión.

- Mensajes de Error Para Paquetes Descartados.

Algunos cortafuegos y routers devuelven mensajes de error al host origen para notificar que el paquete recibido ha sido descartado. Esta función emplea el Internet Control Message Protocol (ICMP).

Sin embargo, esa información no se suele retrasmitir al usuario. Pero, cuando sí es retransmitido, no informa a este último del motivo o lugar donde ha fallado la conexión. Esto se debe a los mensajes de error fijos definidos por el ICMP.

b.- <u>Aplicaciones Proxy.</u>

Las aplicaciones proxy son programas que se encuentran en cortafuegos de gateways a nivel de aplicación y que actúan en representación del usuario que solicita el servicio a través del cortafuego. La figura 2.8 ilustra el proceso.

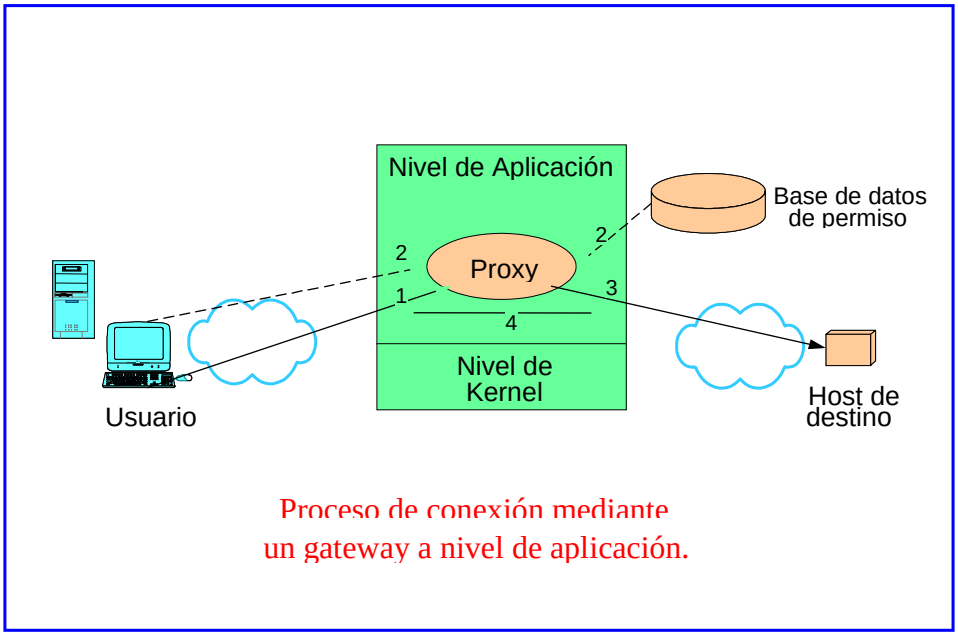


FIG. 2.8 Gateway a nivel de aplicación.

El usuario establece en primer lugar una conexión con la aplicación proxy del cortafuegos (paso 1), que reúne información acerca de la conexión y del usuario solicitante (paso2) y la emplea par determinar si debe autorizarse o no la solicitud.

De aprobarse la conexión, el proxy crea otra conexión desde el cortafuegos hacia el destino previsto (paso 3).A continuación, el proxy transmite los datos del usuario desde una conexión a otra (paso 4).

- Conexión Directa

El primer método utilizado en un sistema de aplicación proxy consiste en que el usuario debe conectarse directamente al proxy del cortafuegos utilizando la dirección de este y el número de puerto del proxy.

El proxy solicita entonces al usuario la dirección del host al que desea conectarse. Este en un método abrupto que empleaban los primeros cortafuegos y por diversas razones es el que goza de menos preferencias.

En primer lugar, la técnica obliga a los usuarios a conocer la dirección del cortafuegos. Asimismo, precisa que el usuario introduzca dos direcciones para cada conexión: la del cortafuegos y la del destino deseado.

Por último, impide a las aplicaciones o programas del computador del usuario realizar conexiones por el usuario, dado que desconocen la forma especial con que deben comunicarse con el proxy.

II.- Auditorias.

En función de un conjunto de reglas o de un archivo de permiso de una aplicación proxy se autoriza la conexión entre dos partes.

Recuerde que una estrategia de ataque básica a una red consiste en averiguar cuales son los puntos vulnerables de la misma. De concederle tiempo suficiente, un atacante persistente puede encontrarlo. Como verá, la auditoría es la mejor defensa contra estos tipos de ataques.

a.- Registro de Actividades.

A fin de proporcionar a un administrador información sobre la actividad de una red, la mayoría de cortafuegos registran y guardan información de dicha actividad en archivos de disco.

He aquí la información estándar que ofrecen los registros de auditoria o archivos de registro:

- Hora y fecha del inicio de sesión.

- Hora y fecha del fin de sesión.
- Dirección del host origen.
- Dirección del host destino.
- Protocolo (TCP o UDP).
- Puerto de destino (servicio solicitado).
- Acción realizada (conexión aceptada o denegada).
- Nombre del usuario si se ha efectuado una autentificación.

Algunos registros de auditoria incluyen el número de paquetes que se ha hecho pasar durante la sesión. Los administradores pueden revisar la información de auditoria en busca de actividades sospechosas como:

- Repetidos accesos infructuosos hacia servicios distintos desde un host.
- Conexiones efectuadas a horas de la noche.
- Múltiples intentos de autentificación infructuosos.

b.- Alarmas.

Las alarmas son condiciones configuradas que al activarse, desencadenan una acción definida, como el envío de un mensaje

de correo electrónico al administrador, la presentación de un mensaje en la consola, incluso, una llamada telefónica a un aparato buscapersonas. Las alarmas son útiles para alertar a un administrador de un posible ataque antes de que este ocasione cualquier daño.

2.2.4.- ¿Qué Características son importantes?

No existe un conjunto de características estándar para los productos cortafuegos. Las características se corresponden con la política de seguridad y con los controles de seguridad establecidos.

I.- Requisitos de Seguridad.

Ningún conjunto de características puede ser en abstracto el más adecuado para todos los entornos. Las características que se seleccionan para el cortafuegos deben basarse en los requisitos propios y exclusivos del posible usuario. Los factores importantes para la elección de las características de un cortafuego son:

- La importancia de la amenaza para la red.

- Las perdidas potenciales que podría causar un intruso con su entrada en la red.

- Otros mecanismos de seguridad empleados para proteger la red y los recursos de la misma.

- Las perdidas que supondrían para la compañía u organización un fallo del cortafuegos y que este impidiera cualquier acceso hacia o desde Internet por un fallo de hardware o de software o que el propio cortafuegos sufriera un ataque de negación de servicio.

- Los servicios que se desea soportar hacia y desde internet. Todos los servicios, como Telnet o correo electrónico, conllevan riesgos exclusivos a los mismos.

- Los requisitos de rendimiento de procesamiento para la conexión, es decir, el número de usuarios que atravesarán simultáneamente el cortafuego.

- La capacidad y competencia de sus administradores de Cortafuegos. Según sean estas, tal vez debiera optar por un Cortafuego fácil de administrar.

- Los requisitos futuros potenciales, es hacer frente a un aumento de la actividad a través del cortafuegos o la implementación de nuevos servicios internet solicitados por los usuarios.

II.- Control Básico de Acceso.

La función primordial de un cortafuegos es controlar el acceso a la red en función de la dirección del host y del servicio solicitado. Algunas características son:

a.- Reglas / Listas de Acceso.

Los cortafuegos de filtrado de paquetes o de sesiones emplean reglas de acceso para definir el control básico de acceso desde y hacia la red, las reglas de acceso pueden soportar cualquier servicio, esto es así porque, para una regla de acceso, un servicio es simplemente un número.

Los cortafuegos a nivel de aplicación emplean dos tipos de listas de acceso: las basadas en los hosts y las basadas en los servicios. Las primeras describen los conjuntos de servicios autorizados para cada host o red. Las segundas identifican los conjuntos de hosts o redes que pueden utilizar cada uno de los servicios.

b.- Filtro de sesiones.

Los filtros de sesiones son filtros de paquetes que mantienen información referente a cada sesión para permitir a los primeros tomar decisiones más inteligentes y, por tanto, más seguras.

Los cortafuegos de aplicaciones no necesitan esta seguridad porque trabajan a un nivel incluso más alto.

c.- Controles de suplantación de hosts.

Los controles básicos de acceso emplean una dirección IP no autentificada para identificar al solicitante. Sin embargo, esto deja una puerta abierta para los atacantes que utilicen la

dirección IP de un host interno de confianza. Los controles son dos:

- La restricción de la “opción de la ruta origen” permite a un host controlar la ruta emprendida para regresar a la dirección del host origen. Cualquier cortafuego debería permitir desactivar la opción de la ruta origen.

- La posibilidad de ejercer el control a través de la interfaz de la red puede ayudar también a reducir los casos de suplantación de direcciones IP. La inclusión de la identificación de la interfaz de red en la regla o en la lista de acceso garantiza que un host de internet no pueda pretender ser un host de la red interna. Se debe poder permitir a un host el acceso a través del cortafuegos en función de la interfaz de red desde la que se recibe el paquete.

III.- <u>Servicios Soportados.</u>

Los servicios de uso más generalizados que se soportan desde y hacia internet, se refieren a los protocolos a nivel de

aplicación que el cortafuegos reconoce y autoriza. Es muy importante que los cortafuegos nieguen cualquier servicio que no puedan reconocer.

La lista de los servicios incluidos a continuación puede darle una idea del conjunto de servicio mínimo que puede solicitarte a un gateway a nivel de aplicación.

a.- DNS (Protocolo TCP o UDP, numero de puerto 53*).*

El Domain Name System (DNS) no es un servicio que utilicen directamente los usuarios.

Los servidores DNS comparten información. Es precisamente esta capacidad de la que debemos protegernos, pues no es deseable que ningún servidor DNS de internet pueda actualizar los nombres de servidor de la red propia. En una situación de este tipo, los atacantes pueden redefinir la dirección de un host de confianza de la red con la dirección de un host externo a esta que se encuentre en internet. Además, un servidor DNS interno puede compartir información, como nombres de host, que es preferible mantener reservada del exterior.

El cortafuego debe permitir a los servidores DNS de la red propia el acceso a servidores de nombre del exterior e incluso su actualización con direcciones nuevas negando a los servidores DNS externos poder actualizar los servidores de nombres propios. Algunos cortafuegos incorporan una función de DNS dividido que proporciona la información apropiada para cada uno de los lados del cortafuego. Esta característica permite proporcionar únicamente la información mínima que precisan los hosts de internet. Los cortafuegos a nivel de aplicación desprovistas de la capacidad de un proxy invisible, no necesitan soporte DNS.

b.- Finger (Protocolo TCP, Puerto79).

El servicio finger es desarrollado para permitir a los usuarios de una red poder localizar a otros usuarios. Gracias a finger es posible averiguar nombres de entrada en el sistema (login), nombres reales de los usuarios e información referente a la última entrada al sistema por parte de un usuario. Esta es una información valiosa para un intruso potencial, por lo que el cortafuegos debe prohibir cualquier solicitud de finger procedente del exterior. La amenaza que suponen las

peticiones de finger hechas al exterior es menor. Un proxy de finger situado en el cortafuego puede autorizar solicitudes de finger hacia el exterior y bloquear las peticiones entrantes.

c.- FTP (Protocolo TCP, Puerto numero 21*).*

FTP son las siglas de file transfer protocol (protocolo de transferencia de archivos). Se trata del protocolo estándar para transferir archivos entre sistemas. Soporta la autentificación sencilla de contraseñas, que puede evitarse o escribirse en un programa de secuencias mediante un archivo de configuración estándar de FTP en el host origen. Para cada archivo FTP o transferencia de información, se establece habitualmente una conexión de red aparte desde el host de destino hacia el host desde donde se origina la conexión FTP. El cortafuegos debe ser capaz de permitir esta segunda conexión en el sentido inverso o de lo contrario no se transferirán los datos. Por lo general, un puerto origen TCP de 20 identifica la conexión de datos.

Algunos clientes FTP y la mayoría de servidores FTP soportan una función PASV (modo pasivo), que permite a la conexión

de datos originarse desde el cliente en lugar de desde el servidor. El proxy FTP debe poder soportar ambos tipos de conexión.

d.- Gopher (Protocolo TCP, Puerto número 70 y otros).

El protocolo y servicio gopher proporciona un sistema sencillo de menú textuales cuya función es ayudar a encontrar información en Internet.

e.*- ICMP (Protocolo ICMP*).

Internet Control Message Protocol(ICMP) es un protocolo soportado por encima de IP a nivel de TCP o UDP, IP lo utiliza para enviar mensajes de error o de prueba entre sistemas distintos. Un mensaje ICMP contiene campos de tipo y de código que indican un mensaje predefinido como “no se puede contactar con la red” o “acceso negado para propósitos de administración”. La conocida aplicación de prueba ping emplea el protocolo ICMP para enviar mensajes de petición de eco (ICMP tipo 8, código 0) para comprobar si es posible acceder a un host. El host destino responde con un mensaje de

respuesta de eco (ICMP tipo 0, código 0). El cortafuegos puede configurarse para permitir algunos mensajes ICMP y negar otros.

f.- IRC (TCP,Puerto número 6667).

La aplicación Internet Relay Chat (IRC) ofrece la posibilidad de participar en conferencias con múltiples usuarios en un entorno de texto. Con una aplicación IRC cliente, un usuario puede ponerse en contacto con un servidor IRC y unirse a una conversación.

La principal amenaza asociada a este servicio es inherente al protocolo y representa una amenaza de ingeniería social.

Entre otras cosas, la ingeniería social es el acto que puede perpetrar un atacante para obligar a un usuario o administrador a que proporcione información de autentificación o a que reduzca los controles de seguridad.

Un proxy IRC situado en el cortafuegos no tiene una gran utilidad para contrarrestar esta amenaza.

g.- Mail (Protocolo TCP, Puerto número 25).

Mail, o “e- Mail”, es el servicio más utilizado en Internet. Permite a los usuarios enviar mensajes sin que sea necesario establecer una conexión directa entre el host remitente y el host destinatario. Un mensaje de correo puede recorrer un gran número de “agentes de transferencia de correo“ antes de llegar a su destino. El protocolo de correo estándar que se emplea en internet es el Simple Mail Transfer Protocol (SMTP).

h.- Network News (Protocol TCP, Puerto numero 119).

Permite a los usuarios acceder a newsgroups a fin de leer información o de participar en debates.

Los newsgroups constan de una serie de mensajes que tienen un tema común. Existe un newsgroups para prácticamente cualquier tema imaginable.

El protocolo empleado es el network News Transfer Protocol (TNP).

i.- NFS (Protoclo UDP, Puerto numero 2049).

Network File system (NFS) permite a los usuarios compartir sistemas de ficheros con otros usuarios. El NFS estándar proporciona muy poca seguridad y, por este motivo, es muy vulnerable a los ataques. De todos modos, los gateways a nivel de aplicación no soportan habitualmente este servicio y el filtrado de paquetes no elimina el riesgo que conlleva el mismo.

j.- NTP (Protocolo UDP, Puerto numero 123).

Network Time Protocol (NTP) es un servicio que se emplea para sincronizar relojes entre computadoras. Los clientes se ponen en contacto con servidores NTP para conocer la hora correcta y estos, a su vez, se comunican con otros servidores NTP a fin de seguir sincronizados.

k.- PORT MAPPER (Protocol TCP o UDP, Puerto numero 111).

Las aplicaciones Remote Procedure Call (RPC) emplean un asignador de puerto para obtener el número de puerto TCP o

UDP actual de un servidor. Las aplicaciones servidor utilizan números de puerto conocidos. Sin embargo, esto no es siempre cierto. Algunas aplicaciones servidor pueden ejecutarse en cualquier número de puerto y depender de la aplicación del servidor de asignación de puerto para dirigir los clientes hacia el número de puerto apropiado.

Esto dificulta enormemente la posibilidad de que el cortafuegos pueda realizar el filtrado o establecer un proxy para dichas aplicaciones, puesto que el número de puerto de las mismas puede cambiar en cualquier momento, además de diferir de un sistema a otro.

I.- Rlogin (Protocolo TCP, Puerto numero 513*).*

El comando rlogin (login remoto) forma parte de un conjunto de comandos que gozan de gran aceptación y dicho conjunto es conocido como la serie “r”, donde “r” significa remoto. Estos comando son útiles para acceder de un sistema local a otro, pero no se recomienda su uso para acceder a/o desde Internet porque la mayoría de ellos no soportan funciones adecuadas para la autentificación de usuarios. De hecho, existe una

característica destinada específicamente a proporcionar acceso no autentificado a los usuarios en función de la dirección del host de estos. Otros comandos “r” incluyen rcp (copia remota), rsh (shell remoto), que utilizan el puerto TCP 514, y rexec (ejecución remota), que emplea el puerto TCP 512.

m.- Telnet (Protocolo TCP, Puerto número 23).

Telnet es el protocolo y aplicación estándar para la entrada (login) en sistemas remotos. Proporciona una conexión entre dos sistemas basados en caracteres. Todos los cortafuegos de gateways basados en aplicaciones soportan este proxy. Muchos de ellos pueden además autentificar el usuario Telnet en el cortafuegos.

n.- SNMP (Protocolos TCP y UDP, Puerto 161 y 162).

Simple Network Management Protocol (SNMP) es el protocolo que emplea una estación gestión para supervisar y configurar dispositivos de red como routers, puentes, hubs y hosts. Los dispositivos de red escuchan en el puerto 161 a la espera de órdenes procedentes de la estación gestión de la red.

La estación de gestión de la red escucha en el puerto 162 a la espera de trampas, es decir, alarmas procedentes de los dispositivos de la red.

La versión 1 de SNMP es un protocolo que está extensamente implementado, pero no incluye funciones robustas de autentificación. Los dispositivos de red responden a las peticiones que reciben, además de reconfigurarlas. Por este motivo, un gran número de dispositivos de red están configurados para proporcionar solamente información de estado y desautorizar cualquier intento de reconfigurar procedente de la red.

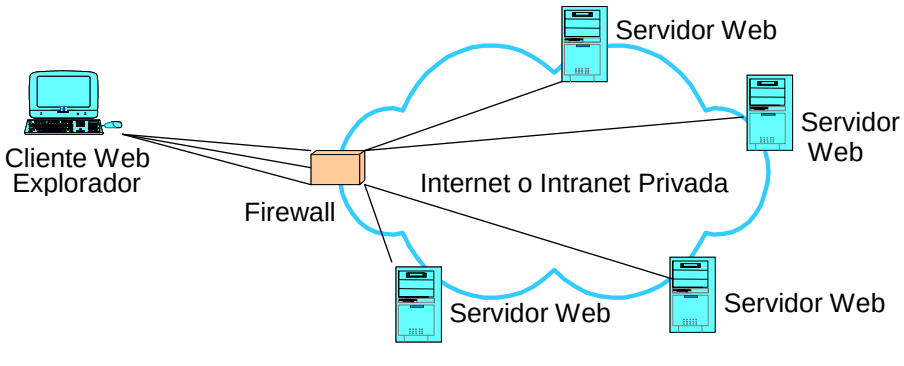
La versión 2 estándar de SNMP soporta funciones de autentificación robustas. Lamentablemente, esta nueva versión ha tardado mucho en aparecer. Por este motivo los cortafuegos no deberían permitir a los paquetes SNMP entrar en la red interna.

o.- WWW (Protocolo TCP, Puerto numero 80 y otros*).*

Probablemente, la Word Wide Web (WWW) es la principal

responsable del repentino interés y expansión que ha experimentado internet actualmente El principal protocolo de servicio empleado por la Web es el Hypertext Transfer Protocol (http), que permite a los usuarios transferir documentos desde un servidor HTTP. Este protocolo está soportado por aplicaciones clientes gráficas conocidas como navegadores.

No es una red aparte, sino un conjunto de servidores de información repartidos por internet o por una intranet, accesibles mediante aplicaciones cliente, es decir, navegadores con el fin de obtener datos, que pueden ser texto, imágenes, sonidos, videos u otros formatos multimedia. La figura 2.9 incluye un esquema de la web.



La World Wide Web permite intercambiar datos en cualquier formato.

FIG. 2.9 La World Wide Web.

p.- X11 (Protocolo TCP, Puerto numero 6000 y superiores*).*

X11 se refiere a la especificación correspondiente al entorno gráfico de usuarios, de uso generalizado en estaciones de trabajo UNIX. La mayoría de servidores X soportan más de un puerto Xserver 6001, y es posible emplear números de puerto superiores a este último.

El protocolo X11 es un servicio muy potente que permite a una aplicación remota presentar gráficos y aceptar órdenes de un ratón en una estación de trabajo X o en un PC que soporta una interfaz Xwindows. Sin embargo, esta potencia se proporciona a expensas de un cierto riesgo para la seguridad.

La aplicación remota pueda tomar completamente el control de la pantalla, del teclado e incluso del ratón. Si tiene previsto establecer conexiones X11 desde Internet, el cortafuegos debe poder soportar este tipo de operaciones, además de filtrar las conexiones o comandos X11 no deseados.

IV.- Administración.

Con una política de seguridad lo suficiente hermética y un cortafuegos eficaz, el mayor riesgo de penetración en la red provendrá de un error humano del administrador del cortafuegos. Los cortafuegos pueden incorporar un gran número de funciones, que complican su trabajo de administración. Los cortafuegos que cuentan con una buena interfaz de administración reducen la posibilidad de errores humanos y simplifican el trabajo del administrador del cortafuegos.

a.- Interfaz del Administrador.

Los primeros cortafuegos utilizaban ficheros de texto para almacenar la información de la configuración. Este sistema era apropiado para cortafuegos que poseían pocas funciones y que eran mantenidas por administrador que probablemente habían desarrollado el cortafuego desde cero o a partir de un paquete de utilidades. Sin embargo, la mayoría de compañías no disponen del tiempo ni del personal necesario para gestionar cortafuegos de este tipo.

b.- Administración remota/ centralizada.

Muchas compañías cuentan con múltiples puntos de acceso a internet. Hay dos razones principales: en primer lugar, la separación geográfica entre las distintas plantas de la compañía y, en segundo lugar, por la necesidad de disponer de un acceso de respaldo en el caso de avería de algunos de los puntos de acceso. Cada uno de estos puntos de acceso precisa de un cortafuego como protección. Con el fin de asegurar un cumplimiento sólido y consistente de la política de seguridad de la compañía, estos cortafuegos deben ser administrados por un sólo grupo.

Una alternativa preferida a la administración remota es la administración centralizada. En esta, el administrador configura los cortafuegos desde una base de datos central compartida por todos ellos. La base de datos se distribuye en cada cortafuego de forma segura. La administración centralizada requiere menos trabajo porque solamente es necesario introducir una sola vez los parámetros comunes a todos los cortafuegos. Además, reduce la posibilidad de que

se produzcan variaciones no deseadas en la configuraciones de los cortafuegos.

V*.- <u>Auditorias y alarmas</u>*.

Los registros de auditoria son una herramienta eficaz para evaluar la política de seguridad que ofrece el cortafuegos y para determinar que aspectos son susceptibles de mejora.

Como mínimo, el cortafuegos debe registrar las direcciones del host origen y del host destino, el protocolo, los puertos de aplicación, la hora y la duración del acceso y la acción realizada. Asimismo. Debe incorporar un método para revisar el archivo de auditoria o el registro correspondiente a las 24 horas previas y a una semana anterior. Deberíamos poder examinar el registro de auditoria. Además, el cortafuegos debe poder archivar los archivos de auditoria en medios de almacenamiento extraíble como son las cintas o disquetes.

Las alarmas permiten a los administradores de cortafuegos asignar una acción específica a un evento identificado. Estas son conocidas como alarmas de tiempo real cuando se generan

al cabo de un periodo breve de tiempo, es decir, unos segundos.

Una característica de alarma más potente consiste en incorporar un mecanismo o lenguaje para la detección de alarmas. Esto permite que las alarmas sean más perfeccionadas y detectar los eventos relacionados con diversos accesos o intentos de acceso. Por ejemplo, quizás no se desee crear una alarma cada vez que se niega a un host el acceso a la red propia; no obstante, si que seria útil crear una alarma cuando un host ha intentado repetidamente acceder a la red.

Las acciones efectuadas a partir de eventos de alarma varían de un cortafuego a otro. Estos eventos incluyen:

- Registrar la acción en un fichero de registro o alarma.
- Enviar un mensaje por correo electrónico al administrador.
- Presentar un mensaje en la consola del cortafuegos.
- Enviar una ventana de alarma a un terminal Xwindows.
- Enviar una alarma SNMP a un sistema de gestión de red.

- Activar y enviar un mensaje en busca de llamadas del administrador.
- Ejecutar en el cortafuegos una aplicación o fichero de secuencias de comandos.

Vi.- Integridad del Cortafuegos.

El cortafuego es el guardián de la red y de los valiosos recursos que esta contiene. Si el cortafuegos puede ser atacado con éxito, el pirata informático tendrá las llaves de entrada a la red. Las características de integridad que analizamos a continuación proporcionan un concepto de seguridad estratificada que impide que el cortafuego sufra un ataque en el caso de errores de diseño o de administración.

a.- Sistema operativo Reforzado.

Un sistema operativo reforzado es aquel que ha sido diseñado con características especiales y sometido a rigurosas pruebas de resistencia de ataque.

El mecanismo fundamental consiste en utilizar una versión básica del sistema operativo, eliminando todo el software y componentes del mismo innecesarios para las funciones del cortafuegos.

Todos los administradores coinciden en que un cortafuegos debería incorporar en su diseño múltiples niveles de seguridad. Un sistema operativo reforzado puede ser uno de esos niveles.

b.- Cortafuegos Basados en Sistemas Host Duales.

Si el cortafuego está construído sobre un sistema operativo no reforzado, es posible repartir las funciones del mismo entre los hosts. Esta disposición obliga a los piratas informáticos a entrar en dos sistemas para que su ataque tenga éxito, para lo cual se emplea habitualmente una conexión especial que dificulta extraordinariamente el poder entrar en el segundo sistema, aún cuando haya sido posible entrar en el primero.

Este enfoque se conoce en ocasiones como cortafuegos basados en gateways a nivel de circuito. Otra implementación

de este mecanismo es utilizar un router de filtrado delante de un host que contiene un cortafuegos a nivel de aplicación. Dado que este sistema limita el tráfico que puede soportar el cortafuegos, muchos de los ataques mas habituales no consiguen llegar al mismo.

c- Explorador de Integridad.

Un explorador de integridad es una aplicación incluida en el cortafuegos que lo explora continuamente en busca de cambios no autorizados en archivos o dispositivos. Este mecanismo de seguridad se encuentra frecuentemente en los servidores de red. La aplicación registra una suma de comprobación o un hash seguro para cada archivo protegido que existe en el sistema. Cuando se modifica un archivo, la suma de comprobación o el hash seguro hacen lo propio. A intervalos regulares, el explorador de integridad calcula nuevamente la suma de comprobación o hash seguro para asegurarse de que el archivo no ha experimentado ningún cambio. Si la aplicación detecta cualquier cambio no autorizado, activa un determinado tipo de alarma.

d.- Invisibilidad

Los cortafuegos basados en el filtrado de paquetes y de sesiones son invisibles a los usuarios finales, debido a que no tienen una dirección directa y los paquetes no son enviados a la capa de aplicación. Los cortafuegos basados en aplicaciones más recientes soportan actualmente una nueva característica que se conoce como proxy invisible. Estos cortafuegos tampoco poseen un dirección directa y tienen la apariencia de routers, con la excepción de que los paquetes se envían a la capa de la aplicación para ser procesados.

Aun así todos estos cortafuegos siguen teniendo una dirección IP, por lo que un pirata informático experimentado podría acceder a ellos. Una nueva característica de los cortafuegos consiste en no tener una dirección IP y funcionar simplemente a nivel de LAN a fin de recibir y trasmitir paquetes. Esto proporciona un nivel de seguridad adicional y disminuye el tamaño del software del cortafuegos encargado de la gestión de los paquetes, lo cual reduce la posibilidad de producirse un fallo en el mismo.

VII.- Características Especiales.

Los cortafuegos que pueden adquirirse en el mercado presentan e incorporan nuevas características a un ritmo veloz. Aquí discutimos algunas características especiales.

a.- Correlación de Direcciones.

Antes de producirse el auge de Internet, muchos organizaciones poseían redes privadas desprovistas de una conexión con otras redes. Como estaban aisladas, no tenían que solicitar a las autoridades de Internet direcciones de red no utilizadas. En lugar de ello, escogieron cualquier clase de dirección IP que les apetecía. Con el advenimiento de la Internet como parte de la infraestructura global, estas organizaciones han comenzado con conectarse a Internet y no podrán utilizar las mismas direcciones por que probablemente habían sido asignadas a otro usuario.

Una solución consistirá en que el cortafuegos correlacionará direcciones origen ilegales con direcciones legales en el momento que abandona la intranet interna.

En esta situación, es necesario cambiar la dirección de destino de los paquetes de retorno o restaurarla a la dirección original. La mayoría de gateways a nivel de aplicación no precisan esta característica, conocida como correlación de direcciones, porque todo el tráfico de salida emplea habitualmente la dirección del cortafuegos a nivel de aplicación.

Algunos cortafuegos son capaces también de correlacionar direcciones de destino o puertos de origen y destino TCP y UDP. Estas características avanzadas pueden utilizarse para redirigir conexiones de entrada al vuelo hacia otros proveedores de servicios o para poner trampas a los piratas informáticos.

b.-Control de la Carga.

El control es otra nueva característica que ofrecen algunos cortafuegos. Para la mayoría de estos, cuando se permite el acceso, el host o la red pueden efectuarse un número ilimitado de conexiones. Es útil poder establecer limitaciones al número de conexiones simultáneas con un host o una red de hosts que

puede haber activas. Esta característica puede ayudar a impedir ataques por “ inundación”, mediante los cuales un pirata informático inunda la red con conexiones a fin de ocultar el ataque real.

c.- Canalización.

La canalización es la capacidad de combina múltiples servicios de aplicación en una única conexión. Un cortafuegos puede proporcionar también la característica de canalización para permitir a dos sitios de un compañía compartir servicios en Internet que no serian autorizados normalmente a través del mismo. Los paquetes NFS pueden enviarse a través de una conexión existente y autorizada entre los dos sitios. Estas conexiones emplean a menudo sistemas de autentificación especiales par autorizar el establecimiento de la canalización. Algunos cortafuegos ofrecen canales cifrados para conseguir la máxima protección.

d.- Redes Privadas Virtuales

Algunas compañías desearían utilizar Internet como canal de

comunicación entre dos sitios sin embargo, debido a la inseguridad de Internet y la confidencialidad de las comunicaciones entre las distintas sucursales, estas compañías desearían gozar de protección adicional. Algunos cortafuegos permiten cifrar todas las comunicaciones, o algunas de ellas, entre dos o más sitios. Esta característica, conocida como red virtual privada (VPN), precisa que hayan un convenio entre los cortafuegos par cifrar o descifrar los paquetes a medida que se envían y reciben. Además en el caso de haber un gran número de sitios, tal vez sea necesario un sistema de gestión de claves de encriptación para distribuír automáticamente las nuevas claves de encriptación a medida que se necesitan.

2.3.- FIREWALL EN REDES PRIVADAS VIRTUALES.

La criptografía también es importante para permitir la comunicación encriptada entre distintos cortafuegos. Estas comunicaciones criptográficas permiten crear redes virtuales privadas que pueden utilizarse en el intercambio seguro de información de dirección. Estas redes adquieren especial importancia en el contexto de las intranet provistas de

múltiples puntos de entrada y, por ende, de múltiples cortafuegos que necesitan conectarse entre sí. En un gran número de entornos, la gestión de los cortafuegos de una red se lleva a cabo desde una ubicación de administración remota y centralizada al igual que un centro de gestión de red, en lugar de ser una sesión distribuída y negociada entre un grupo de cortafuegos. En este tipo de disposiciones, las comunicaciones criptográficas desempeñan un útil papel al proteger la seguridad de los canales que van desde la gestión centralizada hasta los cortafuegos de la arquitectura.

de servicios de red. La mejor definición de red privada virtual es la siguiente.

Es un proceso de comunicación cifrado o encapsulado que transfiere datos desde un punto hacia otro de manera segura; la seguridad de los datos se logra gracias a una tecnología robusta de cifrado, y los datos que se transfieren pasan a través de una red abierta, insegura y enrutada.

Esta definición revela varias cosas. Primero, una VPN es un proceso de comunicación cifrada o encapsulada. Cualquier comunicación entre dos nodos está cifrada y es el mismo proceso de cifrado lo que garantiza la seguridad y la integridad de los datos. Notará que los datos pasan a través de una red abierta, insegura y enrutada. De esta manera, a diferencia del circuito virtual en el ejemplo de la llamada telefónica, los datos de la VPN pasan a través de una línea compartida, y los datos en si pueden tomar muchas rutas hasta su destino final.

Las VPN también pueden utilizarse en las líneas rentadas, enlaces ATM/Frame Relay (retransmisión de tramas) o servicios de red telefónica simple (POTN), como las redes digitales de

servicios integrados (ISDN) y las líneas de suscrición digital (XDSL).

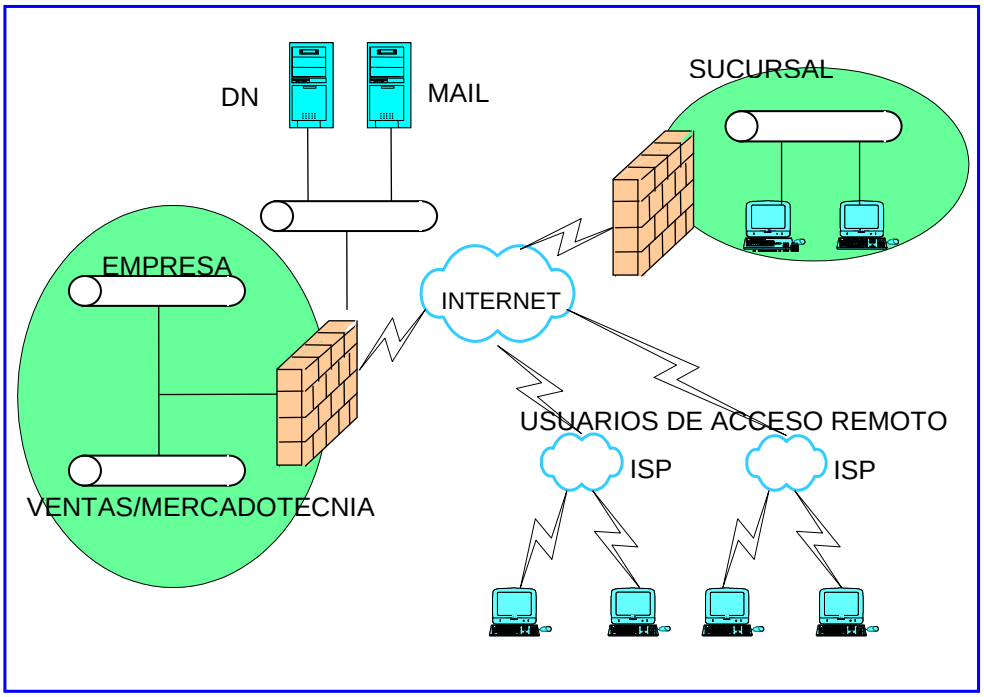


FIG. 3.1 Una VPN Corporativa.

La figura 3.1 muestra una red corporativa conectada a una red pública como transporte, una ubicación común utilizada en las tecnologías de VPN actuales. Notará que Internet se utiliza como la compañía de transporte de la tecnología VPN, pero la nube Internet podría reemplazarse fácilmente por una nube ATM o de retransmisión de tramas.

La figura 3.2 ilustra otra configuración de VPN con un sistema heredado.

Las VPN dependen del cifrado, y la mayoría del software de cifrado no está escrito para este tipo de sistemas heredados.

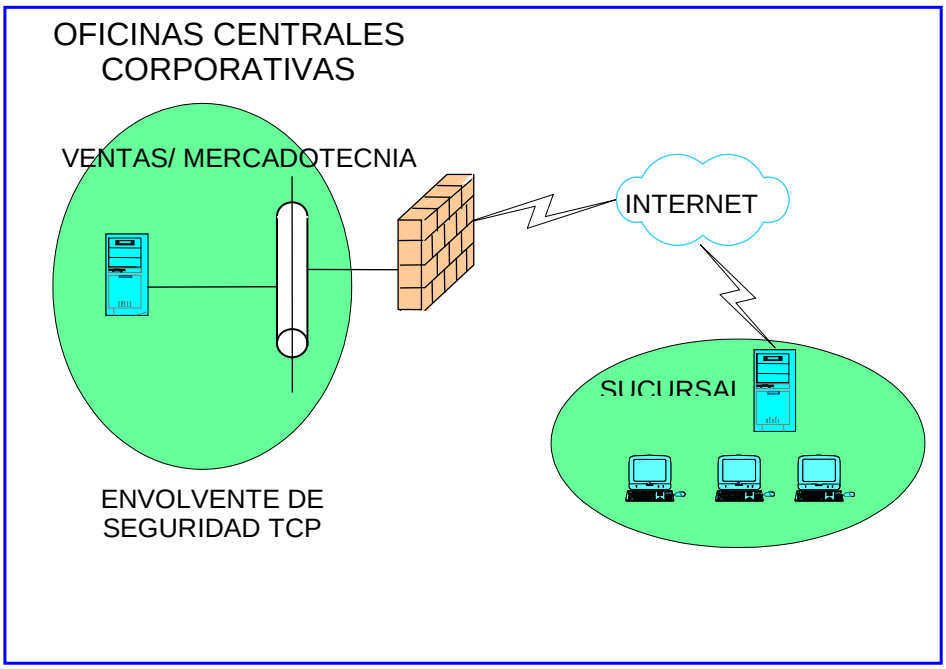


FIG. 3.2 VPN corporativa con sistema mainframe heredado.

Una gran característica de la tecnología VPN es su facilidad de ampliación. Conforme los proveedores de red incrementan el ancho de banda en sus redes de columna vertebral, las VPN pueden crecer y aprovechar este ancho de banda adicional, además, puesto que las VPN son independientes de la

plataforma y no dependen de ningún sistema operativo en particular, casi cualquier dispositivo en su compañía puede funcionar como cliente o como servidor de la VPN. Las VPN también dan cabida al crecimiento; muchos dispositivos de VPN manejarán cualquier servicio que se coloque en ellas. Le permitirán crear “túneles” o comunicaciones punto a punto con cifrado, bajo demanda podrá crear túneles hacia otros sitios, como uno que valla de las “oficinas centrales corporativas hasta las oficinas principales de venta” y más adelante podrá crear más túneles hacia otras oficinas.

El encapsulamiento es el proceso de tomar un paquete de datos y envolverlo dentro de un paquete IP.

I.- <u>Las VPN se presentan en 4 áreas.</u>

Las áreas simplemente significan implementaciones comunes de VPN.

a.- Intranets. Una VPN de Intranet se crea entre la oficina central corporativa y una oficina de ventas remota, o entre las oficinas centrales y las oficinas dependientes. La fig. 1.3,

ilustra una Intranet típica la única diferencia es que se tiene acceso a la Intranet desde fuera de la red, lo que significa que el acceso viene desde el exterior. Normalmente, solo se utiliza dentro de la red de una compañía y únicamente acceden los empleados de la misma. A una VPN de Intranet puede ser solo para acceso de los empleados, pero el acceso viene desde el exterior y no desde el interior.

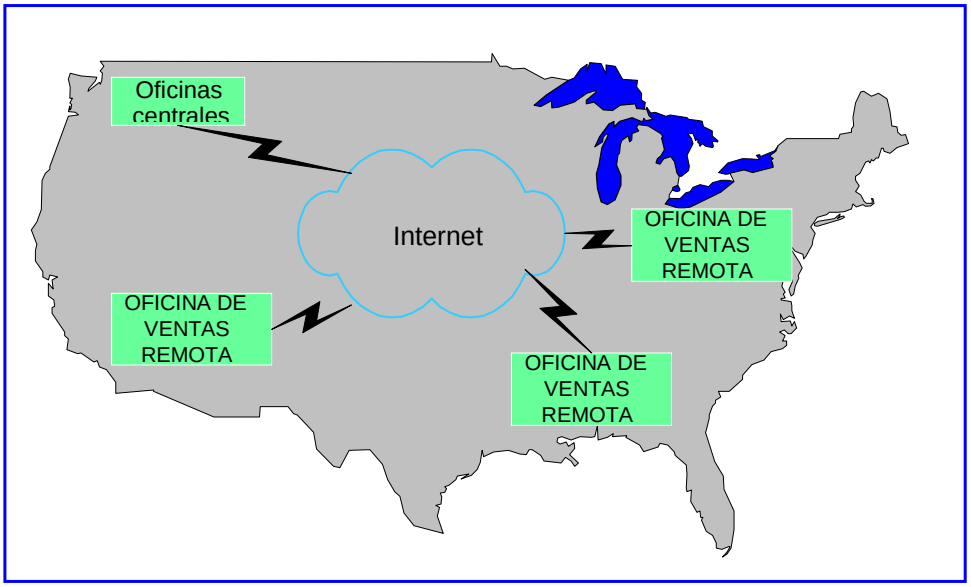


FIG. 3.3 Una PVN de intranet.

b.- Acceso remoto. Una VPN de acceso remoto se crea entre las oficinas centrales y los usuarios móviles remotos. Con el software de cifrado cargado en una laptop, un individuo

establecerá un túnel cifrado al dispositivo de las VPN en las oficinas centrales corporativas.

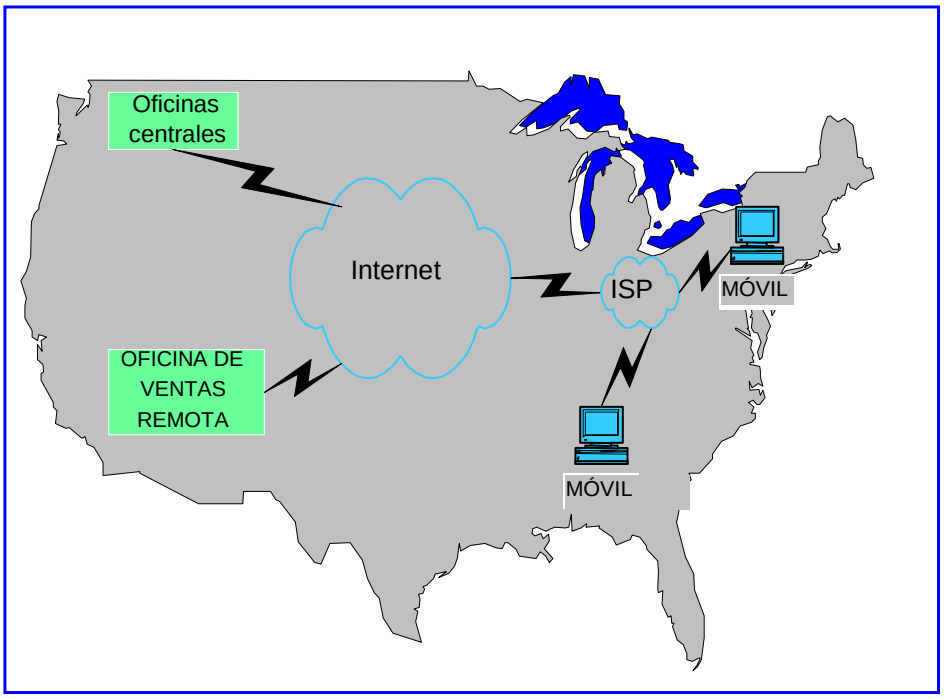


FIG. 3.4 Una VPN de acceso remoto.

c.- Extranet. Una VPN de extranet se crea entre la empresa y sus clientes o proveedores. En la figura 3.5, la extranet permitirá el acceso con el protocolo http normal utilizado por los navegadores Web actuales o permitirá que se realice la conexión utilizando otro servicio y protocolo acordado por las partes involucradas. Aquí es donde el comercio electrónico tiene su mayor impacto.

Esta configuración le dará a la empresa la capacidad para realizar transacciones de manera segura y efectiva con sus principales socios comerciales y con clientes que generan ingresos.

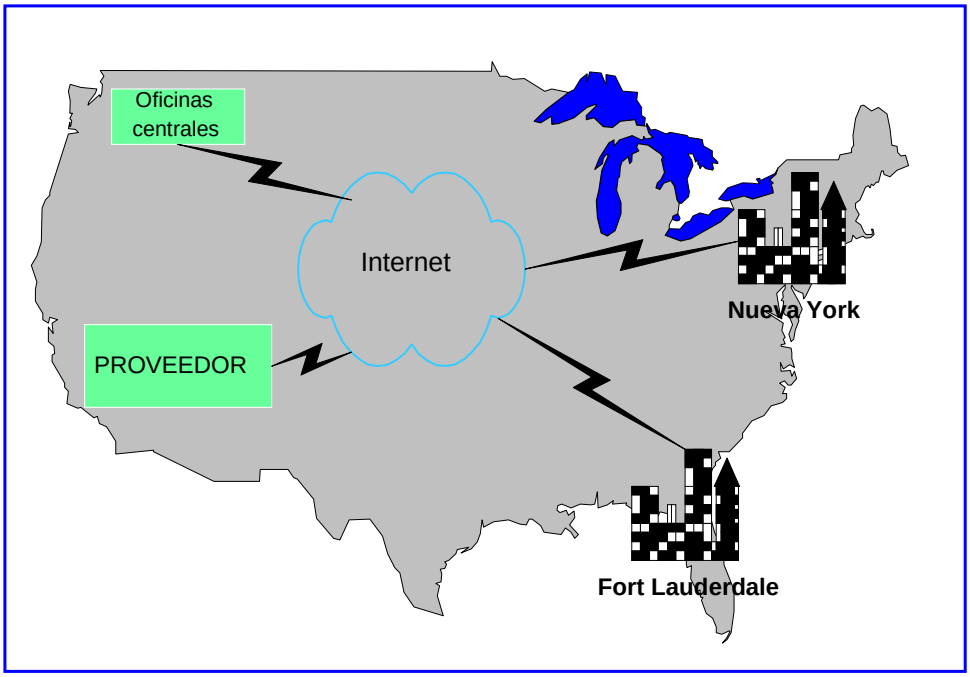


FIG. 3.5 Una VPN de extranet.

d.- VPN interna. Una cuarta área de la que no hacen uso las compañías actualmente, es una VPN interna.

¿Qué motivos hará que una compañía utilice una VPN interna?

Algunos de estos motivos son los estudios sobre seguridad que indican que los ataques por empleados internos ocupan el primer lugar. Este resultado es que impulsará en forma más definitiva la configuración de la topología de VPN interna, la cual se muestra en la figura 3.6.

Todo el tráfico que una compañía considera crítico puede pasar por un cable cifrado y almacenarse de manera segura sin que sea manipulado indebidamente.

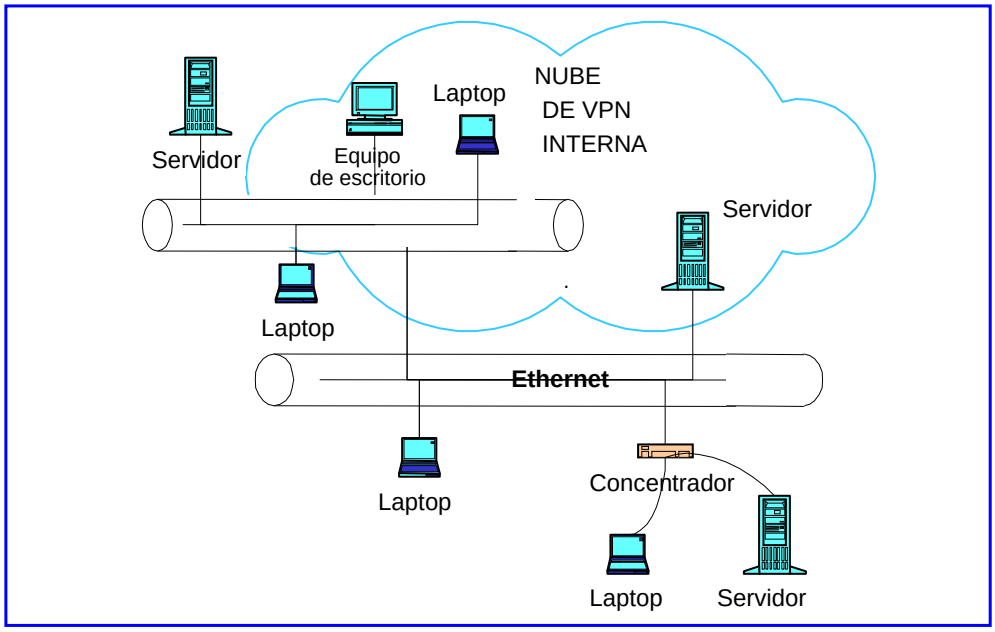


FIG. 3.6 Una VPN interna.

3.1.2 Componentes que forma una VPN.

Las VPN consisten en Hardware y Software y además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la VPN sea segura, esté disponible y sea fácil de mantener.

I.- Disponibilidad.

La disponibilidad se aplica tanto al tiempo de actualización como al de acceso. Lamentablemente, muchos de estos problemas están fuera de su control y a veces incluso del control del PSI local. Si utiliza una VPN de retransmisión de tramas o ATM, es probable que obtenga algunas garantías de su PSI sobre la disponibilidad, pero no sobre Internet.

II.- Compatibilidad.

Para utilizar tecnologías VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet.

Esto implica que su compañía debe estar al tanto del IP y saber que si los protocolos SNA o IPX están en ejecución, no se puede establecer una conexión directa a Internet, a menos que convierta primero el SNA o IPX a IP. Muchos dispositivos hacen esto, por ejemplo una compuerta, pero añaden otro nivel de complejidad a la red.

III.- Seguridad.

La seguridad lo es todo en una VPN. Una VPN no es la red privada de una compañía; otros pueden interceptar recolectar y analizar los datos. La seguridad abarca todo en una VPN, desde el proceso de cifrado que implementa y los servicios de autenticación que Usted elige hasta las firmas digitales y las autoridades emisoras y certificados que utiliza. La seguridad también abarca el software que implementa el algoritmo de cifrado en un dispositivo de la VPN.

IV.- Interoperabilidad.

Puesto que la tecnología VPN es relativamente nueva desde el punto de vista de la implementación, surgen muchos problemas

de compatibilidad a partir de la seguridad, el usuario y las normas de cifrado. Existen muchos productos de proveedores que ofrecen hardware, software, cifrado y esquemas de autenticación para la tecnología VPN; por lo tanto es muy difícil elegir alguno.

V. Autenticación de datos y usuarios.

La autenticación de VPN consiste en autenticación de datos y usuarios. **La autenticación de datos** reafirma que el mensaje ha sido enviado completamente y que no ha sido alterado en ninguna forma. **La autenticación de usuarios** es un proceso que permite que el usuario tenga acceso a la red. Es importante que se ofrezcan ambas en cualquier tecnología de VPN.

Talvez quiera que usuarios externos tengan acceso a su red interna.

Esto requiere una autenticación segura y la verificación de usuarios antes de que los usuarios externos entren a la red interna. Debe haber una manera de proporcionar una

verificación adecuada para permitir el acceso interno y una autorización para permitir a los usuarios autenticados solo el acceso a los servicios que requieren.

VI.- Sobrecarga de tráfico.

En todo tipo de tecnología existe sacrificio: velocidad contra desempeño, seguridad contra flexibilidad. Las VPN caen en la misma categoría cuando se habla de tamaños de paquete, paquetes cifrados, encabezados, etc; la sobrecarga entra en juego. Si un dispositivo de la VPN cifra cada paquete que sale los adaptadores de red entonces puede imaginar el tipo de capacidad de procesamiento de CPU que se necesita en esa máquina. Si la VPN encapsula cada paquete, puede incrementar el tamaño del paquete y por lo tanto afectar la utilización del ancho de banda.

Para reducir esto, debe decidir que tipo de tráfico necesita proteger. Las transmisiones generales, las transmisiones múltiples y el tráfico similar no necesitan cifrarse; sin embargo, necesita autenticarse. Los dispositivos de las VPN pueden agregar autenticaciones a estos paquetes sin la sobrecarga

asociada al incremento del tamaño el paquete y al receptor puede estar seguro de que los datos no han sido adulterados. Por lo tanto, un buen servicio de VPN le dará la opción de especificar que tipo de datos se cifrarán, que tipos de datos se autenticaran y que tipo de datos puede fluir libremente sin modificarse.

VII.- Ipv6.

El nuevo protocolo Internet en desarrollo es el IP versión 6 (IPv6); con el vienen nuevas características y problemas. Considerando que el tamaño del paquete será más grande que el Ipv4, entonces ¿cómo afectaran las técnicas de encapsulado a los dispositivos de red que necesitan descifrar/cifrar los nuevos paquetes más grandes?.

VIII.- Mantenimiento.

Debe decidir que tipo de tecnología y que tipo de soporte necesita su compañía. ¿Usara el servicio de VPN administrada por un PSI o la construirá usted mismo con los propios

recursos de su compañía? Si decide implementar usted mismo la VPN.

¿Cuenta con el equipo de seguridad? ¿Puede responsabilizarse su departamento de TI de los aspectos de seguridad?.

IX.- Sin repudio.

Sin repudio es el proceso de identificar positivamente el emisor de tal manera que no pueda negarlo. El comercio electrónico, los documentos legales y las negociaciones financieras se basan en saber quien realiza el pedido. Si existe aunque sea un poco de incertidumbre, una compañía no puede garantizar quien realiza el pedido. Para que el comercio electrónico en Internet se vuelva una opción viable, debe existir un proceso sin repudio.

3.1.3 ¿Quién Soporta las VPN?

Conforme difieren las tecnologías VPN, también lo hacen las implementaciones de las redes virtuales privadas por parte de los IPS. Algunos IPS buscan solamente dispositivos de

hardware para cifrado pueden cifrar y asegurar paquetes más rápidamente que los dispositivos de software.

Los IPS también experimentan con los túneles de VPN más recientes y con los protocolos de seguridad.

Los tres principales protocolos de seguridad que existen actualmente son el protocolo de reenvío de nivel 2 (L2F), el protocolo para establecimiento de túneles punto a punto (PPTP) y el protocolo de seguridad Internet (IPSEC).

El protocolo de reenvío de nivel 2 y el protocolo para establecimiento de túneles punto a punto se habían combinado en lo que se conoce como el protocolo para establecimiento de túneles de nivel 2 (l2TP).

3.1.4 El crecimiento de las VPN.

Algunos de las razones por las que muchos negocios utilizaran las VPN para conducir sus negocios son las siguientes:

- Las VPN utilizan Internet como su medio de transporte.
- Internet es un medio propicio tanto para clientes comerciales como privados.

- Internet se extiende por todo el mundo.

- La conductividad en Internet es extremadamente eficiente en el mercado actual, y muchos IPS procuran mantener la conexión.

- Las VPN son flexibles, dinámicas y escalable.

- Las VPN (en algunos casos) pueden utilizar la inversión que la compañía haya hecho en hardware.

- La tecnología base de las VPN es el conjunto de protocolos TCP/IP de Internet, lo cual la hace más fácil de comprender e implementar que una tecnología completamente nueva.

3.1.5 reas en las que la tecnología VPN puede ser benéfica para su organización.

- Acceso remoto de usuarios.
- Aplicaciones de extranet.
- Sitios internacionales.
- Base de usuarios geográficamente diversa
- La necesidad de soportar una base de clientes geográficamente diversa
- Expansión barata del mercado
- Requisitos razonables de ancho de banda
- Necesidad de un alcance global de bajo costo
- Acceso a servicios externos
- Líneas rentadas virtuales

Junto con el área de beneficio, también existen algunas áreas donde la tecnología VPN puede no ser recomendable para su compañía. Estas se aplican a la infraestructura interna y a sus requisitos particulares.

3.2 SEGURIDAD PARA LAS VPN.

3.2.1 ¿Qué es la seguridad de redes?

El modelo OSI se ha utilizado virtualmente en todos los sistemas de cómputo actuales. Describe la forma en que los componentes de los niveles individuales están a cargo de un conjunto específico de servicios y en que cada nivel se ubica por encima de otro. Esto permite que los fabricantes construyan productos sin tener que preocuparse por aspectos de interoperabilidad.

La pila de OSI consta de siete niveles:

- Aplicación,
- Presentación,
- Sesión,

- Transporte,
- Red,
- Enlace de datos,
- Físico.

Cada nivel es responsable de su propio conjunto de funciones individuales, por ejemplo, confiabilidad, configuración, corrección, etc. Pero en esto reside un problema de seguridad fundamental. Los ataques más comunes en la actualidad, como puede ser la sobrecarga de la memoria intermedia (buffer), los aprovechamientos indebidos del CGI y otros ataques a la seguridad, suceden a través de todos estos niveles.

En la figura 3.7, la tecnología VPN esta implementada en los niveles más bajos posibles de la pila de OSI. Esto crea un beneficio y un problema en potencia. Tener esta tecnología tan abajo como sea posible en la pila ayuda a eliminar muchos de los ataques que podrían suceder si estuviese mas arriba.

No obstante, tenga en mente que esta ubicación puede provocar problemas de compatibilidad. Al implementar el

software de la VPN en los niveles más bajos de la pila de OSI, la tecnología tiene la posibilidad de interactuar mas con los componentes específicos que forman el sistema operativo.

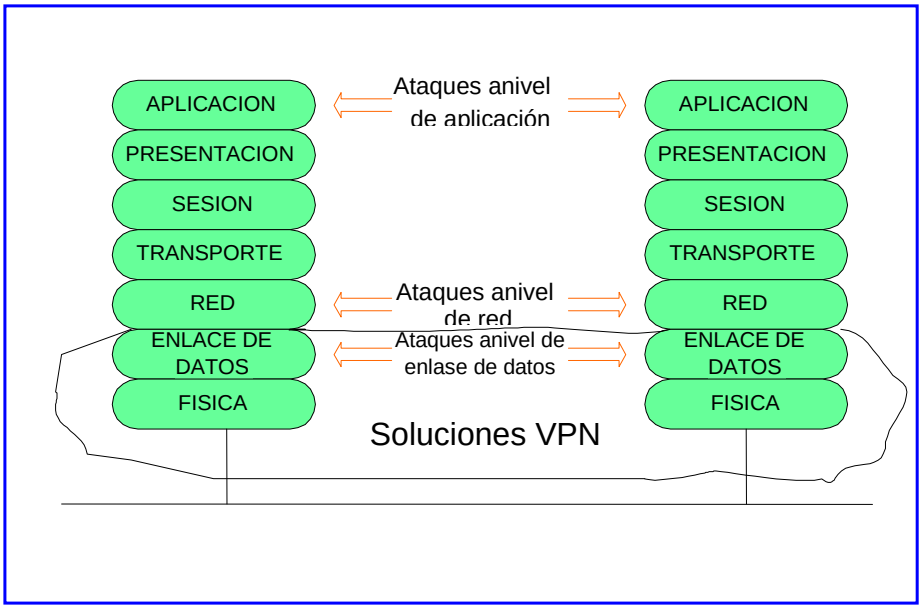


FIG. 3.7 Tecnología VPN en la pila de OSI.

3.3 VENTAJAS Y DESVENTAJAS DE LA TECNOLOGÍA VPN.

Las redes privadas virtuales implican costos, requisitos organizacionales y cargas de trabajo al personal de TI adicionales para una organización. También permiten que una compañía obtenga ahorros en el costo de utilizar una red

publica en ves de una instalación de línea rentada y su mayor ventaja radica en la flexibilidad para usar dicha red con el fin de hacer negocios.

3.3.1 Beneficios de la VPN.

Los beneficios de las VPN se dividen en áreas independientes y existen ventajas que se aplican a cada área de la organización.

Algunos de estos beneficios son los siguientes:

- Cargos de telecomunicaciones.
- Líneas rentadas.
- Números 1 800.
- Administración.
- Equipo de acceso remoto por marcación.
- Facilidad de mantenimiento.
- Diseño de administración de red simplificada.

Aunque es verdad que las VPN tiene el potencial para ahorrar mucho dinero, también tienen el potencial para implicar su costo

económico y, como ocurre con todo, existen ventajas y desventajas.

Esto implica que hay desventajas en la tecnología VPN en si misma, si no más bien en la manera en que se diseña e implementa.

3.3.2 Ahorros en el costo de las VPN.

Al eliminar dispositivos como las líneas rentadas y el equipo de acceso remoto costoso, también se reduce el tiempo que el personal de TI de la corporación invierta en la administración y en el mantenimiento de estos dispositivos, por lo tanto se producen ahorros en un rango de 60 a 80 por ciento.

Para llegar a esta cantidad, los estudios simplemente eliminan el número de líneas de acceso que tiene una corporación típica, junto con un número estimado de líneas rentadas, y luego multiplican el resultado por el número de usuarios que accederán al equipo. Por consiguiente, el mantenimiento y el soporte para estos dispositivos no serán necesarios, así que usted puede estimar el número de horas eliminadas que se

necesitaron para darle soporte a este tipo de equipo y calcular un ahorro en los costos. De esta manera, esta estadística financiera incluye el equipo actual, las líneas de telecomunicaciones y la estructura de soporte.

3.3.3 Beneficios del diseño de red.

El diseño de red es un área donde la tecnología VPN realmente puede ser benéfica desde el punto de vista de diseño arquitectónico, flexibilidad y mantenimiento. La necesidad de un diseño WAN complejo, de cálculos del desempeño del enlace, ajustes en el tamaño de los conductos de ancho de banda y redundancia, no representa un problema para una organización. En estos puntos, la principal preocupación es la conexión a Internet de su proveedor PSI local, quien manejará todos los problemas asociados con su conexión.

Antes de Internet, una organización padecía el inconveniente de tener que diseñar e instalar un conjunto de líneas rentadas en ciertas ubicaciones. Era necesario tomar en consideración el tiempo de inactividad, los enlaces redundantes y los problemas de ampliación y desempeño. El tipo de arquitectura de línea

rentada lamentablemente no se ampliaba fácilmente y era extremadamente cara. La figura 3.8 ilustra lo que tiene que enfrentar un administrador de una red típica cuando diseña una WAN sobre líneas rentadas.

La figura 3.8 muestra claramente la complejidad del esquema elaboro el diseñador. Lo que es importante resaltar es el número de enlaces requeridos por esta topología. Esto forzó al personal de administración de la organización a decidir cuales ciudades se consideraban las más importantes, que los gastos de los enlaces redundantes dictaron que no todas las ciudades podrían contar con las líneas duales para estar conectadas.

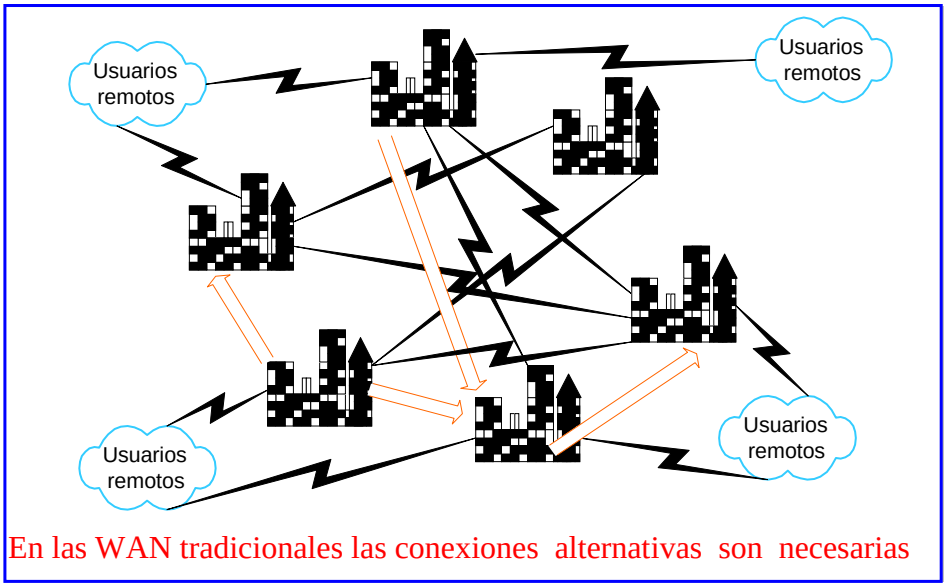


FIG 3.8 Diseño de una WAN.

Con la arquitectura VPN, todo el trabajo se redujo. Como se muestra en la figura 3.9, todo lo que se requiere es una conexión a Internet, y PSI se encarga del transporte.

Ahora a la red WAN puede ser escalable, redundante y estar basada en normas (TCP/IP), y soportar capacidades de administración distribuídas.

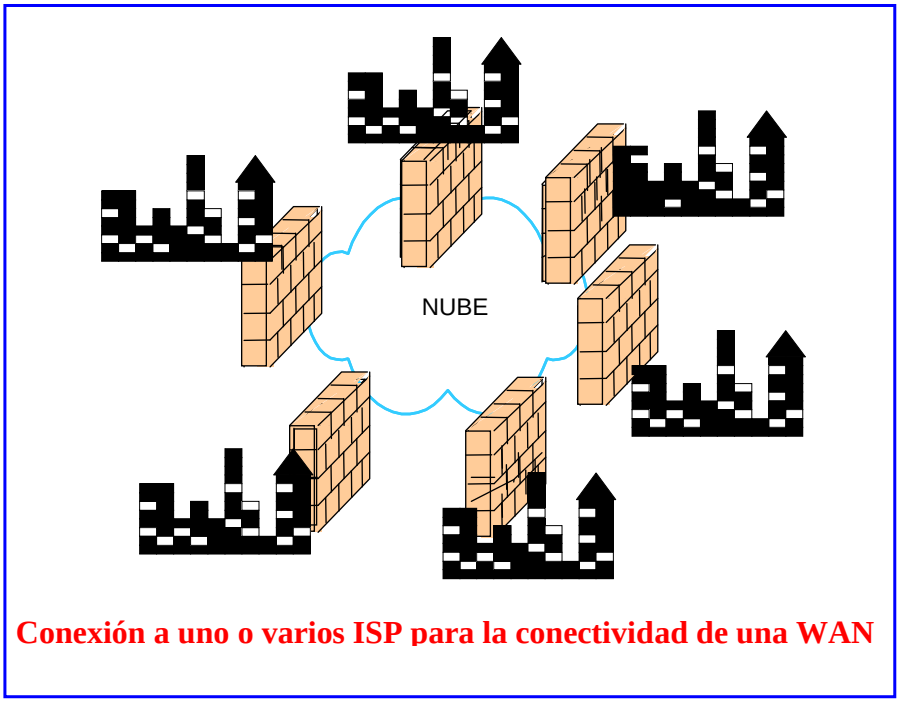


FIG. 3.9 Conexión a un ISP por medio de Internet de una matriz a sus sucursales.

I.- Administración centralizada.

Contar con esta característica de administración centralizada simplifica en gran medida los procesos de mantenimiento y la solución de problemas de infraestructura de su VPN.
Elimina la necesidad de personal de varios departamentos de TI y reduce sus cargas de administración

3.3.4 Beneficios de las VPN para el usuario final.

Los negocios actuales deben ir a donde este el cliente, esto añade una carga a la organización puesto que demanda una fuerza de trabajo móvil y geográficamente dispersa. Con el acceso a través del PSI y la tecnología VPN existe la oportunidad de cerrar tratos, verificar contratos, etc.

I.- Pagar solo lo que se requiere.

Con líneas rentadas, retransmisión de tramas u otra infraestructura, usted tiene que pagar por el tiempo de inactividad. En el caso de Internet, usted solo paga por el

tiempo en la línea, lo cual generalmente consiste en una llamada local además de una cuota mensual.

II.- Acceso a datos.

Con la VPN instalada puede establecer una conexión directa al servidor en cuestión y transferir el material apropiado, eliminando la necesidad del exterior que pueda utilizar para establecer una conexión por marcación.

III.- Asignación de prioridades de tráfico.

Ya que las VPN ofrecen acceso a una extranet, a una Intranet o a servidores internos de una organización, es posible decidir que solo se permita pasar libremente cierto tipo de trafico, con el fin de conservar el ancho de banda, mientras que otro tipo de trafico queda en la cola de espera, según su importancia.

3.3.5 Beneficios de un alcance global.

Con Internet se obtiene el acceso global que permite que cualquier usuario en el planeta se conecte a la LAN de su

compañía, siempre y cuando exista un proveedor ISP en esa área. Esto hace que una organización pueda extender su presencia en todo el mundo y vender sus productos a cualquiera que pueda desearlos.

I.- Tele conferencias.

La tele conferencia continuará creciendo y los I tendrán una demanda creciente para proporcionarla. Si bien es cierto que usted podrá disfrutar la tele conferencia desde cada oficina pequeña en todo el planeta, contara con la capacidad de establecer una tele conferencia en puntos estratégicos a través del mundo, ahorrando tiempo y dinero.

II.- Telefonía IP.

Es un servicio de rápido crecimiento debido a los ahorros en el costo que pueden lograrse utilizando a Internet como un medio de comunicación en las llamadas internacionales.

3.3.6 Costo de la tecnología VPN

Algunos de los costos adicionales que por lo general no se mencionan pero en los que si se incurre son:

- Infraestructura de red del ISP.
- Equipo de VPN.
- Costos de mantenimiento.
- Licencias.
- Aspectos legales de la compatibilidad con el año 2000.
- Costos de la solidez del cifrado.
- Administración.
- Personal de seguridad.
- Servicio de ayuda para resolver problemas.
- Costos de telecomunicaciones adicionales.

I.- <u>Infraestructura de red del PSI.</u>

¿Por qué la infraestructura de red del PSI añadiría un costo adicional a una compañía?

La figura 3.10 revela un problema potencial. ¿Cuántos puntos de entrada desea tener en su organización? Desde el punto de vista de la seguridad, solo debería tener uno, pero desde un punto de vista realista relacionado con trabajo, no puede pagar el costo de tener solo uno. La figura 3.10 muestra una sola forma de llegar a su organización.

Las corporaciones se encontrarán a si mismas luchando por mantener su conexión a Internet sin qué se interrumpan, así que pregunto ¿Qué debe hacer realmente una compañía para protegerse?.

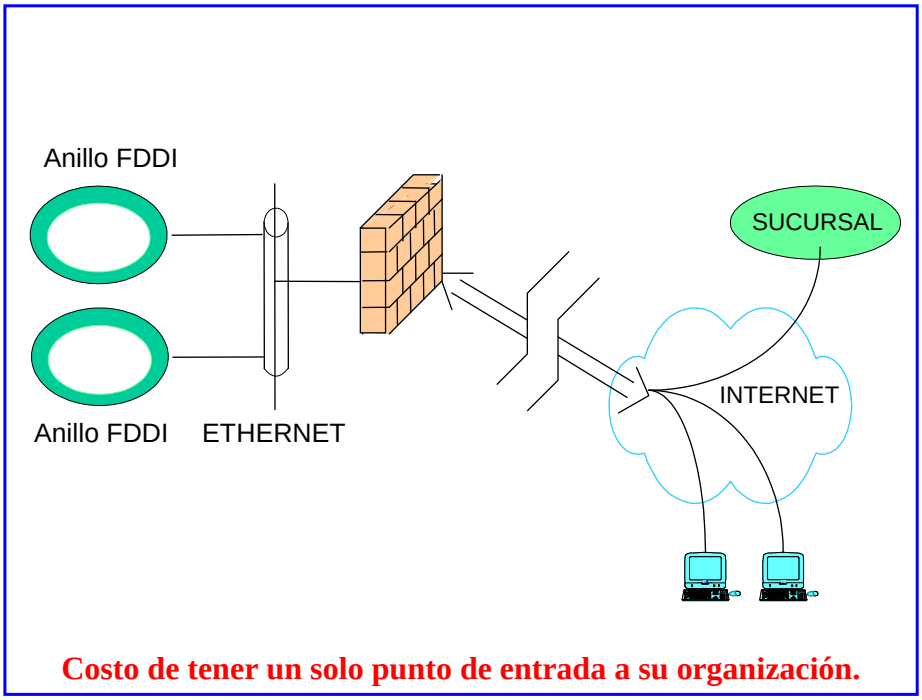


FIG. 3.10 Falla del enlace principal.

La figura 3.11 ilustra lo que tiene que hacer una compañía en caso de falla importante de su enlace Internet. Deberá tener un enlace secundario o algún tipo de equipo de acceso remoto para dirigir los negocios.

Ahora recuerde todos los ahorros en el costo, asociados con la VPN. Aquellas estadísticas no toman en consideración factores como los enlaces secundarios a los ISP y el equipo de acceso remoto en caso de una falla importante. Aquí es donde comenzamos a ver los costos adicionales.

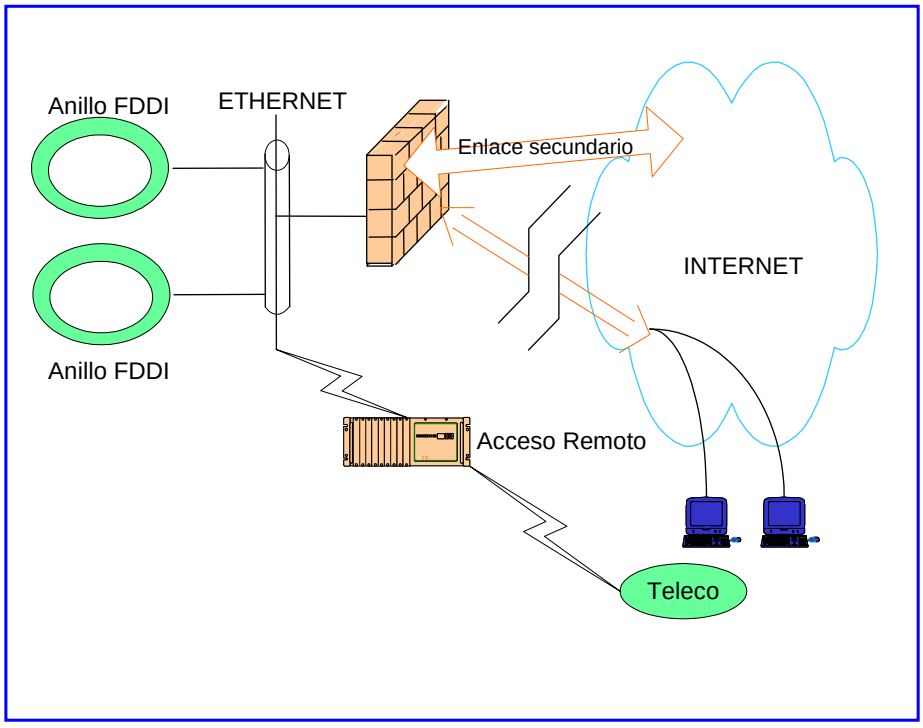


Fig.3.11 Enlaces redundantes a Internet.

II.- Equipos de VPN.

¿De dónde viene todo este equipo y cuánto cuesta? Usted está añadiendo equipo muy sofisticado a la red de su corporación.

Puede tratarse de una configuración independiente o de alguna otra combinación que utiliza otros tipos de equipo.

¿Va .a colocar este equipo en una subred o en una red nueva? ¿Qué hay respecto a añadir equipo para servicio de acceso remoto (RAS)? Sus usuarios necesitarán alguna manera de establecer su autenticación y de obtener autorizaciones.

¿Existe algún otro tipo de hardware y/o software que añadirá, como enrutadores, concentradores, cableados y CSU/DSU?

III.- Costos de mantenimiento.

Al igual que con otro tipo de hardware que tenga, es muy probable que cuente con contratos de mantenimiento para este quipo. Puede seleccionar contratos para hardware, software, o para ambos.

¿El contrato de mantenimiento incluye características de actualización gratuitas? Hablamos de características de interoperabilidad con las futuras normas de seguridad IPSEC, PPTP y L2TP para las VPN de Internet.

¿Su contrato de mantenimiento cubre todas estas actualizaciones si y cuando están disponibles?¿Cuánto tiempo le tomara a su proveedor reparar o remplazar el equipo y el precio?. La porción del gasto será insignificante comparada con el costo de no poder realizar los negocios.

IV.- Licencias.

Las licencias no son las mismas para todos lo productos; para ciertos proveedores, significan el número de usuarios simultáneos que pasan a través de un dispositivo de red.

Mientras que algunos añaden una cuota de licencia simple a un enrutador, lo cual permite conexiones VPN ilimitadas, otros basan sus cuotas de licencias en el número de túneles que usted puede crear.

V.- Costos de solidez de cifrado.

La figura 3.12 ilustra el problema con distintas características de solidez del cifrado.

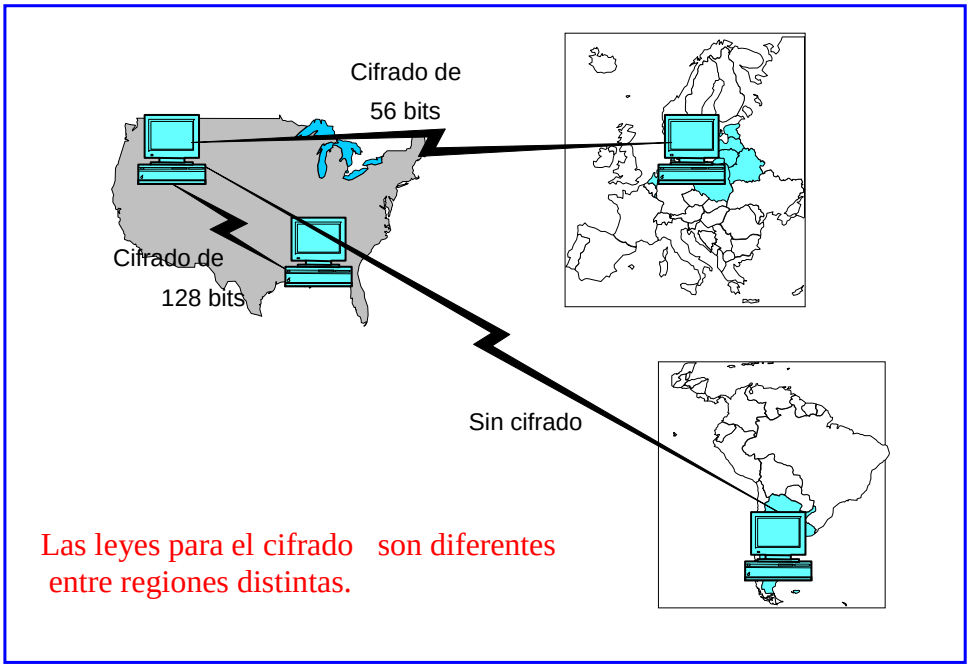


FIG. 3.12 Solidez de cifrado.

Hay que considerar que el software que realiza el cifrado no se adquiere de forma gratuita y por tanto hay que pagar un precio por él.

VI.- Administración.

Alguien tendrá que responsabilizarse de la supervisión y él mantenimiento de la VPN, sea usted o su ISP. Si el ISP provee 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 UNÍS 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 sé instalará la nueva revisión. Si usted 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 usted puede crear un túnel de administración cerrado ente los dispositivos de VPN de tal forma que puede administrarlos remotamente a través de Internet.

- Fuera de Banda. Esta configuración coloca un MODEM de cifrado en los puertos de consola de los dispositivos VPN en diferentes ubicaciones. Necesita tener esta configuración en caso de que no pueda tener acceso en banda a su dispositivo VPN.

VII.- Personal de seguridad.

El aspecto de la seguridad de la VPN recae en la solidez el algoritmo de cifrado en el que se basa. Si usted implementa esta tecnología personalmente,

¿Ésta seguro de que está implementado los algoritmos de cifrado más solidez disponibles? ¿Qué hay respecto a la autenticación de los usuarios de la VPN? ¿Cómo se logra esto y mediante que mecanismo? ¿Va a utilizar un servidor RADIUS, firmas digitales o autoridades emisoras de certificados? Si desea utilizar autoridades emisoras de certificados para la autenticación de los usuarios.

¿Quién mantendrá el servicio de autoridad emisora y certificados, usted o un tercero? .

VIII.- Servicio de ayuda para resolver problemas.

La única responsabilidad de su ISP es asegurarse de que el usuario pueda conectarse a Internet y no de que sus aplicaciones estén en ejecución. Aun si usted esta utilizando un servicio administrado, el ISP estará administrando el dispositivo VPN y no los cientos o incluso miles de computadoras portátiles con que cuenta su organización.

Usted a su ISP instalará algún dispositivo VPN de un proveedor especifico, y el producto puede incluir un software para equipo portátil que le ofrezca la funcionalidad de crear una VPN para su compañía.

3.3.7 Garantías de calidad de servicio.

La calidad de servicio es un proceso en que los conmutadores y los enrutadores instalan recursos para mover datos en forma rápida y confiable.

Las garantías de calidad de servicio intentan cubrir algunos de los a tributos siguientes:

- Definír los retrasos.
- Inestabilidad.
- Limites de pérdida de celdas/ paquetes.
- Seguridad.
- Ancho de banda con base en aplicaciones.
- Especificar los retrasos aceptables.
- Descartar rangos.

La calidad de servicio ayuda definir un esquema de asignación de prioridades donde las aplicaciones que consumen gran ancho de banda obtendrán los servicios que necesitan y las aplicaciones de uso menos intenso también verán satisfechas sus necesidades de ancho de banda.

3.3.8 Ventajas y desventajas de las VPN.

Existen ahorros en las cargas de administración y en la eliminación. De.algún equipo de acceso remoto por marcación.

La finalidad de mantenimiento y los diseños de administración de red simplificada también representan ventajas.

Por otra parte, la tecnología VPN requiere desembolsos adicionales por parte de la organización. Algunos de estos desembolsos involucran aspectos relacionados con la infraestructura de red del ISP, el costo del equipo de VPN, el costo de mantenimiento, el costo de las licencias.

Para todas estas ventajas y desventajas, si se deberá calcular los verdaderos ahorros en el costo de la tecnología VPN, para esto se utiliza la siguiente fórmula:

Ahorros de la VPN =

[(costos eliminados) – (costos adicionales)+ (Ventaja competitiva)]

I.- <u>Costos eliminados.</u>

- Líneas rentadas.
- Líneas por marcación.
- Equipo de acceso por marcación.
- Tiempo que invierte el personal para configurar el equipo del usuario final.
- Tiempo que invierte el personal para mantener el equipo del usuario final.

- Contratos de mantenimiento de equipo.
- Equipo PBX (propiedad del cliente).
- Servidor de autenticación por marcación.
- Sistemas UPS para equipo de marcación.
- Costosos enlaces ATM o por tramas.
- Conexiones ISDN.
- Soporte para IP, DNS y enrutamiento.

I.- Costos adicionales.

- Equipos de VPN.
- Costos de mantenimiento.
- Licencias.
- Asuntos relativos a la solidez del cifrado.
- Administración.
- Capacidad de supervisión en banda y fuera de banda.
- Personal de seguridad.
- Servicio de ayuda para resolver problemas.
- Larga distancia.
- Contratos de calidad de servicio.

3.4 ARQUITECTURA DE LA VPN.

3.4.1 Introducción a la arquitectura.

Existen innumerables opciones para la instalación de las VPN, desde las VPN independientes basadas en caja negra y las VPN basadas en enrutador hasta las VPN basadas en software y en cortafuego. Además de estas arquitecturas, existen una amplia variedad de servicios y características que pueden implementarse en estos dispositivos.

El software antivirus y el software de cifrado son aplicaciones que requieren un uso muy intensivo del CPU. Debe tener cuidado si instala estas aplicaciones en una plataforma única.

3.4.2 ¿Cuál es la mejor VPN para usted?

La seguridad de una VPN se basa en su dispositivo de hardware en su sistema operativo, en la solidez del algoritmo de cifrado utilizado en la tecnología VPN y en la infraestructura de administración de claves que tiene instalada. Además de estos elementos debe validar a la autoridad emisora de certificados en la que ha decidido confiar como en una fuente autorizada. La

experiencia técnica de su personal interno de TI debe examinarse, junto con la experiencia técnica del proveedor con quien este tratando, usted ésta suponiendo que se trata de expertos en el área de VPN/seguridad.

3.4.3 VPN proporcionada por un proveedor de servicios de red.

El proveedor de servicios de red tal vez establecerá un dispositivo en las oficinas de su compañía que creará el túnel de VPN para usted. Sin embargo, este no es un requisito absoluto; algunos ISP pueden instalar un conmutador PPTP frontal en sus oficinas el cual creara en forma automática los túneles de VPN para su tráfico.

También podría agregar un cortafuego a este tipo de ambiente, por lo general justo en frente de un dispositivo de red o entre ellos. De manera similar a la vieja forma de instalar una DMZ (zona desmilitarizada), el enrutador interno se conecta a un puerto del cortafuego, el otro puerto del cortafuego se conecta al enrutador externo y el puerto serial del enrutador externo se conecta al ISP. También debe encargarse de asuntos tales como el direccionamiento de IP, el enrutamiento y el correo.

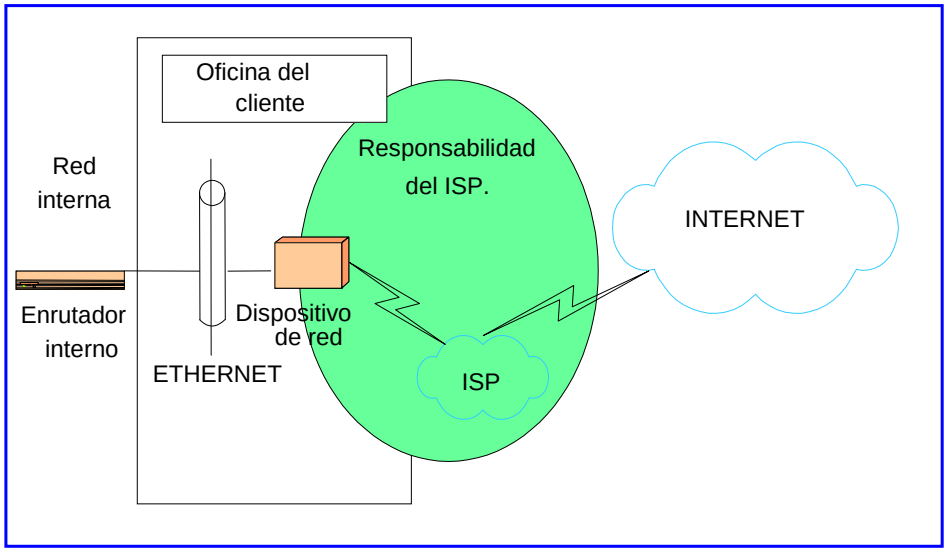


FIG. 3.13 VPN proporcionada por un ISP

En la figura 3.13 las líneas de responsabilidades están claramente definidas por el ISP.

En la figura 3.14 la responsabilidad de nuevo es la solución VPN del ISP, pero ahora las líneas divisorias de responsabilidad no están claramente definidas.

¿Quién es responsable por el punto de marcación, las líneas de telecomunicaciones o los concentradores presentes? Algunas organizaciones tienen el mismo ISP y al mismo proveedor de telecomunicaciones pero otras no.

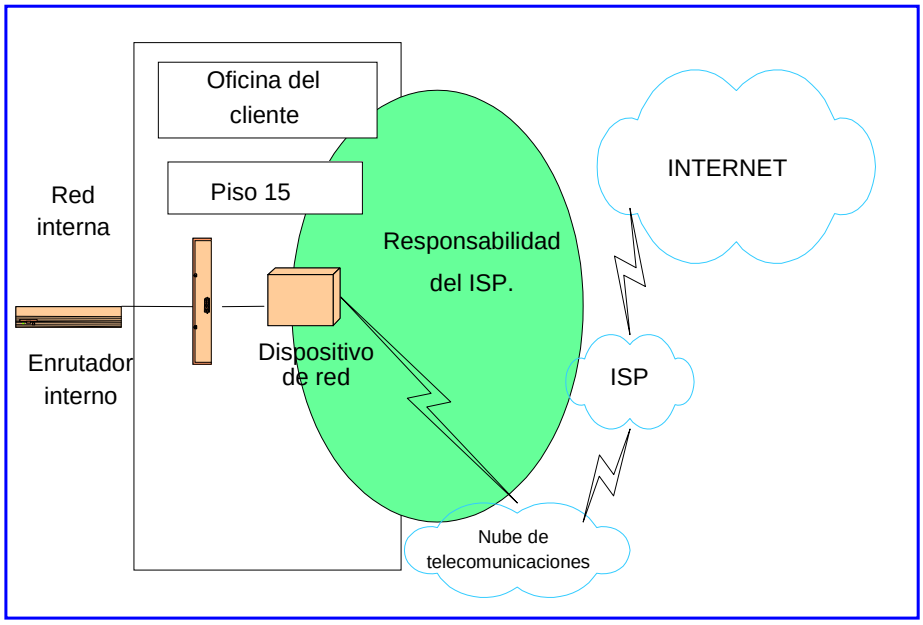


FIG. 3.14 Zonas de la solución no claramente definidas por el ISP

I.- Seguridad.

La seguridad de la VPN se basará en normas aceptadas por la basta comunidad de la sociedad de Internet los ISP primero proporcionan servicios de Internet y en segundo lugar servicios de VPN pero son las acciones de los usuarios las que podrían haber ocasionado problemas en la seguridad.

II.- Control de Cambios.

Si solicito un cambio en su arquitectura existente debe saber

como y cuando se implemento esa solicitud. Es importante la retroalimentación para verificar los controles de cambio que usted desea, sea este mediante el correo electrónico o a través de una llamada telefónica y deberá saber como se implemento el cambio. Recuerde, al añadir nuevos servicios es posible que se requiera un proceso de detección y solución de problemas, de tal forma que eventualmente podría pasar por varios controles de cambios y necesitara seguirle la pista a cada uno de ellos y supervisarlos.

III.- Solución de problemas.

Usted reúne a su equipo técnico y sus consultores, pero si el problema persiste podrían pasar semanas antes de resolverlo.

Usted verdaderamente necesita asegurarse de que su contrato se detalle con claridad la buena disposición del ISP para invertir tiempo en resolver el problema y en diagnosticarlo sin importar cuanto tiempo se requiera. Por supuesto, esto añade un costo al precio del contrato, pero es mejor pasar meses tratando de resolver un problema.

IV.- Características.

Si su compañía desea utilizar Internet para su tele conferencias o emplear la telefonía IP, realmente debe discutirlo con su proveedor. ¿Qué sucede si su compañía decide que necesita una configuración diferente de la que se implemento originalmente?

Es posible que no se le permita implementar su aplicación específica. La redundancia, la tolerancia frente a las fallas, la sincronización, y la tecnología push es solo alguno de los casos especiales.

v.- Autorización.

Usted necesita saber como y cuando se añadieron usuarios a una base de datos lo cual les permitirá crear el túnel de VPN hacia su organización

¿La base de datos está en el dispositivo en el VPN del proveedor o en algún servidor interno bajo su control? Es imperativo que usted tenga acceso inmediato a la base de

datos para revocar los privilegios de acceso o que cuente con una manera de conectar a su proveedor en forma inmediata para llevar a cabo esta tarea.

VI.- Utilización de la red.

Es imprescindible estar consciente de cómo funciona la red en general. Usted o su PSI deben vigilar el enlace para el uso del tráfico en el ancho de banda. La empresa comenzará a crecer y a requerir más servicios de VPN, lo cual aumentará el ancho de banda.

VII.- Utilización de dispositivos.

Un dispositivo VPN es justo como cualquier máquina o pieza de software ubicada en alguna parte de su organización. Alguien tendrá que observar su desempeño, vigilar su salud y prevenir los problemas.

El trafico diario, el número de usuarios y los procesos de administración de claves y de cifrado consumen bastantes

recursos del CPU. Debe conocerlo con el fin de actualizarlo cuando sea necesario.

VIII.- Aplicaciones cliente.

Con el fin de que las computadoras portátiles creen un túnel de VPN, será necesario instalar software especial en ellas.

¿Quién reparara a todas estas laptot equipos de escritorios y demás, y quien les dará mantenimiento? Usted pensó que compro un servicio de VPN. Bueno, si lo hizo, pero lamentablemente esta es una de esas áreas grises de las cuales tendrá que responsabilizarse su organización.

Seria imposible para su ISP lograr esta tarea, pero una vez que haya cargado el software, le ayudará a resolver los problemas de las conexiones al dispositivo VPN.

El principal problema si existe algún software cargado en esas máquinas y crea conflictos con el software de la VPN. Como se mencionó previamente debido a la ubicación del software VPN

que se encuentra entre los niveles de enlace de datos y de red, podrían presentarse problemas al ejecutar el software.

IX.- Administración de claves.

Las claves de su VPN deben ser parte de un procedimiento rutinario. No se trata de la generación y el mantenimiento de las claves, sino de donde obtenerlas si se requiere duplicarlas.

En estas arquitecturas, las claves generadas y administradas deben guardarse en un lugar seguro, no solo para propósito de seguridad sino también para recuperarlas. Estas incluyen claves públicas de dispositivos y cualquier certificado del que usted sea responsable. Las claves de cifrado para el túnel también deben ser capaces de reproducirse en caso de que el dispositivo VPN falle y se requiera un nuevo dispositivo.

3.4.4 VPN basadas en un cortafuego.

Las VPN basadas en cortafuego probablemente son la formas más comunes de implementación de VPN hoy en día, y muchos proveedores ofrecen este tipo de configuración esto no significa

que las VPN basadas en cortafuego sean superiores a otras formas de VPN, sino más bien se trata de una base establecida a partir de la cual se puede crecer. Actualmente este servicio se esta dando con algún ISP aunque su implementación todavía es relativamente costosa.

Existen algunos proveedores para elegir cuando se considera una VPN basada en cortafuego, y los productos están disponibles en todas las plataformas. Un aspecto importante de la seguridad es el sistema operativo subyacente.

¿En que plataforma se esta ejecutando el cortafuego? ¿Se trata de un dispositivo basado en UNÍX, basado en NT, en NetWare o en algún otro dispositivo basado en plataforma, y cuales son los puntos vulnerables de este sistema operativo?

No existe un dispositivo que sea 100% seguro a sí, que si se crea la VPN en ese dispositivo necesitará asegurarse de que el sistema operativo subyacente sea seguro. Si observa la figura 3.7 podrá ver de nuevo porque la tecnología VPN debería ubicarse en el nivel más bajo de la pila de OSI. Entre mas arriba se encuentre en la pila se presentaran mayores

oportunidades de que ocurran violaciones en la seguridad que en las capas inferiores de las que depende.

La figura 3.15 ilustra una VPN basada en cortafuego.

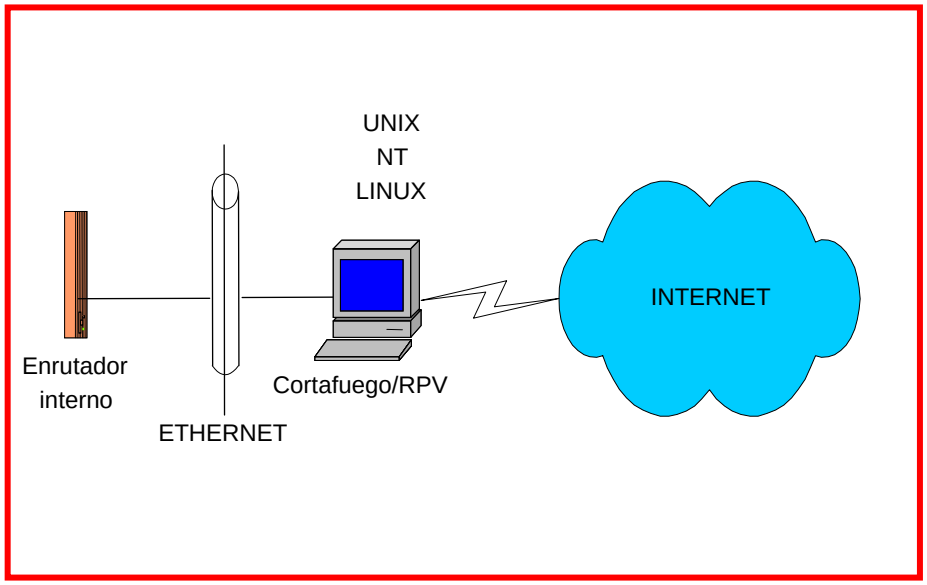


FIG. 3.15.- VPN basada en cortafuego.

Debe decidir que tipo de norma VPN desea. Por ejemplo ¿Desea utilizar la norma PPTP, L2TP, o IPSEC?.

Hasta el momento existen tres tipos de implementaciones de cortafuego entre los que se puede elegir: inspección de estados, Proxy y filtrado de paquetes. Cuando decimos “añada tecnología VPN a un cortafuego” nos referimos a añadir

tecnología VPN únicamente a un cortafuego de inspección de estados. De la misma manera que la tecnología VPN en si misma se ejecuta en los niveles más bajos de la pila de OSI, el cortafuego debe hacerlo o puede caer en problemas de desempeño importantes.

Un servidor Proxy se ejecuta en el nivel 7, el nivel de aplicaciones del modelo OSI y el cortafuego de filtrado de paquetes también tiene que examinar el paquete completo cada vez que pasa un cortafuego de inspección de estados se ejecuta en los niveles 2 y 3.

Debido a este requisito de procesamiento, usted solo debería añadir tecnología de VPN a un cortafuego de inspección de estados.

3.4.5 VPN Basadas en caja negra.

En el escenario de caja negra, un proveedor ofrece exactamente eso, una caja negra. Se trata básicamente de un dispositivo cargado con software descifrado para crear un túnel de VPN.

Algunas cajas negras vienen con software que se ejecutan en un equipo cliente, para escritorio como ayuda al administrar ese dispositivo, y otras pueden configurarse a través de un explorador Web. Se cree que estos tipos de dispositivo de cifrado de hardware son más veloces que los tipos de software, ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado con mayor rapidez. Aunque eso puede ser verdad, no todos ofrecen una característica de administración centralizada, y por lo general no soportan el acceso a sí mismo; es necesario enviar este acceso a una base de datos para consultas. También se requiere otro servidor si se desea llevar a cabo la autenticación, aunque algunos dispositivos permiten añadir usuarios si así lo desea. Pero,

¿Quiere mantener a todos sus usuarios con un dispositivo?

En este punto los proveedores deberían soportar los tres protocolos para establecimiento de tuéneles, PPTP, L2TP e IPSEC, pero no dé esto por sentado. Los proveedores han dado grandes pasos para hacer que la implementación de los dispositivos dedicados al cifrado sea lo más sencilla posible. Como todo lo que sucede en la tecnología, es fácil, puede no

ser tan flexible. Sin embargo, el desempeño puede ser bueno, lo cual es más que suficiente para su compañía. La figura 3.6 ilustra una solución de VPN de caja negra.

El cortafuego proporciona seguridad a su organización; pero no provee seguridad para sus datos. Así mismo, su dispositivo VPN le brindará seguridad a sus datos pero no a su organización.

Notará que el cortafuego estará enivo VPN y lo más probable es que usted haya instalado una política basada en reglas en el cortafuego. En la configuración de su cortafuego, asegúrese de que puede pasar aquellos paquetes cifrado.

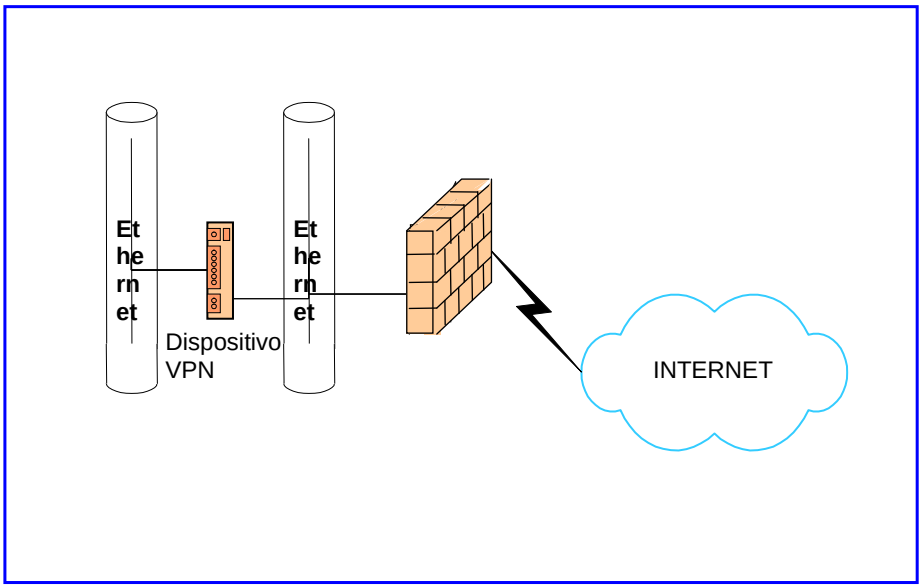


FIG. 3.16 VPN de caja negra.

El cortafuego esta ahí para protección. Si usted está filtrando en los puertos TCP y los paquetes vienen cifrados, el cortafuego tratara de examinar el paquete se dará cuenta de que no puede hacerlo y lo soltara. Por consiguiente, debe asegurarse de que su cortafuego pasara esos paquetes.

3.4.6 VPN basadas en enrutador.

Existen dos dispositivos de VPN basados en enrutadores. En uno de ellos el software se añade al enrutador para permitir que el proceso de cifrado ocurriera. En el segundo método se inserta una tarjeta externa de otro proveedor en el mismo chasis que el enrutador. Este método esta diseñado para endosar el proceso de cifrado del CPU del enrutador a la tarjeta adicional.

Tenga en mente que el desempeño puede ser un problema con las VPN basadas en enrutador. Debido a la adición de un proceso de cifrado al proceso de enrutamiento, usted puede agregar una carga mas pesada al enrutador especialmente si este está manejando una gran cantidad de rutas o implementando un algoritmo de enrutamiento intensivo.

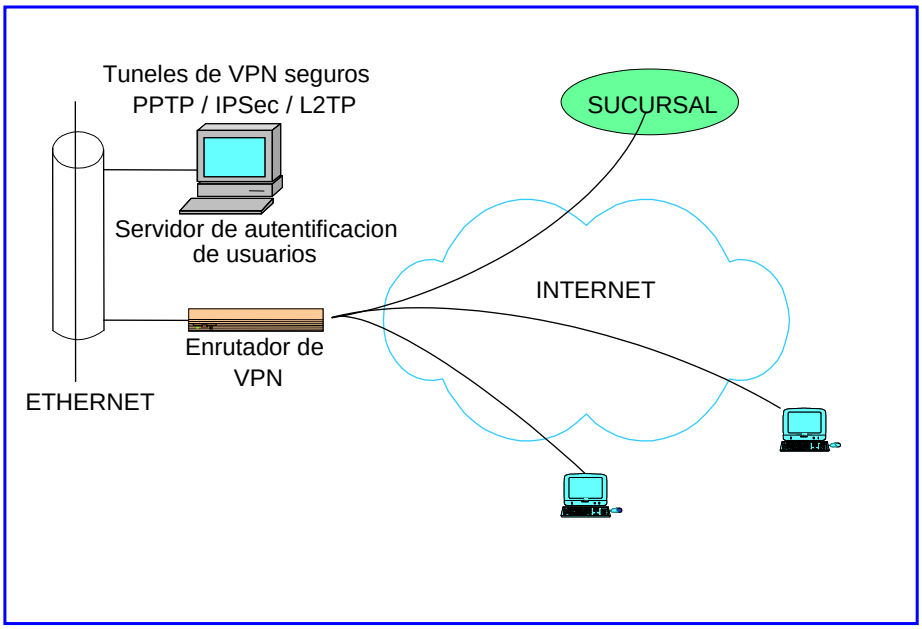


FIG. 3.17 VPN basada en enrutador.

La Figura 3.17 es una VPN típica basada en enrutador en la cual los paquetes se cifran desde el origen hacia el destino, por ejemplo, de las oficinas centrales a las oficinas remotas.

3.4.7 VPN basadas en acceso remoto.

Si alguien de fuera esta tratando de crear un flujo de paquetes cifrados hacia su organización. Así que, de manera más literal tal vez el término se aplique al software que se ejecuta en las máquinas de los usuarios remotos, las cuales están tratando de crear un túnel hacia su organización y un dispositivo en su red

que permita esa conexión. Este túnel podría venir de Internet, pero también podría venir de una línea de marcación, una línea ISDN o una red X.25. La figura 3.18 ilustra un escenario típico de acceso remoto.

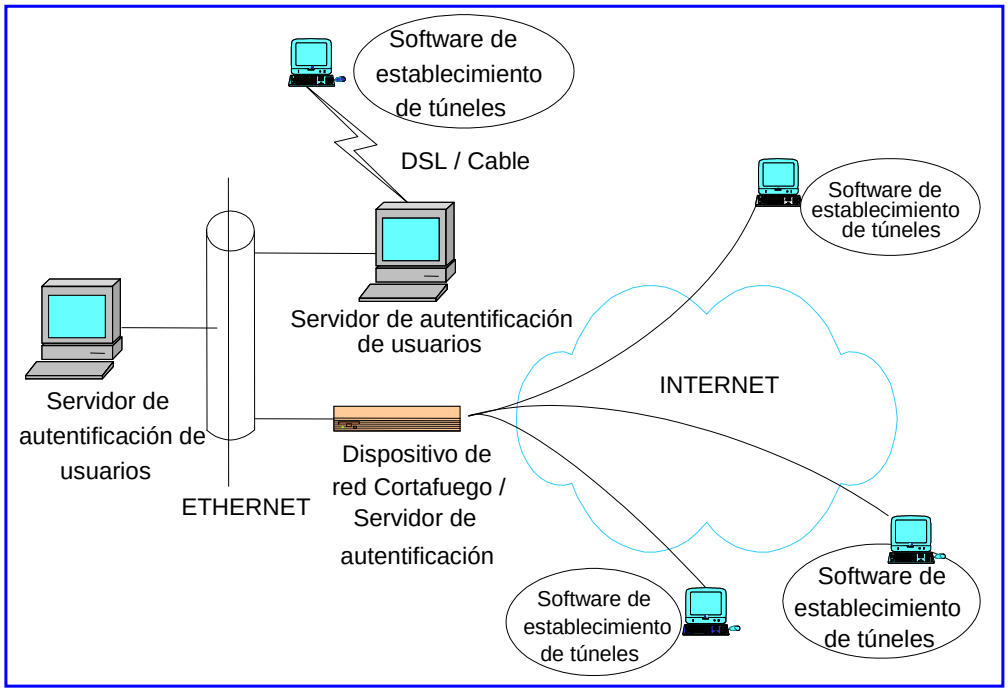


FIG. 3.18 Escenario de acceso remoto.

Este escenario tiene software que se ejecuta en una máquina remota en alguna parte y esa máquina intenta establecer una conexión a través de un túnel cifrado al servidor interno de la compañía o desde una línea de acceso por marcación como

ISDN hacia un servidor de autenticación. Un servidor de acceso instalado en su red, sea este un enrutador, un cortafuego, una caja negra o un servidor de autenticación independiente, que concede el acceso. Este dispositivo de acceso remoto recude la cantidad de los costosos equipos de líneas rentadas y acceso por marcación remota.

3.4.8 Aplicaciones de múltiples servicios con VPN.

Algunas de las aplicaciones de múltiples servicios para VPN son la filtración de contenido Web y la revisión antivirus. La filtración de contenido Web se añade a su dispositivo de cortafuego/VPN para permitirle ver que clase de sitios Web está visitando sus usuarios internos. Usted necesitara seguirle la pista. El proceso de cifrado de VPN en sí mismo consume mucho poder de procesamiento, así que necesita estar al tanto del trafico. El software antivirus, el cual puede cargarse en el propio dispositivo o endosarse a otro servidor, es un servicio muy importante que debe implementar. Necesita mantener los virus en un nivel mínimo y digo mínimo por que usted no creería cuantas veces se retransmitirá el mismo virus en toda su organización. Aun cuando es posible que no haya ningún virus

del cual este consciente, necesita considerar el riesgo y añadir esta característica si surge la necesidad.

En la figura 3.19 todo el trafico que llega a la organización se analiza primero por el software antivirus que se esta ejecutando en el dispositivo de cortafuego/VPN o por un servidor ubicado en la DMZ. Prefiero la zona DMZ por que el antivirus consume mucho poder de procesamiento. Cuando el tráfico entrante se ha revisado, entonces se pasa a la red interna. Esta ubicación es un acceso muy importante si usted no está utilizando una combinación de cortafuego /VPN en caso de que el paquete que entre este cifrado deberá descifrarse antes de ser analizado.

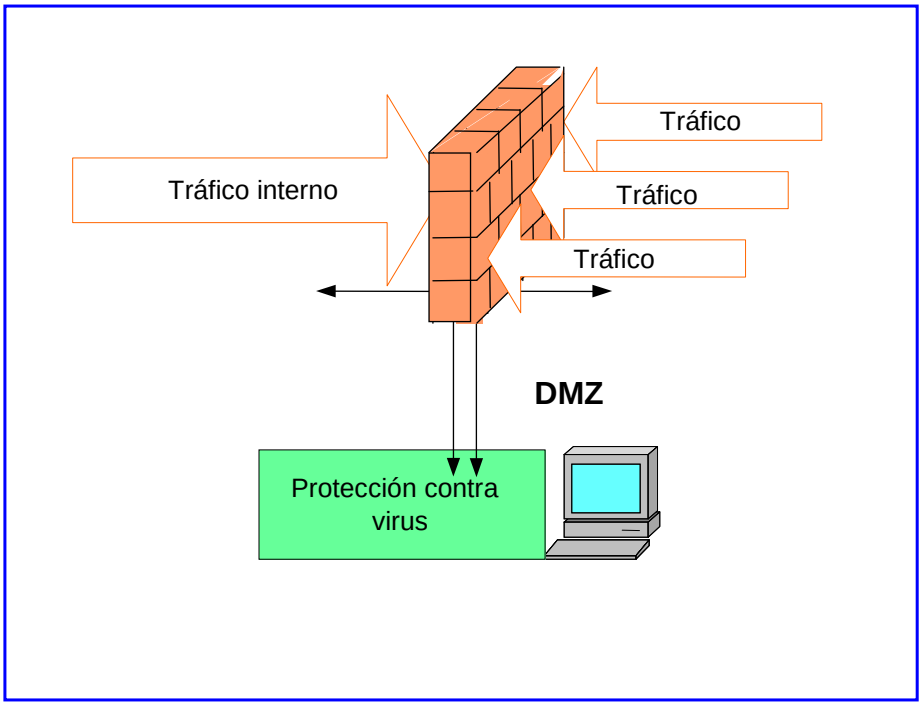


FIG. 3.19 VPN de múltiples servicios.

3.4.9 VPN basadas en software.

Por lo general se utiliza desde un cliente aun servidor. Por ejemplo en una VPN de PPTP, el software cargado en el cliente se conecta al software cargado en el servidor y establece una sesión de VPN. Cuando se selecciona una VPN de software se necesitará tener proceso de administración claves adecuados y posiblemente una autoridad emisora de certificados en sus oficinas.

El tráfico inicia desde su anfitrión específico en su organización y establece una conexión a algún servidor en otra parte. El trafico que sale del anfitrión se cifra o se encapsula, dependiendo de la VPN instalada, y se enruta a su destino. Lo mismo ocurre para alguien que esta tratando de conectarse a su red interna; una máquina cliente en alguna parte inicia una sesión de cliente VPN e inicia un diálogo de comunicación con el servidor VPN de su organización. Esta comunicación establece que tipo de cifrado y cual algoritmo de autenticación deben utilizarse y otros datos importantes para utilizar la comunicación.

Después de que la instalación inicial se ha completado, comienza el flujo de datos. En este ejemplo, si su cortafuego no es el dispositivo VPN, asegúrese de que esta configurado para pasar el algoritmo de cifrado de su elección.

3.4.10 Conmutadores de túnel para VPN.

Este dispositivo tiene toda la funcionalidad tradicional de la arquitectura de VPN de hoy en día, con la característica agregada de estar en un único dispositivo físico. Esta arquitectura de VPN de múltiples propósitos está diseñada para combinar todas las características de los dispositivos de red tradicionales asociados con la conexión de Internet. Los cortafuegos, el enrutamiento y la funcionalidad de VPN están combinados en un producto independiente para producir un escenario empresarial todo en uno, incluyendo el establecimiento de túneles de VPN de sitio a sitio, el acceso de usuarios remotos y el acceso de túneles en cualquier parte de su empresa. Están construidos para ampliarse a miles de usuarios, sea en un modo de encapsulamiento o en un modo de cifrado. También soportan el encapsulamiento dinámico de los

protocolos que no están basados en IP, como IPX y SNA. Soportan los protocolos PPTP tradicionales para usuarios de marcación remota, y algoritmos de cifrado como IPSEC para conexión de túneles de LAN a LAN.

3.4.11 Comparaciones de desempeño.

Es posible que la instalación de la VPN adecuada sea difícil pero existen muchos factores que puede estudiar para decidir si un producto de VPN es adecuado para su organización. En la tabla 3.1 se observa una lista de algunas de las ventajas y desventajas asociadas con cada tipo de arquitectura de VPN.

Arquitectura de RPV	Ventaja	Desventaja
Hardware	*Buen desempeño; buena seguridad, carga de cifrado minima para paquetes grandes; un poco de soporte para balanceo de cargas.*	Flexibilidad limitada, precio alto; sininterfaces ATM, FDI o Token Ring, la mayoria son semiduplex; se necesita reiniciar para que los cambios tengan efecto algunos tienen problemas de desempeño importantes con paquetes pequeños (64 bytes); funcionalidad de subred limitada; algunos carece de NAT
Software	Amplia variedad de plataforma facilidad de instalacion; buena paara una amplia gama de compañias	Problemas de desempeño con el soporte NAT; algunos tienen tecnologias de cifrado viejas; propietario; algunos carecen de capacidad de administracion remota sin capacidad de supervision.
Enrutar	Uso del hardware existente seguridad solides disponible bajo costo si se utilizan los enrutadores existentes.	Algunos pueden necesitar tarjetas de cifrado adicionales; problemas de desempe ño; pueden requerir una actualizacion a un enrutador mas potente.
Cortafuego	mas; uso del hardware existente; soporte para balance de cargas y cortafue- gos redundantes; IPSEC de bajo costo.	Posibles problemas de seguridad debido al sistema operativo; no todos son completamente interoperables con soporte RADIOUS; algunos tienen problemas de licencias.
Marcacion	Facil establecimiento de RPV; el costo es bajo.	Problemas con compresion de datos cifrados; el soporte para RADIOUS es minimo.

Tabla 3.1 Comparacion dedesempeño entre las diferentes arquitecturas de RPV

3.5 EJEMPLO DE APLICACIÓN.

COMERCIO ELECTRÓNICO ENTRE SOLECSA ECUADOR E INDURA CHILE A TRAVÉS DE VPN.

La empresa SOLECSA (Soldaduras Ecuatorianas S.A.) es una empresa dedicada a la venta de gases y soldadura que ha venido creciendo en los últimos 5 años, su competencia directa es AGA. SOLECSA vende solo productos que compra directamente al fabricante INDURA Chile. Al incrementarse el inventario que manejan, se ha presentado una serie de problemas debido a que muchos de sus productos se compran bajo pedido y no se pueden dejar en cualquier parte por un tiempo excesivo sin vigilancia permanente.

Los proveedores INDURA Chile empiezan la elaboración de los productos solo después de haber recibido la orden de compra y cualquier retraso en la misma provoca que la entrega del pedido de un cliente en Ecuador se detenga para la próxima semana, en la que se hace el nuevo envío desde Chile, provocando que el cliente compre obligadamente los materiales

a otro proveedor porque sino sus trabajos se retrasarían por varios días.

En este entorno, se hace sumamente necesario un sistema de ñautomatizaci· n de compra-venta entre SOLECSA e INDURAò o sea una aplicación de e-commerce, a continuación analizamos una solución con VPN.

SITUACIÓN ACTUAL.

- Aplicación Contable:

  FLEX

- Forma de Comercio entre SOLECSA E INDURA Chile:

  FORMA TRADICIONAL (E-MAIL)

- Sistema de Mensaje:

  OUTLOOK 97 STANDARD EDITION.

Problemas Actuales:

Los datos son ingresados 2 y hasta 3 veces esto es debido a

que el sistema de SOLECSA no es compatible para recibir transacciones desde el sistema INDURA Chile, no existe funcionalidad que garantice autenticidad e integridad entre los 2 sistemas.

- Los usuarios se autentifican primero al sistema de mensajería y luego nuevamente a la aplicación contable FLEX.

- Los errores cometidos por uno de los dos lados deben esperar a ser detectados por el otro lado, luego esperar que el otro lado notifique a los primeros, y finalmente esperar a que los primeros detecten y corrijan el error para luego recién enviar la transacción corregida vía e-mail.

Todo esto se observa en la figura 3.20, la forma de compra y venta tradicional de SOLECSA e INDURA de Chile.

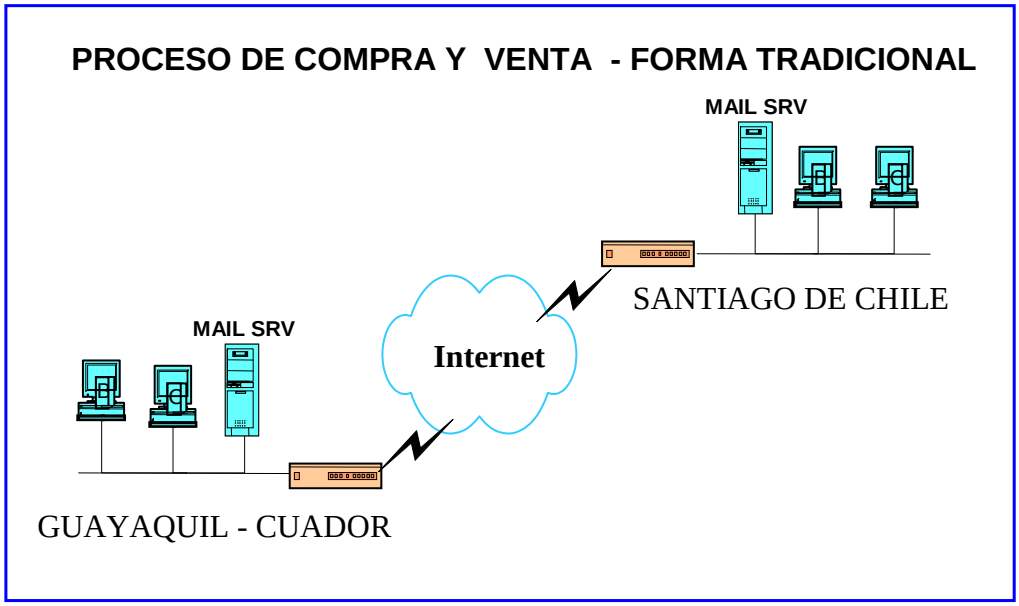


FIG. 3.20 Proceso de Compra y Venta - Forma Tradicional.

SITUACIÓN DESPUES DE QUE SE IMPLEMENTE SOLUCIÓN DE E-COMMERCE.

- Aplicación Contable:

  SAP

- Forma de Comercio Electrónico entre SOLECSA e INDURA:

  SAP

- Sistema de Mensaje:

NO INDISPENSABLE.

Problemas Resueltos:

- Los datos son ingresados una sola vez al sistema, y pueden ser acezados instantáneamente por el siguiente participante del proceso sin importar si este es de la empresa que compra o de la empresa que vende.

- El sistema de acreditar la transacción garantiza el movimiento de compra y/o venta del usuario.

- Los usuarios se autentifican una sola vez al sistema y relegan el sistema de mensajería para casos especiales, que tiene con el sistema de comercio electrónico toda la información que necesitan en línea.

- Los errores humanos se reducen debido a un mayor número de datos, puede ser depurados y comparados automáticamente con el otro lado de la transacción.

- Los errores que no pueden ser detectados por el sistema pueden ser corregidos más rápido y pueden ser detectados instantáneamente por el otro participante de la transacción.

Comparacion de Costos:

El costo de implementar un sistema SAP básico supera los USD 300.000 unas 20 veces más del valor del sistema que se está usando actualmente, pero esta inversión si es aceptable cuando las pérdidas por mala sistematización alcanzan el USD 1´000.000 al año.

Nuevos Problemas Presentes:

La mayoría de las soluciones de e-commerce terminadas y probadas trabajan con tecnología EDI, esto implica que sus bloques de datos van a viajar en forma llana (no encriptada),

Cuando se creó el EDI (Electronic Document Interchange), la preocupación principal era que las transacciones fueran compatibles y legibles por cualquier sistema.

Esta forma hace necesario que el canal de comunicación entre comprador y el proveedor sea un canal dedicado punto a punto. Como se observa en la figura 3.21.

Creyendo de esta forma que la transacción de compra y venta sea rápida y segura para la empresa.

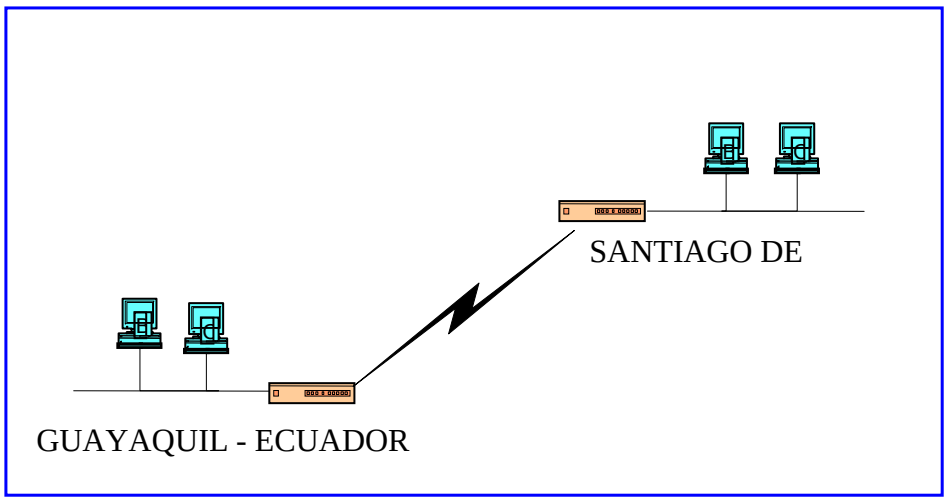


FIG. 3.21 Comercio Electrónico - Con un Enlace Dedicado.

SITUACIÓN DESPUÉS DE USAR UN ENLACE VPN:

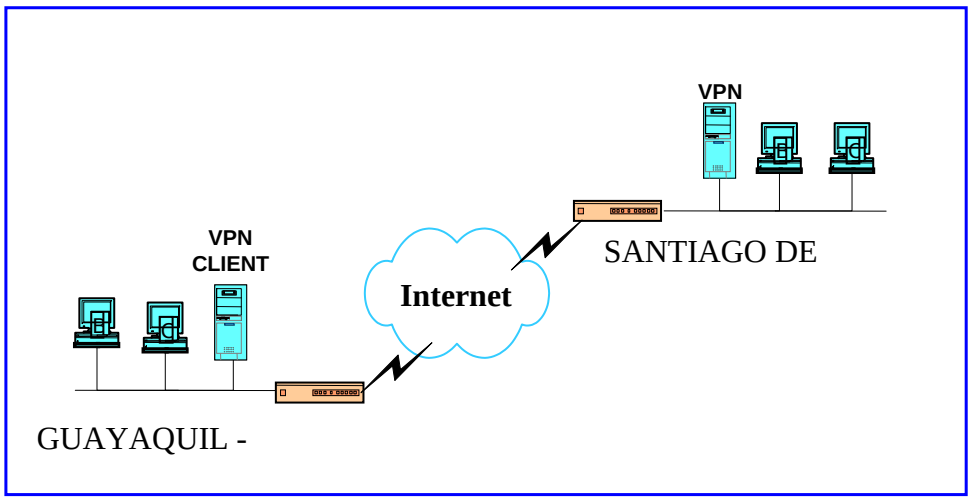


FIG. 3.22 Comercio Electrónico a través de VPN.

Problema Resuelto:

La data puede viajar de forma segura a través de un enlace a Internet, garantizando su confidencialidad e integridad.

Comparación de Costos:

Al usar tecnología de VPN se reduce el costo debido a que un enlace de 256 Kbps punto a punto SOLECSA (Guayaquil) ï indura (Santiago de Chile) tiene un costo de USD 2800,00

CAPITULO IV.

SITUACIÓN ACTUAL DEL E-COMMERCE EN EL ECUADOR.

4.1. INTRODUCCIÓN.

Hoy en día estamos seguros cada vez más de lo que se puede hacer a través de Internet, y la diferencia a otros tiempos es la rapidez con que se trabaja. Cuando hubo el Boon de Internet, no se pensó que todo se iba a manejar mediante él y así darle una facilidad a las personas, esto nos hizo hacer un enfoque hacia el consumidor. Se pensó que todo se iba a comprar a través de la red, que no iban haber centros comerciales ni compras por teléfono. Y lo que estamos aprendiendo poco a poco es que esa no es la situación, en la Red hay un espacio para el consumidor, pero hay otros relacionados con el ¨bussiness to bussiness¨ (B2B).

El Internet es comercialización hacia el exterior, y, por eso, era necesaria la concentración de la ley de comercio electrónico.

principales y comentarios del mismo, cabe indicar que este cuerpo de leyes se encuentra aún ciertos detalles por mejorar.

TITULO PRELIMINAR.

- Principios Generales. Se refiere al ámbito de aplicación de esta ley y la definición de varios términos a los que se refiere la misma. A continuación enumeramos sus artículos con sus respectivos títulos:

Art. 1.- Objeto de la ley.

Art. 2.- Reconocimiento jurídico de los mensajes de datos.

Art. 3.- Incorporación por remisión.

Art. 4.- Propiedad intelectual.

Art. 5.- Confidencialidad y reserva.

Art. 6.- Información escrita.

Art. 7.- Información original.

Art. 8.- Conservación de los mensajes de datos.

Art. 9.- Protección de datos.

Art. 10.- Procedencia e identidad de un mensaje de datos.

Art. 11.- Envío y recepción de los mensajes de datos.

Art. 12.- Duplicación del mensaje de datos.

TÍTULO II. DE LAS FIRMAS ELECTRÓNICAS, CERTIFICADOS DE FIRMA ELCTRÓNICA, ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN, ORGANISMOS DE PROMOCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS.

- CAPÍTULO I. DE LAS FIRMAS ELECTRÓNICAS.- Enfoca los efectos de la firma electrónica, requisitos, obligaciones, duración y revocación de firmas electrónicas. A continuación enumeramos sus artículos con sus respectivos títulos:

Art. 13.- Firma electrónica.

Art. 14.- Efectos de la firma electrónica.

Art. 15.- Requisitos de la firma electrónica.

Art. 16.- La firma electrónica en un mensaje de datos.

Art. 17.- Obligaciones del titular de la firma electrónica.

Art. 18.- Duración de la firma electrónica.

Art. 19.- Extinción de la firma electrónica.

- CAPÍTULO II. DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA.- Especifica los requisitos de certificados, duración, extinción y revocación de los certificados de firma electrónica, suspensión y reconocimiento de certificados de firma electrónica. A continuación se enumeran sus artículos con sus respectivos títulos.

Art. 20.- Certificado de firma electrónica.

Art. 21.- Uso del certificado de firma electrónica.

Art. 22.- Requisitos del certificado de firma electrónica.

Art. 23.- Duración del certificado de firma electrónica.

Art. 24.- Extinción del certificado de firma electrónica.

Art. 25.- Suspensión del certificado de firma electrónica.

Art. 26.- Revocatoria del certificado de firma electrónica.

Art. 27 Tanto la suspensión temporal, como la revocatoria, Surtirán efectos desde el momento de su comunicación con relación a su titular.

Art. 28.- Reconocimiento internacional de certificados de firma electrónica.

- CAPÍTULO III.- DE LAS ENTIDADES DE CERTIFICACIÓN.- Abarca las obligaciones, responsabilidades, protección de datos, terminación y cesación de actividades. A continuación enumeramos sus artículos y sus respectivos títulos:

Art. 29.- Entidades de certificación de información.

Art. 30.- Obligaciones de las entidades de certificación de información acreditada.

Art. 31.- Responsabilidades de las entidades de certifica ción acreditadas.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.

Art. 33.- Prestación de Servicios de Certificación por parte de terceros.

Art. 34.- Terminación contractual.

Art. 35.- Notificación de cesación de actividades.

- CAPÍTULO IV.- DE LOS ORGANISMOS DE PROMOCIÓN Y DIFUCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS.- Detalla los organismos encargados de la administración, sanciones, infracciones y funciones de tales organismos. A continuación enumeramos sus artículos con sus respectivos títulos:

Art. 36.- Organismo de promoción y difusión.

Art. 37.- Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.

Art. 38.- Organismo de control de las entidades de certifica ción de información acreditadas.

Art. 39.- Funciones del organismo de control.

Art. 40.- Infracciones Administrativas.

Art. 41.- Sanciones.

Art. 42.- Medidas cautelares en los procedimientos instau- rados por infracciones graves.

Art. 43.- Procedimiento.

TÍTULO III.- DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INTRUMENTOS PÚBLICOS.- Consta de tres capítulos:

- CAPÍTULO I.- DE LOS SERVICIOS ELECTRÓNICOS.- Indica que las actividades electrónicas que se realicen a través de redes de datos se someterán a los requisitos y solemnidades en la ley que las rija.

  Art. 44.- Cumplimiento de formalidades.

- CAPÍTULO II.- DE LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA.- Enfoca la validez de los contratos, recepción, aceptación y jurisdicción de los contratos electrónicos. A continuación enumeramos sus artículos con sus respectivos títulos.

  Art. 45.- Valides de los contratos electrónicos.

  Art. 46.- Perfeccionamiento y aceptación de los contratos electrónicos.

Art. 47.- Jurisdicción.

- CAPÍTULO III.- DE LOS DERECHOS DE LOS USUARIOS O CONSUMIDORES DE SERVICIOS ELECTRÓNICOS.- Señala la protección al usuario y la reserva para el envío o la recepción de la información. A continuación enumeramos sus artículos con sus respectivos títulos.

Art. 48.- Consentimiento para aceptar mensajes de datos.

Art. 49.- Consentimiento para el uso de medios electrónicos.

Art. 50.- Información al consumidor.

- CAPÍTULO IV.- DE LOS INTRUMENTOS PÚBLICOS.- Reconoce la validez jurídica de los instrumentos públicos, y el tipo de notificación de controversias. A continuación enumeramos su artículo con su respectivo título:

Art. 51.- Instrumentos públicos electrónicos.

TÍTULO IV.- DE LA PRUEBA Y NOTIFICACIONES ELECTRÓNICAS.- Se considera a los mensajes, firmas y documentos electrónicos medios de prueba válida, presunción de firmas electrónicas, pruebas como tal y valoración de las pruebas presentadas. A continuación enumeramos sus artículos con sus respectivos títulos:

Art. 52.- Medios de prueba.

Art. 53.- Presunción.

Art. 54.- Práctica de la prueba.

Art. 55.- Valoración de la prueba.

Art. 56.- Notificaciones electrónicas.

TÍTULO V.- DE LAS INFRACCIONES INFORMÁTICAS.- Reseña el fraude informático, daños informáticos, falsedad informática, intrusión indebida a los sistemas informáticos, recopilación de información no autorizada, violaciones del derecho de la privacidad y el robo electrónico. A continuación enumeramos sus artículos con sus respectivos títulos:

Art. 57.- Infracciones informáticas.

Art. 58 al Art. 64.- Son reformas al código penal y no tienen título.

DISPOSICIONES GENERALES, TRANSITORIAS Y FINALES.- Trata sobre las infracciones que vayan en contra de otras vigentes y sobre la constitución.

4.3. DESVENTAJAS QUE HACEN QUE NUESTRO PAIS ESTÉ ENTRE LOS ÚLTIMOS EN EL RANKING DE COMPETITIVIDAD.

La conexión a Internet por parte de las masas es una dificultad en nuestro país. Según las estadísticas luego de Bolivia, Ecuador tiene la segunda menor penetración de Internet en Latinoamérica.

Eso es un gran impedimento. En lo que debe trabajar tanto el sector público como el privado es en esto: en Ecuador nunca se llegará a una penetración como, por ejemplo EEUU o Europa, pero lo que sí se puede tener es centros de Internet. No deben

ser solo ¨Cafés Net¨ como negocios privados, sino como penetró Internet en EEUU: las bibliotecas de las universidades fueron los primeros lugares que lo tuvieron. La gente se enseñó y empezó a apreciar su valor. Ese es un impedimento, pero no algo que no se pueda superar.

Obviamente en otras áreas no directamente vinculadas con la red hay algunos desafíos respecto a la competitividad. Entre ellos está la mentalidad de la gente. Hay que cambiar. Hay muchos negocios familiares, o dirigentes de una generación que tienen la idea de que como han tenido éxito en 20 años, seguirán ese modelo. No quieren cambiar porque creen que si funcionó en el pasado, funcionará en el futuro.

Pero la verdad es que los productos y servicios tienen ciclos. Por ejemplo, la máquina de escribir tuvo un ciclo de vida y se acabó.

Ahora hay Internet y computadoras. Pero también los diseños y estrategias para manejar un negocio tienen ciclos de vida y hay que cambiar con el tiempo. En pocos años el mercado

ecuatoriano se abrirá a América mediante el ALCA; el Presidente y el Congreso se han comprometido a ello porque realmente no hay otra opción. Si Ecuador queda fuera del ALCA, no tendrá donde vender sus productos, y no tiene una economía suficientemente grande para producir todo lo que se necesita.

Entonces primero hay que cambiar la mentalidad. Hay que trabajar en un mundo globalizado, en un mercado globalizado, y eso significa que, en vez de contar solo con una fuerza laboral barata, hay que empezar a implementar tecnología, máquina, computadoras, en los procesos para que las compañías lleguen a ser más competitivas.

Otra desventaja es la inevitable globalización, que hace los productos más caros para la exportación. No hay duda. Pero no hay que caer en la misma trampa Argentina, que dijo que la convertibilidad, en el caso de Ecuador, la dolarización es todo.

Los argentinos dijeron: “tenemos estabilidad, estamos felices, ganamos en dólares”. Entonces, llegaron a la idea de mejorar los

procesos, mejorar el servicio al cliente y planeación estratégica. Pensaron que la convertibilidad era una opción.

4.4. QUE ESTRATEGIA DEBE TENER EL ECUADOR PARA SER MÁS COMPETITIVO.

Ecuador tiene un grave problema de balanza comercial. Todavía estamos a tiempo de mejorar, aunque si se ven las cifras, cada año crece el déficit comercial. Por supuesto, Ecuador no puede dejar la dolarización por ello porque regresaría a lo mismo. Los sucres se devaluaban; nadie ahorraba dinero porque todos gastaban lo poco que tenían y no era bueno para el desarrollo del país.

Hay que trabajar para que Ecuador y sus productos sean competitivos en el ámbito global y aquello se hace mediante mejores procesos, tecnológicos y planeación estratégica, para compensar. Sin la dolarización se vuelven los productos más caros para exportar, hay que encontrar otra herramienta en la caja- porque la dolarización solo es una herramienta para

bajar los precios de exportación. Hay países que lo han logrado, y su mejor arma ha sido siempre la optimización del uso de la tecnología. No significa que halla que estar adquiriendo continuamente la mejor tecnología, sino que al contrario se debe dar el mejor aprovechamiento a la tecnología existente o adquirida.

Ecuador está en un cambio de la generación de ejecutivos.

Ejecutivos jóvenes que todavía no son gerentes generales de empresas sino de operaciones o mercadeo, y estos jóvenes les interesa Internet como una herramienta.

En este entorno de competencia es de vital importancia que en el país se utilicen herramientas seguras y económicas como las VPN que pueden ser implementadas sobre cualquier plataforma y configuradas desde el nivel básico hasta el más estricto requerido según la situación.

CONCLUCIONES Y RECOMENDACIONES

Como se puede ver en este trabajo, las distintas infraestructuras de red y los diferentes requisitos organizacionales exigen diversos tipos de arquitecturas. Toda la información proporcionada permite elaborar una solución potencial en cuanto a la seguridad, la autorización y el acceso de los usuarios, la interoperabilidad con la infraestructura de red interna y con los clientes y proveedores externos de cualquier empresa.

Las VPN continuarán creciendo. Con el comercio electrónico y cada vez más negocios son dirigidos a través de Internet, es necesario establecer un ambiente seguro. Cada encuesta que usted lea le indicará el crecimiento de Internet y la dirección del crecimiento futuro.

Los servicios que empujan este crecimiento global de Internet y en consecuencia los servicios relacionados con Internet son la telefonía IP, el envío de fax por Internet, las conferencias en red y las aplicaciones multimedia, por nombrar algunos. La velocidad de esa información puede depender de su conducto

de ancho de banda de Internet y de los diversos ISP que deba atravesar para llegar a ella y, como sucede con todo lo demás en la tecnología, la velocidad se incrementará.

Las VPN satisfacen las más estrictas necesidades de seguridad; son rápidas y sencillas. Las personas se acostumbrarán tanto a Internet que ni siquiera se preocuparán porque sus paquetes lleguen cifrados, se supondrán para ese momento la seguridad de la red es optima.

Esta es una de las principales razones por las que debemos usar tecnologías como la VPN para proporcionar este nivel óptimo de seguridad necesario en las transacciones de comercio electrónico muestra cada vez más pequeña la “Aldea Global”.

GLOSARIO

Blowfish = (pez globo), Comunicaciones Seguras
Criptográficas= Técnicas para tener segura la información.
Cyber Cash = Ciber efectivo
Diffie-Helman = Sistema para intercambio de llaves
DNS = Domain Name system
DNSSEC = Domain Name Security
DSS = Digital Signature Estándar
HMAC = Hashed Message Autenthication Code
http = Hypertext Transfer Protocol
Hash = Sistema de prueba de seguridad
ICMP = Internet Control Message Protocol
IDEA = International Data Encription Algorithm
IETEF = Internet Engineering Task Force
IRC = Internet Relay Chat
MAC = Message Autentication Codes
MD2 = Message Digest # 2
MD4 = Message Digest # 4
MD5 = Message Digest # 5
message digest = compendio de mensajes
MIME = Multipurpose Internet Mail Extensions
NTP = Network Time Protocol

PASV = modo pasivo
PCT = Private Comunications Technology (Tecnología de
PGP = Pretty Good Privacy
rlogin = login remoto

RPC = Procedure Call

RPV = redes privadas virtuales

SET = Transacciones Electrónicas Seguras, Secure Electronic
SHA = Secure Hash Algorithm
SMTP = Simple Mail Transfer Protocol.

SNMP = Simple Network Management Protocol

SSH = secure shell
SSL = Secure Sockets Layer
VPN = Virtual Private Network

www = World Wide Web

BIBLIOGRAFÍA

http://www.verising.com

http://www.rsa.com

http://www.monografias.com

http://www.nist.com

http://www.computerprivacy.com

http://ipsec-wit.antd.nist.gov

RFC 1702 Generic Routing Encapsulation over Ipv4 networks.

RFC 2410 The NULL Encriptation Algorithm and its use with IPSec.

RFC 2411 IP Security Document Roadmap.

Private Network Virtual Implementation. Steven Brown.

Cryptography and Data Security. Denning Dorothy E.

Criptography Policy. Hoffman Lance J.

Protocols for Public Key Cryptosystems. G. J. Simmons.