UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SEGURIDAD EN REDES DE TELECOMUNICACIONES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JOSÉ SAÚL BRAÑES PAGÁN

PROMOCIÓN
1995 - II

LIMA – PERÚ
2003

Dedico este trabajo a:

A mi hijo Keith por regalarme momentos agradables.

A mis padres Rayda y Elías por ser los forjadores de mi persona,

además de ser mis amigos en todo momento, y

A mi tía Berti por su apoyo incondicional.

SEGURIDAD EN REDES DE TELECOMUNICACIONES

SUMARIO

El presente informe recoge los principales métodos y tecnologías para lograr que las redes de telecomunicaciones brinden los elementos necesarios para asegurar la información transmitida por dichas redes.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

El objetivo principal de asegurar una red es la búsqueda del control de acceso, disponibilidad, integridad, confidencialidad y autenticidad de la información.

Siendo el tema de seguridad de redes de telecomunicaciones bastante amplio el presente trabajo intenta rescatar lo más importante de como proteger las redes y lograr así tener conexiones seguras.

El capítulo I se realiza una introducción a la seguridad brindando conceptos fundamentales. El capítulo II reseña en forma breve los tipos de redes existentes en la actualidad. El capítulo III se describe el protocolo de seguridad para IP (IPSec). El

capitulo IV detalla los tipos de redes privadas virtuales (VPNs) y los protocolos que se utilizan. El capítulo V explica las características de los cortafuegos, sus diferentes tipos y arquitecturas. El capítulo VI describe a los sistemas de detección de intrusos (más conocidos como IDSes). En el capítulo VII se explica los conceptos de infraestructura de clave publica y uso de la encriptación para asegurar la información. El capítulo VIII detalla las fases fundamentales del diseño e implementación de una red segura. Por último se detallan las principales conclusiones del presente informe, las abreviaturas usadas y el material bibliográfico.

ÍNDICE

CAPÍTULO IV

REDES PRIVADAS VIRTUALES

CAPÍTULO V

CORTAFUEGOS (FIREWALLS)

PRÓLOGO

Las redes de telecomunicaciones han tenido un crecimiento exponencial dentro de los últimos 50 años y se han convertido en un medio importante dentro de las comunicaciones globales, a pesar de estos grandes avances que han llegado a satisfacer muchas necesidades con distintos servicios (entre las cuales podemos mencıonar: La telefonía, teletexto, servicios de conmutación de paquetes, videoconferencia, voz sobre IP, etc.), las redes fueron vulneradas porque no fue un aspecto considerado en el diseño inicial de los protocolos de comunicación es así que se vio la necesidad de asegurar la comunicación extremo a extremo para que personas inescrupulosas no tengan oportunidad de acceder de forma no autorizada a información importante transmitida por las redes. Debido a dicho crecimiento abrupto, pocas empresas y/o personas se dedicaron a prestar atención a la seguridad de las comunicaciones, presentándose problemas serios que en los últimos 10 años se esta tratando de corregir con distintos métodos y tecnologías nuevas que serán tratados en el presente informe de suficiencia.

CAPÍTULO I

INTRODUCCIÓN

La seguridad ha sido un elemento que tomó importancia en la última década dentro del mundo de las Telecomunicaciones, debido al crecimiento de forma exponencial de las redes se perdió las características de conocimiento y confianza entre quienes interactúan en una comunicación extremo a extremo. La seguridad no fue un aspecto considerado en el diseño inicial de los protocolos de comunicación y sistemas operativos, lo que ha ocasionado oportunidades diversas para acceder de forma no autorizada a redes y sistemas y ha dado lugar a una de las actividades más populares en estos días en el ciberespacio: la intrusión de sistemas.

En 1988 en los Estados Unidos se crea el primer "Equipo de Respuesta a Emergencias de Computadoras" CERT, conformado en su mayor parte por voluntarios expertos calificados con el único objetivo de brindar una respuesta rápida a los problemas de seguridad, debido a que a finales de ese año se reporto el primer incidente que llego a afectar a miles de computadoras conectadas a Internet cuando un programador llamado Robert Morris creo el primer gusano (worm) que generó

muchas perdidas, desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta.

Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Actualmente se estima que Internet es una red con más 90 millones de computadoras conectadas, de más de 200 países de todos los continentes, millones de usuarios, de diferentes culturas, con diferentes propósitos, inquietudes, edades, etc. En el año 2001 se registraron con respecto al año 2000, el doble de incidentes de seguridad, y por consiguiente el doble de computadoras afectadas por estos incidentes, cabe mencionar que hasta Septiembre de 2002 incluso se había triplicado el número de incidentes con respecto a año 2000.

En los últimos años se han desarrollado una gran variedad de herramientas, metodologías y técnicas para contrarrestar estas deficiencias de origen y proteger a los sistemas de intrusos, sobre todo al nivel de aplicaciones del usuario o del administrador de la red.

1.1. ¿QUÉ ES SEGURIDAD?

Desde el punto de vista gramático la seguridad es sinónimo de garantía, estabilidad, inmunidad, protección y tranquilidad.

Entendemos por seguridad la característica de cualquier sistema que nos indica que ese sistema esta libre de todo peligro, daño o riesgo, y que es, en cierta manera infalible. Como ésta característica, particularizando para el caso para redes de telecomunicaciones, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) mas que de

seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

1.2. OBJETIVOS DE SEGURIDAD

Los objetivos fundamentales en Seguridad son: prevenir la revelación, la modificación y la utilización no autorizada de datos, recursos de computadora y de red. La definición del estándar ISO 7498-2 define cinco elementos básicos que constituyen la seguridad de un sistema: la confidencialidad de los datos, la autenticación de los datos, la integridad de los datos, el control de acceso (disponibilidad) y el no repudio.

1) Confidencialidad implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas.

2) Autenticación define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de computadora.

3) Integridad implica que los datos no deben ser modificados o corrompidos de manera alguna desde su transmisión hasta su recepción.

4) El control de acceso establece la forma en que el recurso está disponible cuando es requerido.

5) El no repudio es la garantía de transmisión y recepción de información, busca proteger al emisor de que el receptor niegue haber recibido el mensaje, y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

En seguridad de información, se consideran seis elementos sobre los cuales se han hecho desarrollos en busca de proporcionar ambientes protegidos:

a) Seguridad física: un elemento de atención básica, los recursos deben ser protegidos físicamente de accesos no autorizados, accidentes, robos, etc.

b) Seguridad de procedimientos: elemento enfocado a las medidas de protección en los procesos y procedimientos.

c) Seguridad de personal: elemento enfocado a la definición de privilegios, y accesos de personal involucrado con los recursos.

d) Seguridad de emanación de compromisos: elemento enfocado a la definición de responsabilidades y compromisos en el manejo de la información.

e) Seguridad de sistemas operativos: elemento enfocado a la protección de servicios y usuarios, accesos no autorizados al sistema operativo de una computadora.

f) Seguridad de comunicaciones: elemento enfocado a la transmisión segura de información a través de medios de comunicación.

Prevención es la palabra clave en Seguridad, se han desarrollado una gran diversidad de técnicas y herramientas de prevención a nivel de aplicaciones, siempre dependientes del sistema operativo o la aplicación que se utilice. Los protocolos de seguridad buscan brindar servicios de seguridad en la transmisión de información, sin importar el tipo, procedencia, sistema operativo o aplicación que la genere.

1.3. TERMINOLOGÍA

Dentro del área de Seguridad, se manejan diversos términos para identificar los factores que intervienen, los conceptos principales son: vulnerabilidades, ataques, contramedidas y amenazas.

1.3.1 Vulnerabilidades

El software está desarrollado por humanos, quienes modelan e implantan programas a su criterio, concepto y conocimiento del lenguaje de programación que utilizan, es común, en consecuencia, encontrar imperfecciones en los sistemas. Son éstas imperfecciones las que propician oportunidades para accesos no autorizados, las que se conocen como vulnerabilidades de los sistemas.

1.3.2 Ataques

Los ataques son los medios por los cuales se explotan las vulnerabilidades, se identifican dos tipos de ataques: extracción (wiretapping) pasiva y extracción activa. En la extracción pasiva el atacante escucha, sin modificar mensajes o afectar la operación de la red. Generalmente no puede detectarse este tipo de ataque, pero sí prevenirse mediante mecanismos como la encriptación de información.

Los objetivos del atacante son la interceptación y el análisis de tráfico en la red. Al estar escuchando el tráfico, el atacante puede identificar:

· El origen y destino de los paquetes de comunicación, así como la información de cabecera.

· Monitorear el tráfico y horarios de actividad.

· Identificar el uso de protocolos y observar la transferencia de datos entre protocolos que no utilicen encriptado, por ejemplo la versión no segura de telnet o ftp que transfieren la clave de usuario en texto simple.

En la extracción activa el atacante modifica los mensajes o irrumpe la operación de la red. El atacante tiene como objetivo modificar datos o bien crear tráfico falso. Este tipo de ataque, generalmente puede detectarse, pero no prevenirse. La gama de actividades identificadas sobre ataques conocidos puede clasificarse en cuatro categorías:

1) Modificación de mensajes: al interceptar mensajes, se altera su contenido o su orden para irrumpir su flujo normal.

2) Degradación y fraude del servicio: tiene como objetivo intervenir el funcionamiento normal de un servicio, impide el uso o la gestión de recursos en la red. Ejemplo de este ataque es el de negación de servicio (DoS, Denial of Service), donde se suprimen los servicios de SMTP, HTTP, FTP, DNS, entre otros.

3) Reactuación: al interceptar mensajes legítimos, se capturan y repiten para producir efectos diversos, como el ingresar dinero repetidas veces en una cuenta de banco.

4) Suplantación de identidad: Este es uno de los ataques más completos y nocivos. El intruso o atacante adopta una identidad con privilegios en una red y explota esos privilegios para sus fines. Un ataque con prioridad de atención para todo administrador de red es el "spoofing" donde el intruso obtiene servicios basados en la autenticación de computadoras por su dirección IP. Es recomendable seguir una estrategia y de preferencia tener una herramienta para combatirlos.

Todos estos ataques tienen un impacto relativo a la política de seguridad de un sistema, aunque en Internet dentro de los más temidos se encuentra el DoS por su relevancia al suprimir el funcionamiento de un sistema, y el Spoofing al obtener privilegios de acceso de forma fraudulenta.

1.3.3 Contramedidas

Lo más importante es contar con una Política de Seguridad, un documento legal y con apoyo directivo, que define la misión, visión y objetivos de los recursos de red e información en cuestión. En una política se define lo que es permitido y lo que no, las necesidades de confidencialidad, autenticación y otros servicios de seguridad para los recursos involucrados. Toda red debe contar con una política de seguridad.

Las contramedidas son entonces, las políticas de seguridad apoyadas por todos los medios técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos. Ejemplos: reglamentos, cortafuegos, nessus, ssh, tcp-wappers, antivirus, kerberos, radius, entre muchos otros comerciales o de dominio público.

1.3.4 Amenazas

Las amenazas están dadas por condiciones de entorno, dada una oportunidad y adversarios motivados y capaces de montar ataques que explotan vulnerabilidades, podría producirse una violación a la seguridad (confidencialidad, integridad, disponibilidad y/o uso legítimo). Los perfiles de capacidades de los atacantes se identifican como sigue:

· Inserción de mensajes solamente.

· Escuchar e introducir mensajes.

· Escuchar y obstruir.

· Escuchar, obstruir e insertar mensajes.

· Escuchar y remitir un mensaje ("hombre en el medio")

· Capacidades activas y pasivas de forma unidireccional o bidireccional

Cada enlace en una red y cada recurso es susceptible a diferente tipo de amenazas, de ataques, y quizá a diferentes atacantes. El análisis de riesgos y el monitoreo constante de vulnerabilidades pueden identificar las amenazas que han de ser contrarrestadas, así como especificar los mecanismos de seguridad necesarios para hacerlo.

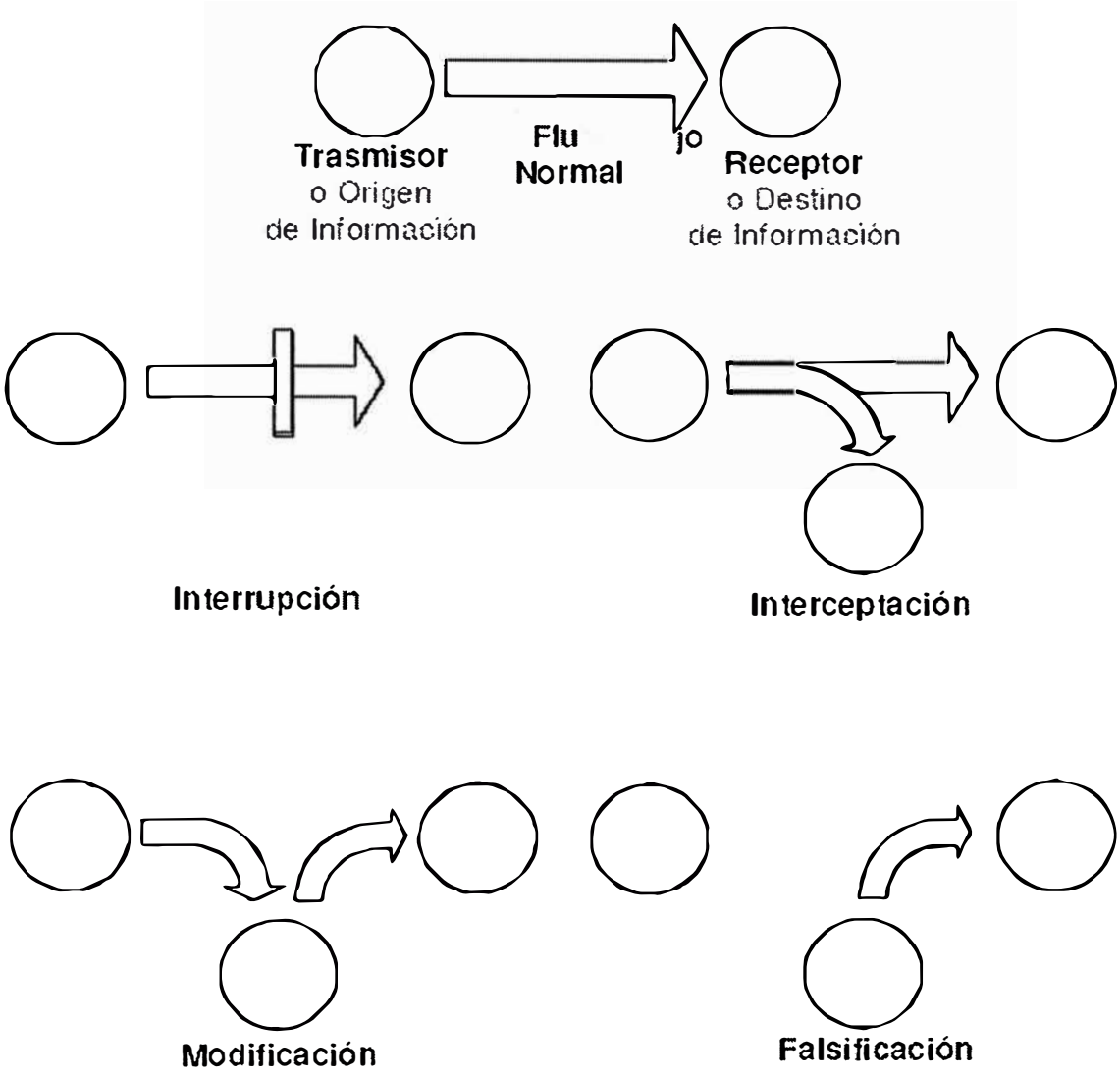


Figura 1.1 Categorías de amenazas a la seguridad

De acuerdo a la figura 1.1, las cuatro categorías generales de amenazas que se utilizan en la actualidad son las siguientes:

1) Interrupción: es una amenaza contra la disponibilidad, el ataque ocasiona que un recurso del sistema deje de estar disponible. Ejemplos: DoS, destruir un elemento de hardware o cortar una línea de comunicación.

2) Interceptación: es una amenaza contra la confidencialidad, el ataque produce la captura no autorizada de información en el medio de transmisión. Ejemplos: Sniffers, lectura de cabeceras, interceptación de datos.

3) Modificación: es una amenaza contra la integridad, el ataque produce no solo el acceso no autorizado a un recurso sino también la capacidad de manipularlo. Ejemplos: modificación del contenido de mensajes interceptados, alterar programas para modificar su funcionamiento.

4) Falsificación: es una amenaza contra la autenticidad, el ataque produce que una entidad no autorizada inserte mensajes falsos en el sistema. Ejemplos: sustitución de usuarios, alterar archivos, inserción de mensajes espurios en la red.

CAPÍTULO II

TIPOS DE REDES

2.1. INTRODUCCIÓN

Cuando una persona establece una empresa siempre piensa en obtener beneficios y para esto, en muchas ocasiones se requiere de compartir recursos (impresoras, digitalizadores, computadoras, discos duros, archivos, el conocimiento de personas, etc.) y una solución es tener una red que puede ser local, metropolitana, nacional, amplia o global, dependiendo su amplitud de la dispersión geográfica de los recursos que queremos compartir. Esos recursos deben están disponibles en el momento adecuado y que los datos o información que produzcan sean altamente confiables, esto es, que no sufran deterioro durante su transmisión. En ocasiones, será vital que contemos con réplicas de algunos recursos para que, dado el caso de un desastre en algún punto de la red, podamos consultar o acceder un recurso similar o de respaldo.

Las compañías también se han dado cuenta que resulta más barato tener una red de computadoras en donde reparten sus procesos productivos que tener una sola supercomputadora en donde concentren todo. Las ventajas de la red son: economía, capacidad de crecimiento más granular, capacidad de soportar fallas, capacidad de tener réplicas más económicas y otras.

2.2. TIPOS DE REDES POR SU DISPERSIÓN

Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen la transmisión de datos. Al primer factor le llamamos nivel físico y al segundo protocolos.

En el nivel físico generalmente encontramos señales de voltaje que tienen un significado preconcebido. Esas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma como se acceden a esos paquetes determina la tecnología de transmisión y se aceptan dos tipos: "broadcast" y "point-to-point".

Las redes de tipo "broadcast" se caracterizan porque todos los miembros (nodos) pueden acceder a todos los paquetes que circulan por el medio de transmisión.

Las redes punto a punto sólo permiten que un nodo se conecte a otro en un momento dado.

Por la extensión de las redes "broadcast" o "punto a punto", podemos clasificarlas de acuerdo a la tabla siguiente.

Distancia/CPU's	Ubicación de CPU's	Nombre
0.1 m	Tarjeta Principal CPU	Nodo
1 m	Cluster, Sistema	Multicomputadora
10 m	Sala de Computo	Red de Área Local
100 m	Edificio	Red de Área Local
1 Km	Campus	Red de Área Local
10 Km	Ciudad	Red de Área Metropolitana
100 Km	País	Red de Área Amplia
1000 Km	Continente	Red de Área Amplia
10 000 Km	Planeta	Internet

Tabla 2.1 Tipos de Redes por su dispersión

2.3. REDES DE AREA LOCAL

Las redes de área local son el punto de contacto de los usuarios finales. Su finalidad principal es la de intercambiar información entre grupos de trabajo y compartir recursos tales como impresoras y discos duros. Se caracterizan por tres factores: extensión, su tecnología de transmisión y su topología.

2.3.1 Extensión de las redes de área local

Su extensión va de unos cuantos metros hasta algunos kilómetros. Esto permite unir nodos que se encuentran en una misma sala de cómputo, en un edificio, en un campus o una empresa mediana y grande ubicada en una misma locación.

2.3.2 Tecnologías de transmisión de las redes de área local

Las redes tradicionales operan con medios de transmisión tales como cable de par trenzado (Unshielded Twisted Pair), cable coaxial (ya casi obsoleto porque presenta muchos problemas), fibra óptica (inmune a la mayoría de interferencias), portadoras de rayo infrarrojo o láser, radio y microondas en frecuencias no comerciales. Las velocidades en las redes de área local van desde 10 Megabits por segundo (Mbps) hasta 622 Mbps.

2.3.3 Topologías de las redes de área local

La topología de una red se refiere a la forma que ésta toma al hacer un diagrama del medio físico de transmisión y los dispositivos necesarios para regenerar la señal o manipular el tráfico. Las topologías generales son: anillo, bus, estrella, árbol y completas.

Las topologías de anillo, bus y árbol se adecuan mejor para redes de tipo "broadcast" y el resto para redes de tipo punto a punto.

Los estándares más comunes son el IEEE 802.3 llamado Ethernet y el IEEE 802.5 llamado Token Ring. Ethernet opera entre 10 y 100 Mbps. En este estándar, todo nodo escucha todos los paquetes de está red broadcast, saca una copia y examina el destinatario. Si el destinatario es el nodo mismo, lo procesa y si no lo deshecha para escuchar el siguiente. Para enviar un paquete escucha cuando el medio de transmisión esté libre. Si ocurre que dos nodos enviaron un paquete al mismo tiempo, se provoca una colisión y cada nodo vuelve a retransmitir su paquete después de esperar un tiempo aleatorio. Token Ring opera entre 4 y 16 Mbps y utiliza una ficha (token) que permite enviar paquetes al nodo que la posee mientras los otros escuchan. Una vez que un nodo termina de enviar paquetes, pasa la ficha a otro nodo para que transmita.

2.4. REDES DE ÁREA METROPOLITANA

Una red de área metropolitana es una versión más grande de una LAN en cuanto a topología, protocolos y medios de transmisión que abarca tal vez a un conjunto de oficinas corporativas o empresas en una ciudad. Las redes de servicio de televisión por cable se pueden considerar como MANs y, en general, a cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros. El estándar IEEE 802.6 define un tipo de MAN llamado DQDB por sus siglas en inglés Distributed Queue Dual Bus. Este estándar usa dos cables half-duplex por los cuales se recibe y transmiten voz y datos entre un conjunto de nodos.

2.5. REDES DE ÁREA AMPLIA

Una red de área amplia se expande en una zona geográfica de un país o continente. Los beneficiarios de estas redes son los que se ubican en nodos finales llamados también sistemas finales que corren aplicaciones de usuario (por ejemplo, algún

procesador de palabras o un navegador de WWW). A la infraestructura que une los nodos de usuarios se le llama subred y abarca diversos ruteadores y líneas de comunicación que une a las redes de área local. El término de subred también se aplica a una técnica para optimizar el tráfico en una red de área local de tamaño medio.

En la mayoría de las redes de área amplia se utilizan una gran variedad de medios de transmisión para cubrir grandes distancias. La transmisión puede efectuarse por microondas, por cable de cobre, fibra óptica o alguna combinación de los anteriores. Sin importar el medio, los datos en algún punto se convierten e interpretan como una secuencia de unos y ceros para formar marcos de información (frames), luego estos frames son ensamblados para formar paquetes y los paquetes a su vez construyen archivos o registros específicos de alguna aplicación.

Las redes clásicas se caracterizan porque utilizan ruteadores para unir las diferentes LANs. Como en este caso los paquetes viajan de LAN en LAN a través de ciertas rutas que los ruteadores establecen, siendo dichos paquetes almacenados temporalmente en cada ruteador, a la subred que usa este principio se le conoce como punto-a-punto, almacena-y-envía o de enrutado de paquetes (point-to-point, store-and-forward, packet-switched).

Las topologías comunes en una red punto a punto son: de estrella, anillo, árbol, completa, anillos intersectados e irregular.

2.6. REDES INALÁMBRICAS

La posibilidad de usar el aire como medio de transmisión nos da lugar a las redes inalámbricas. Se pueden construir usando estaciones de radio o satélites que envían ondas a diferentes frecuencias para enlazar los correspondientes ruteadores. Como el

alcance de estas ondas no puede ser restringido en un cierto radio, se deben tomar algunas medidas especiales para no entrar en conflicto con otras ondas y para restringir el acceso.

2.7. RED GLOBAL O INTERNET

La red Internet es aquella que se ha derivado de un proyecto del departamento de defensa de Estados Unidos y que ahora es accesible desde más de 2 millones de nodos en todo el mundo, y cuyos servicios típicos son: el WWW (Servicio Web), el correo electrónico, los foros de información globales netnews.

Por otro lado, se consideran como internets (con la letra "i" minúscula) a aquellas redes públicas o privadas que se expanden por todo el mundo. El asunto interesante es que estas internets pueden valerse del Internet en algunos tramos para cubrir el mundo. La restricción mayor para que una red privada se expanda en el mundo usando Internet es que puede verse atacada por usuarios del Internet. Un esquema de seguridad para este caso puede ser que, para las LANs que conforman la internet privada, cada una de ellas encripte su información antes de introducirla a Internet y se decodifique en las LANs destinos, previo intercambio de las claves o llaves de decodificación. Este tipo de esquemas se puede lograr con el uso de cortafuegos.

2.8. PROTOCOLOS DE COMUNICACIÓN

Un protocolo es un conjunto de reglas que indican cómo se debe llevar a cabo un intercambio de datos o información. Para que dos o más nodos en una red puedan intercambiar información es necesario que manejen el mismo conjunto de reglas, es decir, un mismo protocolo de comunicaciones.

Debido a la gran variedad de protocolos, se hizo necesario estandarizarlos y para eso se tomó un diseño estructurado o modular que produjo un modelo jerárquico conocido como modelo de referencia OSI (Open Systems Interconnection).

2.8.1 Modelo de Referencia OSI

La Organización Estándares Internacionales (ISO por sus iniciales en Inglés) emitió un modelo de referencia para la interconexión de sistemas abiertos (Open Systems Interconnection OSI). En este modelo, el propósito de cada nivel es proveer servicios al nivel superior, liberándolo de los detalles de implementación de cada servicio. La información que se envía de una computadora a otra debe pasar del nivel superior al nivel inferior atravesando todos los demás niveles de forma descendente, dentro de la computadora que origina los datos.

A su paso por cada nivel a los datos se les adiciona información que será removida al llegar a su destino. La información adicionada se clasifica en:

· Información de Control, dirigida a su nivel correspondiente en la computadora de destino. Cada nivel se comporta como si estuviera comunicándose con su contraparte en el otra computadora.

· Información de Interface, dirigida al nivel adyacente con el cual se está interactuando. El objeto de esta información es definir los servicios provistos por el nivel inferior, y como deben ser accedidos estos servicios. Esta información tras ser empleada por el nivel adyacente es removida.

El modelo OSI se estructura en 7 niveles:

1) Nivel Físico: este nivel dirige la transmisión de flujos de bits, sin estructura aparente, sobre un medio de conexión. Se encuentra relacionado con condiciones eléctricas-ópticas, mecánicas y funcionales del interfaz al medio de transmisión. A su

vez esta encargado de aportar la señal empleada para la transmisión de los datos generados por los niveles superiores. En este nivel se define la forma de conectarse el cable a las tarjetas de red, cuanto pines debe tener cada conector y el uso funcional de cada uno de ellos. Define también la técnica de transmisión a emplear para el envío de los datos sobre el medio empleado. Se encarga de activar, mantener y desactivar un circuito físico. Este nivel trata la codificación y sincronización de los bits y es el responsable de hacer llegar los bits desde una computadora a otra.

2) Nivel de Enlace de Datos: este nivel se encarga, en la computadora de origen, de alojar en una estructura lógica de agrupación de bits, llamada Trama (Frame), los datos provenientes de los niveles superiores. En la computadora de destino, se encarga de agrupar los bits provenientes del nivel físico en tramas de datos (Frames) que serán entregadas al nivel de red. Este nivel es el responsable de garantizar la transferencia de tramas libres de errores de un computador a otro a través del nivel físico.

3) Nivel de Red: es responsable del direccionamiento de mensajes y de la conversión de las direcciones lógicas y nombres, en direcciones físicas. Esta encargado también de determinar la ruta adecuada para el trayecto de los datos, basándose en condiciones de la red, prioridad del servicio, etc. El nivel de red agrupa pequeños fragmentos de mensajes para ser enviados juntos a través de la red.

4) Nivel de Transporte: se encarga de la recuperación y detección de errores. Garantiza también, la entrega de los mensajes de la computadora originados en el nivel de aplicación. Es el nivel encargado de informar a los niveles superiores del estatus de la red.

5) Nivel de Sesión: permite que dos aplicaciones residentes en computadoras diferentes establezcan, usen y terminen una conexión llamada sesión. Este nivel realiza reconocimientos de nombres y las funciones necesarias para que dos aplicaciones se comuniquen a través de la red, como en el caso de funciones de seguridad.

6) Nivel de Presentación: determina el formato a usar para el intercambio de datos en la red. Puede ser llamado el traductor de la red. Este nivel también maneja la seguridad de emisión pues, provee a la red servicios como el de encriptación de datos.

7) Nivel de Aplicación: sirve como ventana para los procesos que requieren acceder a los servicios de red.

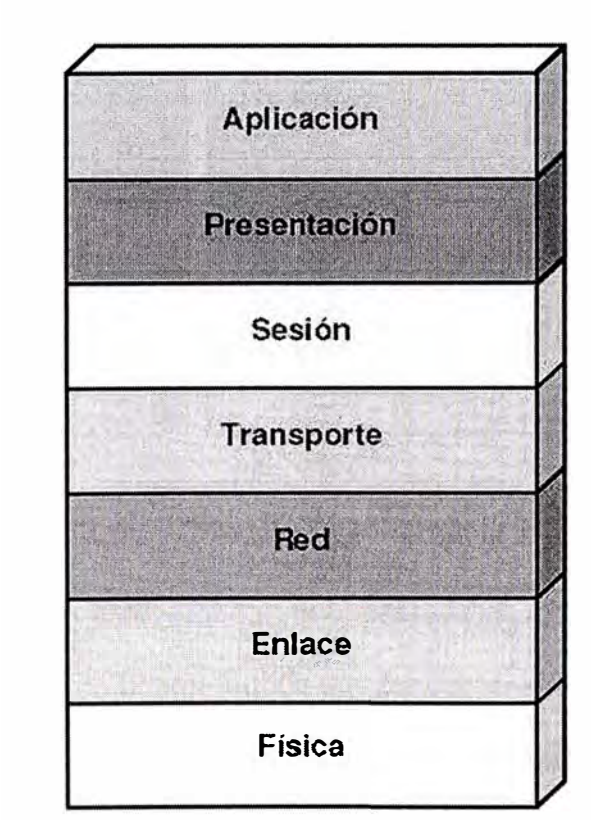


Figura 2.1 Modelo de Referencia OSI

2.8.2 Modelo de Referencia TCP/IP

La Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos de Norteamérica definieron un conjunto de reglas que establecieron cómo conectar computadoras entre sí para lograr el intercambio de información, soportando incluso desastres mayores en la subred. Fue así como se definió el conjunto de protocolos de TCP/IP (TCP/IP Internet Suite of Protocols). La Suite de TCP/IP consta de 4 capas principales que se han convertido en un estándar a nivel mundial.

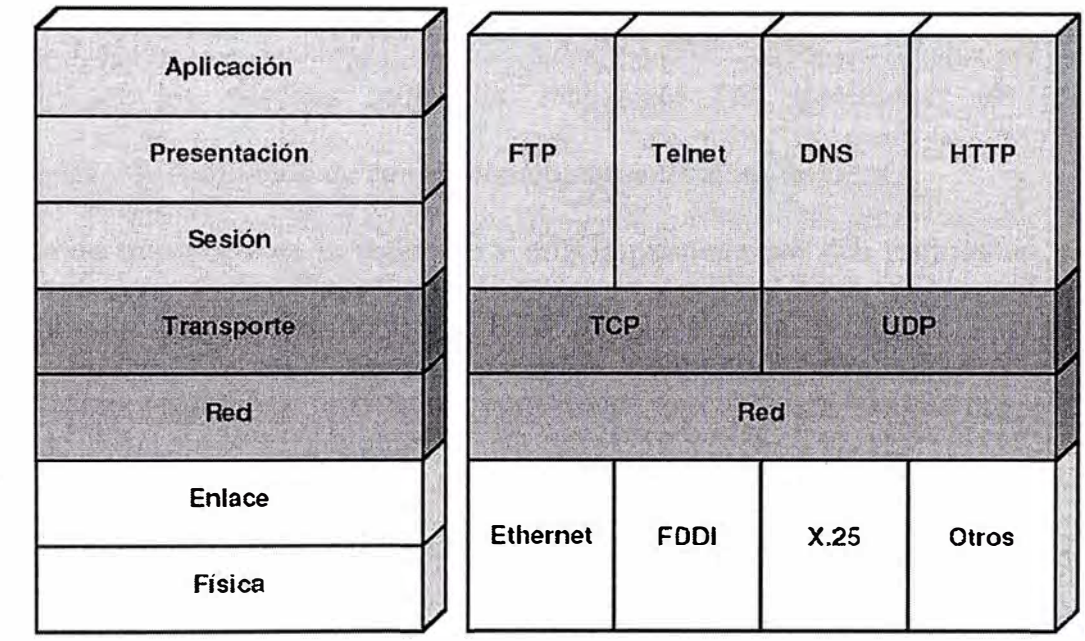


Figura 2.2 Modelo de Referencia TCP/IP

1) Las capas del modelo TCP/IP

Las capas de la suite de TCP/IP son menos que las del modelo de referencia OSI, sin embargo han convertido en un estándar defacto que actualmente une a más de 3 millones de nodos en todo el mundo.

La capa inferior, que podemos nombrar como física respecto al modelo OSI, contiene varios estándares del Instituto de Ingenieros Electrónicos y Eléctricos (IEEE

en inglés) como son el 802.3 llamado Ethernet que establece las reglas para enviar datos por cable coaxial delgado (10Base2), cable coaxial grueso (10Base5), par trenzado (10Base-T), fibra óptica (10Base-F) y su propio método de acceso, el 802.4 llamado Token Bus que puede usar estos mismos medios pero con un método de acceso diferente, el X.25 y otros estándares denominados genéricamente como 802.X.

La siguiente capa cumple, junto con la anteriormente descrita, los niveles del modelo de referencia 1,2 y 3 que es el de red. En esta capa se definió el protocolo IP también conocido como "capa de internet". La responsabilidad de este protocolo es entregar paquetes en los destinos indicados, realizando las operaciones de enrutado apropiadas y la resolución de congestionamientos o caídas de rutas.

La capa de transporte es la siguiente y está implantada por dos protocolos: el TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). El primero es un protocolo confiable y orientado a conexiones, lo cual significa que nos ofrece un medio libre de errores para enviar paquetes. El segundo es un protocolo no orientado a conexiones y no es confiable. El TCP se prefiere para la transmisión de datos a nivel red de área amplia y el otro para redes de área local.

La última capa definida en la suite de TCP/IP es la de aplicación y en ella se encuentran decenas de aplicaciones ampliamente conocidas actualmente. Las más populares son el protocolo de transferencia de archivos (FTP), el emulador de terminales remotas (Telnet), el servicio de resolución de nombres (Domain Name Service DNS), el WWW, el servicio de correo electrónico (Simple Mail Transfer Protocol SMTP), el servicio de tiempo en la red (Network Time Protocol NTP), el

protocolo de transferencia de noticias (Network News Transfer Protocol NNTP) y muchos más.

CAPÍTULO III

SEGURIDAD EN IP (IPSEC)

3.1. INTRODUCCIÓN

La nueva tendencia en seguridad es crear protocolos que funcionen a menor nivel que el de aplicaciones, de tal forma que se brinde seguridad tanto a IP como a protocolos de capas superiores de forma transparente para el usuario; protocolos que funcionen sin que el usuario deba hacer o instalar algo particular en su computadora, y protejan su tráfico sin importar la aplicación que lo genere. El Grupo de Seguridad de la IETF desarrolló mecanismos para proteger al protocolo IP al cual se denomina IP Security Protocol (IPSEC), el cual es un protocolo de seguridad de la capa de red para proveer servicios de encriptación con flexibilidad para soportar combinaciones de autenticación, integridad, control de acceso y confidencialidad.

IPSec es considerado el mejor protocolo de seguridad en la actualidad, representa un gran esfuerzo del grupo de trabajo de la IETF, aunque existen controversias al respecto, como los resultados de una evaluación criptográfica donde se presentan una serie de recomendaciones y observaciones, es considerado una excelente opción para implementar VPN (Virtual Private Networks), de hecho se le conoce también como el protocolo VPN.

3.2. ¿QUÉ ES IPSEC?

IPSec (Internet Protocol Security) es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.

3.3. ARQUITECTURA DE IPSEC

La arquitectura de IPSec define la granularidad con la que el usuario puede especificar su política de seguridad. Permite que cierto tráfico sea identificado para recibir el nivel de protección deseado.

IPSec está diseñado para proveer seguridad de alta calidad basada en criptografía, tanto para IPv4 como para IPv6 (RFC2401). Está compuesto por dos protocolos de seguridad de tráfico, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), además de protocolos y procedimientos para el manejo de llaves encriptadas. AH provee la prueba de los datos de origen en los paquetes recibidos, la integridad de los datos, y la protección contra-respuesta. ESP provee lo mismo que AH adicionando confidencialidad de datos y de flujo de tráfico limitado.

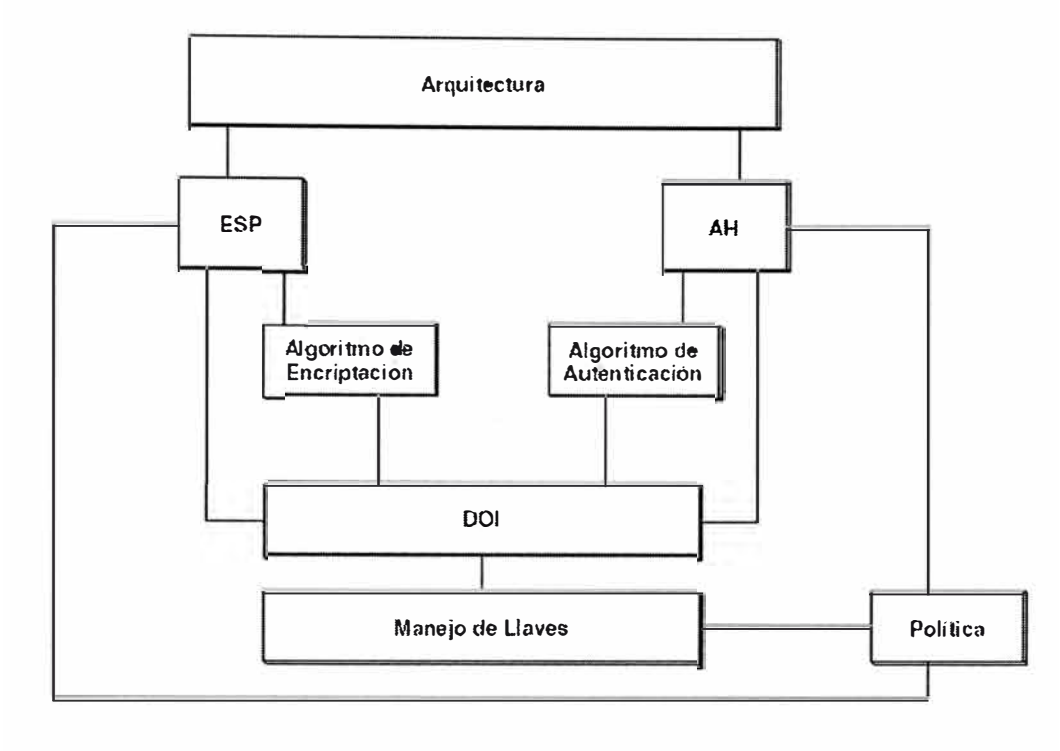


Figura 3.1 Arquitectura IPSec

En la figura 3.1 se aprecia la arquitectura de IPSec. Al utilizar el mecanismo de AH se aplican algoritmos de autenticación, con la aplicación del mecanismo ESP, además de autenticación, también algoritmos de encriptación. El esquema de interoperabilidad se maneja a través de Asociaciones de Seguridad (SA), almacenadas en una base de datos. Los parámetros que se negocian para establecer los canales seguros se denominan Dominio de Interpretación IPSec (Domain of Interpretation, DOI), bajo políticas pre-establecidas dentro de un esquema de funcionamiento estático con valores fijos y previamente establecidos, o bien, en un esquema de funcionamiento dinámico utilizando un protocolo de manejo de llaves, Interchange Key Exchange (IKE).

3.4. MODOS DE FUNCIONAMIENTO DE IPSEC

El diseño de IPSec plantea dos modos de funcionamiento para sus protocolos: transporte y túnel, la diferencia radica en la unidad que se esté protegiendo, en modo

transporte se protege la carga útil IP (capa de transporte), en modo túnel se protegen paquetes IP (capa de red) y se pueden implementar tres combinaciones: AH en modo transporte, ESP en modo transporte, ESP en modo túnel (AH en modo túnel tiene el mismo efecto que en modo transporte).

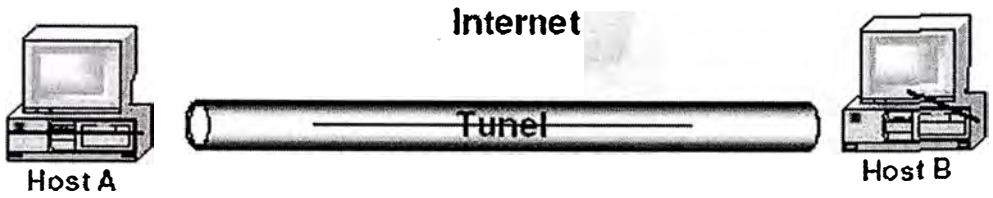


Figura 3.2 Host A y B implementando ESP en modo transporte

El modo transporte se aplica a nivel de hosts. AH y ESP en este modo interceptarán los paquetes procedentes de la capa de transporte a la capa de red y aplicarán la seguridad que haya sido configurada. En la figura 3.2 se aprecia un esquema de IPSec en modo transporte, si la política de seguridad define que los paquetes deben ser encriptados, se utiliza ESP en modo transporte, en caso que solo haya sido requerida autenticación, se utiliza AH en modo transporte. Los paquetes de la capa de transporte como TCP y UDP pasan a la capa de red, que agrega el encabezado IP y pasa a las capas inferiores; cuando se habilita IPSec en modo transporte, los paquetes de la capa de transporte pasan al componente de IPSec (que es implementado como parte de la capa de red, en el caso de sistemas operativos), el componente de IPSec agrega los encabezados AH y/o ESP, y la capa de red agrega su encabezado IP. En el caso que se apliquen ambos protocolos, primero debe aplicarse la cabecera de ESP y después de AH, para que la integridad de datos se

aplique a la carga útil de ESP que contiene la carga útil de la capa de transporte, esto se ilustra en la figura 3.3.

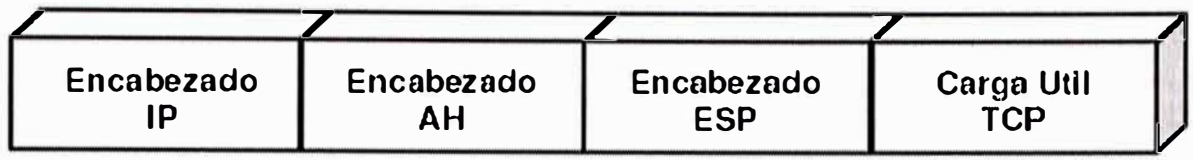


Figura 3.3 Formato de Paquete con AH y ESP

El modo túnel se utiliza cuando la seguridad es aplicada por un dispositivo diferente al generador de los paquetes, como el caso de las VPN, o bien, cuando el paquete necesita ser asegurado hacia un punto seguro como destino y es diferente al destino final, como se ilustra en la figura 3.4, el flujo de tráfico es entre A y B, e IPSec puede aplicarse con una asociación de seguridad entre RA y RB, o bien, una asociación de seguridad entre A y RB.

Figura 3.4 Aplicación de IPSec en modo tunel

IPSec en modo túnel, tiene dos encabezados IP, interior y exterior. El encabezado interior es creado por el host y el encabezado exterior es agregado por el dispositivo que está proporcionando los servicios de seguridad. IPSec encapsula el paquete IP con los encabezados de IPSec y agrega un encabezado exterior de IP como se ilustra en la figura 3.5.

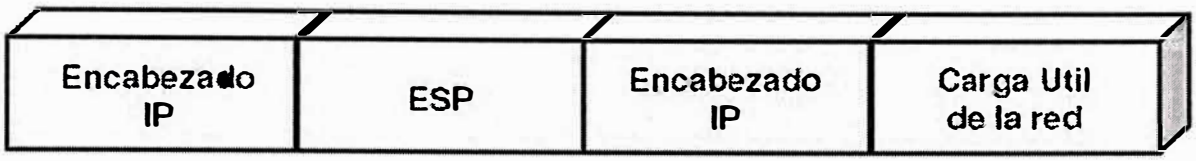


Figura 3.5 Formato del Paquete aplicando IPSec en modo tunel

IPSec también soporta túneles anidados, aunque no son recomendados por lo complicado de su construcción, mantenimiento y consumo de recursos de red. La figura 3.6 muestra dos túneles, A envía un paquete a B, la política indica que debe ser autenticado con el ruteador RB, además existe una VPN entre RA y RB, de tal forma que el paquete que ve RB es el que se muestra en la figura 3.7, el encabezado exterior es un paquete ESP entunelado y contiene un paquete AH entunelado, el paquete AH contiene el paquete IP para el host B generado por el host A.

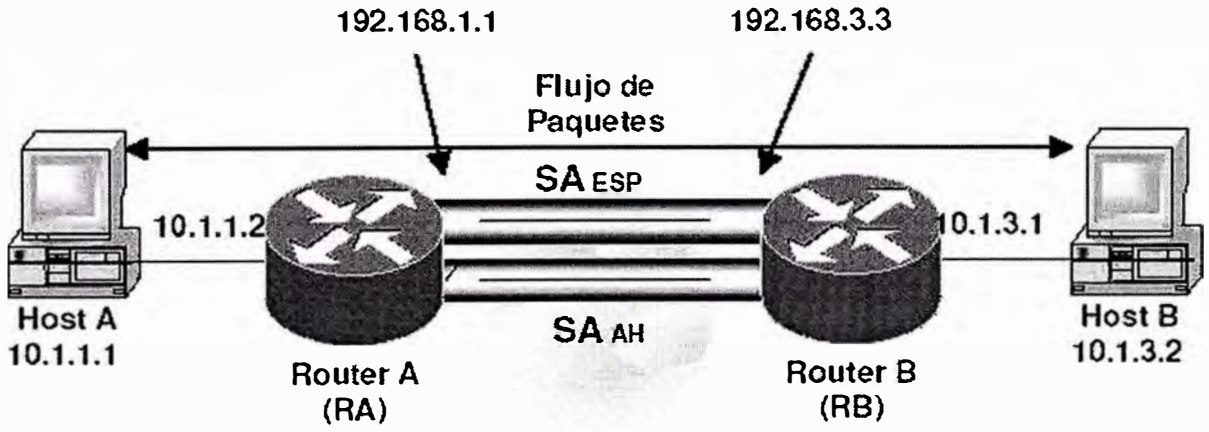


Figura 3.6 Ejemplo de Tuneles Anidados

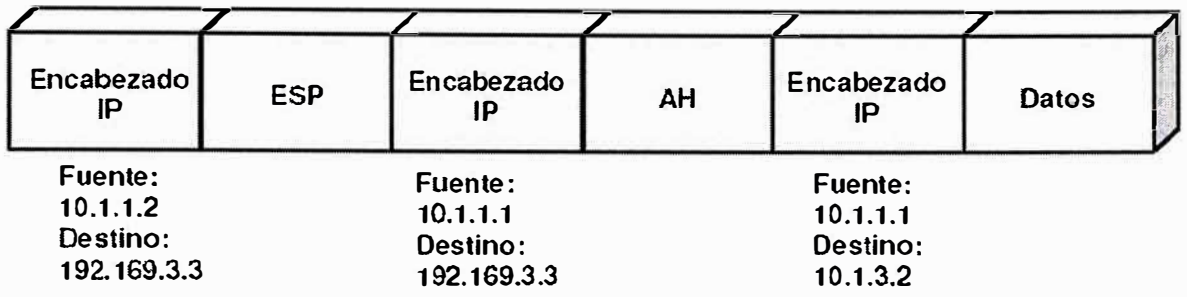


Figura 3.7 Formato del Paquete del tunel anidado

3.5. ASOCIACIONES DE SEGURIDAD

Una asociación de seguridad (SA) es la forma básica de IPSec, es el contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los protocolos a utilizar, las transformaciones, las llaves y la duración de validez de dichas llaves. Las SA son almacenadas en una base de datos (SADB), son de un solo sentido, es decir, cada entidad con IPSec tiene una SA para el tráfico que entra, y otra SA para el tráfico que sale.

Además de ser unidireccionales, también son específicas al protocolo, hay SA separadas para AH y para ESP.

3.5.1 Índice de Parámetros de Seguridad (SPI)

El SPI (Security Parameter Index) es una entidad de 32 bits que identifica de manera única una SA. Es el mecanismo concebido para que en una comunicación segura, la fuente identifique cual SA utilizar para asegurar un paquete por enviar, y el destino identifique cual SA utilizar para verificar la seguridad del paquete recibido. El SPI se incluye en los encabezados ESP y AH, el destino utiliza los parámetros <spi, dst, protocol> para identificar de forma única la SA.

3.5.2 Gestión de la SAs

Para el manejo de SA se establecen dos tareas: creación y borrado; estas actividades pueden ser manuales o a través del protocolo de manejo de llaves (IKE).

La creación es un proceso de dos etapas:

1) Negociación de parámetros de la SA,

2) Actualización de la SADB.

El manejo manual de llaves es obligatorio en toda implementación, el proceso de definición de SPI y parámetros es totalmente manual, y permanecerán hasta que sean manualmente borrados. En el manejo dinámico de llaves, se utiliza un protocolo de manejo de llaves en Internet como IKE. El kernel con IPSec habilitado, invoca IKE si se trata de una comunicación segura y no encuentra una SA. IKE negocia la SA con el destino o con el siguiente salto (host o ruteador), dependiendo de la política y crea la SA en la SADB.

Igualmente las SA pueden ser borradas manualmente o con IKE, los criterios de borrado pueden ser: tiempo de vida expirado, llaves comprometidas, solicitud explícita para borrarse, el número de bytes utilizado excede un umbral especificado en la política.

3.5.3 Parámetros

Los parámetros por negociar en una SA, tanto para AH como para ESP son los siguientes:

· Número de secuencia: un campo de 32 bits utilizado en el procesamiento de paquetes de salida, es parte de los encabezados de AH y/o ESP, su valor inicial es 0, se incrementa en uno cada vez que la SA es utilizada, se utiliza para detectar ataques del tipo “replay”.

· Sobreflujo del número de secuencia: campo utilizado en el procesamiento de paquetes de salida y se establece cuando hay sobreflujo del campo de número de secuencia. La política determina qué hacer si este campo está activado.

· Ventana de antireply: campo utilizado en el procesamiento de paquetes de entrada. Se activa si IPSec detecta paquetes retransmitidos por hosts sospechosos.

· Tiempo de vida: El tiempo de validez de una SA, se especifica en términos de bytes asegurados con la SA, no se recomienda enviar más de 4Gb de paquetes utilizando la misma SA. Para evitar la pérdida de la conexión segura, se manejan dos límites, soft y hard. Al llegar al límite soft el kernel es notificado para que inicie una nueva negociación antes del límite hard que es cuando la SA expira.

· Modo: los valores son: túnel, transporte o indistinto. Si el valor es indistinto la SA puede ser utilizada para modo túnel o modo transporte.

· Destino del túnel: campo utilizado para modo túnel, indica la dirección IP de destino del encabezado exterior.

· Parámetros PMTU: IPSec no fragmenta o reensambla paquetes, sin embargo, agrega un encabezado IPSec y por lo tanto impacta la longitud del PMTU. IPSec debe participar en la determinación del PMTU (Protocol Maximum Transfer Unit), una SA mantiene dos valores: el PMTU y el campo de edad.

3.6. POLÍTICAS DE SEGURIDAD EN IPSEC

La política es uno de los componentes más importantes de la arquitectura de IPSec, determina los servicios de seguridad que serán aplicados a un paquete. Las políticas de seguridad son también almacenadas en una base de datos (Security Policy Database, SPD) indexada por seleccionadores.

La SPD es consultada tanto para el procesamiento de salida como el de entrada, se propone un administrador de la SPD para agregar, borrar y modificar; no hay un estándar que lo defina, pero se propone que los seleccionadores contengan los siguientes campos:

· Dirección fuente: puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica. Indistinta en el caso de que sea la misma política para todos los paquetes con un mismo host de origen, el rango de direcciones y prefijo de red, para los gateways de seguridad y para VPNs, la dirección específica para un host con varias direcciones, o en un gateway cuando los requerimientos de algún host sean específicos.

· Dirección destino: puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica (homologada o no). Los tres primeros para gateways de seguridad, la dirección específica como índice para la SPD.

· Nombre: nombre de un usuario o sistema sobre el cual se aplique la política de forma específica.

· Protocolo: el protocolo de transporte.

· Puertos de capas superiores: los puertos de la fuente y destino sobre los que se aplica la política.

3.7. IP ENCAPSULATING SECURITY PAYLOAD (ESP)

ESP es un encabezado de protocolo insertado en el datagrama IP para proveer servicios de confidencialidad, autenticación del origen de los datos, antireplay e integridad de datos a IP. Es un estándar definido en el RFC 2406. El encabezado ESP se inserta después del encabezado IP y antes del encabezado del protocolo de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel).

El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado ESP contendrá el valor 50 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6).

El formato de los paquetes ESP para una SA dada es fijo durante la duración de la SA. El encabezado ESP tiene la forma definida en la figura 11, el SPI y número de secuencia ya fueron definidos, la carga útil de datos son los datos protegidos, el relleno (de hasta 255 bytes) se utiliza en ESP por varias circunstancias: algunos algoritmos criptográficos requieren que el elemento de entrada sea un múltiplo del tamaño de su bloque, si no se especifica confidencialidad en la SA, se utiliza el relleno para justificar los campos "Longitud de relleno" y "Siguiente cabecera" del encabezado ESP, para esconder el tamaño real de la carga útil; el contenido del relleno es dependiente del algoritmo de criptografía, el algoritmo puede definir un valor de relleno que debe ser verificado por el receptor para el proceso de desencriptado. El campo de longitud de relleno define cuánto relleno se agregó, el campo de siguiente cabecera indica el tipo de dato contenido en la carga útil de acuerdo al conjunto de Números de Protocolo IP definidos por IANA (Internet Assigned Numbers Authority). El campo de datos de autenticación contiene el valor de verificación de integridad calculado sobre el paquete ESP menos los datos de autenticación.

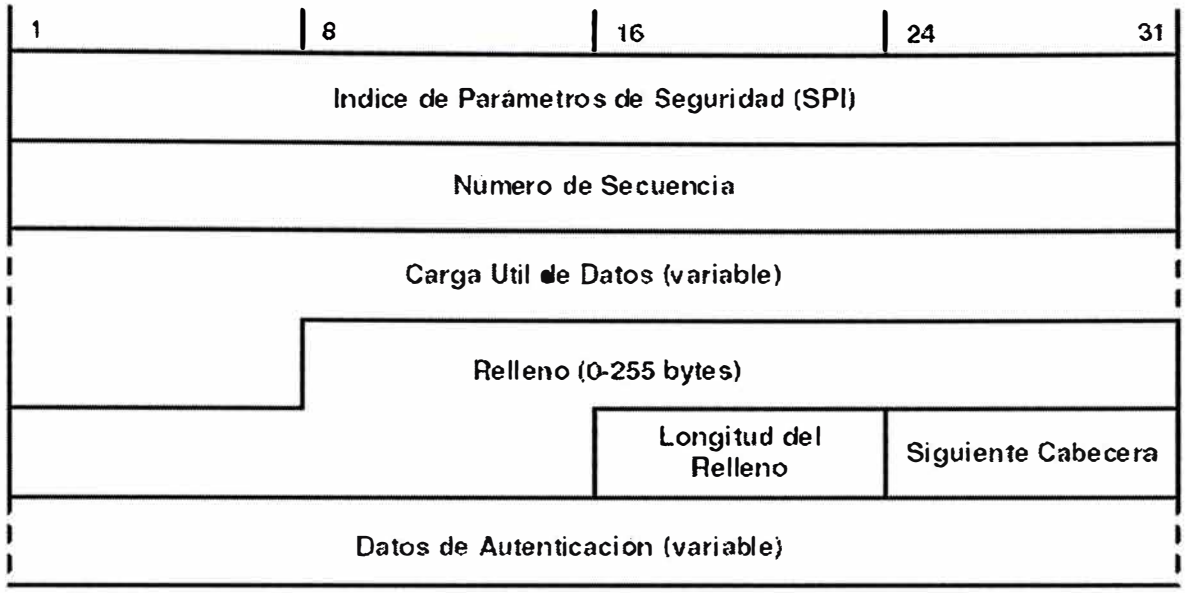


Figura 3.8 El Encabezado ESP

ESP aplicado en modo transporte solo se utiliza en implementaciones del tipo host y provee protección a los protocolos de capas superiores, pero no al encabezado IP. El encabezado ESP se inserta después del encabezado IP y antes del protocolo superior (TCP, UDP, ICMP, etc.) o antes de cualquier encabezado IP que haya sido previamente insertado. En la figura 3.9 se ilustra la transformación del paquete IP al aplicar ESP en modo transporte para IPv4.

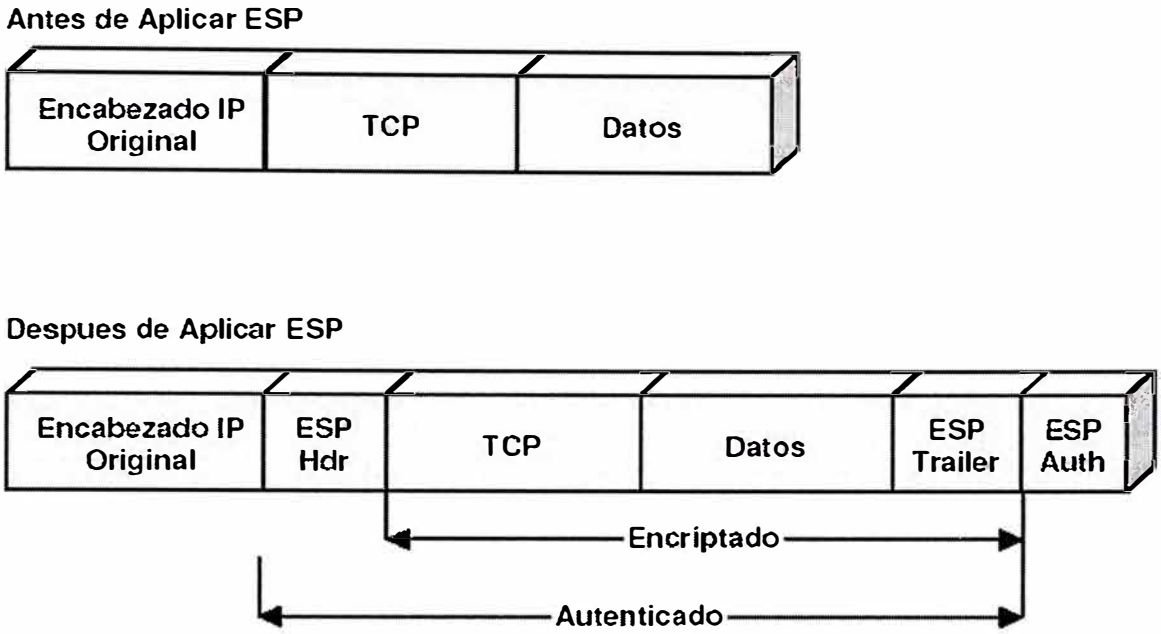


Figura 3.9 Transformación del paquete Ipv4 al aplicar ESP en modo transporte

En modo túnel, ESP puede ser empleado en hosts o en gateways. El encabezado IP interior contiene las direcciones del destino y origen del paquete, y el encabezado exterior puede contener direcciones diferentes, comúnmente direcciones de gateways de seguridad en el camino entre el origen y destino. La posición de los encabezados ESP en modo túnel con respecto a los encabezados IP exteriores es igual que en modo transporte. En la figura 3.10 se muestran el encabezado ESP para IPv4

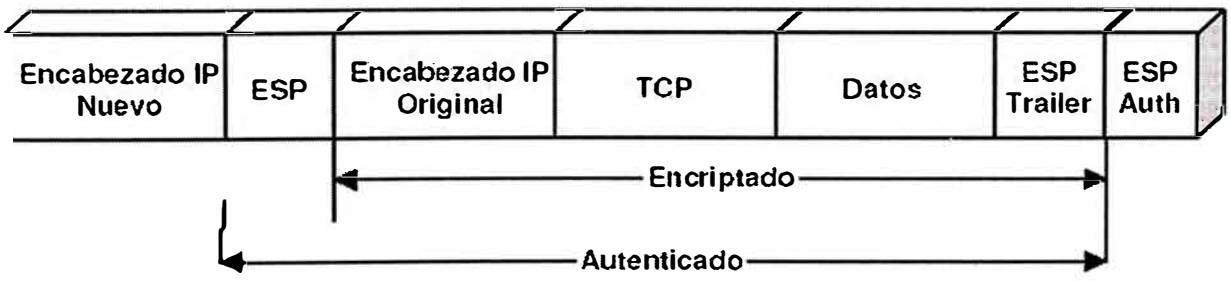


Figura 3.10 Transformación del paquete IP al aplicar ESP en modo tunel

En caso de no haberse indicado la confidencialidad en la SA, el algoritmo de criptografía es Nulo, en caso de aplicar confidencialidad a un paquete que se envía, el proceso aplicado en general es el siguiente:

1) Encapsular en el campo de carga útil de ESP:

· Para modo transporte, solo la información original del protocolo de capa superior.

· Para modo túnel, el datagrama IP original completo.

2) Agregar el relleno necesario.

3) Encriptar el resultado (carga útil de datos, relleno, longitud del relleno y la siguiente cabecera) usando la llave, el algoritmo de criptografía, el modo indicado en la SA y si existe, datos de sincronización criptográfica.

En la parte del receptor se sigue en general el siguiente procedimiento para desencriptar los paquetes recibidos:

1) Desencriptar la carga útil de ESP, relleno, longitud del relleno, y siguiente cabecera, utilizando la llave, el algoritmo de criptografía, el modo y en su caso, los datos de sincronización criptográfica, indicados en la SA.

2) Procesar el relleno según haya sido especificado por el algoritmo utilizado.

3) Reconstruir el datagrama IP original:

· Para modo transporte, el encabezado IP original más la información del protocolo de capa superior original en el campo de carga útil de ESP.

· Para modo túnel, el encabezado IP entunelado, más el datagrama IP completo en el campo de carga útil de ESP.

Es importante mencionar que el encriptamiento no debe ser sustituto por la autenticación, la autenticación es el servicio básico de una comunicación segura, reforzada con el encriptamiento de datos.

3.8. IP AUTHENTICATION HEADER (AH)

AH es el protocolo IPSec utilizado para proveer servicios de integridad de datos, autenticación del origen de los datos, y antireplay para IP. Es un estándar definido en el RFC 2402. La principal diferencia entre la autenticación provista entre ESP y AH tiene que ver con la cobertura, ESP no protege los campos del encabezado IP, a menos que sean encapsulados por ESP (modo túnel). El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado AH contendrá el valor 51 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6).

La figura 3.11 muestra el encabezado AH, todos los campos son obligatorios, tienen funciones similares a las explicadas en ESP, el campo reservado no se utiliza y su valor debe ser cero.

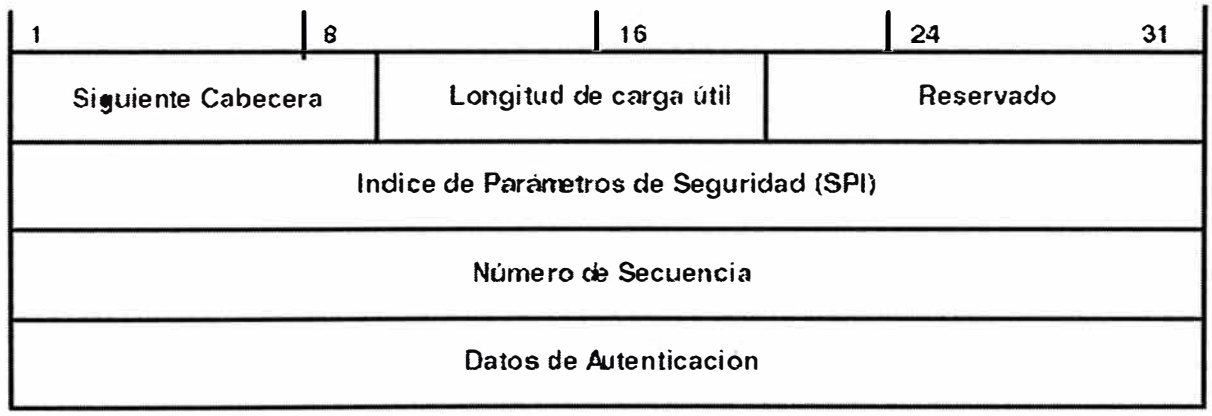


Figura 3.11 El Encabezado AH

Al igual que ESP, AH puede aplicarse tanto en modo túnel como transporte. La figura 3.12 muestran la ubicación de AH al aplicar IPSec en modo transporte en los paquetes IP.

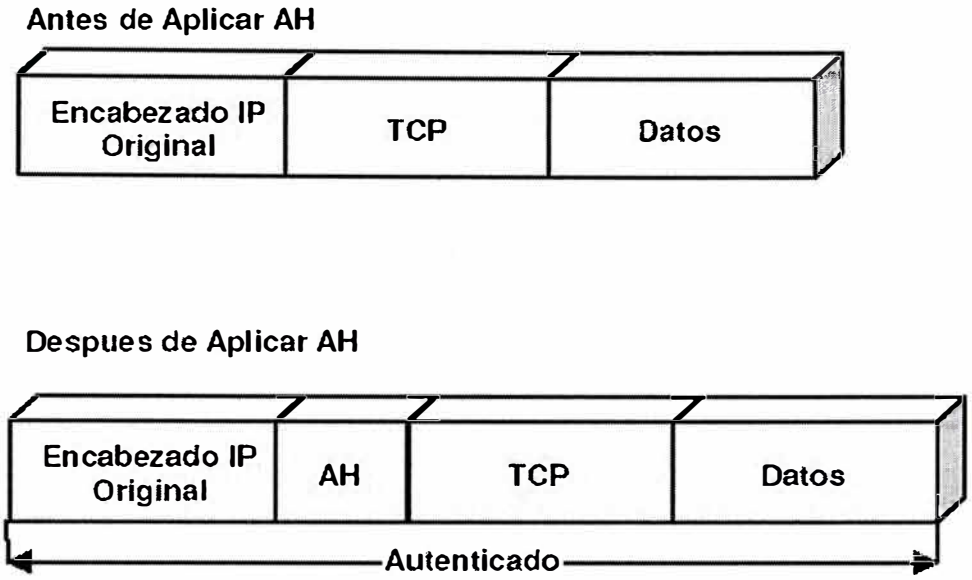


Figura 3.12 Transformación del paquete IPv4 al aplicar AH en modo transporte

La aplicación de AH en modo túnel, tiene una ubicación similar a la de ESP, en la figura 3.13 se muestra la transformación de los paquetes IP al aplicar AH en modo túnel.

Figura 3.13 Transformación del paquete IP al aplicar AH en modo tunel

El proceso de cálculo del valor de verificación de integridad (Integrity Check Value, ICV) que utiliza AH, llena con ceros los campos vulnerables a cambios en tránsito (TOS, Flags, Fragment, TTL, Header checksum en un encabezado IPv4) y se calcula sobre lo siguiente:

· Los campos del encabezado IP que sean inmunes a cambios en tránsito o pueda predecirse su valor (Versión, longitud de carga útil, longitud total, identificación, dirección de fuente y destino en un encabezado IPv4).

· El encabezado AH (siguiente cabecera, longitud de relleno, reservado, SPI, número de secuencia y datos de autenticación (que es puesta a cero para este cálculo), y bytes de relleno en caso que existan.

· Los datos del protocolo de capa superior, que se asume son inmunes a cambios en tránsito.

3.9. INTERNET KEY EXCHANGE (IKE)

El protocolo IKE no es parte de IPSec, es una alternativa para crear las Asociaciones de Seguridad de forma dinámica, está definido en el RFC 2409. IKE es un protocolo híbrido basado en el marco definido por el Protocolo de manejo de llaves y asociaciones de seguridad de Internet (Internet Security Association and Key Management protocol, ISAKMP) definido en el RFC2408, y otros dos protocolos de manejo de llaves Oakley y SKEME. Las implementaciones de IPSec están forzadas a soportar el manejo manual y solo algunas de ellas consideran IKE, que ha resultado demasiado complejo e inapropiado. El uso de IKE en el 2001 fue congelado por la IETF, el planteamiento sobre manejo dinámico en el 2001 es llamado "hijo de IKE" o IKE versión 2 y se encuentra en discusión en el área de seguridad de la IETF.

3.10. IMPLEMENTACIÓN DE IPSEC

La implementación de IPSec puede hacerse en hosts, gateways/ruteadores, y/o cortafuegos, resultando conveniente la implementación en éstos últimos al complementar mutuamente sus funciones. Típicamente modificando la pila de IP para soportar IPSec de forma nativa, cuando esto no es posible, puede implementarse como interceptor que extrae e inserta paquetes en la pila de IP "Bump in the Stack" (BITS), o bien utilizando un dispositivo de encriptación externo dedicado "Bump in the Wire" (BITW) como se esquematiza en la figura 17.

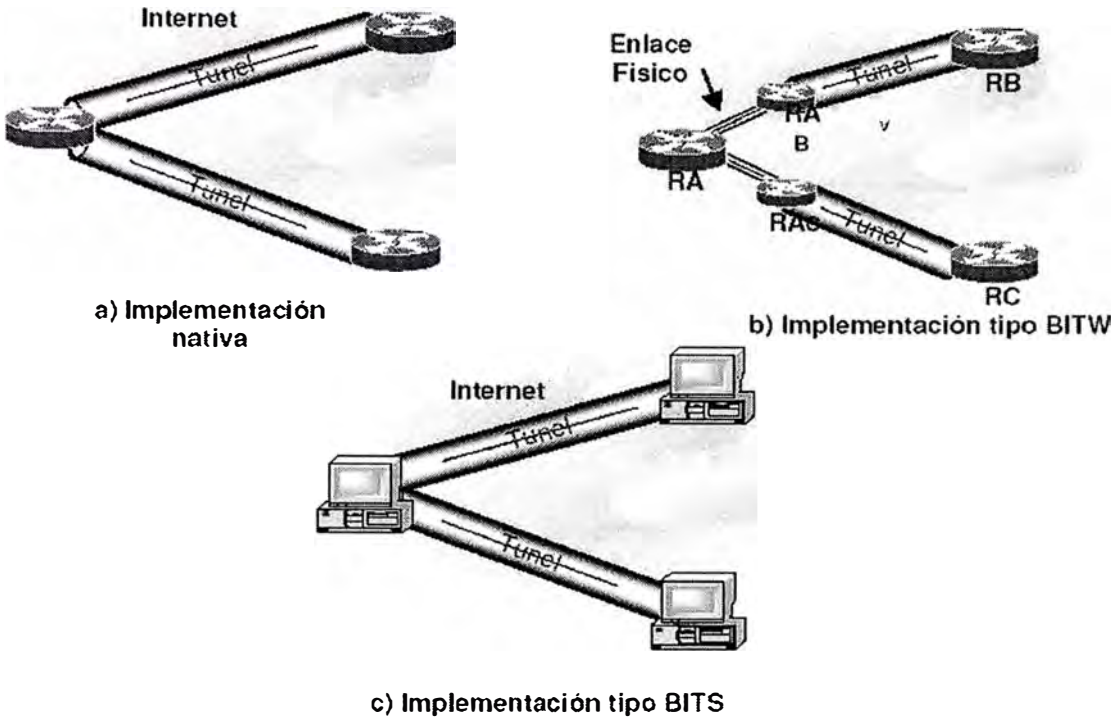


Figura 3.14 Tipos de implementaciones de IPSec

IPSec está diseñado para operar en hosts y/o en gateways, en modo túnel para proteger datagramas IP completos (VPN), o en modo de transporte para proteger protocolos de capas superiores. A la fecha existen algunas implementaciones, sin embargo, la mayoría limitadas a la aplicación de VPN únicamente, sobre todo en implementaciones de forma nativa, de hecho es denominado por algunos como el "protocolo VPN". En los últimos años han emergido los proyectos para implementar seguridad en sistemas operativos, esquemas BITS, en busca de brindar una plataforma base de seguridad independiente de las aplicaciones preferidas por el usuario.

3.11. CONFIGURACIONES DE IPSEC

Cuando la implementación de IPSec radica en un host o sistema final, los paquetes pueden ser asegurados de extremo-a-extremo, es decir desde el origen de los datos hasta su destino final. La figura 3.15 muestra este esquema, donde cada paquete que

sale del host es asegurado y puede inclusive determinarse que todo paquete que no haya sido asegurado por IPSec sea eliminado.

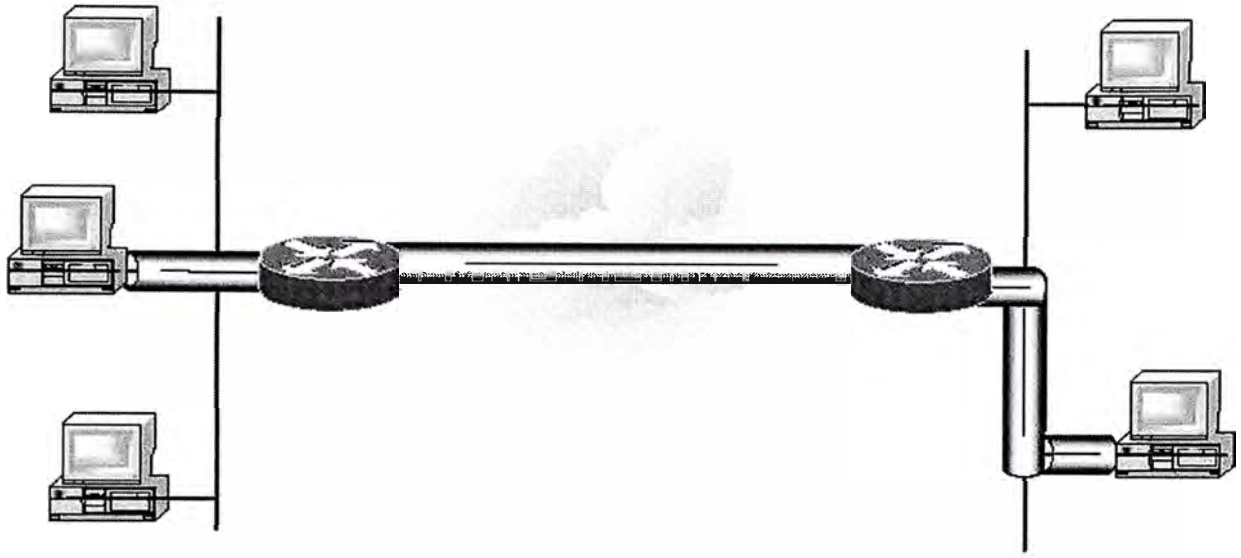


Figura 3.15 Seguridad extremo a extremo a través de la red

El resultado de un esquema de seguridad extremo-a-extremo, IPSec en modo transporte generalmente, donde todo el tráfico (Telnet, SMTP, HTTP, etc.) entre ambos extremos puede ser asegurado, o bien, de forma particular a través de la definición explícita de SA.

Algo importante de mencionar de la seguridad extremo-a-extremo, es que puede afectar el funcionamiento de otras aplicaciones que requieran inspeccionar los paquetes en tránsito (Cortafuegos, QoS, etc.), y no puedan hacerlo, ya que verán solo paquetes ESP. Quizá la implementación más común son las VPN, que han sido vistas como una excelente alternativa de ahorro, en lugar de contratar líneas dedicadas, utilizar la red pública con servicios de seguridad. Cuando IPSec se aplica a ruteadores en modo túnel, y dos ruteadores establecen túneles a través de los cuales envían tráfico desde una subred localmente protegida hacia otra subred remotamente protegida se denomina una VPN, la figura 3.16 muestra un esquema de este tipo.

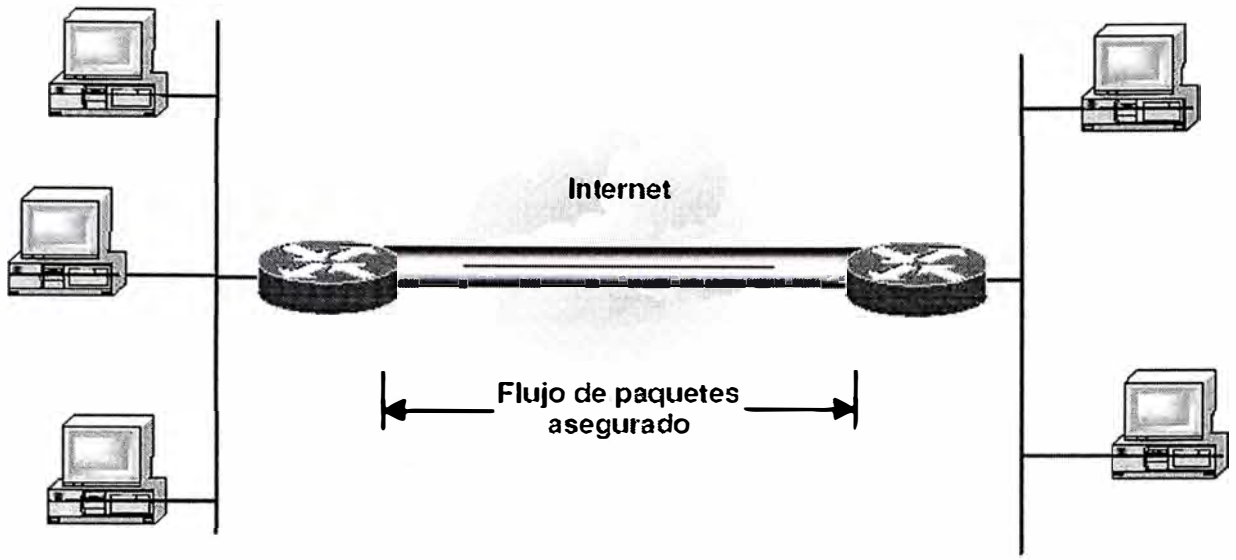


Figura 3.16 Una VPN a través de Internet

Existe otro tipo de implementación que es una combinación de la extremo-a-extremo donde un host encripta y desencripta tráfico que envía y recibe, y la VPN en donde es un ruteador el que hace este trabajo. En la configuración del tipo "Road Warrior", una computadora implementa IPSec y es capaz de asegurar los paquetes que envía y verificar la seguridad de los paquetes que recibe, su extremo IPSec es un ruteador que protege la red con la cual se desea establecer la comunicación. La figura 3.17 ilustra este esquema.

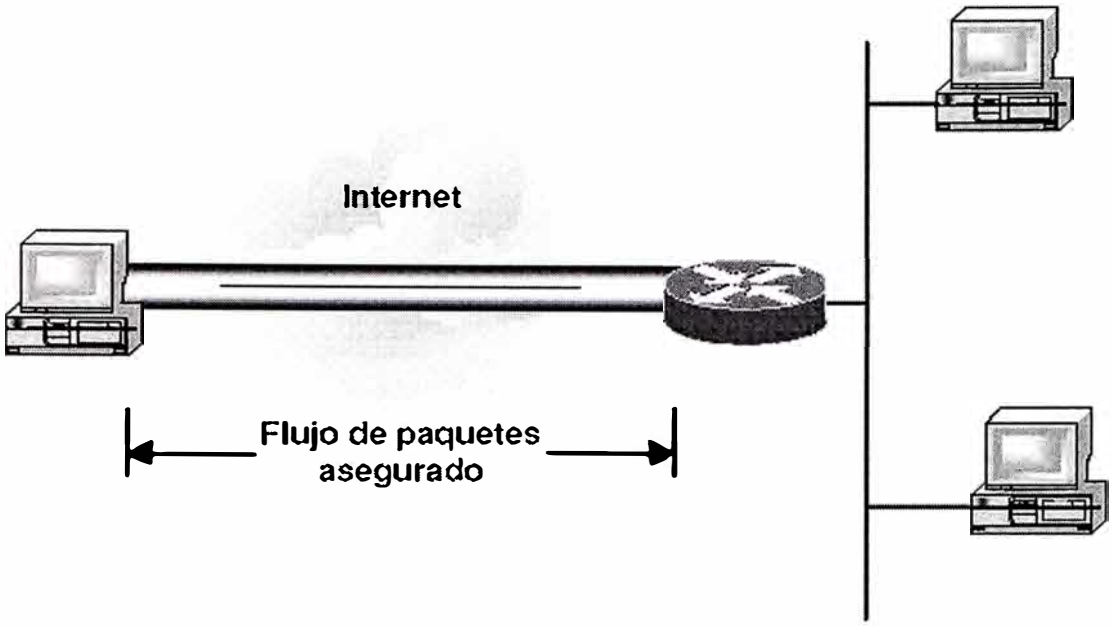


Figura 3.17 Esquema de configuración de un Road Warrior

También es posible la implementación de túneles anidados, un ejemplo podría ser una institución que tiene un gateway de seguridad para proteger su red de ataques del exterior, pero además tiene otro gateway de seguridad en su red interna para protección de ataques internos. La figura 3.18 muestra este esquema, difícil de mantener y establecer, pero quizá útil y necesario para ciertas necesidades entre instituciones con instalaciones remotas.

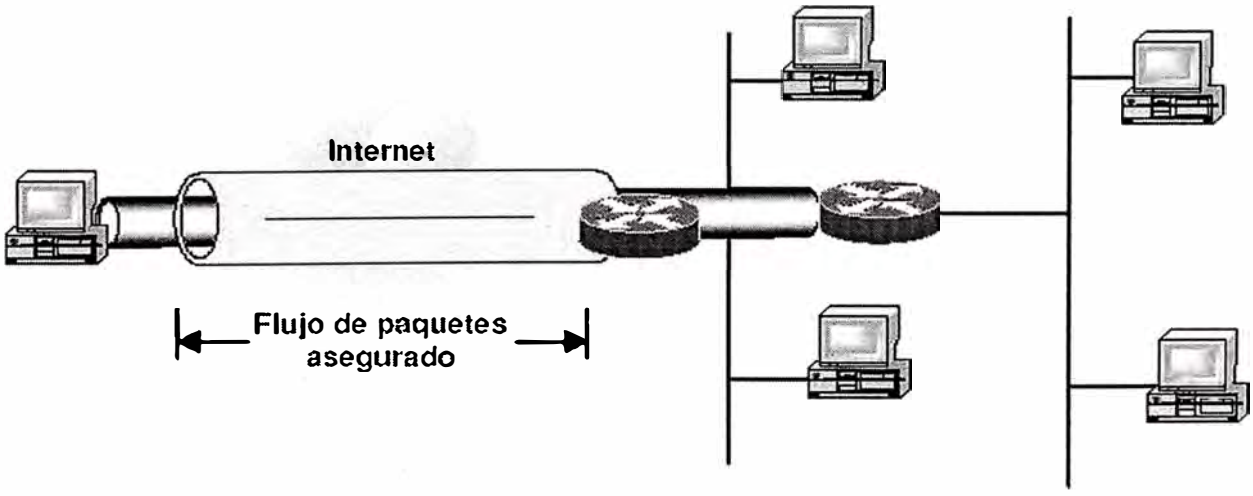


Figura 3.18 Esquema con túneles anidados

CAPÍTULO IV

REDES PRIVADAS VIRTUALES (VPNS)

4.1. INTRODUCCIÓN

En los últimos años ha habido un gran desarrollo tecnológico y hoy en día la computadora se ha convertido en un aparato común en los hogares y algo casi imprescindible en las oficinas. Lo mismo ha ocurrido con Internet, cada vez más extendida. Las empresas y gobiernos usan la red Internet como una herramienta más, confiándole información importante. El problema está en que no es una red segura y es 'fácil' el acceder a información confidencial y que en malas manos puede ser peligrosa. Por este motivo, en los últimos años se le da mucha importancia a la seguridad, el uso de la encriptación es común y las empresas buscan soluciones lo más eficaces y baratas posibles a la inseguridad de Internet. Para dar solución a estas demandas surgieron las VPN (redes privadas virtuales).

4.2. CONCEPTO DE VPN

La VPN es una red que ofrece conexiones transparentes y seguras a través de Internet. Se trata de una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas IP.

Estas redes permiten conectar teletrabajadores, empleados móviles, oficinas y delegaciones separadas geográficamente, socios y clientes de una forma relativamente barata y muy segura. Las empresas obtienen de esta forma reducción de gastos, aumentan su seguridad y mejora en las comunicaciones.

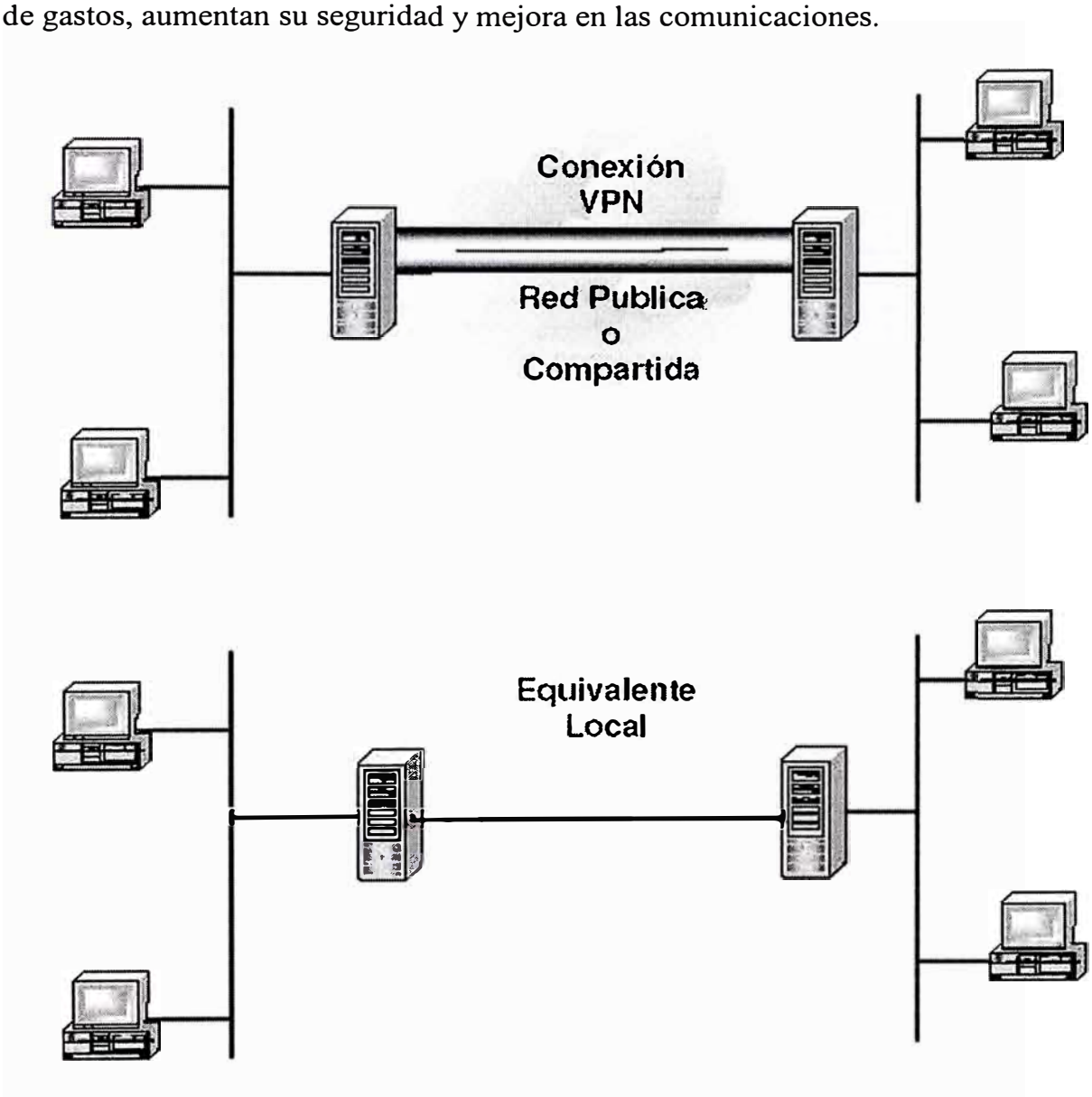


Figura 4.1 Concepto de VPN

4.2.1 Ventajas del uso de VPNs

A continuación se detalla las principales ventajas: .

1) Reducción de Gastos

Con estas redes podemos reducir gastos de varios tipos:

· Costos de telecomunicaciones por el mantenimiento de muchas líneas de acceso, las compañías suelen tener contratadas dos tipos de líneas de acceso: unas de alta velocidad de acceso a Internet y otras del tipo Frame Relay o ADSL. Con las redes VPN sólo necesitamos un tipo de líneas ya que podremos utilizar una red pública IP para transportar todo tipo de datos.

· Costos en la administración del equipo de acceso remoto, Ahorro de gastos operativos. Se permite tener un acceso a una red vía una VPN de manera que la compañía no tiene que preocuparse del mantenimiento y problemas de administración de un banco de módems y servidores de acceso remoto.

2) Aumenta la Seguridad

Un VPN permite crear un perímetro de seguridad de operación. Incorpora ruteadores y cortafuegos como base, y por encima utiliza mecanismos de seguridad como son:

· Encriptación de datos. Se utilizan varias técnicas: DES, 3DES, RSA

· Compresión de datos

· Autenticación. El servidor VPN autentica al cliente para asegurarse que tienen los permisos necesarios. Si además el cliente autentica al servidor se protege contra la suplantación de servidores.

· Administración distribuida de claves.

· Tuneling (tunelado) para establecer las conexiones punto a punto.

· Acceso desde el exterior controlado por ser acceso remoto a un servidor seguro.

3) Mejora en las Comunicaciones

Las VPN se abren paso a través de la red pública IP o por redes compartidas IP creando una conexión que emula las propiedades de un enlace punto a punto privado. Para el usuario es como si realizase una conexión dentro de una LAN (red de área local).

Para conseguir esto se emplean técnicas de tunelaje en las que se crea un túnel que conecte a ambos extremos y por los que se transmite la información. Los datos se encapsulan con una cabecera que contenga la información para su ruteo a través de los túneles previa encriptación de los datos. Cuando los datos salen a la red IP su seguridad está garantizada ya que sin la clave de desencriptación no se puede conocer su contenido.

4.3. ELEMENTOS DE UNA CONEXION VPN

Los elementos generales son:

1) Servidor VPN. Programa servidor instalado en una computadora que proporciona conexiones de acceso remoto VPN o conexiones ruteador a ruteador.

2) Cliente VPN. Programa cliente VPN que es quien solicita al servidor las conexiones de uno u otro tipo.

3) Conexión VPN. Porción de la conexión entre dos usuarios, donde se encriptan los datos. Una conexión de acceso remoto se da cuando una computadora personal se conecta a la red privada bien para obtener los servicios del servidor o para acceder a la red completa. Una conexión ruteador a ruteador conecta dos porciones de la red privada. En ambos casos el servidor pide autenticación del cliente. La autenticación puede ser mutua.

4) Túnel. El fragmento de conexión que está dentro de la red VPN de la organización, en el cual se encapsulan los datos para que al salir a la red IP viajen

seguros hasta su destino. Estos datos pueden estar encriptados o no. Si lo están el túnel será en sí una conexión VPN.

5) Protocolos de Túnel. Los protocolos empleados en estas redes son: PPTP, IPSec, L2TP, GRE y SSH, que serán detallados mas adelante.

6) Datos de túnel. Datos a enviar.

7) Red de tránsito. La red IP intermedia que se emplea para enviar los datos. Puede ser Internet o una red Intranet IP privada que hayamos alquilado.

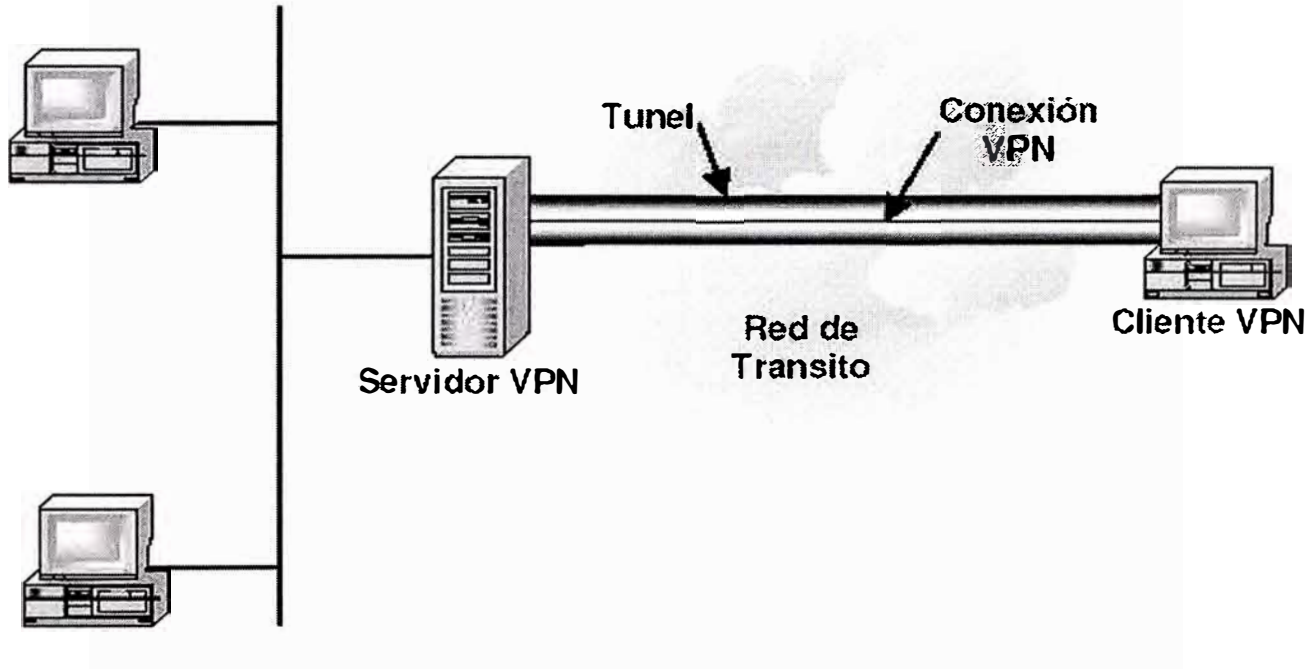


Figura 4.2 Elementos de una Conexión VPN

4.4. FUNCIONAMIENTO GENERAL

En primer lugar es necesario instalar la VPN detrás del cortafuegos corporativo y el ruteador.

El segundo paso es iniciar el intercambio de llaves y autenticación de servidores y sitios de forma que el administrador consiga un servidor seguro.

Los ruteadores deben ser configurados para que envíen al servidor seguro la información a encriptar, dejando seguir su ruta normal al resto de tráfico. En el cortafuegos se configura un puerto por el que pase la información al servidor seguro sin filtrarla.

Cuando el VPN recibe un paquete TCP/ IP lo comprime y encapsula en un nuevo paquete especial para enviarlo por un túnel hasta su destino. El receptor desencapsula el paquete original, lo desencripta y lo envía a su destino dentro de la LAN.

4.5. CONEXIONES VPN

Las conexiones VPN pueden ser utilizadas siempre que se requiera una conexión punto a punto segura. Las conexiones VPN típicas están construidas sobre Internet o sobre intranets.

4.5.1 Conexiones VPN sobre Internet

El concepto general es que el cliente, que puede ser un usuario externo a la VPN o un ruteador de una VPN que se quiere conectar con otra VPN, hace una conexión a su ISP local y desde ahí se le conecta al servidor VPN, como si se tratase de cualquier acceso a un servidor web remoto.

1) Acceso Remoto Sobre Internet

En lugar de que un cliente de acceso remoto tenga que hacer una llamada de larga distancia a un servidor de acceso remoto (Network Access Server , NAS) corporativo, el cliente puede llamar a un ISP local. Al utilizar la conexión física establecida con el ISP local, el cliente de acceso remoto inicia una conexión a través de Internet hacia la el servidor VPN de la organización Una vez que la conexión VPN es creada, el cliente de acceso remoto tiene acceso a los recursos de la intranet privada.

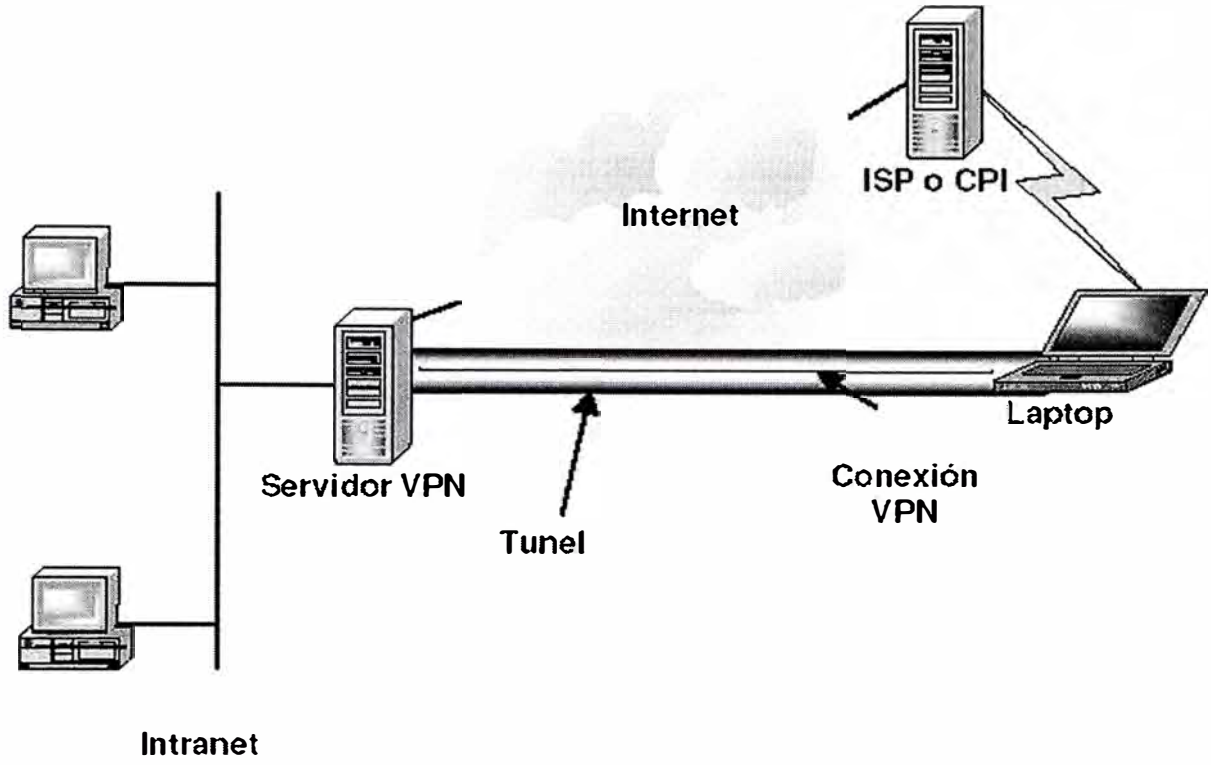


Figura 4.3 Acceso Remoto sobre Internet

2) Conectando Redes sobre Internet

Cuando las redes se conectan sobre Internet (figura 4.4), un ruteador dirige los paquetes hacia otro ruteador a través de una conexión VPN. Para los ruteadores, la VPN opera cono un enlace en la capa de enlace de datos.

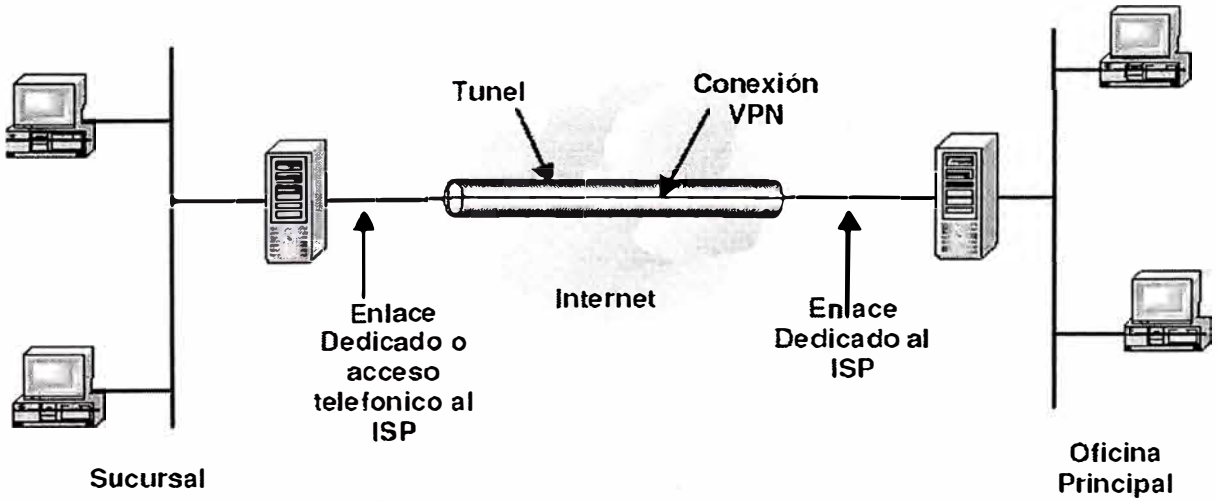


Figura 4.4 Conexión de dos redes utilizando internet

4.5.2 Conectando Redes usando WAN

En lugar de utilizar un enlace WAN dedicado y caro de larga distancia entre sus oficinas, los ruteadores de las oficinas se pueden conectar a Internet usando enlaces WAN dedicados locales hacia un ISP local. Una conexión VPN de ruteador a ruteador es entonces iniciada por cualquiera de los dos ruteadores a través de Internet. Una vez que se conectan, los ruteadores pueden dirigir tráfico directo o con protocolo de enrutamiento entre ellos usando la conexión VPN.

Si el enlace WAN es de acceso telefónico el proceso es el mismo que el anterior pero los ruteadores serán ruteadores concentradores. El ruteador concentrador que actúa como un servidor VPN debe de estar conectado al ISP local utilizando un enlace WAN dedicado.

Emplear enlaces WAN con acceso telefónico sólo es posible si el ISP soporta enrutamiento de marcado por demanda (demand- dial routing) para sus clientes; el ISP llama al ruteador del cliente cuando un datagrama IP va a ser enviado al cliente. El enrutamiento de marcado por demanda para los clientes no está ampliamente soportado por los ISPs.

4.5.3 Conexiones VPN sobre una Intranet

La conexión VPN sobre una intranet aprovecha la conectividad IP en la intranet de la organización.

1) Acceso Remoto sobre una Intranet

En algunas intranets de la organización, hay datos que son muy importantes y hay que protegerlos especialmente. En este caso el departamento que los contiene se conecta a un segmento de red físicamente desconectado del resto de la intranet de la

organización. Esto protege los datos pero crea problemas de accesibilidad de información.

4.6. PROTOCOLOS DE SEGURIDAD

Existen varios protocolos posibles. Las distintas compañías que instalan y administran este tipo de redes eligen unos u otros protocolos. En todos los casos serán túneles entre origen y destino. Dentro de estos túneles viaja la información, bien por una conexión normal (en este caso no se encriptan los datos) o bien por una conexión VPN.

4.6.1 GRE 47 (Generic Routing Encapsulation)

Es el protocolo de Encapsulación de Enrutamiento Genérico. Se emplea en combinación con otros protocolos de túnel para crear redes virtuales privadas.

El GRE está documentado en el RFC 1701 y el RFC 1702. Fue diseñado para proporcionar mecanismos de propósito general, ligeros y simples, para encapsular datos sobre redes IP. El GRE es un protocolo cliente de IP que usa el protocolo IP 47.

Este protocolo es normalmente usado con VPN de Microsoft entre servidores con acceso remoto (RRAS) configurados para el enrutamiento entre redes de área local.

GRE se encarga del encapsulamiento de los datos para enviarlos por un túnel, pero él no crea los túneles, de eso de encarga el protocolo PPTP u otro que estemos empleando.

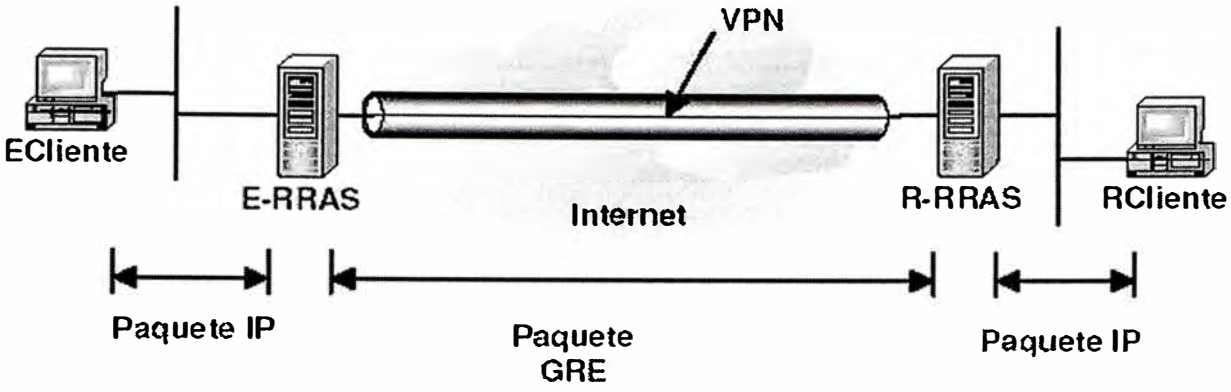


Figura 4.5 Conexión de dos redes utilizando Internet

El proceso de encapsulamiento tiene los siguientes pasos:

1) El paquete IP con los datos se transmite desde el Ecliente al servidor E-RRAS.

2) Se le añade la cabecera del PPP y se cifra todo junto obteniendo un 'fragmento PPP'.

3) Los datos cifrados se colocan dentro de un paquete GRE con su correspondiente cabecera.

4) Se envía el paquete GRE del servidor E-RRAS al servidor R-RRAS a través de Internet. Este envía se realiza por una conexión VPN creada anteriormente.

5) El servidor R-RRAS elimina el encabezados GRE, descifra, elimina el encabezado PPP y transmite los datos (paquete IP) al Rcliente.

Figura 4.6 Formato de un paquete GRE

4.6.2 PPTP (Point-to-Point Tunneling Protocol)

El Protocolo de Túnel Punto a Punto (PPTP) encapsula los paquetes (frames) del Protocolo Punto a Punto (Point- to- Point Protocol , PPP) con datagramas IP para transmitirlos por una red IP como Internet o una intranet privada.

Nota: El PPTP está documentado en " Point- to- Point Tunneling Protocol ," un borrador de Internet llamado "pptp- draft- ietf- ppext- pptp-x .txt" donde x denota la versión actual del borrador.

El PPTP utiliza una conexión TCP conocida como la conexión de control de PPTP para crear, mantener y terminar el túnel, y una versión modificada de GRE, para encapsular los paquetes PPP como datos para el túnel.

Las cargas de los paquetes encapsulados pueden estar encriptadas o comprimidas o ambas cosas.

El PPTP supone la disponibilidad de una red IP entre un cliente PPTP (un cliente de túnel que utiliza el protocolo PPTP) y un servidor PPTP (un servidor de túnel que utiliza el protocolo PPTP). El cliente PPTP podría estar ya conectado a una red IP por la que puede tener acceso al servidor PPTP, o podría tener que llamar telefónicamente a un servidor de acceso remoto (Network Access Server , NAS) para establecer la conectividad IP como en el caso de los usuarios de accesos telefónicos para Internet.

La autentificación que ocurre durante la creación de una conexión VPN con PPTP utiliza los mismos mecanismos de autentificación que las conexiones PPP, tales como el Protocolo de Autentificación Extendible (Extensible Authentication Protocol , EAP), el Protocolo de Autentificación con Reto/ Negociación de Microsoft (Microsoft Challenge- Handshake Authentication Protocol , MS- CHAP), el CHAP,

el Protocolo de Autentificación de Claves Shiva (Shiva Password Authentication Protocol , SPAP) y el Protocolo de Autentificación de Claves (Password Authentication Protocol , PAP). El PPTP hereda la encriptación, la compresión o ambas de las cargas PPP del PPP.

Para servidores PPTP sobre Internet, el servidor PPTP es un servidor VPN con PPTP con una interfase con Internet y una segunda interfase con la intranet.

Mantenimiento del Túnel con el Control de Conexión de PPTP

El control de conexión del PPTP está entre las direcciones IP del cliente PPTP que utiliza un puerto TCP asignado dinámicamente y la dirección IP del servidor PPTP que utiliza el puerto TCP reservado 1723. El control de conexión PPTP lleva a cabo el control de la llamada del PPTP y la administración de mensajes que son utilizados para mantener el túnel PPTP. Esto incluye la transmisión periódica de mensajes "PPTP Echo_ Request" y "PPTP Echo_ Reply" para detectar fallos en la conexión.

Los paquetes de control de conexión PPTP consisten de una cabecera IP, una cabecera TCP y un mensaje de control PPTP. El paquete de control de conexión PPTP en la figura 4.7 también incluye una cabecera de la capa de enlace de datos y una cola.

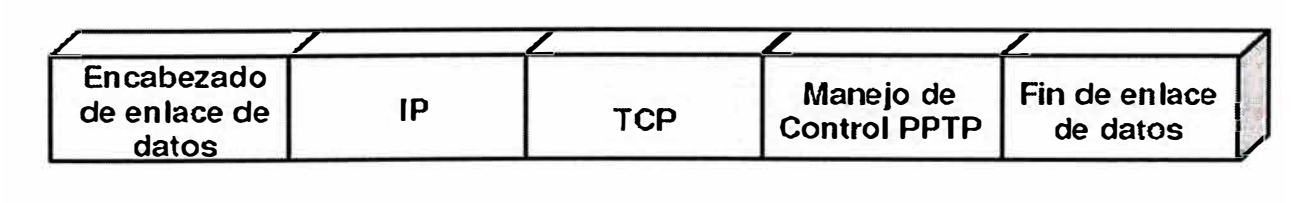


Figura 4.7 Paquete de control de conexión PPTP

1) Envío de Datos con PPTP

El envío de datos con PPTP se logra con múltiples niveles de encapsulación.

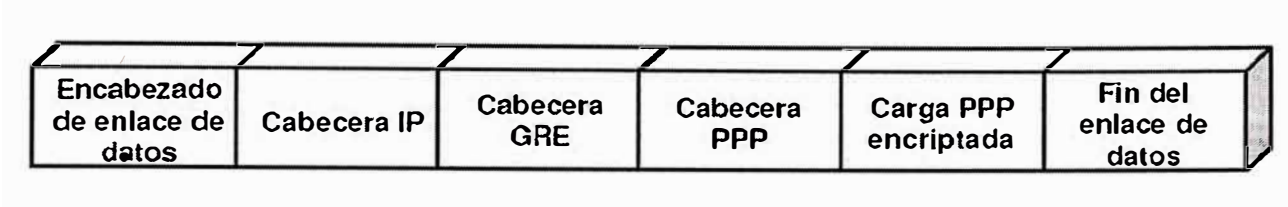


Figura 4.8 Datos del Tunel PPTP

2) Encapsulación del paquete PPP

La carga inicial PPP es encriptada y comprimida con una cabecera PPP para crear un paquete (frame) PPP. El paquete PPP es luego encapsulado con una cabecera GRE modificada.

Para PPTP, la cabecera GRE es modificada de la siguiente manera:

· Un bit de confirmación (acknowledgement bit) que es utilizado para indicar que un campo de confirmación de 32 bits está presente y es significativo.

· El campo de clave (key) es reemplazado con un campo de Longitud de Carga (Payload Length) de 16 bits y un campo de identificación de llamada (Call ID). El campo de identificación lo establece el cliente PPTP durante la creación de un túnel PPTP.

· Se agrega un campo de confirmación de 32 bits.

Dentro de la cabecera GRE, el Tipo de Protocolo (Protocol Type) se establece a 0x880B, el valor EtherType para un paquete PPP.

Para ser enviado por un enlace LAN o WAN, el datagrama IP es finalmente encapsulado con una cabecera y una cola de acuerdo a la tecnología de la capa del enlace de datos de la interfase física del emisor. Por ejemplo, cuando los datagramas IP son enviados en una interfase Ethernet, el datagrama IP es encapsulado con una cabecera y una cola Ethernet. Cuando los datagramas IP son enviados sobre un

enlace WAN punto a punto, tal como una línea telefónica analógica o RDSI, el datagrama IP es encapsulado con una cabecera y una cola PPP.

3) Procesamiento de los Datos Enviados con PPTP

Al recibir los datos enviados por el túnel PPTP, el cliente o el servidor PPTP:

· Procesa y elimina la cabecera y la cola del enlace de datos.

· Procesa y elimina la cabecera IP.

· Procesa y elimina las cabeceras GRE y PPP.

· Desencripta, descomprime, o ambas, la carga PPP (si se requiere).

· Procesa la carga para recepción o reenvío.

4) Encriptación

PPTP hereda la encriptación MPPE, la cual utiliza el cifrador de flujos RSA RC4. El MPPE está disponible solamente cuando se utiliza el protocolo de autenticación MS-CHAP (versión 1 o versión 2).

El MPPE puede utilizar claves de encriptación de 40 o de 128 bits. La clave de 40 bits está diseñada para uso internacional y la clave de 128 bits está diseñada para su uso en Norte América. Por defecto, la clave que ofrece la mayor seguridad que soporten el cliente y el servidor VPN es la que se negocia durante el establecimiento de la conexión. Si el servidor VPN requiere una clave que ofrezca mayor seguridad que la que soporta el cliente VPN, el intento de conexión es rechazado.

El MPPE fue diseñado para encriptación a través de enlaces punto a punto donde los paquetes llegan en el mismo orden en que se envían y hay poca pérdida de paquetes. Con estas condiciones, la desencriptación de cada paquete depende de la desencriptación del paquete anterior.

Puesto que las VPNs emplean Internet como red intermediaria, no se garantiza el orden de llegada de los paquetes y es más elevada la cantidad de éstos que se pierden. Por lo tanto, el MPPE para las conexiones VPN cambia la clave de encriptación para cada paquete de forma que la desencriptación de cada paquete es independiente del paquete previo. El MPPE incluye una secuencia de números en la cabecera MPPE. Si los paquetes se pierden o llegan en desorden, las claves de encriptación son cambiadas en relación al número de secuencia.

5) Filtrado

Un servidor VPN sobre PPTP típicamente tiene dos interfases físicas: una interfase hacia la red pública o compartida como Internet y otra en la intranet privada. También tiene una interfase virtual conectada a todos los clientes VPN. Para que el servidor VPN redirecciones el tráfico entre los clientes VPN, el redireccionamiento IP debe estar activado en todos los clientes. Sin embargo, la activación del redireccionamiento entre dos interfases físicas provoca que el servidor VPN enrute todo el tráfico IP desde la red pública o compartida hacia la intranet. Para proteger a la intranet del tráfico que no es enviado al cliente VPN, debe de configurarse el filtrado de paquetes PPTP (PPTP packet filtering) para que usuarios potencialmente mal intencionados no establezcan conexiones con la intranet.

El filtrado de paquetes PPTP puede configurarse tanto en el servidor VPN como en un cortafuegos intermedio.

4.6.3 IPSec (IP Security Protocol)

Descrito en el capitulo 3 con mayor detalle, resumiendo IPSec es un grupo de extensiones de la familia del Protocolo IP pensado para proveer servicios de seguridad a nivel de red, de un modo transparente a las aplicaciones de niveles

superiores. Este protocolo ofrece sus servicios a la capa IP en los entornos de Ipv4 e Ipv6. Nos ofrece servicios de control de acceso, fiabilidad de la conexión, autenticación del origen de los datos, protección contra réplicas y confidencialidad dentro de un flujo de tráfico limitado, y la posibilidad de crear túneles cifrados (VPNs).

4.6.4 L2TP (Protocolo de Tunelado Nivel 2)

Es un componente de creación importante para las VPN de acceso. Es una extensión del protocolo Punto a Punto, fundamental para la creación de VPNs. L2TP combina las mejores funciones de los otros dos protocolos tunneling. Layer 2 Forwarding (L2F) de Cisco Systems y Point- to- Point Tunneling (PPTP) de Microsoft. L2TP es un estándar que cuenta con el respaldo de Cisco Systems, Microsoft, Ascend, 3Com y otros líderes en la industria de la conectividad.

A continuación una serie de términos relacionados con este protocolo:

1) L2TP Access Concentrator (LAC). Se añade un dispositivo LAC a los componentes físicos de la red conmutada; como la red telefónica convencional o RDSI, o se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC sólo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o más LNS.

Puede "tunelizar" cualquier protocolo que incluya el PPP. LAC es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes.

2) L2TP Network Server (LNS). Un LNS opera sobre cualquier plataforma con capacidad de terminación PPP. LNS gestiona el lado del servidor del protocolo L2TP. Ya que L2TP se apoya sobre el medio al que llegan los túneles L2TP, LNS sólo puede tener un única interfaz LAN o WAN, aunque es capaz de terminar las

llamadas entrantes en cualquiera de la amplia gama de las interfaces PPP LAC (asíncronos, RDSI, PPP sobre ATM, PPP sobre Frame Relay).

3) Network Access Server (Servidor de acceso a la red). NAS es un dispositivo que proporciona a los usuarios acceso temporal a la red bajo demanda. Este acceso es punto a punto, de uso típico en líneas de la red telefónica convencional o RDSI. En la implementación Cisco, un NAS sirve como LAC.

4) Seguridad

L2TP es un protocolo tunneling que soporta autenticación de túnel y usuario. Para la protección de seguridad VPN de acceso, las compañías ofrecen los siguientes servicios:

5) Autenticación, Autorización y Contabilidad (AAA), que incluye:

· Soporte para nombre de usuario/ clave de acceso para determinar la autorización de los servicios VPN de acceso.

· Soporte para la autenticación de usuario.

· Soporte de configuración por usuario, que incluye abastecimiento por usuario de la asignación de direcciones IP, ruteo estático y filtros de acceso.

· Contabilidad que puede ejecutarse en el LAC y el LNS, que incluye conexión, inicio/ parada y generación de informes completos de los intentos de conexión fallidos.

6) Arquitectura L2TP VPN de Acceso

En un entorno de conexiones telefónicas, un túnel L2TP puede iniciarse desde un servidor de acceso remoto (NAS) (como un túnel iniciado NAS) o desde software cliente (como un túnel iniciado por el cliente) hacia un ruteador que actúa como un punto de terminación del túnel.

7) Ventajas

Dado que L2TP es un protocolo estándar, todos los clientes (proveedores de servicios y administradores de redes corporativas) pueden disfrutar de un amplio rango de ofertas de servicios disponibles de diversos fabricantes. La interoperatividad entre los fabricantes ayudarán a garantizar una rápida implementación internacional de un servicio estándar VPN de acceso.

L2TP ofrece la posibilidad de separar las aplicaciones de datos de la conmutación de voz, y llevar los datos a las redes construidas especialmente para datos. Esta característica es interesante para los proveedores de servicios Internet (ISP). La meta de éstos es construir y mantener redes disponibles a partir de sus PoP (Puntos de Presencia) geográficamente dispersos. Mediante la contratación externa del acceso telefónico y ADSL de los comerciantes Internet, compañías de telecomunicación, empresas de operaciones regionales, u otros proveedores de servicios que ya tiene PoP dispersos, la ISP de tamaño medio puede generar ingresos a la vez que aprovechar al máximo los recursos. Estos servicios de contratación externa, conocidos como "venta al por mayor de Internet" o "acceso al por mayor", pueden utilizar tecnología L2TP para descargar el tráfico de red por conexión telefónica de la red de voz convencional del proveedor, creando nuevos flujos entrantes sobre los ya existentes y ofreciendo flexibilidad adicional a los ISP en crecimiento.

4.6.5 SSH (Secure Shell)

Tradicionalmente en sistemas Unix en el momento de entrar en el sistema, tanto el login como el password, así como el resto de la sesión, se transmiten a través de nuestra LAN o incluso a través de ruteadores y nodos ajenos al nuestro en texto claro. Esto quiere decir que cualquiera que tenga activado un sniffer puede capturar

nuestras sesiones con el potencial peligro que ello conlleva. La manera de evitar que alguien pueda espiar nuestras claves y sesiones, es utilizar una herramienta muy potente, fácil de instalar y muy cómoda para el usuario.

ssh/ sshd actúan basándose en la arquitectura cliente/ servidor, en este caso concreto sshd se ejecuta en el servidor en un puerto (el defecto es el 22) a la espera de que alguien utilizando un cliente ssh se conecte para ofrecerle una sesión segura encriptándola de extremo a extremo.

Todo es como en una sesión telnet tradicional, pero con la particularidad de que todas las comunicaciones serán encriptadas. El manejo de cualquier programa cliente de SSH es muy sencillo. Básicamente hay que introducir el servidor al que te quieres conectar (por ejemplo servidor. dominiopublico.net) y que algoritmo de encriptación quieres usar (por ejemplo 3DES). Si no se dispone de un programa cliente de SSH, puede bajarse de Internet.

Los programas que vienen con la distribución son:

· sshd Es el servidor propiamente dicho, escucha a la espera de conexiones.

· ssh Es el cliente, con él nos podemos conectar a un servidor sshd así como ejecutar comandos.

· scp Copia archivos con seguridad entre hosts. (Sustituto ideal de rcp).

· ssh-keygen Usado para crear RSA keys (host keys y user authentication keys).

· ssh-agent Agente de autentificación. (Usado para manejar RSA keys en la autentificación.)

· ssh-add Se usa para añadir nuevas llaves con el agente.

· make-ssh-known-hosts Usado para crear el archivo /etc/ ssh_ known_ hosts.

Entre las principales ventajas se tienen:

· Previene ataques hechos mediante Ip-spoofing.

· Utiliza varios algoritmos (RSA para la llave de intercambio e IDEA, DES o triple DES para la encriptación de la sesión).

· Permite sesiones X Window.

· Permite redirección arbitraria de puertos en ambas direcciones. (Ideal para transferencias monetarias a través de la red, ejemplo e- cash).

· Transferencia segura de archivos

1) Seguridad

Cada servidor de SSH tiene asociado un par de claves pública/ privada, equivalentes al par de claves de un usuario. Estas claves se utilizan para identificar al servidor frente al usuario; de esta forma, se evita que otra máquina (posiblemente hostil) pueda suplantarlo.

La primera vez que nos conectamos a la máquina remota, SSH solicita al servidor su clave pública, y la acepta sin hacer ninguna comprobación.

Esta clave queda registrada en el directorio $HOME/. ssh2/ hostkeys del usuario; en futuras conexiones el cliente comparará la clave que le suministra el servidor con la que tiene almacenada. Si ambas claves no coinciden, el cliente no establecerá la conexión, para evitar que alguna máquina hostil pueda suplantar impunemente al servidor.

2) Autenticación por clave simétrica ó pública

Proceso de autentificación:

· El servidor nos envía un mensaje, que debemos devolver cifrado con nuestra clave privada.

· El servidor descifra el mensaje de respuesta con nuestra clave pública.

· El servidor compara el mensaje resultante con el texto original; si coinciden, el servidor nos considera debidamente autentificados El punto más débil es cómo hacer llegar nuestra clave pública al servidor.

La principal ventaja de este método de autentificación es que, aunque un atacante lograra comprometer el servidor, sólo podría conseguir acceso a nuestra clave pública, pero nunca a nuestra clave privada. De todas formas, en prevención de un posible compromiso del cliente, es necesario que la clave privada esté protegida con una frase de paso adecuada. De esta forma, nadie podrá utilizarla aún en el caso de que consiguiera de alguna manera hacerse con ella.

En el caso de realizar la conexión desde una máquina Unix, una ventaja secundaria es que se puede utilizar un agente de autentificación para evitar tener que teclear la frase de paso en cada conexión.

El mayor inconveniente de la autentificación por clave pública es la fase de configuración previa, que puede resultar algo engorrosa. Los pasos a seguir son:

· Generación de las claves (Para esto se utiliza el programa ssh-keygen)

· Propagación de la clave pública. Primero copiar nuestra clave pública en todas las máquinas a las que queramos conectarnos. La forma más sencilla es utilizar el comando sftp. A continuación crearemos el directorio ssh2 en la máquina remota y almacenaremos en él nuestra clave pública.

· Selección del par de claves. Podemos tener múltiples parejas de claves y tendremos que listarlas explícitamente tanto en el servidor como en el cliente. En la máquina cliente, tendremos que crear un archivo "identification" que liste las claves privadas que queremos utilizar cuando nos conectemos a un servidor de SSH. En cada una de

las máquinas remotas, tendremos que crear un archivo "authorization" que liste las claves públicas que se aceptarán para iniciar una conexión.

CAPÍTULO V

CORTAFUEGOS (FIREWALLS)

5.1. INTRODUCCIÓN

La tecnología de Cortafuegos ha crecido sustancialmente desde que fue introducido a inicios de los noventas. En sus inicios la tecnología de Cortafuegos inicio con los simples cortafuegos de filtrado de paquetes y progreso a más sofisticados cortafuegos capaces de examinar múltiples capas de contenido y actividad de la red.

Así como Internet se ha desarrollo y convertido en una red compleja y moderna, la seguridad de Internet ha llegado a ser cada vez más problemática, los ataques e intrusión a redes son comunes y son tema del cada día. La tecnología de Cortafuegos es parte del estándar de la arquitectura de seguridad de cualquier organización. Hoy en día, los usuarios en sus hogares que usan servicios comerciales tales como cable/ADSL también emplean cortafuegos personales y cortafuegos de hardware (appliances).

Los modernos cortafuegos son capaces de trabajar en conjunto con herramientas tales como los detectores de intrusión y escaneadores de contenido correo/webs en búsqueda de virus y aplicaciones con códigos maliciosos. Pero los cortafuegos por si solo no proveen una completa protección de los problemas que surgen en Internet.

Por lo tanto, ellos son una parte del programa integral de seguridad de información. Generalmente los cortafuegos son vistos con la primera línea de defensa, sin embargo seria mejor verlos como la ultima línea de defensa de una organización; las organizaciones deberían priorizar la seguridad de los sistemas internos. Los servidores internos, computadoras personales, y otros sistemas deberían mantenerse actualizados con los últimos parches de seguridad y software de antivirus.

5.2. ¿QUÉ ES UN CORTAFUEGOS?

Un cortafuegos es un sistema o grupo de sistemas que impone una política de seguridad entre la red privada de una organización (Intranet), Internet y Extranet, controlando el acceso entre las diferentes redes empleando diferentes niveles de seguridad. El cortafuegos determina cual de los servicios de red pueden ser accedidos dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

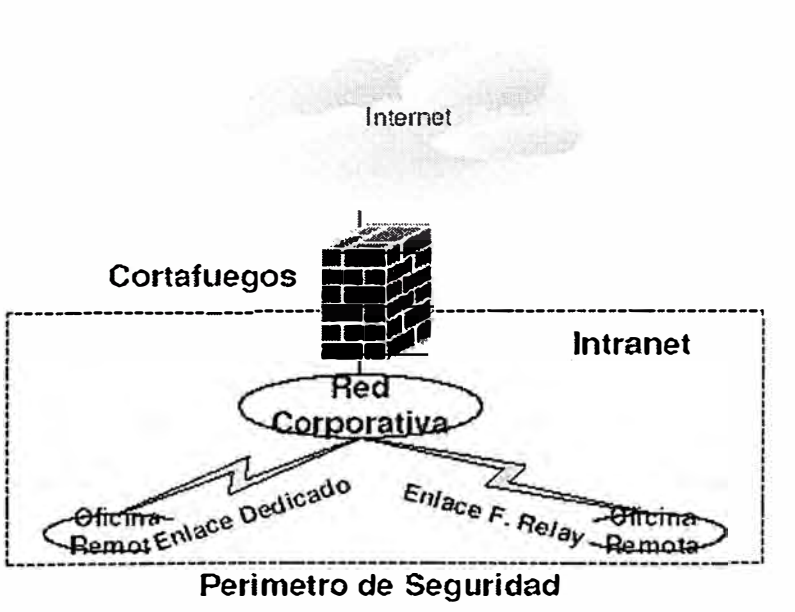


Figura 5.1 La política de seguridad crea un perímetro de defensa

Para que un cortafuegos sea efectivo, todo tráfico de información a través Internet deberá pasar a través del mismo donde podrá ser inspeccionada la 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 cortafuegos de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

5.3. BENEFICIOS DE UN CORTAFUEGOS

Los cortafuegos en Internet administran los accesos posibles Internet a la red privada. Sin un cortafuegos, cada uno de los servidores propios del sistema se expone a ataques externos.

El cortafuegos permite al administrador de la red definir una especie de embudo, manteniendo al margen los usuarios no-autorizados (tales como, hackers, crakers, vándalos, espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles.

El cortafuegos ofrece un punto donde la seguridad puede ser monitorizada y si aparece alguna actividad sospechosa, este puede generar una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del trafico significativo a través del cortafuegos.

Más beneficios de los cortafuegos:

· Concentra la seguridad

· Centraliza los accesos

· Genera alarmas de seguridad.

· Traduce direcciones (NAT)

· Monitoriza y registra el uso de servicios de Internet

Con el paso de algunos años, Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Un cortafuegos es un lugar lógico para desplegar una traslación de Direcciones de Red (NAT)

5.4. LIMITACIONES DE UN CORTAGUEGOS

Un cortafuegos no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo, si existe una conexión dial-out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP a través de algún proveedor de servicios de Internet (ISP).

Este tipo de conexiones debilitan la seguridad provista por el cortafuegos creando una puerta de ataque.

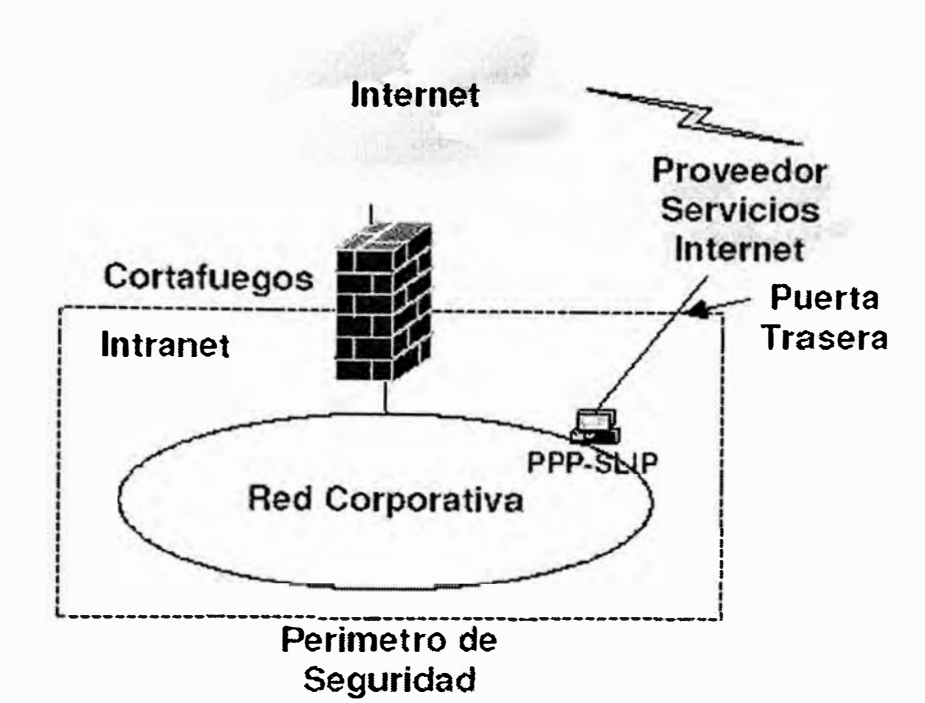


Figura 5.2 Conexión no controlada por el cortafuegos

El cortafuegos no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software obtenidos de Internet, el cortafuegos puede no contar con un sistema preciso de escaneo para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él.

La solución real está en que la organización debe ser consciente en instalar software anti-virus en cada despacho para protegerse de los virus que llegan por medio de diskettes o cualquier otra fuente.

5.5. PRINCIPIOS DE DISEÑO DE CORTAFUEGOS

Cuando se diseña un cortafuegos, se tienen que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

· Posturas sobre la política del cortafuegos.

· La política interna propia de la organización para la seguridad.

· Los componentes o la construcción de secciones del cortafuegos.

5.5.1 Política de Cortafuegos

La política de un cortafuegos describe la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un cortafuegos puede tomar:

· "Todo lo que no está explícitamente permitido está prohibido".

· "Todo lo que no está explícitamente prohibido está permitido".

La primera postura asume que un cortafuegos puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

Esta propuesta es recomendada únicamente a un limitado número de servicios soportados cuidadosamente, seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es más importante que el de facilitar el uso de los servicios. Esta propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el cortafuegos puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso.

Esta propuesta crea ambientes más flexibles al disponer mas servicios para los usuarios de la organización. La desventaja de esta postura se basa en la importancia de "facilitar el uso" mas que la propia seguridad del sistema.

5.5.2 Política Interna de Seguridad

Un cortafuegos no está sólo, es parte de la política de seguridad total en una organización, la cual define todos los aspectos competentes al perímetro de defensa.

Para que esta sea exitosa, la organización debe de conocer que es lo se esta protegiendo. La política de seguridad se basará en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación de la organización. Si no se posee la información detallada de la política a seguir, aun que sea un cortafuegos cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible ataque.

5.6. TIPOS DE CORTAFUEGOS

5.6.1 Filtro de Paquetes

Es el cortafuegos más básico, esencialmente es un dispositivo de ruteo que tiene la funcionalidad de control de accesos por direcciones y servicios. Este ruteador, también llamado ruteador de selección, toma las decisiones de rechazar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interfase de entrada del paquete, y la interfase de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

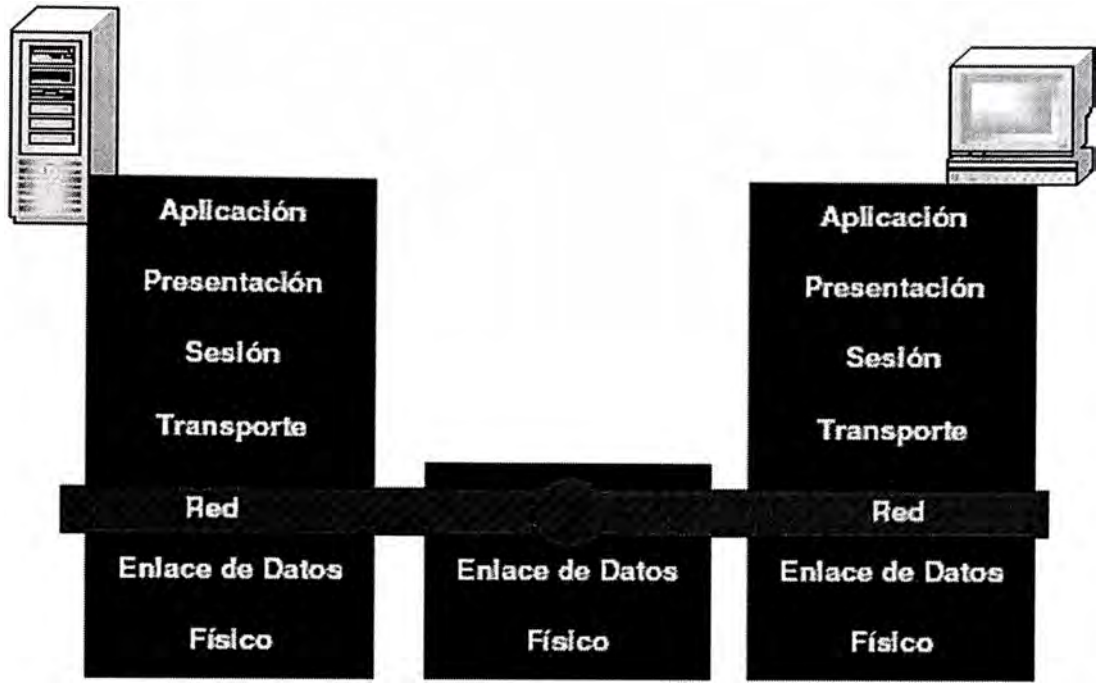


Figura 5.3 Filtro de Paquetes

Algunos ejemplos de tipo de ataques a estos ruteadores son:

· Agresiones Originadas por el direccionamiento IP.

Para este tipo de ataque, el intruso trasmite paquetes desde el exterior pretendiendo pasar como servidor interno. Los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema y conocida por el atacante. El agresor espera que usando esta suplantación se pueda penetrar al sistema para emplearlo seguramente como dirección fuente donde los paquetes que trasmita sean autenticados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente "interno" si el paquete llega en una de las interfaces del ruteador "externo".

· Agresiones originadas en el ruteador.

En un ataque de ruteo, la estación de origen especifica la ruta que un paquete deberá de tomar cuando cruce a través de Internet. Este tipo de ataques son diseñados para cuantificar las derivaciones de seguridad y encauzan al paquete por un inesperado camino a su destino. Los ataques originados en el ruteador pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de ruteo opcionales.

· Agresiones por fragmentación.

Por este tipo de ataques, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a separarse en paquetes.

Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado de un ruteador examinando los primeros fragmentos y el resto pasa sin ser visto.

Aunque si bien únicamente es explotado por sencillos decodificadores, una agresión pequeñísima puede ser frustrada si se descartan todos los paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

1) Limitaciones del ruteador filtra-paquetes.

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo más difícil su administración y comprensión.

Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Cualquier paquete que pasa directamente a través de un ruteador puede ser posiblemente usado como parte inicial un ataque dirigido de datos.

Generalmente, los paquetes en torno al ruteador disminuyen conforme el numero de filtros utilizados se incrementa. Los ruteadores son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interface apropiada de la transmisión. Si está autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aún aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el trafico. Un ruteador Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto/dato del servicio. Por ejemplo, un administrador de red necesita filtrar el tráfico de una capa de aplicación - limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateways a nivel de aplicación.

5.6.2 Gateways a nivel de aplicación (Proxys)

Los gateways nivel de aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes.

Se instala en el gateway un código de propósito especial (un servicio Proxy) para cada aplicación, servicio que se desee proteger.

Un aumento de seguridad de este tipo incrementa los costos en términos del tipo de gateway seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el gateway, y un decrecimiento en el nivel de los servicios que podrán obtener nuestros usuarios, dando como resultado un sistema carente de transparencia en el manejo de los usuarios en un ambiente "amigable". Como en todos los casos el administrador de redes debe de tomar una decisión de compromiso entre las necesidades propias en seguridad de la organización con la demanda de "fácil de usar" demandado por los usuarios.

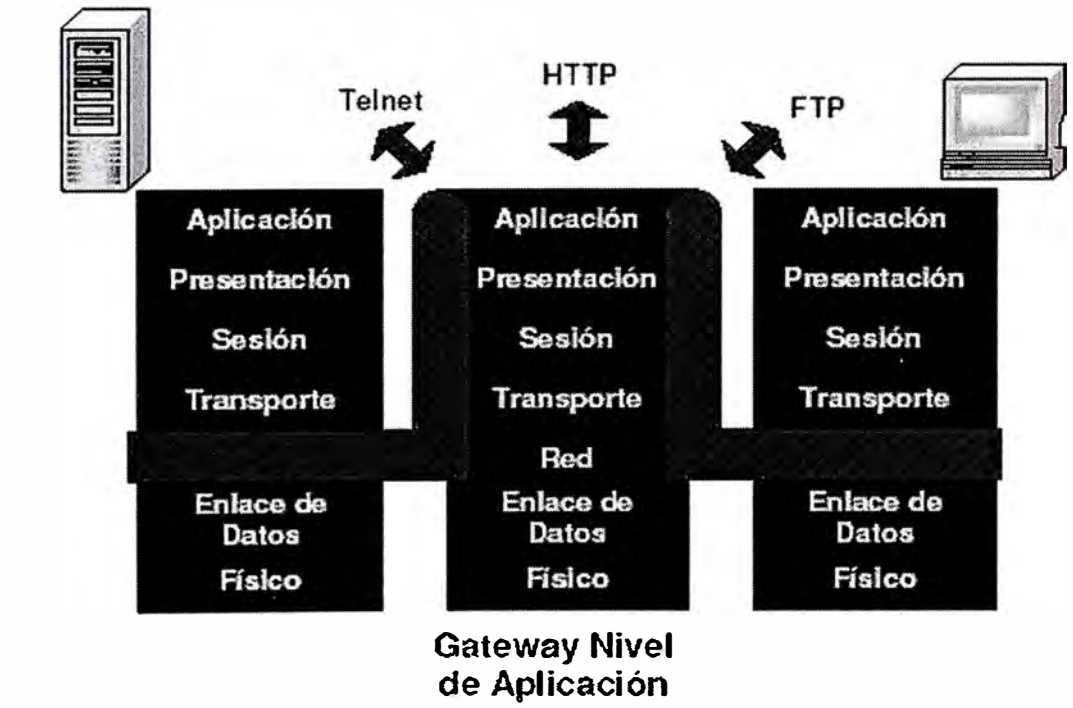


Figura 5.4 Gateway a Nivel de Aplicación

Un Gateway a nivel de aplicación por lo regular es descrito como un "servidor de defensa" (o Bastion Host en ingles) porque es un sistema diseñado específicamente

blindado y protegido contra cualquier ataque. Hay varias características de diseño que son usadas para hacer más seguro un servidor de defensa:

· La plataforma de hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo. Por ejemplo, si el servidor de defensa es una plataforma UNIX, se ejecutará una versión segura del sistema operativo UNIX que está diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del cortafuegos.

· Únicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no está instalado, este puede no ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor.

· El servidor de defensa podrá requerir de una autenticación adicional para que el usuario acceda a los servicios Proxy. Por ejemplo, el servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización (tal como la tecnología "una-sola vez" de contraseña donde una tarjeta inteligente generaba un código de acceso único por medios criptográficos). Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión.

· Cada Proxy se configura para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.

· Cada Proxy está configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características y

comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.

· Cada Proxy mantiene la información detallada y auditada de todos los registros del tráfico de cada conexión y la duración de esta. Esta auditoria es una herramienta esencial para descubrir y finalizar el ataque de un intruso.

· Cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si se suscitara un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones.

· Un Proxy generalmente funciona sin acceso al disco; lo único que hace es leer su archivo de configuración inicial. De esta forma un intruso podrá encontrar más dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.

· Cada Proxy corre como un usuario no-privilegiado en un directorio privado y seguro del servidor de defensa.

1) Beneficios del gateway a nivel-aplicación

Son muchos los beneficios desplegados en un gateway a nivel de aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede acceder a los servicios. Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado. Los gateways a nivel de aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información

detallada de registro. Finalmente, las reglas de filtrado para un gateway de este tipo son mucho más fáciles de configurar y probar que en un ruteador filtra-paquetes.

2) Limitaciones del gateway a nivel-aplicación

Probablemente una de las grandes limitaciones de un gateway a nivel de aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accede a los servicios Proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel de aplicación demanda modificar la conducta del usuario desde el momento en que se requiere de dos pasos para hacer una conexión mejor que un paso.

5.6.3 Cortafuegos de Inspección de Estados

Los Cortafuegos de Inspección de Estados son filtros de paquetes que incorporan adicionales funcionalidades en la capa cuatro del modelo de OSI. La Inspección de Estados evolucionó de la necesidad de acomodar ciertas características del conjunto de protocolos TCP/IP que hizo dificultoso el desarrollo de los cortafuegos. Cuando una aplicación TCP (orientado a conexión) crea una sesión con un sistema remoto, se crea un puerto en el equipo que inicia la sesión (origen) con el propósito de recibir el trafico de red desde el sistema remoto (destino). De acuerdo con las especificaciones TCP, este puerto del origen será un numero mayor a 1023 y menor que 65535. De acuerdo con la convención, el puerto destino en el equipo remoto será un numero menor a 1024. Por ejemplo puede ser el 25 para SMTP (Simple Mail Transport Protocol).

Los cortafuegos filtro de paquetes deben permitir el trafico entrante de red en todos los puertos "altos" para que pueda ocurrir una sesión orientado a conexión, por ejemplo, los paquetes retornan desde el sistema "destino". Al abrir muchos puertos

crea un riesgo enorme de intrusión por usuarios no autorizados que pueden emplear una variedad de técnicas para abusar estas convenciones. Los cortafuegos de inspección de estados salvan este problema creando un directorio de las conexiones TCP salientes, correspondiente a cada sesión del puerto del cliente "puertos altos". Esta "tabla de estados" es luego usada para validar cualquier trafico entrante.

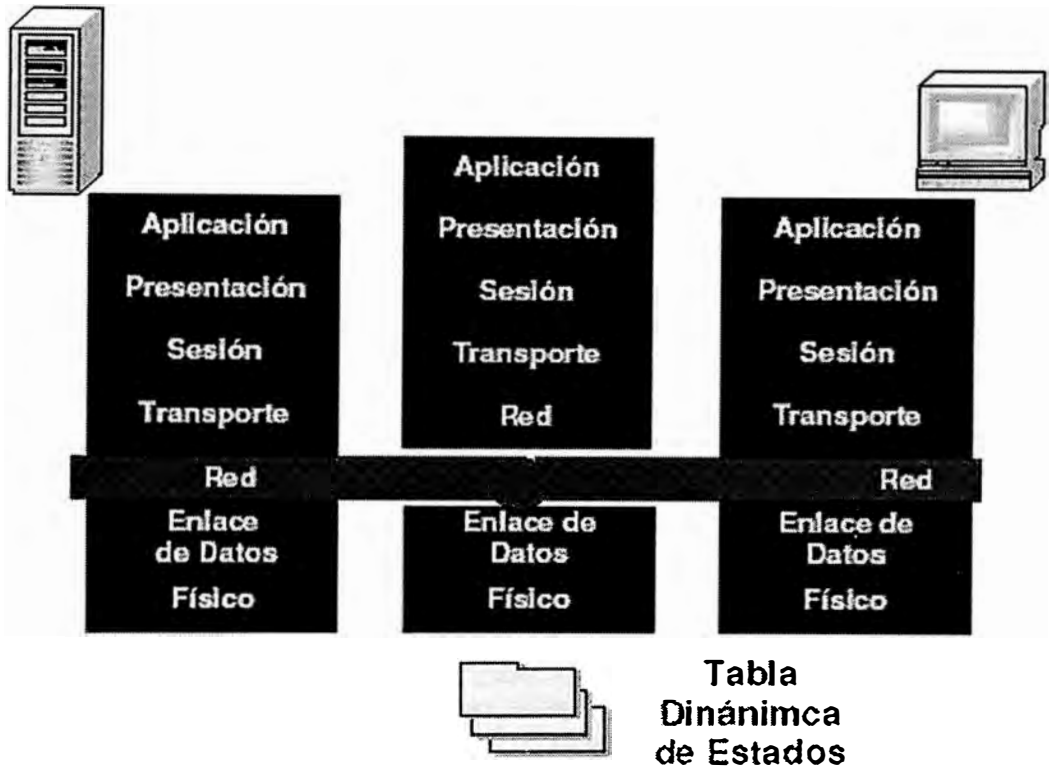


Figura 5.5 Firewall de Inspección de Estados

La solución de inspección de estados es más segura debido a que el cortafuegos rastrea los puertos del cliente individualmente en vez de abrir todos los puertos "altos" para acceso externo.

En esencia, los cortafuegos de inspección de estados añaden capacidades de análisis en la capa cuatro a la arquitectura estándar de filtrado de paquetes. Los cortafuegos de inspección de estados comparten las fuerzas y debilidades de los cortafuegos de filtrado de paquetes, pero debido a la implementación de la tabla de estados, los

cortafuegos de inspección de estados son generalmente considerados como más seguros que los cortafuegos de filtro de paquetes.

Un cortafuegos de inspección de estados también se diferencia de un filtro de paquetes en que esta inspección de estados es útil o aplicable solo en infraestructuras de TCP/IP. Los cortafuegos de inspección de estados pueden acomodar otros protocolos de red de la misma manera que un filtro de paquetes, pero la tecnología actual de inspección de estados es relevante solo en TCP/IP. Por esta razón, muchos textos clasifican a los cortafuegos de inspección de estados como un conjunto de la funcionalidad superior que los cortafuegos de filtro de paquetes.

5.7. TRASLACIÓN DE DIRECCIONES DE RED

La tecnología de Traslación de Direcciones de Red (NAT) fue desarrollado en respuesta a las dos mayores problemas en ingeniería de red y seguridad. Primero, la traslación de direcciones de red es una herramienta efectiva para "ocultar" el esquema de direccionamiento de red detrás de un cortafuegos.

En esencia, la traslación de direcciones de red permite a una organización la implementación de un esquema de direccionamiento a su elección, mientras aun se mantiene la habilidad para conectar los recursos externos a través del cortafuegos. Segundo, el agotamiento del espacio de direcciones IP ha causado que algunas organizaciones usen NAT para asociar direcciones IP no ruteadas a un conjunto de números pequeño de direcciones legales, de acuerdo con el RFC 1918.

La traslación de direcciones de red puede ser de tres tipos:

5.7.1 Traslación de direcciones de red de forma estática

En una traslación de direcciones de red de forma estática, cada sistema interno en la red privada es tiene una direcciones externa correspondiente, o sea una dirección IP

ruteable asociada con esta. Esta técnica particular se usa raramente, debido a la escasez de direcciones IP disponibles. Con una traslación de direcciones de red estática, es posible ubicar recursos detrás del cortafuegos, mientras se mantiene la habilidad de proveer acceso selectivo a usuarios externos. En otras palabras, un sistema externo puede acceder a un servidor web interno cuya dirección ha sido asociada con una traslación de dirección de red estática. El cortafuegos podría realizar mapeos ya sea en dirección saliente o entrante.

Dirección IP Interna (RFC 1918)	Dirección IP Externa (Ruteable en Internet)
192.168.100.1	206.100.3.61
192.168.100.2	206.100.3.62
192.168.100.3	206.100.3.63
192.168.100.4	206.100.3.64
192.168.100.5	206.100.3.65
192.168.100.6	206.100.3.66
192.168.100.7	206.100.3.67
192.168.100.8	206.100.3.68
192.168.100.9	206.100.3.69
192.168.100.10	206.100.3.70
192.168.100.11	206.100.3.71

Tabla 5.1 Traslación de direcciones de red estática

La tabla 5.1 muestra un ejemplo de traslación de direcciones de red estática que podría asociar direcciones IP internas, no ruteables de acuerdo con el RFC 1918, a direcciones ruteables externas.

Con una traslación de direcciones de red de forma oculta, todos los sistemas detrás del cortafuegos comparten la misma dirección IP externa. Así, con un sistema de traslación de direcciones de red de forma oculta, cinco mil sistemas detrás de un cortafuegos podría verse como un único sistema. Este tipo de traslación de direcciones de red es más común, pero tiene una debilidad en que no es posible hacer que los recursos este disponibles para los usuarios externos una vez que estos son ubicados detrás del cortafuegos. Asociar de forma inversa desde sistemas externos a sistemas internos no es posible, por consiguiente los sistemas que deben ser accesibles desde sistemas externos no deben tener su dirección asociada. Otra debilidad de esta implementación particular de traslación de direcciones de red es que el cortafuegos empleado para este tipo de traslación debe comúnmente usar su propia direcciones de la interfaz externa con el "sustituto" o dirección trasladada para todos los sistemas y recursos residentes detrás de él. Este requerimiento tiende a impactar a la flexibilidad de este mecanismo.

5.7.3 Traslación de direcciones de puertos (PAT)

Existe dos principales diferencias entre PAT y NAT "oculto". Primero, PAT no requiere el uso de la dirección IP de la interfase externa del cortafuegos para todos el trafico de red; otra dirección puede ser creada para este propósito. Segundo, con la traslación de direcciones de puerto, es posible ubicar los recursos detrás del sistema de cortafuegos y aun hacer que ellos serán accedidos selectivamente a usuarios externos. Este acceso se logra reenviando las conexiones entrantes sobre ciertos puertos a computadores específicos. Por ejemplo, un cortafuegos empleando traslación traslación de direcciones de puerto puede dejar pasar todas las conexiones

traslación de direcciones de puerto puede dejar pasar todas las conexiones entrantes al puerto 80 a un servidor web interno que emplea un esquema de direccionamiento de red diferente.

Dirección IP del Equipo Interno	Puerto Cliente del Equipo Interno	Puerto Saliente (PAT)
192.168.100.11	1030	3315
192.168.100.2	1039	3316
192.168.100.103	1400	3317
192.168.100.44	1515	3318
192.168.100.23	1027	3319
192.168.100.108	1026	3320

Tabla 5.2 Tabla de Traslación de Direcciones de Puerto

La traslación de direcciones de puerto trabaja usando las direcciones del puerto del cliente para identificar las conexiones entrantes. Por ejemplo, si un sistema detrás del cortafuegos que emplea PAT uso el telnet para conectarse a un sistema en Internet, el sistema externo ve una conexión de la interface externa del cortafuegos, junto con el puerto cliente del sistema originador de la conexión. Cuando un sistema externo responde a la conexión de red, podría usar la información de direccionamientos anterior. Cuando el cortafuegos usando PAT recibe la respuesta, podría ver el puerto cliente del origen proveído por el sistema remoto, y basado en este puerto, puede determinar cual de los sistemas internos inicio la sesión. En el ejemplo mostrado en la Tabla 5.1, un sistema remoto podría responder a la conexión requerida usando la dirección IP de la interfaz externa del cortafuegos, seguido por el puerto PAT de salida como puerto origen del cliente. El puerto PAT de salida se genera dinámicamente en el cortafuegos, y es secuencial en algunas implementaciones y

aleatoria (con los parámetros de puerto origen del cliente normal) en otras implementaciones.

En términos de fortalezas y debilidades, cada tipo de traslación de direcciones de red tiene aplicabilidad en ciertas situaciones, siendo variable la cantidad de flexibilidad ofrecida por cada tipo.

La traslación de direcciones de red estática ofrece la mayor flexibilidad, pero como se indico anteriormente, la traslación de direcciones de red estática no es normalmente práctica dado al pequeño rango de direcciones de red en IP versión 4.

La tecnología de traslación de direcciones de red de forma oculta fue un paso de ínterin en el desarrollo de la tecnología de traslación de direcciones de red, y es raramente usada porque la traslación de direcciones de puertos ofrece características adicionales superiores a las que presenta la traslación de direcciones de red de forma oculta mientras mantiene el mismo diseño básico de las consideraciones de ingeniería. PAT es a menudo la más conveniente y solución segura.

5.8. ARQUITECTURA DE CORTAFUEGOS

Aunque existen infinitas posibilidades en la combinación de elementos de seguridad para la construcción de un cortafuegos, hay algunas implementaciones o arquitecturas que, por su simplicidad, o por su interés en un número elevado de casos, presentan un uso más frecuente. Se pueden fijar cinco factores a tener en cuenta a la hora de examinar cada uno de los tipos de cortafuegos:

· Control de daños: si un cortafuegos es vulnerado ¿a que tipo de accesos deja abierta la red privada?. Si se destruye, ¿a que tipo de accesos permitirá entrar a la red privada?

· Modo de fallo: si se entra en el cortafuegos, ¿con qué facilidad se puede detectar?. Si el cortafuegos es destruido, ¿con que facilidad se puede detectar?. Tras morir el cortafuegos, ¿cuánta información se mantiene para diagnosticar el ataque?. Facilidad de uso: ¿en que medida el cortafuegos constituye un estorbo?

· Política: "lo que no está permitido está prohibido" y "lo que no está prohibido está permitido".

Antes de entrar a comentar alguna de estas implementaciones o arquitecturas de seguridad vamos a recordar un elemento que en muchas de dichas arquitecturas aparece y que en la sección anterior ya se explicó: el bastion host. Un bastion host es un sistema identificado por el administrador del cortafuegos como un punto crítico en la seguridad de la red. Generalmente dispondrán de un grado extra de atención a su seguridad, pueden estar sometidos a auditorias regulares y pueden tener software modificado. Es frecuente que antes de convertir una computadora en bastion host sea fortificado. El proceso de fortificación reduce la posibilidad de fallos e incrementa todos los controles de acceso, monitorización y auditoria.

5.8.1 Ruteadores de Filtrado

Son una implementación formada únicamente por un ruteador de filtrado (screening routers) entre la red privada e Internet. En este tipo de cortafuegos existe una posibilidad de comunicación entre varias computadoras de la red privada y otras computadoras de Internet.

La zona de riesgo es igual al número de computadoras que hay en la red privada y el número y tipo de servicios hacia los que el ruteador de filtrado permite el tráfico.

La zona de riesgo es igual al número de computadoras que hay en la red privada y el número y tipo de servicios hacia los que el ruteador de filtrado permite el tráfico.

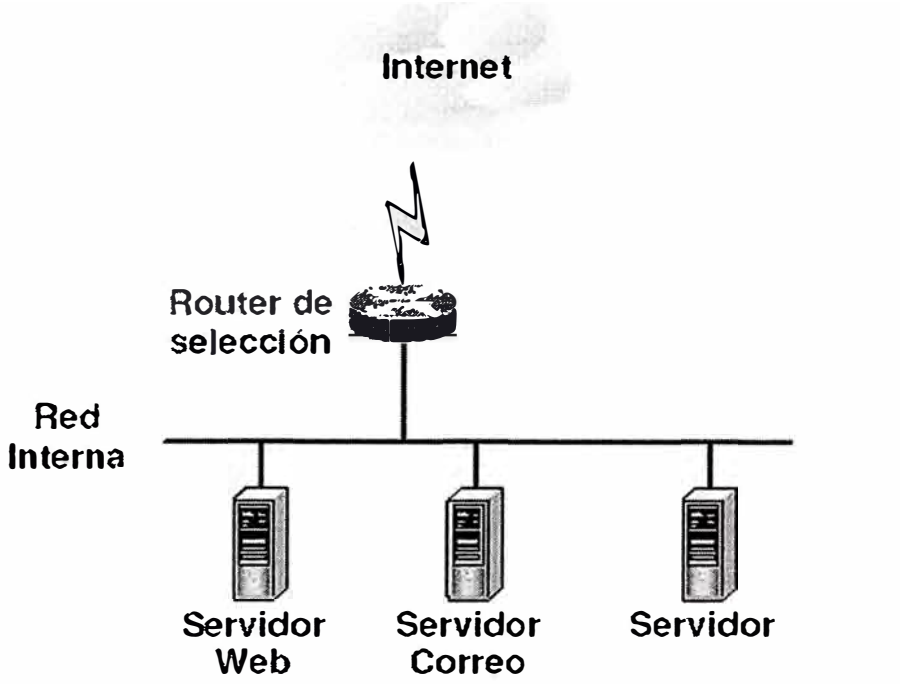


Figura 5.6 Ruteadores de Filtrado

Una zona de riesgo puede ser la parte de la red con capacidad TCP/IP a las que tiene acceso directo a través de Internet, no hay elementos de seguridad entre Internet y los hosts con protocolo TCP/IP. Esos hosts se vuelven vulnerables frente ataques y por consiguiente el resto. Que el protocolo de nuestra red sea diferente del de Internet no importa a la hora de seguridad. Un ruteador no puede eliminar la zona de riesgo pero si reducirla. El funcionamiento de esta arquitectura de seguridad, como parece lógico, es el que ya se citó al explicar los ruteadores de filtrado.

5.8.2 Host de Base Dual

Se trata de un cortafuegos implementado sin ruteador de filtrado, situando una computadora entre la red interna e Internet. El tráfico directo entre las redes es bloqueado. En este caso este host es un bastion host.

El administrador del cortafuegos puede decidir entre dos opciones a la hora de permitir el paso a través del host con dos interfaces de red. La primera sería permitir gateways a nivel de aplicación y la segunda permitir login remoto en el bastion host, para, desde allí acceder al resto de host. En el primer caso los usuarios pueden acceder a los servicios para los cuales hay instalado un gateway (siempre que las reglas de dicho gateway se lo permitan); en el segundo la seguridad es mucho menor.

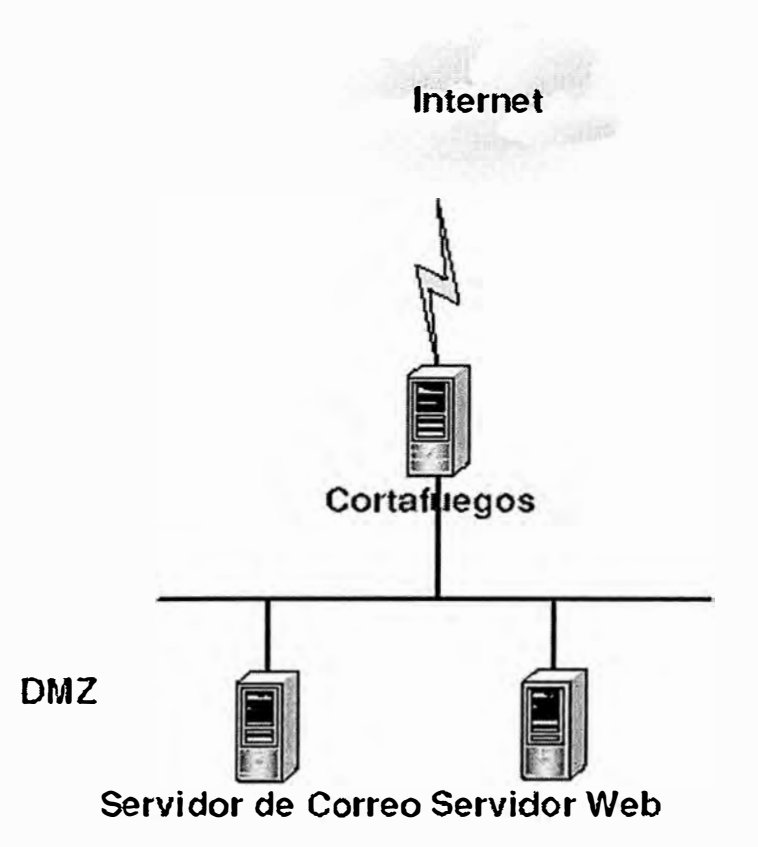


Figura 5.7 Host de Base Dual

La figura 5.7 muestra un host de base dual donde se ha instalado un gateway para el correo Internet:

Este tipo de arquitectura de cortafuegos tiene la ventaja, de que es más sencillo mantener logs, incluso remotos, de las acciones que van aconteciendo en el host. El

5.8.3 Screened Host Gateway

Esta es posiblemente una de las configuraciones más utilizadas, que se implementa utilizando un ruteador de selección y un host bastión. En la mayoría de los casos, el host bastión está en la red privada y el ruteador de selección es configurado de modo el host bastion sea el único alcanzable desde Internet. Normalmente, el ruteador de selección se configura para que parte del tráfico hacia el host bastión se bloquee en función del puerto o la dirección origen, permitiendo sólo que un pequeño número de servicios se comuniquen con él.

Si un atacante consigue hacer un login en el host bastión, tendría bastante fácil atacar el resto de la red (aun así esta implementación es más segura que las dos anteriores).

El host bastión utiliza funciones al nivel de aplicación para determinar si se permiten o se deniegan las solicitudes tanto entrantes como salientes. Para el tráfico saliente, los mensajes que pasan las reglas se envían al ruteador de selección.

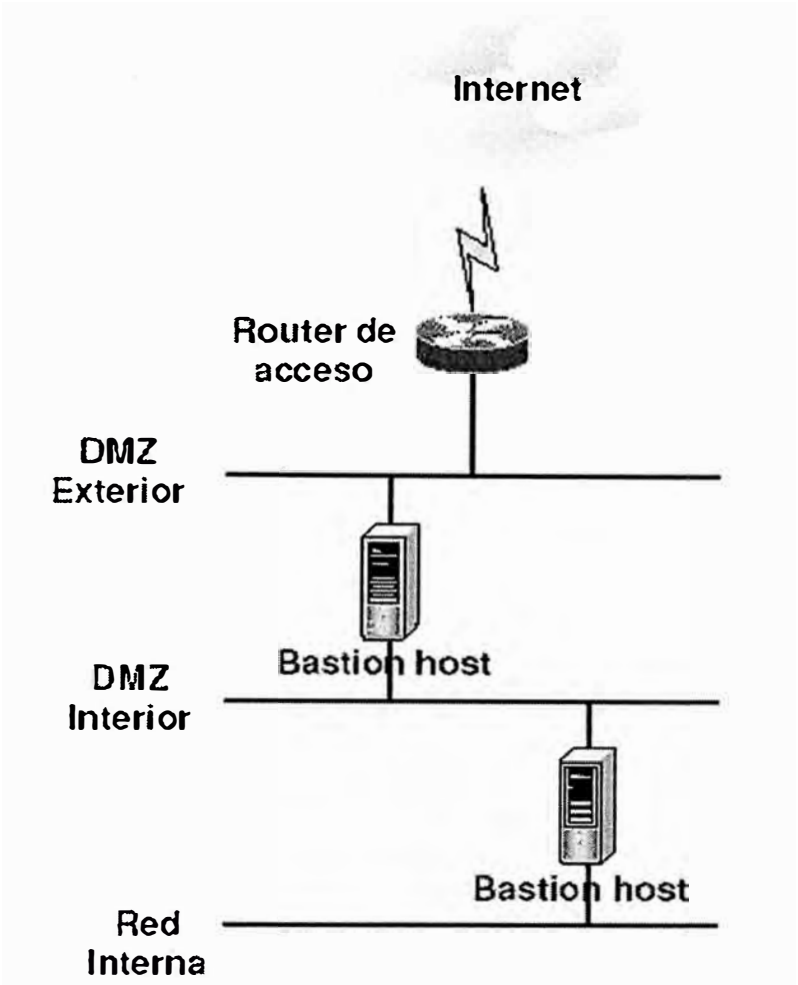


Figura 5.8 Arquitectura de Cortafuegos con uso de dos DMZs

Una posible modificación de esta arquitectura es la de usar un host bastión con ambas interfaces de red configuradas. El host conecta dos subredes, una de las cuales está entre el ruteador de selección y el host bastión.

La otra está detrás del host bastión, unida a él por su otra interfaz de red. Esto permite que en la subred que está entre el ruteador y el host bastión se coloquen ciertas máquinas que se quieren dejar accesibles y cuya seguridad no es importante (a esta subred se le suele llamar DMZ, que son las siglas de zona desmilitarizada). Este planteamiento puede extenderse a varios niveles de protección, por ejemplo en el caso de la figura 5.8

interior. La red privada proporciona un nivel de protección similar al del caso del host seleccionado. Una organización puede colocar parte de sus hosts en la red privada y mantener los más delicado detrás del host bastión inferior.

El ruteador de selección debe estar configurado para que envíe al host bastión interior todo el tráfico recibido por la red interna desde las redes externas. Antes de enviar el tráfico al host bastión, el ruteador aplicará sus reglas de selección.

Un intruso debe enfrentarse inicialmente al ruteador de selección. Si consigue entrar en él se tendrá que enfrentar al host bastión exterior.

Aunque las defensas en la red exterior tengan una brecha, el intruso deberá penetrar en el host bastión interior.

5.8.4 Subnet de Filtrado

En algunas configuraciones de cortafuegos, se crea una subred aislada, situada entre Internet y la red privada. Normalmente, esta red se aísla usando ruteadores de selección, con los que se pueden implementar varios niveles de filtrado. Generalmente, una subred seleccionada es configurada de forma Internet y la red privada tengan acceso a dicha subred, pero que el tráfico no puede fluir directamente entre las dos subredes.

Existen muchas configuraciones posibles de este tipo de cortafuegos, incluso con varios niveles de protección mediante la creación de varias screened subnet. En la mayoría de los casos se coloca el host bastión (o varios) en la screened subnet, permitiendo el acceso desde la red interna a Internet mediante gateways.

Si un cortafuegos de este tipo es atacado en un intento de destruirlo, el atacante tiene que reconfigurar el enrutamiento en las tres subredes, sin desconectarse o bloquearse, y sin que los cambios se pueden llegar a observar. Esto es posible pero muy difícil.

Si un cortafuegos de este tipo es atacado en un intento de destruirlo, el atacante tiene que reconfigurar el enrutamiento en las tres subredes, sin desconectarse o bloquearse, y sin que los cambios se pueden llegar a observar. Esto es posible pero muy difícil.

Trabajando con cortafuegos no es razonable decir que una aproximación es mejor que otra, debido a que hay muchos factores que determinarán el mejor cortafuegos para cada caso. El coste, la política corporativa, la tecnología de red existente, el personal, etc. Son algunas veces más importantes que otras consideraciones técnicas.

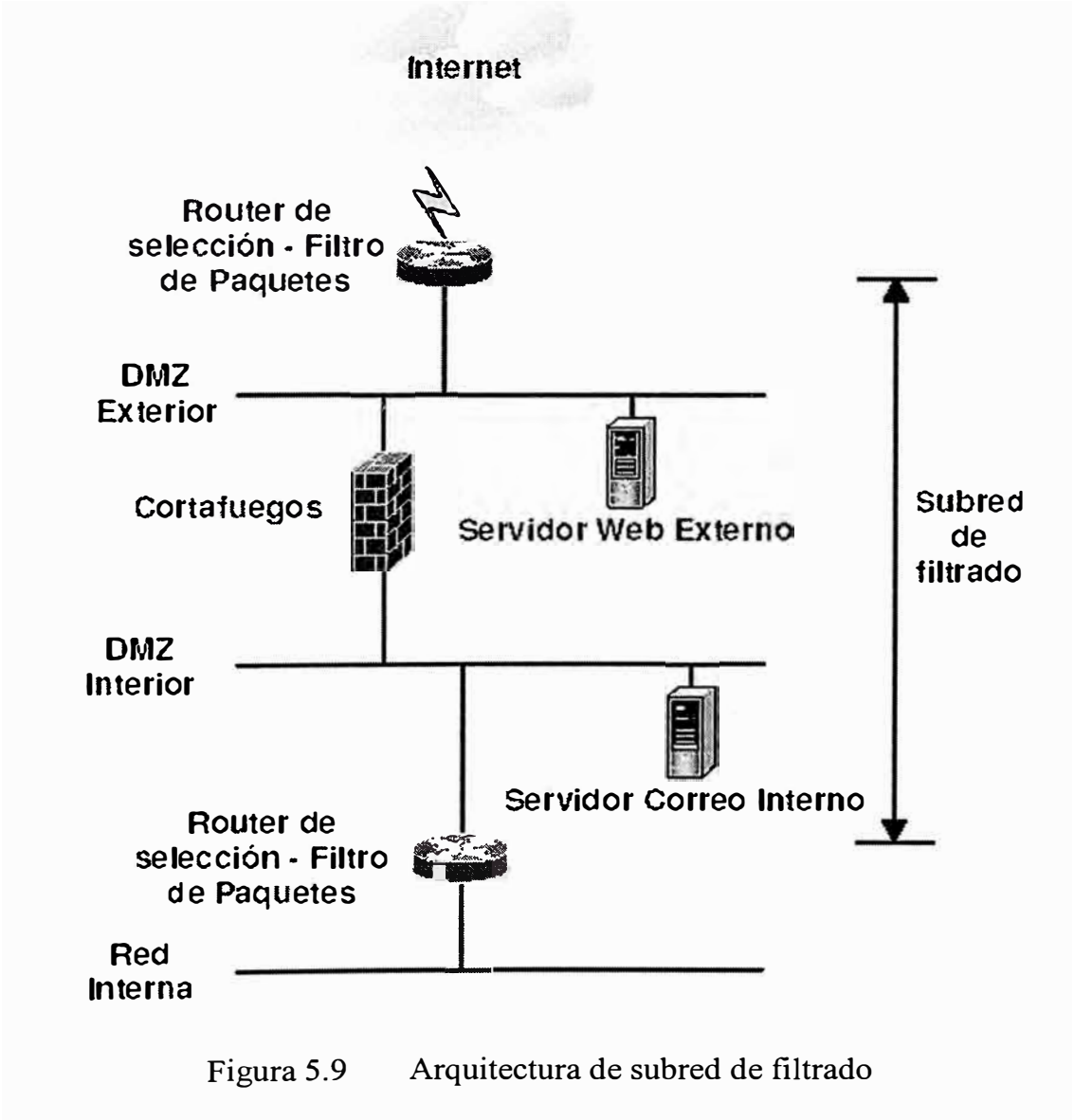


Figura 5.9 Arquitectura de subred de filtrado

CAPÍTULO VI

SISTEMAS DETECTORES DE INTRUSOS (IDSes)

6.1. INTRODUCCIÓN

Una intrusión es un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso; analizando esta definición, podemos darnos cuenta de que una intrusión no tiene por que consistir en un acceso no autorizado a una maquina: también puede ser una negación de servicio. A los sistemas utilizados para detectar las intrusiones o los intentos de intrusión se les denomina sistemas de detección de intrusiones (Intrusion Detection Systems, IDS) o, mas habitualmente y aunque no sea la traducción literal sistemas de detección de intrusos; cualquier mecanismo de seguridad con este propósito puede ser considerado un IDS, pero generalmente solo se aplica esta denominación a los sistemas automáticos de software o hardware que automatizan los procesos de monitoreo de eventos en una sistema de computadoras o red, analizando y buscando indicios de problemas de seguridad. Como los ataques a redes se han incrementado en numero y severidad en los últimos años, los sistemas de detección de intrusos han llegado a ser necesarios en la infraestructura de red de la mayoría de organizaciones.

6.2. CONCEPTOS DE IDSes

6.2.1 ¿Qué es detección de intrusos?

La detección de intrusión es el proceso de monitoreo de eventos que ocurren en un sistema de computadoras o una red, analizando y buscando señales de intrusión, definiendo como "intentos" de comprometer la confidencialidad, integridad, disponibilidad de los mecanismos de seguridad de una red. Las intrusiones son causadas por atacantes accediendo a nuestros sistemas desde Internet, usuarios autorizados de los sistemas que intentan ganar adicionales privilegios a los cuales no están autorizados, y usuarios autorizados quienes hacen mal uso de los privilegios que se le han confiado. Los IDSes son productos de software o hardware que automatizan este monitoreo y análisis de los procesos.

6.2.2 ¿Porqué debería usarse los IDSes?

La detección de intrusos permite a las organizaciones proteger sus sistemas de las amenazas que han llegado a incrementarse con la conectividad de redes y la uso masivo de los sistemas de información. Dado el nivel y la naturaleza de las modernas amenazas a redes, la pregunta para los profesionales de seguridad no debería ser ¿Cuando usar un detector de intrusos? Sino más bien ¿Cuales características se deben usar de un detector de intrusos?.

Los IDSes han ganado aceptación como elementos adicionales dentro de la infraestructura de seguridad de cada organización. A pesar de las contribuciones que los IDSes hacen a los sistemas de seguridad, en muchas organizaciones aun deben justificar la adquisición de los IDSes. Existen varias razones por las que se deben adquirir y usar un IDSes:

· Para prevenir los problemas futuros después del descubrimiento de riesgos y vulnerabilidades, penalizando a quienes podrían atacar y abusar del sistema en riesgo,

· Para detectar ataques y otras violaciones a la seguridad que no son prevenidos por otros elementos de control,

· Para detectar los preámbulos de ataques y como tratarlos (actividades sospechosas),

· Para documentar las amenazas existentes en una organización.

· Para actuar como control de calidad del diseño y administración de la seguridad, especialmente en empresas grandes y complejas.

· Para proveer de información útil acerca de las intrusiones que se presenten, permitiendo el diagnóstico oportuno, recuperación y corrección de las causas.

6.3. TIPOS DE IDSes

Existe diferentes tipos de IDSes disponibles en el mercado hoy en día, que se caracterizan por diferentes tipos de monitoreo y análisis. Cada tipo tiene distintas ventajas y desventajas. Aunque, todos pueden ser descritos en términos del modelo de proceso de los IDSes.

6.3.1 Modelo de Proceso para Detección de Intrusos

Muchos IDSes pueden ser descritos en términos de tres componentes fundamentales:

1) Fuentes de Información, las diferentes Fuentes de los eventos usados para determinar cuando una intrusión ha sido realizada. Estas fuentes pueden ser graficadas desde diferentes niveles de un sistema, siendo los más comunes: red, maquina y monitoreo por aplicación.

2) Análisis, es la parte de un sistema de detección de intrusión que constantemente organiza y revisa los eventos derivados de las Fuentes de información, decidiendo cuando esos eventos indican que una intrusión esta ocurriendo o ha sido realizada. Los más comunes son detección de usos indebidos y detección de anomalías.

3) Respuesta, es el conjunto de acciones que un sistema toma una vez que detecta una intrusión. Estos comúnmente se agrupan en activos y pasivos, los activos toman acciones automáticas en una parte del sistema, y los pasivos reportan los resultados a las personas, quienes están a la expectativa para tomar acción basado en dichos reportes.

6.3.2 Clasificación de IDSes

En base al modelo del proceso de los sistemas de detección de intrusión se pueden clasificar por:

1) Fuente de Información, la forma más común de clasificar los IDSes en agruparlos por la fuente de información. Asi se tiene:

· IDSes basados en red. que analizan paquetes de la red, capturándolos en los backbones de red o segmentos de red LAN, para encontrar intrusos.

· IDSes basados en máquina, analizan las fuentes de información generadas por el sistema operativo buscando señales de intrusión.

· IDSes basados en aplicación, analizan las fuentes de información generadas por una aplicación de software buscando señales de intrusión.

2) Análisis del IDS, existe dos principales formas de analizar los eventos para la detección e ataques: detección de usos indebidos y detección de anomalías.

· Detección de usos indebidos, en el cual el análisis se basa en conocer lo anormal para poder detectarlo (conocer lo "negativo"), es la técnica usada por la mayoría de los sistemas comerciales.

· Detección de anomalías, en el cual el análisis busca los patrones anormales de actividad, ha sido, y continua siéndolo, tema de una gran investigación. La detección de anomalías es usada en forma limitada por algunos IDSes.

3) Opciones de Respuesta del IDS, Una vez que los IDSes han obtenido la información del evento y lo analiza para encontrar síntomas de ataques, estos finalmente generan respuestas. Algunas de estas respuestas generan reportes de lo encontrado en una ubicación predefinida por el usuario. Otras involucran respuestas activas y automatizadas. Actualmente los IDSes comerciales soportan un amplio rango de opciones de respuesta, a menudo categorizadas en respuestas activas, pasivas o una mixtura de los dos.

6.4. IDSes BASADOS EN RED

La mayoría de los sistemas comerciales de detección de intrusión están basados en red. Estos IDSes detectan ataques capturando y analizando paquetes en la red. Escuchando un segmento de red o un switch, un IDS basado en red puede monitorear el tráfico cursado por múltiples hosts que estén conectados a dicho segmento de red, a menudo un IDS basado en red consiste de un conjunto de sensores de propósito único o varios hosts ubicados en diferentes punto en la red. Estas unidades monitorean el tráfico de red, realizando el análisis local de ese tráfico y reportando los ataques a la consola central de administración. Como los sensores son dedicados para este propósito, estos pueden ser fácilmente protegidos ante un ataque. Muchos

de los sensores están diseñados para actuar en modo "oculto", con el objeto de hacer más difícil que un atacante determine su presencia y localización.

1) Ventajas de un IDS basado en red.

· Unos pocos IDSes bien ubicado pueden monitorear una red grande.

· La implementación de IDSes basados en red tiene poco impacto sobre la red existente. Los IDSes basados en red usualmente son dispositivos pasivos que "escuchan" el tráfico en la red sin interferir con la normal operación de la red. Así, es más fácil reestructurar la red para incluir IDSes basados en red con el mínimo esfuerzo.

· Los IDSes basados en red pueden ser muy seguros ante un ataque e incluso son invisibles a muchos atacantes.

2) Desventajas de los IDSes basados en red:

· Los IDes basados en red tiene la dificultad de procesar todos los paquetes en una red grande y congestionada, por consiguiente, pueden fallar en reconocer un ataque realizado durante periodos de alto tráfico. Algunos fabricantes están intentando resolver este problema implementando IDSes completamente en hardware, los cuales son mucho más rápidos. La necesidad de analizar los paquetes mas rápidamente también fuerza a los fabricantes a detectar pocos ataques y con poco recursos de computo, los cuales pueden reducir la efectividad de la detección..

· Muchas de las ventajas de los IDSes basados en red no aplican en modernas redes basadas en switches. Los switches subdividen la red en varios segmentos más pequeños y proveen enlaces dedicados entre los hosts ubicados en el mismo switch. Algunos switches no proveen puertos de monitoreo universal y esto limita el rango de monitoreo de los IDSes basados en red a un único host. Incluso cuando los

switches proveen tales puertos de monitoreo, a menudo el único Puerto no puede reflejar todo el tráfico cursado en el switch.

· Los IDSes basados en red no pueden analizar información encriptada. Este problema esta incrementándose en mas organizaciones debido al uso de redes privadas virtuales.

· La mayoría de IDSes basados en red no pueden mostrar si un ataque fue exitoso o no; solo pueden discernir que el ataque fue iniciado. Esto significa que después que un IDS basado en red detecta un ataque, los administradores deben manualmente investigar cada equipo atacado para determinar si verdaderamente fue vulnerado.

· Algunos IDSes basados en red tienen problemas con ataques de red distribuidos que contempla fragmentación de paquetes. Estos paquetes mal formados causan que el IDS llegue a ser inestable y colapse.

6.5. IDSes BASADOS EN MAQUINA

Los IDSes basados en maquina operan con información recolectada en una computadora de forma individual. Esta ventaja permite a los IDSes basados en maquina analizar las actividades con una gran confiabilidad y precisión, determinando exactamente cual proceso y usuario están involucrados en un ataque en particular sobre el sistema operativo. Además, a diferencia de los IDSes basados en red, los IDSes basados en maquina pueden "ver" el resultado de un intento de ataque, debido a que ellos pueden directamente acceder y monitorear archivos de datos y procesos del sistema que fueron afectados.

Los IDSes basados en maquina normalmente utilizan fuentes de información de dos tipos, la configuración de auditoria del sistema operativo y los archivos log del sistema. Los parámetros de auditoria son usualmente generados en el "corazón" del

sistema operativo (kernel), en donde existe mas información mas detallada y están mas protegidos que los archivos log del sistema. Aunque, los archivos log del sistema sean más fáciles de comprender.

Los IDSes basados en maquina están diseñados para soportar una administración centralizada que permiten desde una única consola de administración monitorear varios hosts.

1) Ventajas:

· Debido a que los IDSes basados en maquina monitorean eventos locales de una maquina, pueden detectar ataques que no pueden ser detectados por un IDS basado en red.

· Los IDSes basados en maquina pueden operar en un ambiente en el cual haya tráfico de red encriptado, donde las fuentes de información son generadas antes que la información sea encriptada y/o después que la información sea desencriptada en la maquina destino

· Los IDSes basados en maquina no son afectados por la segmentación de la red.

· Cuando los IDSes basados en maquina operan con los parámetros de auditoria del sistema operativo, pueden ayudar a detectar "troyanos" o otros ataques que involucran a la integridad del software. Estos aparecen como inconsistencias en el proceso de ejecución.

2) Desventajas:

· Los IDSes basados en maquina son difíciles de administrar, debido a que la fuente de información debe ser configurada en cada maquina a ser monitoreada.

· Debido a que las fuentes de información de un IDS basado en maquina residen en localmente, el IDS puede ser atacado y deshabilitado como parte de un ataque.

· Los IDSes basados en maquina pueden ser deshabilitados por ciertos ataques de denegación de servicios.

· Debido a que los IDSes basados en maquina tienen como fuente de información a los parámetros de auditoria del sistema, la cantidad de información puede ser inmensa, requiriendo un dispositivo de almacenamiento adicional.

· Los IDSes basados en maquina usan recursos de computo de las maquinas que son monitoreadas, por lo tanto pueden afectar el rendimiento de la maquina.

6.6. IDSes BASADOS EN APLICACIÓN

Los IDSes basados en aplicación son un subconjunto especial de los IDSes basados en maquina que analizan los eventos de una determinada aplicación de software. La más común fuente de información usado por este tipo de IDS son los archivos log de transacciones de la aplicación.

Con la facilidad para interactuar directamente con la aplicación y el pleno conocimiento de esta en el motor de análisis, permite a los IDSes basados en aplicación detectar comportamientos sospechosos de usuarios autorizados excediendo su autorización. Esto es porque tales problemas son probables de suceder en la interacción entre el usuario, la información y la aplicación.

1) Ventajas:

· Los IDSes basados en aplicación pueden monitorear la interacción entre el usuario y la aplicación, el cual a menudo permite el monitoreo de la actividad no autorizada de usuarios de forma individual.

· Los IDSes basados en aplicación pueden a menudo trabajar en ambientes encriptados, debido a que ellos pueden interactuar con aplicación hasta el final de la

transacción, donde la información es presentada de forma desencriptada a los usuarios.

2) Desventajas:

· Los IDSes basados en aplicación pueden ser más vulnerable que los IDSes basados en maquina ante ataques a los archivos log de las aplicaciones que no son bien protegidos por el sistema operativo.

· Como los IDSes basados en aplicación a menudo monitorean eventos a nivel de usuario, usualmente estos no pueden detectar un ataque de "troyanos" o otros tal como el ataque con código malicioso insertado intencionalmente. Por lo tanto, es recomendable el uso de un IDS basado en aplicación en combinación con uno basado en maquina y/o un IDS basado en red.

6.7. DETECCIÓN DE USOS INDEBIDOS

Los detectores de usos indebidos analizan la actividad del sistema, buscando eventos o conjunto de eventos que concuerdan con patrones predefinidos de eventos que describen un ataque "conocido". Como los patrones corresponden a ataques "conocidos" son denominados "firmas", la detección de usos indebidos algunas veces es denominado "detección basado en firmas". La forma más común de detección de usos indebidos usado en productos comerciales especifica cada patrón de eventos correspondientes a un ataque como una "firma" por separado. Aunque, existe mas formas sofisticadas para la detección de usos indebidos (denominado técnicas de análisis "basado en el estado") que pueden descubrir una única "firma" para detectar un grupo de ataques.

1) Ventajas:

· Los detectores de usos indebidos son muy efectivos para detectar ataques sin generar un numero excesivo de falsas alarmas.

· Los detectores de usos indebidos pueden rápidamente y de forma confiable diagnosticar el uso de una herramienta de ataque especifico o la técnica que se esta usando. Esto puede ayudar a los administradores de seguridad a priorizar acciones correctivas.

· Los detectores de usos indebidos pueden permitir a los administradores del sistema, sin importar el nivel de especialización en seguridad, el rastreo de los problemas de seguridad de sus sistemas, iniciando los procedimientos para el manejo de estos incidentes.

2) Desventajas:

· Los detectores de usos indebidos pueden solo detectar aquellos ataques que son conocidos por lo tanto estos deben ser constantemente actualizados con nuevas "firmas" de nuevos ataques.

· Muchos detectores de usos indebidos son diseñados para usar patrones predefinidos que previenen la detección de variantes de los ataques comunes. Los detectores de usos indebidos basados en estados pueden superar esta limitación, pero no son comúnmente usados en los IDSes comerciales.

6.8. DETECCIÓN DE ANOMALIAS

Los detectores de anomalías identifican el comportamiento anormal e inusual de una maquina o red. Estos detectores funcionan asumiendo que los ataques son diferentes de una actividad "normal" (legitima) y pueden por lo tanto ser detectados por los sistemas que identifican esas diferencias. Los detectores de anomalías construyen

perfiles que representan el comportamiento normal de los usuarios, maquinas y conexiones de red. Estos perfiles son construidos de información histórica recolectada en un periodo de operación normal. Los detectores luego recolectan información de eventos y usa una variedad de mediciones para determinar cuando dichas actividades se desvían de lo normal.

Estas mediciones y técnicas usadas en la detección de anomalías incluyen:

· Detección en función de "limites", en el cual ciertos atributos del comportamiento de un usuario o sistema son expresados en términos de contadores, con algún nivel establecido o permisible. Tales atributos de comportamientos pueden incluir el numero de archivos accedidos por un usuario en un periodo de tiempo dado, el numero de intentos fallidos para logearse en el sistema, la cantidad de CPU utilizada por un proceso, etc. Este nivel puede ser estático o heurístico (por ejemplo, diseñado para cambiar con los actuales valores observados después de un tiempo)

· Mediciones estadísticas, ya sea parametrizadas, donde se asume que la distribución de los atributos del perfil encajan en un patrón particular, y no parametrizadas, donde la distribución de los atributos del perfil es "aprendido" de un conjunto de valores históricos, observados en un tiempo determinado.

· Mediciones basadas en reglas, los cuales son similares a las mediciones estadísticas no parametrizadas en la que la información observada define el uso de los patrones de forma aceptable, pero difiere en que esos patrones son especificadas como reglas, no cantidades numéricas

Solo las dos primeras mediciones son usadas actualmente por los IDSes comerciales.

Desafortunadamente, los detectores de anomalías y los IDSes basados en ellos a menudo producen una gran cantidad de falsas alarmas, así como los patrones

normales de los usuarios y el comportamiento de los sistemas pueden variar mucho. A pesar de esta limitación, los investigadores afirman que los IDSes basados en detección de anomalías son capaces de detectar nuevas formas de ataques, de forma distinta a los IDSes basados en firmas que hacen relaciona con los patrones de ataques pasados.

Además, algunas formas de detección de anomalías producen salidas que pueden usarse nuevamente como fuentes de información para los detectores de usos indebidos. Por ejemplo, un detector de anomalías basados en "!imites" puede generar una configuración representando el numero "normal" de archivos que son accedidos por un usuario en particular; el detector de usos indebidos puede usar esta configuración como parte de una detección e "firmas" que dice: "si el numero de archivos accedidos por este usuarios excede esta configuración "normal" en un diez por ciento, entonces emita una alarma."

Aunque algunos IDSes comerciales incluyen limitadas formas de detección de anomalías, realmente pocos confían en esta tecnología. La detección de anomalías que existe en sistemas comerciales usualmente trabaja en función de detección de red o escaneo de puertos. Sin embargo, la detección de anomalías se mantiene como un área de investigación de detección de intrusos en forma activa y puede jugar un papel importante en el futuro de los IDSes.

1) Ventajas:

· Los IDSes basados en detección de anomalías detecta comportamientos inusuales y así tiene la habilidad de detectar síntomas de ataques sin tener el "conocimiento" especifico de los detalles.

· Los detectores de anomalías pueden producir información que pueden se usados para definir las "firmas" para los detectores de usos indebidos.

2) Desventajas:

· La detección de anomalías usualmente produce un gran numero de falsas alarmas debido a los comportamientos impredecibles de los usuarios y las redes.

· La detección de anomalías a menudo requiere extensas "sesiones de entrenamiento" para grabar los eventos del sistema con el objeto de caracterizar los patrones de comportamiento normal.

6.9. IMPLEMENTACIÓN DE IDSes

La tecnología de detección de intrusos es importante y necesaria en la infraestructura de seguridad de una red empresarial. Aunque, debido a las deficiencias de los productos de detección de intrusos, y el limitado nivel de entrenamiento en seguridad de muchos de los administradores de la red, una implementación efectiva de IDSes requiere una cuidadosa planificación, preparación, investigación, y adecuada entrenamiento especializado.

Se sugiere realizar un análisis de los requerimientos, selección cuidadosa de la estrategia de detección de intrusión y una solución que sea compatible con la infraestructura de red de la organización, las políticas y el nivel de recursos económicos.

6.9.1 Estrategia para la implementación de los IDSes

Las empresas deberían considerar una implementación de IDSes por fases para permitir que el personal gane experiencia y para determinar cuantos recursos son necesarios para el monitoreo y mantenimiento. Los requerimientos de recursos para cada tipo de IDSes varían ampliamente, dependiendo de la organización. Los IDSes

requieren adecuada preparación e interacción de las personas. Las organizaciones deben tener una apropiada política de seguridad, planes, y procedimientos para disponer de un personal con el conocimiento necesario para gestionar la gran variedad de alarmas generadas por los IDSes.

Se recomienda la combinación de los IDSes basados en red y los IDSes basados en maquina para proteger la red en su conjunto. Se recomienda que la implementación sea por fases, iniciando con los IDSes basados en red que por lo general son simples de instalar y mantener. Luego, proteger los servidores críticos con los IDSes basados en maquina. Utilizar productos de análisis de vulnerabilidades con un periodo de tiempo para probar los IDSes y otros mecanismos de seguridad con la finalidad de que estén adecuadamente configurados y operativos.

6.9.2 Implementación de IDSes basados en red

La pregunta fundamental cuando se implementa los IDSes basados en red es donde localizar los sensores. Existen muchas opciones para ubicar los IDSes basados en red con diferentes desventajas asociadas en cada ubicación:

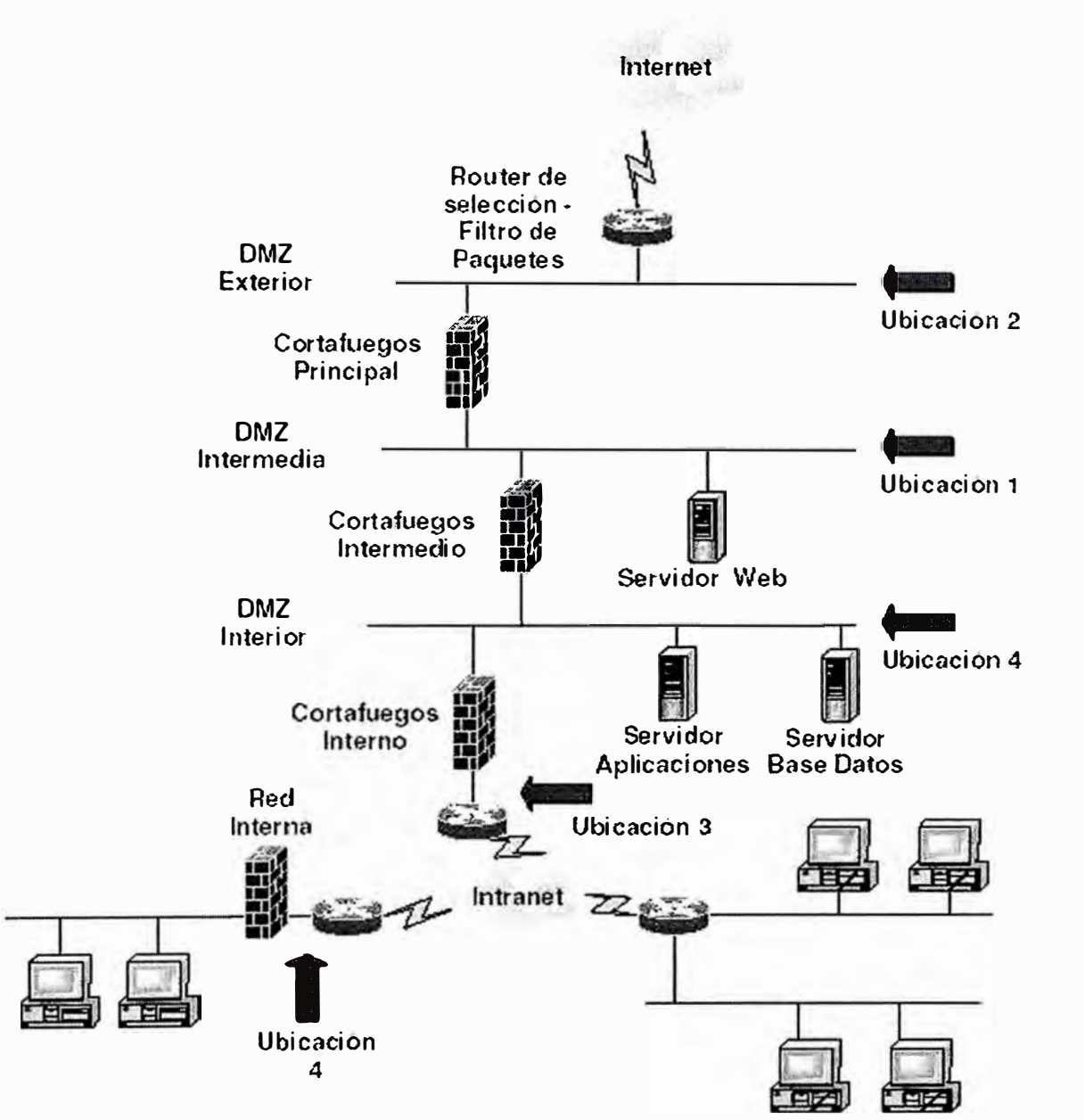


Figura 6.1 Implementación de IDSes basados en red

1) Detrás de cada cortafuegos, en una DMZ

Ver figura 6.1

· Ventajas:

- Monitorea ataques originados desde fuera de la red, que penetrar las defensas perimétricas de la red.

- Detecta problemas con la política o rendimiento del cortafuegos.

- Monitorea los ataques que pueden tener como objetivo a un servidor web o ftp, los cuales comúnmente residen en esta DMZ.

- Si un ataque entrante no es reconocido, los IDSes pueden algunas veces reconocer el tráfico saliente del servidor afectado.

2) Externo al cortafuegos

(Ver Figura 6.1 – Ubicación 2)

· Ventajas:

- Monitorea y genera estadísticas del numero y tipos de ataques originados desde Internet y que tienen como objetivo la red.

3) En el backbone de la red

(Ver Figura 6.1 – Ubicación 3)

· Ventajas:

- Monitorea una gran cantidad de tráfico, aumentando así la posibilidad de detectar los ataques.

- Detecta actividad no autorizada de usuarios dentro de la organización.

4) En sub-redes criticas

(Ver Figura 6.1 – Ubicación 4)

· Ventajas:

- Detecta ataques a sistemas y recursos críticos de la empresa.

- Permite enfocar los recursos a los que son considerados de gran valor.

6.9.3 Implementación de IDSes basados en maquina

Una vez que los IDSes basados en red están ubicados y operando, la adición de los IDSes basados en maquina pueden ofrecer mejores niveles de protección de los sistemas. Sin embargo, la instalación de los IDSes basados en maquina en cada uno

de los servidores de la empresa puede tomar demasiado tiempo, así como la configuración y sintonización en cada servidor especifico.

Por lo tanto es recomendable primero la instalación de los IDSes basados en maquina en los servidores críticos. Así disminuirá los costos de implementación y permitirá que el personal se enfoque en las alarmas generadas por estos servidores importantes. Una vez que la operación de los IDSes basados en maquina es rutina, las organizaciones concientes de la seguridad pueden considerar la instalación de los IDSes en la mayoría de sus servidores. En el caso de adquirir sistemas de IDSes que tienen administración y funciones de reportes centralizada. Estas pueden reducir significativamente la complejidad de la gestión de las alertas de un gran conjunto de servidores.

Otra consideración cuando se usa IDSes basados en maquina es que los operadores deben familiarizarse con el comportamiento de los IDSes en un ambiente de red activa. Mucha de la efectividad de cualquier IDS, pero particularmente de los IDSes basados en maquina depende de la habilidad del operador para discernir entre las alarmas verdades y falsas. En un periodo de tiempo, un operador, trabajando con los IDSes puede adquirir la capacidad de discernir cual es comportamiento normal de la red que es monitoreada por el IDS.

Es importante establecer periodos de revisión de los resultados de los IDSes. Si no se realiza, se incrementara el riesgo de que un atacante juegue con el IDS en el curso de un ataque.

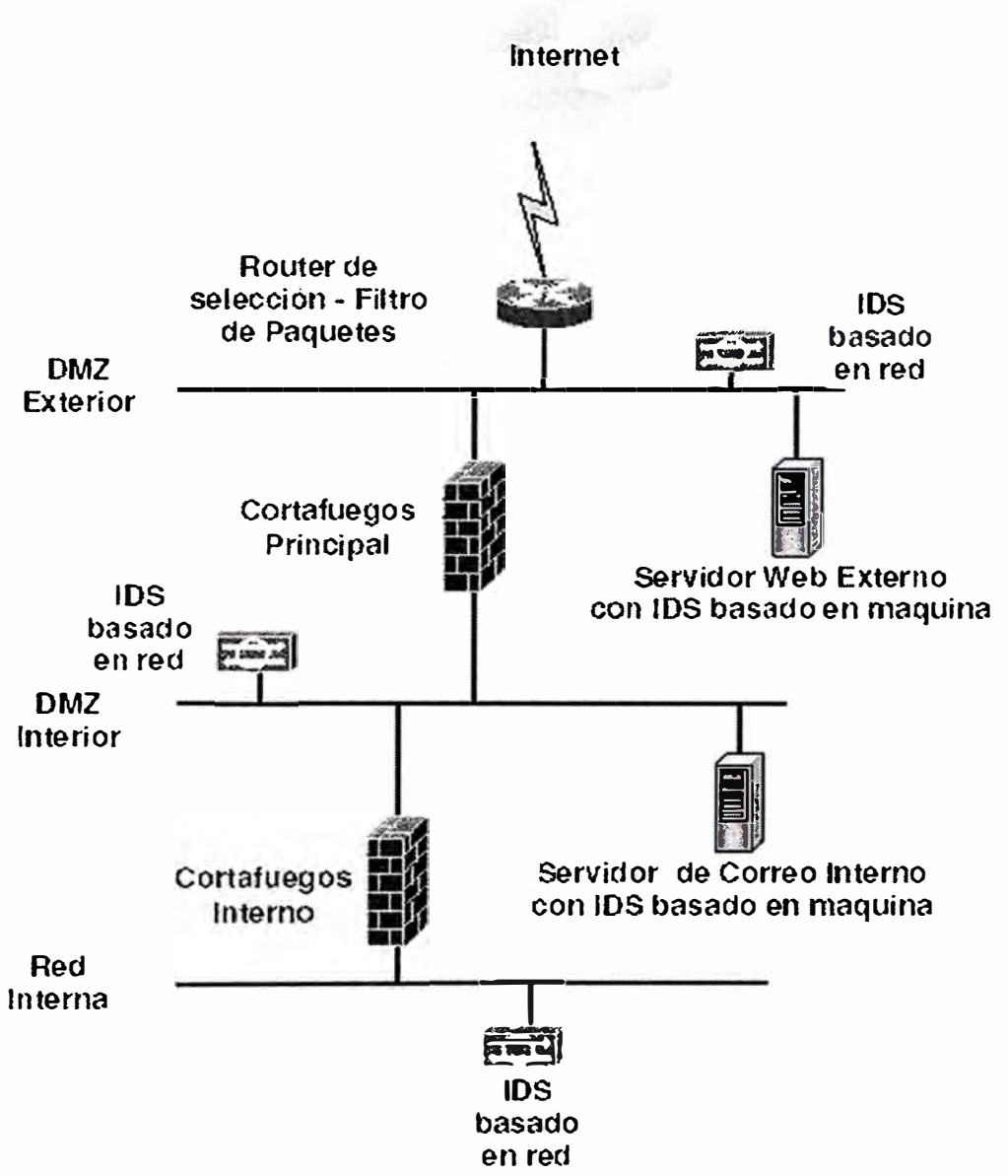


Figura 6.2 Implementación de IDSes basados en maquina

6.9.4 Estrategia de Alarmas

La mayor parte de los IDSes tienen características de alarmas configurables entre ellas: mensajes de correo, mensajes de beeper, envío de "traps" SNMP, y otros que ejecutan acciones de bloqueo automatizadas (ejemplo reconfiguración del cortafuegos en caso de un ataque).

CAPÍTULO VII

INFRAESTRUCTURA DE CLAVE PUBLICA

7.1. INTRODUCCIÓN

La simple existencia de una red de área local extendida a lo largo de un edificio conlleva un notable conjunto de riesgos para la seguridad de la información que por ella circula o que está almacenada en las computadoras a ella conectados. Cuando estos sistemas y redes locales están conectados, a su vez, a redes de ámbito nacional o internacional, el problema se agudiza. Últimamente venimos asistiendo a un crecimiento espectacular del número de usuarios de todo tipo y condición, que se conectan a la red Internet. A raíz de la interconexión del mundo empresarial a esta red, viaja por ella y se almacena información de todo tipo, que abarca desde noticias, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones que requieren amplias medidas de seguridad. La escucha electrónica, que permite la obtención y posible manipulación de información privada, y los sabotajes realizados tanto por atacantes externos como internos, están causando últimamente la pérdida de grandes cantidades de dinero.

Los organismos de normalización proponen una serie de soluciones para evitar los posibles ataques y operaciones ilegales a los que pueden estar sometidas las redes de

telecomunicaciones. Estas soluciones consisten en dotar a las redes de una serie de servicios de seguridad que utilizan en su mayoría técnicas criptográficas como herramienta básica. El objetivo de la criptografía es el de proporcionar comunicaciones seguras sobre canales inseguros, es decir, permitir que dos entidades, bien sean personas o bien aplicaciones, puedan enviarse mensajes por un canal que puede ser interceptado por una tercera entidad, de modo que sólo los destinatarios autorizados puedan leer los mensajes. Pero la criptografía no es en sí la Seguridad, sólo es la herramienta básica que utilizan mecanismos más complejos para proporcionar, además de confidencialidad, otros servicios de seguridad.

La criptografía viene utilizándose desde la Antigüedad, aunque solamente con el concurso de las computadoras han surgido los modernos sistemas criptográficos. Entre este tipo de criptosistemas hay que distinguir entre los de Clave Secreta, en los que el emisor y el receptor de un mensaje utilizan la misma clave para cifrar y descifrar respectivamente el mensaje, la cual deben mantener ambos en secreto, y los de Clave Pública en los que cada usuario está en posesión de un par de claves, una que mantiene en secreto y otra que es pública.

El criptosistema de clave secreta más utilizado es el "Estándar de Encriptación de Datos" (Data Encryption Standard - DES) desarrollado por IBM y adoptado por las oficinas gubernamentales estadounidenses para protección de datos desde 1977. El algoritmo es fácil de implementar tanto en hardware como en software, sin embargo, presenta un grave problema respecto a la gestión de claves. Por un lado, existe un problema con la distribución de claves, ya que si dos usuarios quieren comunicarse confidencialmente, deberán seleccionar una clave secreta que sólo ellos conozcan y comunicársela uno al otro, con el claro riesgo de ser interceptada. Por otra parte,

aparece el problema de manejo de claves cuando el número de usuarios involucrados en la comunicación es grande, ya que en una red de n usuarios, cada pareja necesita tener su clave secreta particular, lo que hace un total de 2n(n-1) claves para esa red.

En 1976 Diffie y Hellman describieron el primer criptosistema de clave pública conocido como el cambio de clave Diffie-Hellman que utilizaba una clave doble compuesta por una componente pública y una privada. Con este algoritmo cuando alguien quiere que le envíen un mensaje secreto le envía a su interlocutor su clave pública, el cual la usa para cifrar el mensaje. Sólo el usuario que está en posesión de la clave secreta puede descifrar el mensaje. Si el mensaje es interceptado, aunque el intruso conozca la clave pública utilizada, no podrá descifrar el mensaje porque no estará en posesión de la componente privada. Con este tipo de algoritmos la clave secreta ya no tiene que transmitirse entre los interlocutores y tampoco es necesario tener claves diferentes para cada pareja de interlocutores, es suficiente con que cada usuario tenga su clave pública y su clave privada.

La primera realización robusta del modelo propuesto por Diffie- Hellman fue desarrollada por Rivest, Shamir y Adleman en 1977 y se conoce como criptosistema RSA. La clave pública y la privada están compuestas por un exponente y un módulo que es producto de dos número primos grandes. La fiabilidad del sistema se basa en que si los primos se escogen lo suficientemente grandes, el proceso de factorización del producto es inabordable en un tiempo razonable. Gracias a ello, la difusión de la componente pública no pone en peligro a la privada. El algoritmo de cifrado RSA es reversible, es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la pública. Este último modo de cifrado no proporciona confidencialidad ya que cualquiera puede descifrar

un mensaje cifrado con una clave secreta al poder obtener siempre la componente pública de su interlocutor, sin embargo el hecho de cifrar un mensaje con la clave secreta de un usuario implica una identificación del usuario al igual que lo hace una firma, por lo que este proceso se conoce con el nombre de firma digital.

A partir de mediados de los 80 se empezaron a buscar nuevos criptosistemas de clave pública que utilizaran menos cantidad de recursos para generar claves y para cifrar y descifrar. Así, en 1985, El Gamal propuso un esquema de clave pública conocido como criptosistema El Gamal, y en la primera mitad de los 90 está progresando el estudio de criptosistemas de curvas elípticas.

La criptografía por sí sola no es suficiente para prevenir los posibles ataques que se perpetran sobre las redes, sino que es necesario establecer unos mecanismos más complejos que utilizan los distintos sistemas criptográficos en sus cimientos. Cuando se utiliza únicamente criptografía de clave simétrica, aunque el sistema de generación de claves suele ser sencillo, ya que no se requiere una gran infraestructura para soportarlo, los mecanismos de distribución de las claves suelen ser muy complejos. En este caso, los principales parámetros que hay que tener en cuenta son el modo de difundir la clave secreta de forma segura a las entidades que van a utilizarla y la frecuencia con la que se deben renovar las claves para evitar que sean desveladas.

En los criptosistemas de clave pública, la clave secreta debe permanecer oculta en el dominio de su propietario, por lo cual el peligro de ser interceptada por un atacante se reduce. Sin embargo, la clave pública puede ser extensamente conocida. La necesidad que tienen las entidades de dar a conocer sus claves públicas plantea nuevos problemas.

En primer lugar, se deben buscar mecanismos para publicar estas claves. Inicialmente se pensó en el Directorio como el lugar ideal para su publicación, pero su poca expansión ha hecho que ya se empiece a hablar de la utilización de servidores accesibles vía e-mail y de servidores web que se encarguen de esta labor.

El segundo problema que se plantea al utilizar criptosistemas de clave pública, es que las claves públicas, por el simple hecho de ser públicas, están expuestas a la manipulación por parte de todos los usuarios, por lo que es necesario buscar un mecanismo que garantice la propiedad y la validez de estas claves. Siguiendo el ejemplo de los actuales sistemas legales, se utiliza un sistema de confianza en una tercera parte (TTP, Trusted Third Party) que se encarga de certificar las claves públicas. Esta TTP, conocida con el nombre de Autoridad de Certificación (CA, Certification Authority), certifica que una determinada entidad es la propietaria de una clave pública y que esa clave es válida durante un periodo determinado de tiempo.

7.2. CRIPTOGRAFÍA DE CLAVE PÚBLICA Y FIRMA DIGITAL

7.2.1 Firma Digital

La firma digital se basa en técnicas criptográficas que permiten emular digitalmente la firma manuscrita, con la misma validez legal.

Características:

· Se emplean algoritmos criptográficos asimétricos.

· Se genera a través de una clave que posee únicamente el firmante.

· Depende del documento que se firma.

· Permite asegurar la integridad y el no repudio de los documentos firmados.

La firma digital sirve, por ejemplo en el caso del correo, para asegurarnos que el remitente de un correo es realmente quien aparece en el campo "de" (from en ingles) del mensaje, es decir, para evitar que se envíen correos en nombre de otras personas.

La firma debe cumplir los siguientes requisitos:

· La firma de un usuario sólo puede ser generada por ese usuario.

· Se genera a través de la clave privada.

· Puede ser verificada por cualquiera que conozca la clave pública.

· Debe ser distinta para documento firmado

· Se debe basar en el contenido del documento.

· No se puede falsificar una firma a partir de la firma de otro documento

La base: Cifrado de Clave pública

· Cada usuario posee un par de claves, una es privada y sólo conoce él (clave privada), otra es pública y puede distribuirse a las personas con las que intercambia información (clave pública).

· La información encriptada con una clave, puede ser desencriptada con la otra, siendo posible:

- Desencriptar una información conociendo sólo la clave con la que se encriptó.

- Averiguar el valor de una clave conociendo la otra.

7.2.2 Cifrado de Clave Pública

1) Encriptación con clave privada

Cualquier persona que conozca la clave pública puede desencriptar, pero se asegura que solo el poseedor de la clave privada ha podido generar el documento encriptado.

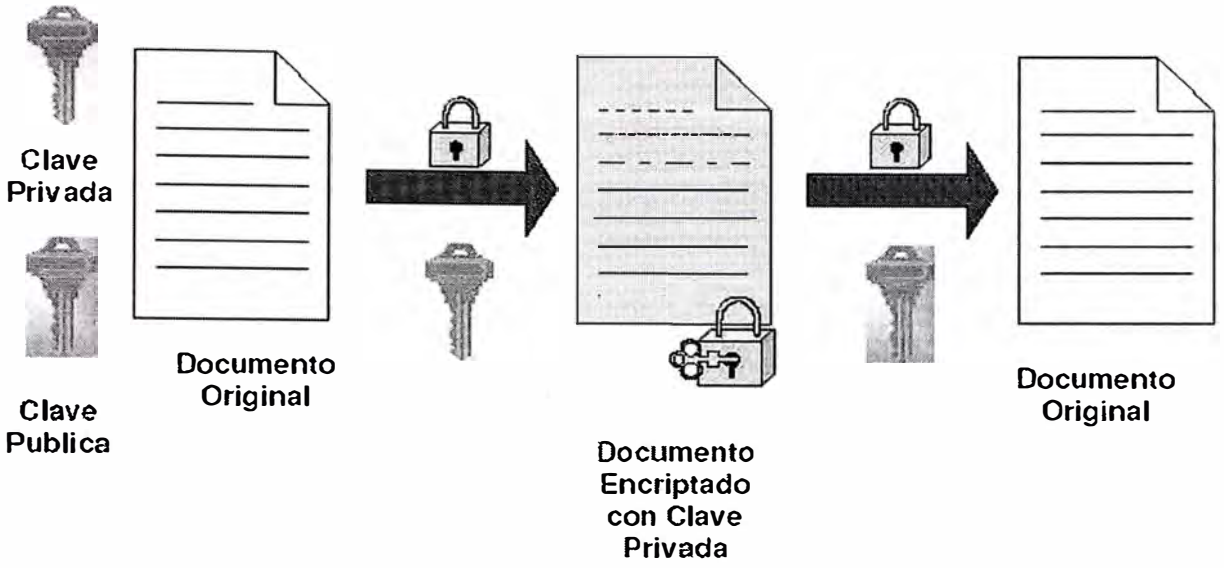
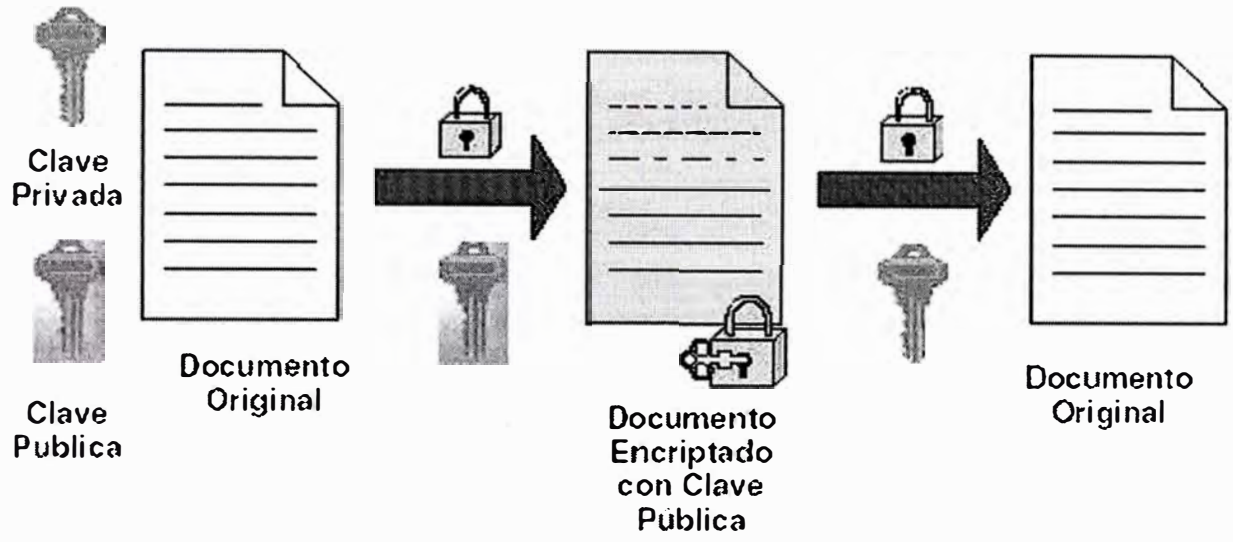


Figura 7.1 Encriptación con Clave Privada

2) Encriptación con clave pública

Cualquier persona que conozca la clave pública puede encriptar, pero se asegura que solo el poseedor de la clave privada puede desencriptar el documento.



Encriptación con Clave Pública

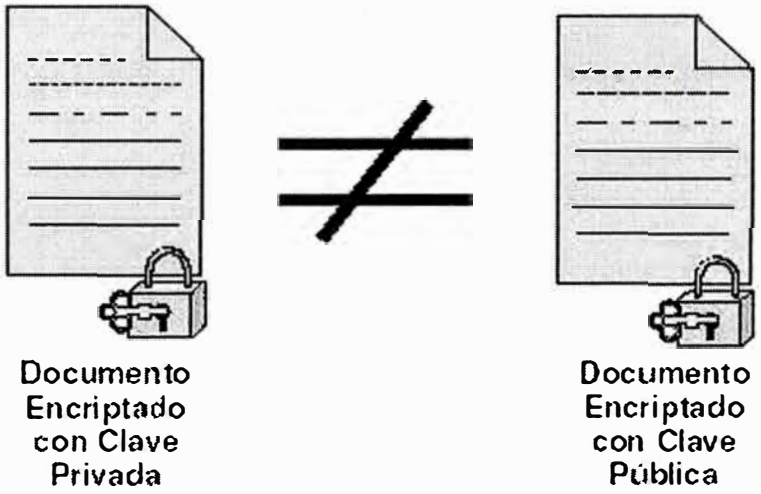


Figura 7.2 Diferentes formas de encriptar un documento

Uso práctico (Usuarios A y B):

· Si A desea enviar información segura a B, se envía empleando la clave pública de B, sólo B podrá descifrarla con su clave privada.

· Si A envía información encriptada con su clave privada, B podrá desencriptarla con la clave pública de A y tendrá la certeza de que sólo ha podido enviarla A.

· Las claves públicas se almacenan en lugares públicos (bases de datos, directorios LDAP, etc) accesibles por todas las personas que intercambien información segura.

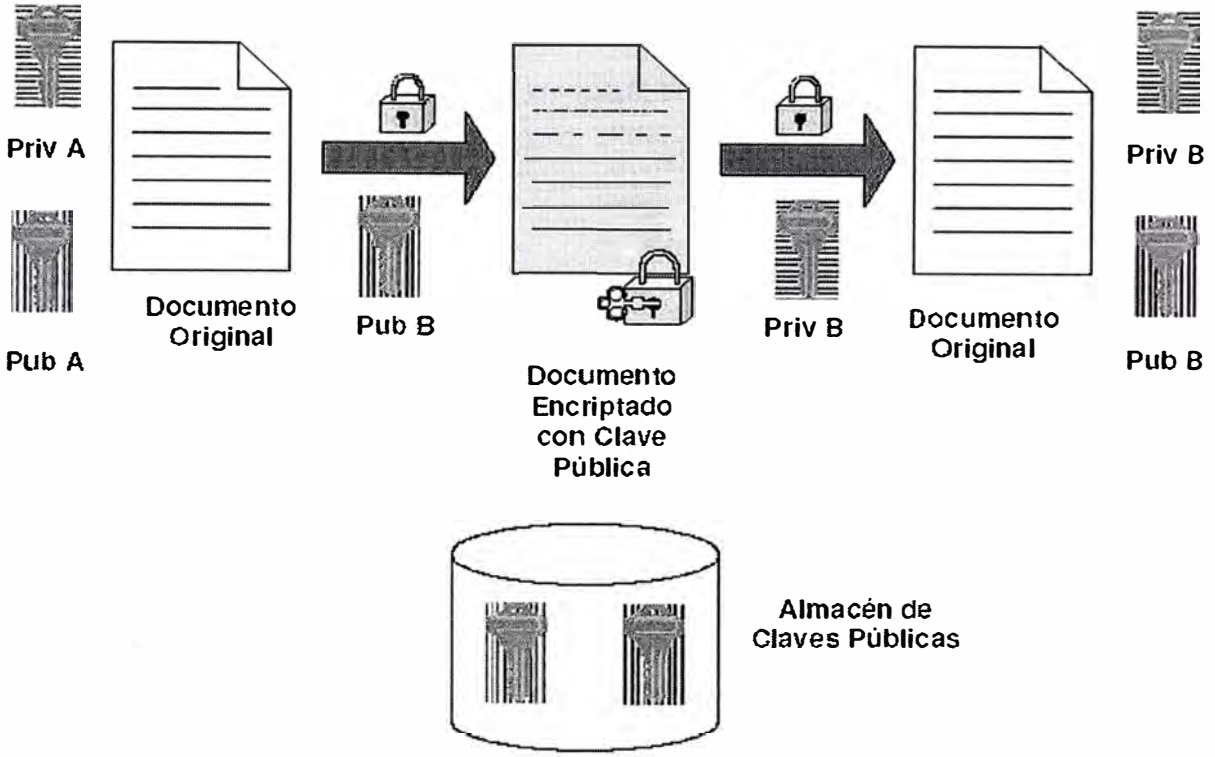


Figura 7.3 A envía información segura a B

7.2.3 Funciones HASH

Las funciones hash sirven para comprimir un texto en un bloque de longitud fija. Se utilizan en autenticación y firma digital para:

· No tener que cifrar todo el texto en los servicios de autenticación y firma digital, ya que este proceso es lento con los algoritmos asimétricos. El resumen sirve para comprobar si la clave privada del emisor es auténtica, no es necesario cifrar todo el texto si no se quiere confidencialidad.

· Para poder comprobar automáticamente la autenticidad. Si se cifra todo el texto, al descifrar solo se puede comprobar la autenticidad mirando si el resultado es inteligible. Evidentemente este proceso debe realizarse de forma manual. Utilizando

un resumen del texto, se puede comprobar si es auténtico comparando el resumen realizado en el receptor con el descifrado.

· Para comprobar la integridad del texto, ya que si ha sido dañado durante la transmisión o en recepción no coincidirá el resumen del texto recibido con el descifrado.

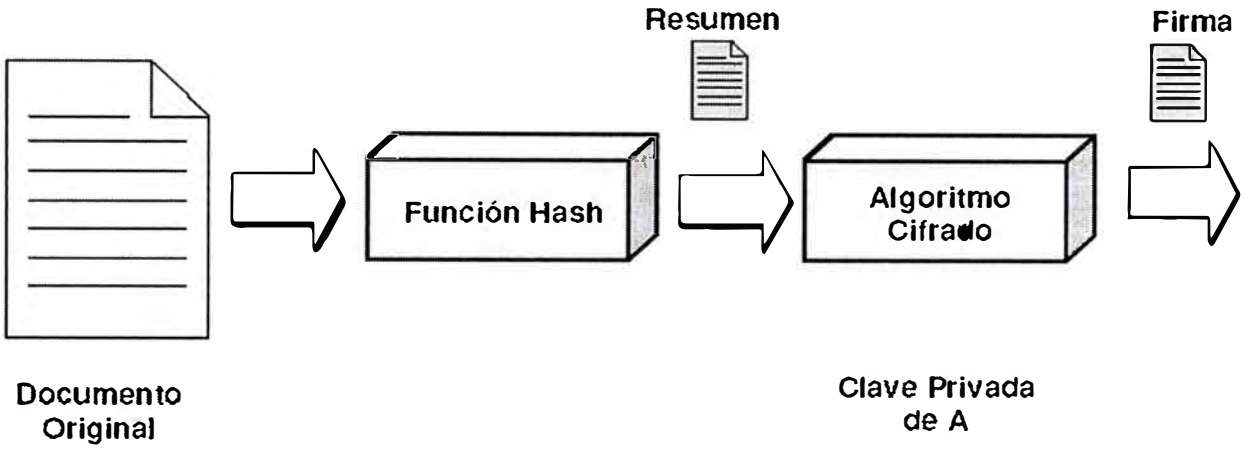


Figura 7.4 Función Hash

Las funciones hash deben ser públicas e irreversibles. No cifran, solo comprimen los textos en un bloque de longitud fija. Son diferentes de las funciones clásicas de compresión de textos (como ZIP, Huffman, V-42, etc.), ya que estas funciones son reversibles e intentan eliminar la redundancia de los textos manteniendo el significado. Las funciones hash deben cumplir las siguientes condiciones:

- Transformar un texto de longitud variable en un bloque de longitud fija.
- Ser irreversibles, es decir, no se puede recuperar el texto desde el resumen.
- Conocido un mensaje y su función hash debe ser imposible encontrar otro mensaje con la misma función hash. Esto se debe cumplir para evitar que los criptoanalistas firmen un mensaje propio como si fueran otra persona.
- Es imposible inventar dos mensajes cuya función hash sea la misma.

Los algoritmos más utilizados son:

· MD5 Inventado en 1992 por Rivest. La longitud del bloque es de 128 bits. El algoritmo MD5 es uno de los más populares para la generación de firmas digitales, debido en gran parte a su inclusión en las primeras versiones de PGP. Es el resultado de una serie de mejoras sobre el algoritmo MD4, diseñado por Ron Rivest. Procesa los mensajes de entrada en bloques de 512 bits, y produce una salida de 128 bits. En los últimos tiempos, el algoritmo MD5 ha mostrado ciertas "debilidades"', aunque sin implicaciones prácticas reales, por lo que sigue considerado en la actualidad un algoritmo seguro, si bien su uso tiende a disminuir.

· SHA-1 Inventado en 1994 por la agencia americana NIST. La longitud del bloque es de 160 bits. El algoritmo SHA-1 fue desarrollado por la NSA, para ser incluido en el estándar DSS. Al contrario que los algoritmos de cifrado propuestos por esta organización, SHA-1 se considera seguro y libre de ``puertas traseras", ya que favorece a los propios intereses de la NSA que el algoritmo sea totalmente seguro. Produce firmas de 160 bits, a partir de bloques de 512 bits del mensaje original.

7.2.4 Generar una Firma Digital

1) Paso 1: Generar el "resumen"

Para la generación del resumen se emplean algoritmos conocidos, como MD5 ó SHA – 1.

2) Paso 2: Cifrar el "resumen" con la clave privada

La encriptación se realiza con algoritmos asimétricos como DSA o RSA.

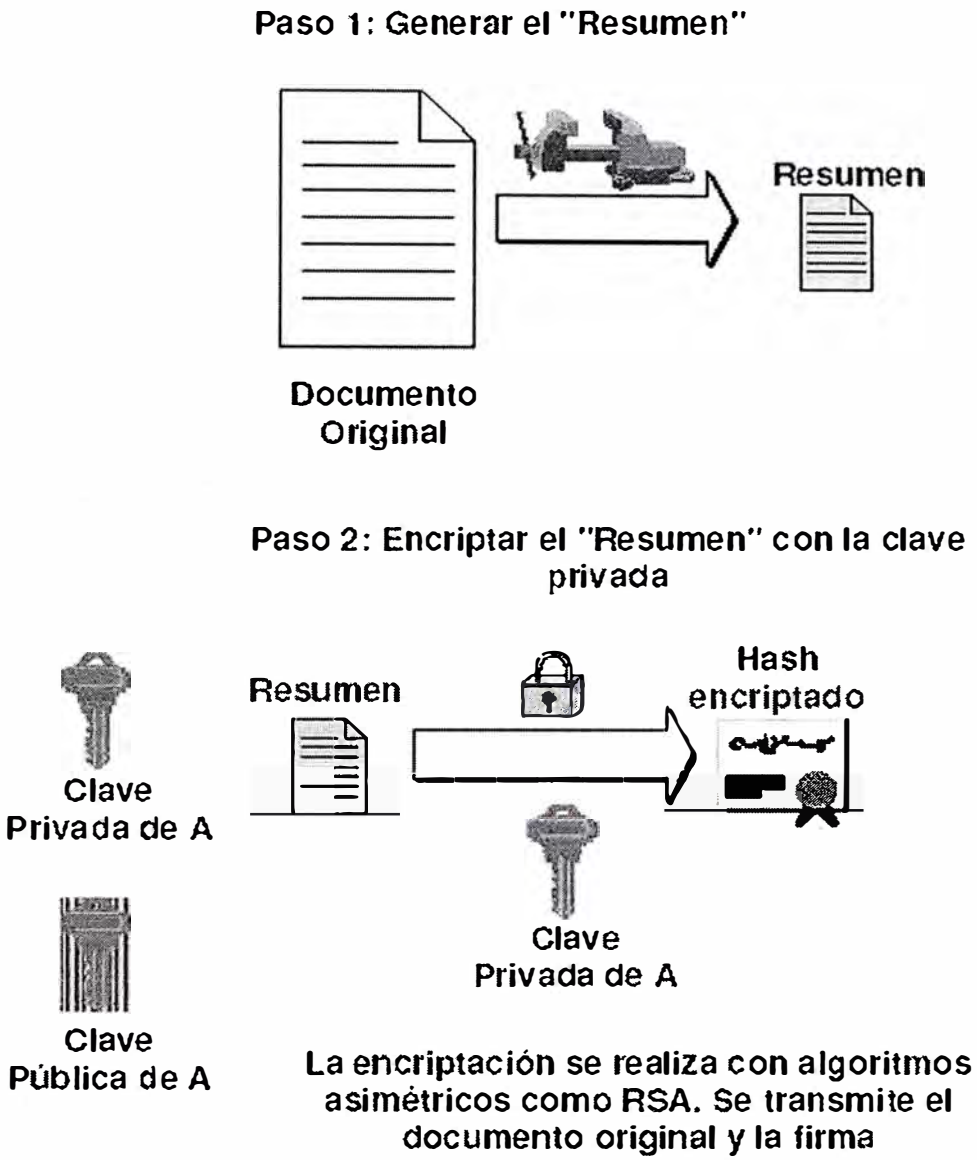


Figura 7.5 Pasos para la generación de la Firma Digital

7.2.5 Comprobar una Firma Digital

Si la comparación tiene éxito, sabemos que el documento ha sido firmado por el usuario A y que no ha sido modificado.

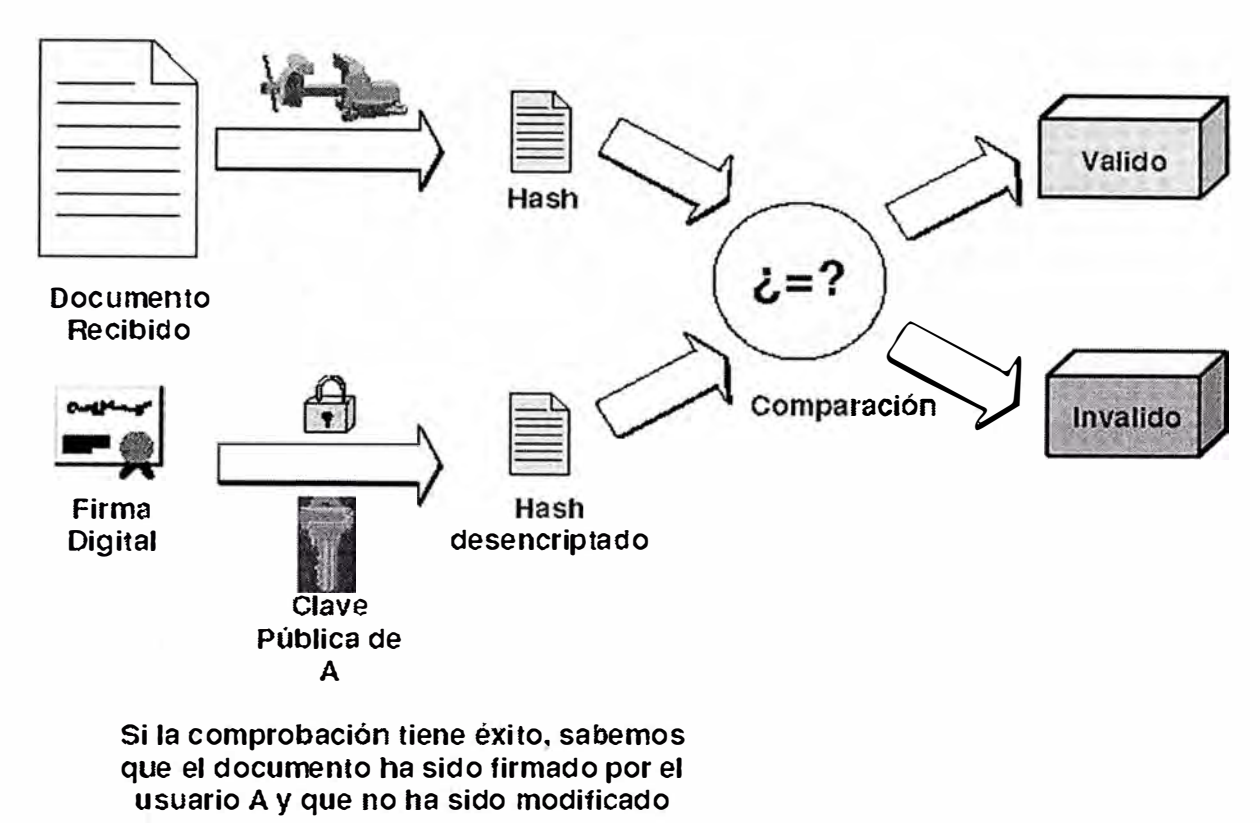


Figura 7.6 Comprobación de la firma digital

7.3. CERTIFICADOS DIGITALES

Un Certificado es un documento emitido y firmado digitalmente por una Autoridad de Certificación que asocia el nombre distintivo de una entidad con su clave pública durante un periodo de tiempo.

Son documentos digitales que sirven para asegurar la veracidad de la Clave Pública perteneciente al propietario del certificado ó de la entidad, con la que se firman digitalmente documentos que puedan proporcionar las más absolutas garantías de seguridad. Es, por tanto, muy importante estar realmente seguros de que la Clave Pública que manejamos para verificar una firma o cifrar un texto, pertenece realmente a quien creemos que pertenece. Sería nefasto cifrar un texto confidencial con una Clave Pública de alguien, que no es nuestro intencionado receptor. Si lo

hiciéramos la persona a quién pertenece la clave pública con la que lo hemos cifrado, podría conocer perfectamente el contenido de este, si tuviera acceso al texto cifrado.

De la misma forma si manejáramos una clave pública de alguien que se hace pasar por otro, sin poderlo detectar, podríamos tomar una firma fraudulenta por válida y creer que ha sido realizada por alguien que realmente no es quien dice ser.

Otro dato a tener en cuenta es que un certificado no puede falsificarse ya que van firmados por la Autoridad de Certificación. Si algún dato se modificase la firma no correspondería con el resumen (hash) que se obtendría de los datos modificados. Por tanto al utilizarlo, el software que los gestiona daría un menaje de invalidez.

Un certificado electrónico contiene una clave pública, y una firma digital. La firma digital de un certificado es su identidad electrónica, previamente autentificada y registrada por la Autoridad de Registro, que es quien asegura al destinatario del mensaje que éste proviene efectivamente de usted y que no ha sido falsificado ni manipulado.

Por lo tanto siguiendo con la estructura y ejemplos de apartados anteriores nos podemos hacer la siguiente pregunta:

¿Cómo podemos estar seguros de que estamos empleando la clave pública del usuario y no la de otro que pueda suplantarle?

- Si el usuario A envía su clave pública a B, alguien podría interceptar el mensaje y suplantarle
- Alguien podría modificar las claves públicas en el directorio

Es necesario certificar que una clave pública pertenece a un usuario.

Para su correcto funcionamiento, los certificados contienen la siguiente información:

- Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.
- Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.
- Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.
- Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.
- Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.

Existen varios formatos de certificado, el más extendido es el Certificado X.509,aunque esta no es la única forma que pueden tomar los certificados, como es el caso de PGP.

No solo hay estándares para el formato de los certificados, también los hay para su solicitud, transporte y almacenamiento. Los más utilizados son los PKCS 7 y PCKS 10.

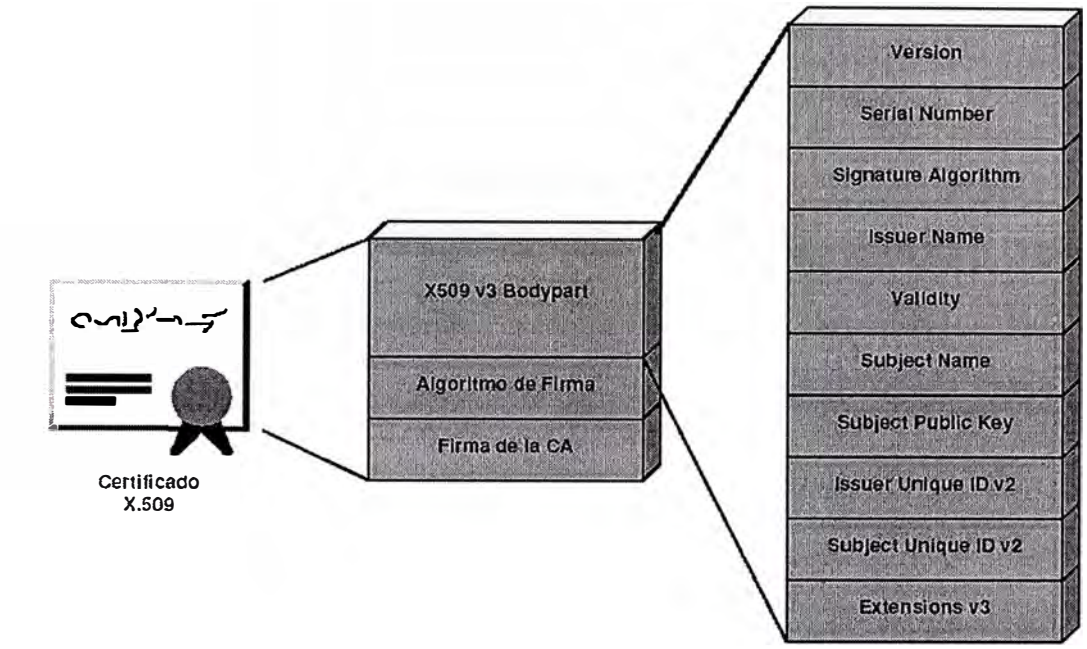


Figura 7.7 Estructura del Certificado X.509

Los certificados X.509 permiten intercambiar información entre usuarios de una forma segura. Es la mejor forma de autentificar los datos en Intranets/Extranets y correo electrónico. Existen servicios de directorio (tipo LDAP) donde se almacenan, a modo de páginas amarillas, las claves públicas de los usuarios que están certificados permitiendo comprobar su legalidad y validez. El X.509 es el protocolo que más se está extendiendo a la hora de garantizar las comunicaciones seguras entre redes de comunicación abierta como Internet, según la recomendación de la ITU-T (International Telecommunication Union-Telecommunication Standarization Sector). Su función principal es la de garantizar la identidad de los participantes en transacciones en redes abiertas, la integridad de esas comunicaciones y la privacidad y el no repudio de los mensajes.

7.3.1 Lista de revocación de Certificados

Las Listas de Revocación de Certificados (Certificate Revocation Lists, CRL), como su propio nombre indica son listas publicadas por las CA donde se incluyen aquellos

certificados que han sido revocados para que los clientes puedan comprobarlas. Los clientes de dominio pueden obtener entonces esta información y almacenarla localmente para utilizarla cuando se verifiquen certificados.

Las causas por las que se revoca un certificado pueden ser varias, pero la más clara aparece cuando se produce la perdida o captura de nuestra clave privada. Para las CA es muy importante ser capaz de detectar los certificados cuya confianza esté dudosa ya que compromete el nivel de confianza que se puede tener sobre una CA.

7.3.2 ¿Cómo se trabaja con Certificados?

Supongamos que un usuario U1 ha obtenido un certificado de una autoridad de certificación cualquiera y envía un documento firmado a otro usuario U2. Este usuario U2 validará la firma de la siguiente manera:

- U2 obtiene el certificado del U1.
- Del certificado obtenido coge la clave pública de U1 y con ella valida la firma. Como ahora el U2 tiene la clave pública de U1, U2 podrá enviar mensajes cifrados a U1.
- Para verificar que la clave pública de U1 es realmente de quien dice ser, se comprobará en la CA que dicho certificado es correcto.

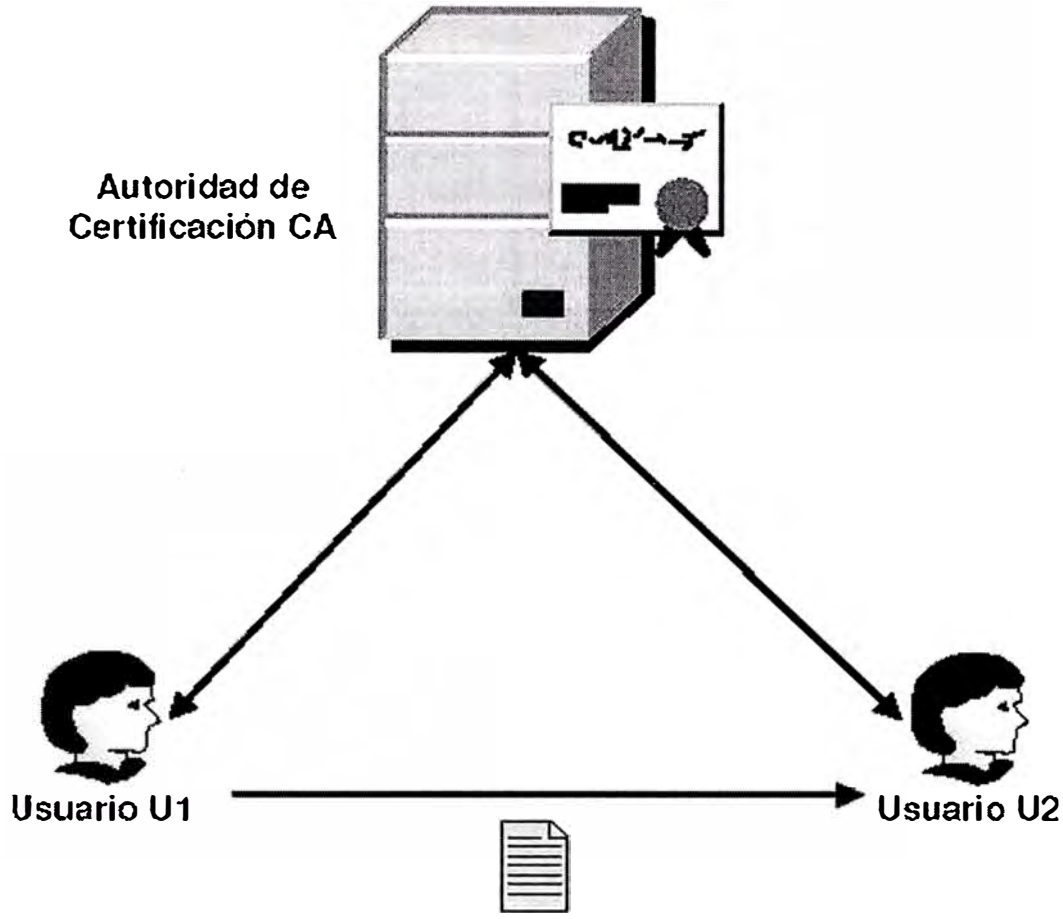


Figura 7.8 Uso de una Autoridad de Certificación

Pero es posible que exista una jerarquía de CA, de tal forma que el proceso de validación de un certificado irá pasando desde un usuario hasta una CA tenga su certificado autofirmado. El proceso de validación en esta jerarquía de CA sería el siguiente:

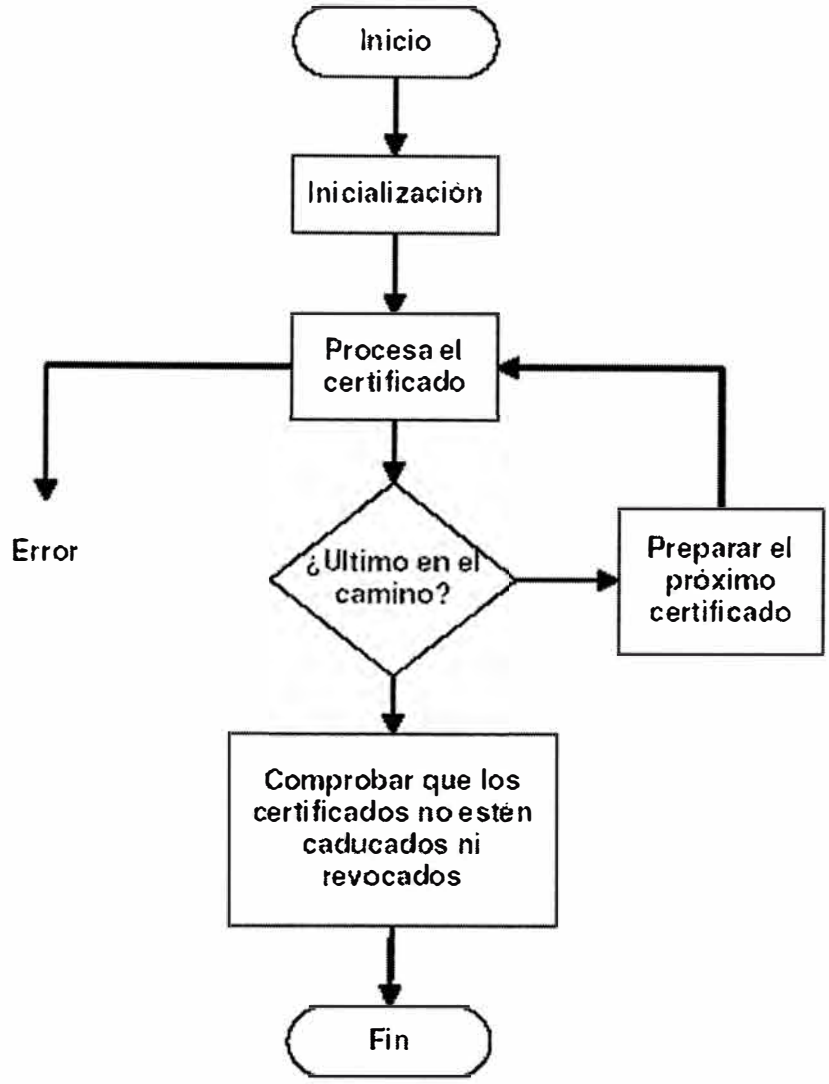


Figura 7.9 Proceso de validación en la jerarquía de CA

7.4. ¿QUÉ ES UNA PKI?

Una infraestructura de clave pública (public-key infrastruture, PKI) es un conjunto de aplicaciones y de servicios que nos permite utilizar la criptografía de clave pública (certificados) de una forma fácil y efectiva.

PKI se basa en la criptografía de clave pública, ya que las propiedades de que goza la criptografía de clave pública, cuyo uso más común se plasma en la firma digital, la convierten en candidata ideal para prestar servicios como la autenticación de usuarios

(para asegurarse de la identidad de un usuario, bien como signatario de documentos o para garantizar el acceso a servicios distribuidos en red, ya que sólo él puede conocer su clave privada, evitando así la suplantación), el no repudio (para impedir que una vez firmado un documento el signatario se retracte o niegue haberlo redactado), la integridad de la información (para prevenir la modificación deliberada o accidental de los datos firmados, durante su transporte, almacenamiento o manipulación), y el acuerdo de claves secretas para garantizar la confidencialidad de la información intercambiada.

Ahora bien, ¿cómo podemos estar seguros de que la clave pública de un usuario, que hemos encontrado por ejemplo en un directorio o una página web, corresponde realmente a ese individuo y no ha sido falsificada por otro? ¿Cómo fiarnos de esa clave pública antes de confiarle algún secreto nuestro? La solución más ampliamente adoptada consiste en recurrir a una tercera parte confiable, erigida en la figura de una autoridad de certificación (CA). La función básica de una CA reside en verificar la identidad de los solicitantes de certificados, crear los certificados y publicar listas de revocación cuando éstos son inutilizados. El certificado contiene de forma estructurada información acerca de la identidad de su titular, su clave pública y la CA que lo emitió.

Por lo tanto una PKI se puede utilizar para:

- Gestión de claves: nos permite crear, revisar o revocar claves, así como gestionar niveles de confianza.
- Publicación de claves: una vez creadas las claves, el PKI permite difundir nuestra clave publica, así como localizar las claves publicas de otros usuarios, junto con su estado (clave revocada, etc).

- Utilización de claves: una vez recuperada una clave, PKI facilita el uso de la misma.

7.5. NECESIDAD DE UNA PKI

La criptografía mediante clave pública, de por sí, no basta si deseamos reproducir en un mundo electrónico las condiciones del comercio tradicional basado en el papel.

También necesitamos:

- Políticas de seguridad para definir las reglas según las cuales deben funcionar.
- Productos para generar, almacenar y gestionar las claves
- Procedimientos para establecer cómo generar, distribuir y emplear las claves y certificados.

En resumen: necesitamos una Infraestructura de Clave Pública (PKI).

La PKI proporciona el marco de acción para un amplio conjunto de componentes, aplicaciones, políticas y prácticas para combinar y obtener las cuatro funciones principales de seguridad para transacciones comerciales, las técnicas criptográficas, en diferentes combinaciones van a permitir proteger la información mediante:

- Confidencialidad: mantener privada la información
- Integridad: demostrar que la información no ha sido manipulada
- Autentificación: demostrar la identidad de una persona o aplicación
- No repudio: garantizar que no se puede rebatir la propiedad de la información

La falta de seguridad, a menudo, se cita como una de las mayores trabas para el crecimiento del comercio electrónico, el cual sólo puede basarse en la confianza que procede de saber que todas las transacciones están protegidas por estas funciones centrales.

Al igual que cualquier tecnología nueva y crítica para el negocio, la evaluación e implementación de una solución PKI es un proceso complicado e intrincado, que requiere una buena planificación, gestión y guía clara.

7.6. COMPONENTES DE UNA PKI

Una Infraestructura de Clave Pública (Public Key Infrastructure -PKI) permite que la tecnología de clave pública se pueda implantar de un modo extenso, proporcionando la base confiable necesaria para la correspondencia electrónica entre aquellos usuarios que no pueden intercambiar manualmente sus claves.

Por lo tanto, mediante la administración de los certificados de claves públicas de una PKI, se puede establecer y mantener un entorno de red seguro, posibilitando el uso de servicios de cifrado y, especialmente, de firma digital en una amplia gama de aplicaciones.

En entornos reales, especialmente en aquellos que involucran a una gran diversidad de empresas y comunidades de usuarios que trabajan de forma conjunta, encontramos el problema de cómo estructurar las relaciones entre las entidades de los diversos dominios involucrados.

De todo esto se desprende que una Infraestructura de Clave Pública es una combinación de productos de hardware y software, políticas y procedimientos. Ofrece la seguridad básica requerida para llevar a cabo negocios electrónicos de forma que los usuarios, que no se conocen entre sí, o están muy alejados entre sí, pueden comunicarse con seguridad a través de una cadena de confianza. La PKI se basa en identidades digitales conocidas como "certificados digitales", que actúan como "pasaportes electrónicos", y vinculan la firma digital del usuario a su clave pública.

La implantación de estos servicios de seguridad en redes supone un coste añadido, tanto en elementos adicionales e incremento de tráfico en la red como en requerimientos para las entidades que participan de estos servicios, ya sea a costa de hardware específico adicional o a costa de capacidad de cálculo de su procesador. La evaluación del coste de la seguridad es requisito necesario para estudiar la viabilidad económica de cada servicio según las necesidades de los usuarios.

La PKI debe constar de:

- Política de Seguridad
- Declaración de Práctica de Certificados
- Autoridad de Certificación (CA)
- Autoridad de Registro (RA)
- Sistema de Distribución de Certificados.

7.6.1 Política de Seguridad

Una política de seguridad establece y define la dirección de máximo nivel de una organización sobre seguridad de información, así como los procesos y principios para el uso de la criptografía. Por lo general, incluye declaraciones sobre cómo gestionará la empresa las claves y la información valiosa, y establecerá el nivel de control requerido para afrontar los niveles de riesgo.

7.6.2 Declaración de Práctica de Certificados (CPS)

Algunos sistemas de PKI se gestionan mediante Autorizadores de Certificados Comerciales (CCA) o Terceras Partes Seguras, y, por lo tanto, requieren un CPS. Éste es un documento en el que se detallan los procedimientos operativos sobre cómo ejecutar la política de seguridad y cómo aplicarla en la práctica. Por lo general, incluye definiciones sobre cómo se construyen y operan los CA, cómo se emiten,

aceptan y revocan certificados, y cómo se generan, registran y certifican las claves, dónde se almacenan y cómo se ponen a disposición de los usuarios.

7.6.3 Autoridad de Certificación (CA)

Una autoridad de certificados (Certificate Authority, CA) es una entidad o servicio que emite certificados. El sistema de CA es la base de confianza de una PKI, ya que gestiona los certificados de clave pública durante toda su vida.

El problema que se plantea ahora es: si la Autoridad Certificadora avala los datos del certificado ¿Quién avala a la autoridad Certificadora?. Para solventar esto se han creado una serie de entidades autorizadas a emitir certificados, de tal forma que éstas a su vez son avaladas por otras entidades de mayor confianza, hasta llegar a la cabeza de la jerarquía, en la que figuran unas pocas entidades de reconocido prestigio y confianza, como Verisign, que se autofirman su certificado.

Cada certificado emitido por una CA debe estar firmado por una CA de mayor grado en el esquema jerárquico de autoridades certificadoras, formándose así una cadena de certificados, en los que unas CAs se avalan a otras hasta llegar a la CA superior, que se avala a sí misma. La jerarquía de firmas y la cadena con ella formada están contempladas en el estándar X.509 v3, que indica la forma correcta de realizar estas cadenas de certificaciones.

El certificado Digital vincula pues indisolublemente a una persona o entidad con una llave pública, y mediante el sistema de firma digital se asegura que el certificado que recibimos es realmente de la persona que consta en el mismo. El sistema de firma digital liga un documento digital con una clave de cifrado.

En resumen se puede decir que la CA:

- Emite certificados vinculando la identidad de un usuario o sistema a una clave pública con una firma digital

- Programa las fechas en la que expiran los certificados

- Garantiza que los certificados se revocan cuando sea necesario, publicando Listados de Revocación de Certificados (CRL).

Al implantar una PKI, una organización puede manejar su propio sistema de CA, o emplear el servicio de CA de un CA Comercial o Tercera Parte Segura.

Jerarquía de autoridades de certificados

El concepto de jerarquía de certificados podría decirse que aparece con el concepto de empresa.

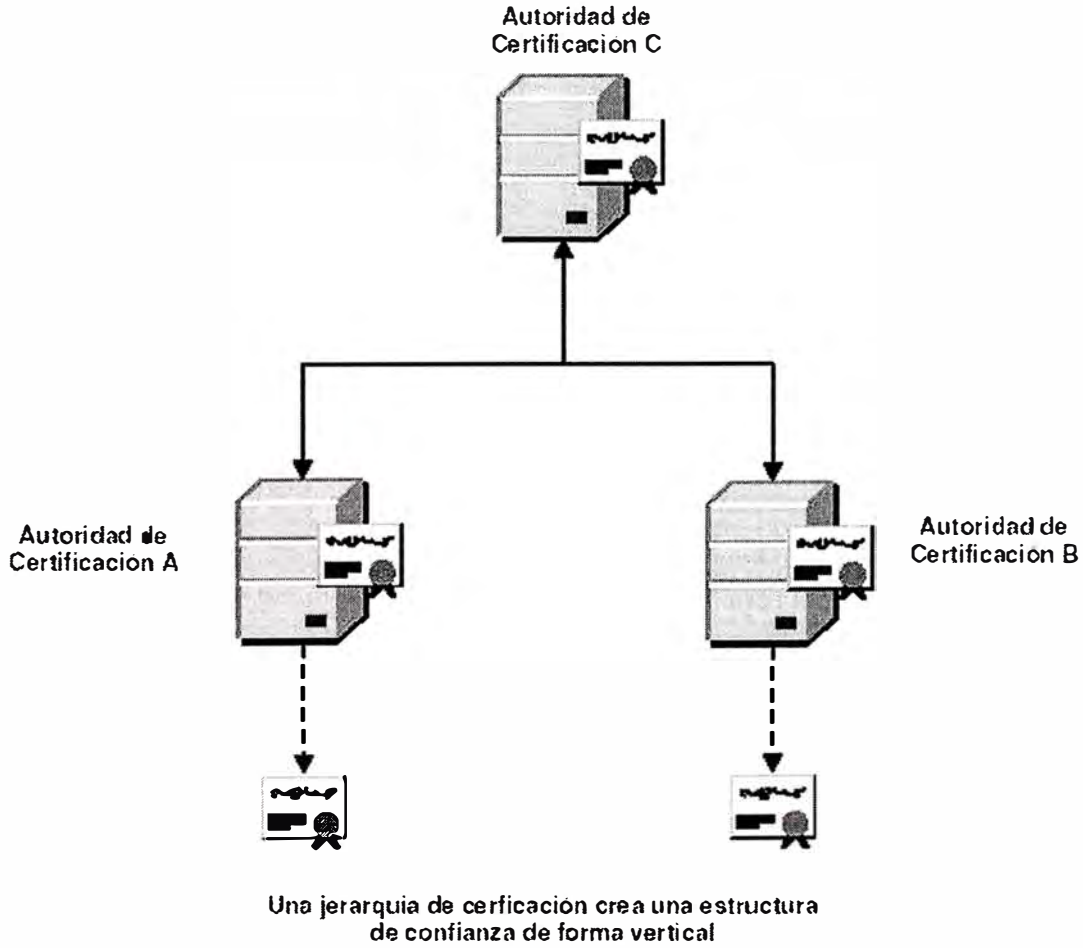


Figura 7.10 Jerarquía de CAs

Si en una empresa con cientos de trabajadores, todos y cada uno de los empleados solicitase un certificado a una CA raíz, supondría un fuerte gasto para la empresa. La solución sería que esta empresa generase sus propios certificados, es decir, que sea su propia CA para sus empleados. Estas pequeñas CA deberán emitir certificados por una CA de un nivel más alto, así hasta que se llegue a una CA cuyo certificado este autofirmado y de la cual se tenga total confianza. Esto es lo que se denomina una PKI.

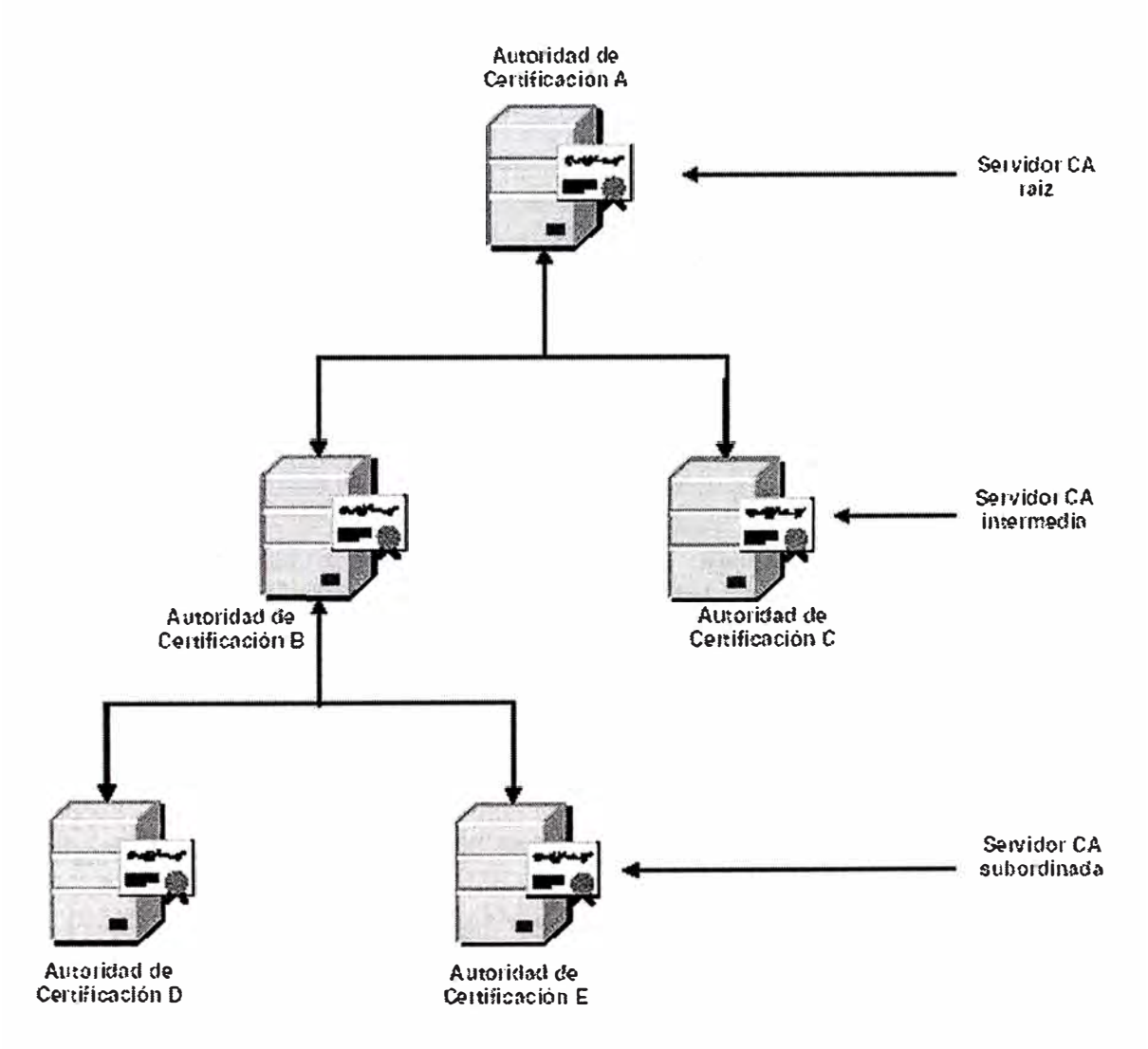


Figura 7.11 Jerarquía de autoridad de certificados

Algunas autoridades de certificación

Algunas de las grandes CA comerciales más importantes son:

· Thawte Consulting. Proveedor internacional de certificados digitales

· VeriSing. Una de las primeras CA. Proporciona tanto certificados de cliente como de servidor

· Belsing: Principal proveedor europeo de certificados digitales.

· Certisign Certification Digital Ltda.Autoridad de certificación brasileña

· Servicios de publicación de Internet. Autoridad de certificados para España y Sudamérica.

7.6.4 Autoridad de Registro (RA)

Con el tiempo, una autoridad de certificación puede verse fácilmente desbordada si cubre un área geográfica muy extensa o muy poblada, por lo que a menudo delega en las llamadas autoridades de registro (RA) la labor de verificar la identidad de los solicitantes. Las RAs pueden abrir multitud de oficinas regionales dispersas por un gran territorio, llegando hasta los usuarios en los sitios más remotos, mientras que la CA se limitaría así a certificar a todos los usuarios aceptados por las RA dependientes de ella. Gracias a esta descentralización se agiliza el proceso de certificación y se aumenta la eficacia en la gestión de solicitudes.

Una RA proporciona la interfaz entre el usuario y el CA. Captura y autentifica la identidad de los usuarios y entrega la solicitud de certificado al CA. La calidad de este proceso de autentificación establece el nivel de confianza que puede otorgarse a los certificados.

En definitiva, una PKI incluirá una o varias autoridades de registro para certificar la identidad de los usuarios; una o varias autoridades de certificación que emitan los certificados de clave pública; un repositorio de certificados, accesible vía web u otro

medio, donde se almacenen los certificados; las listas de revocación de certificados (CRL), donde se listan los certificados suspendidos o revocados; y, por supuesto, los propios certificados.

7.6.5 Sistema de Distribución de Certificados

Los certificados se pueden distribuir de varias formas, dependiendo de la estructura del entorno PKI. Se pueden distribuir, por ejemplo, por los propios usuarios o a través de un servicio de directorios. Puede que ya exista un servidor de directorios dentro de una organización, o se puede suministrar uno como parte de la solución PKI.

7.7. VENTAJAS DE LA INFRAESTRUCTURA PKI

· Las claves no viajan a través de la red desde el cliente al servidor, dado que los certificados constituyen información pública.

· Ofrece mejores medios para identificar al usuario ya que los certificados contienen información verificable relacionada con la identidad del usuario, lo cual no ocurre en la autenticación basada en dirección IP del equipo del usuario, en nombre de dominio o en dirección de mail, dado que las direcciones IP pueden ser dinámicas, y los nombres de dominio y direcciones de mail pueden ser espiadas...

· Los certificados basados en tecnología de clave pública proveen un mecanismo de autenticación más fuerte. Sólo el usuario conoce la forma de acceder a su clave privada.

· Simplificación en la administración y disminución de costos.

7.8. DEBILIDADES DE LA INFRAESTRUCTURA PKI

Existen algunos cuestionamientos que se realizan a esta infraestructura:

· La seguridad de un sistema basado en CA consiste en varios eslabones, algunos de los cuales no son criptográficos: la gente también forma parte de esta infraestructura.

· Un conflicto que permanece sin resolver es la seguridad de la clave privada con respecto al almacenamiento de la misma. Que un empleado guarde su clave privada en una PC resulta un hecho riesgoso partiendo de la base de que esa PC puede ser utilizada por varios miembros de la oficina. Como solución surge la aparición de las smart cards y entonces ahora la seguridad de la clave privada pasará a depender de la seguridad de estos dispositivos. No puede garantizarse el hecho de que una clave privada será únicamente utilizada por su dueño.

7.9. PROBLEMÁTICA DE LA IMPLANTACIÓN DE PKI

Los mayores obstáculos a los que se han enfrentado las empresas pioneras en la implantación de soluciones PKI para sus necesidades de negocio electrónico (e-Business) han sido tradicionalmente:

· La falta de interoperabilidad, ya que el mero hecho de ceñirse al estándar X.509.v3 no garantiza en absoluto que dos certificados generados por dos sistemas desarrollados por casas distintas sean mutuamente compatibles.

· Además, existen problemas de confianza entre CAs de distintas organizaciones, que puede imposibilitar la verificación con éxito de cadenas de certificación cuya CA raíz sea desconocida o no confiable, invalidándose todo el esquema de PKI.

· El coste ha sido un problema desde el principio. Al no existir un mercado suficientemente maduro en PKI, cada empresa que ofrece soluciones de clave pública pone tarifas en función de criterios diversos (por certificado, por uso de certificado, por servidores instalados, etc.) y el costo de loa servicios es también variable, de manera que la inversión en PKI como respuesta a las necesidades de

seguridad y accesibilidad a los activos informáticos de la empresa puede resultar cuando menos inesperadamente elevada.

· PKI termina presentando problemas de escalabilidad, cuando el número de certificados emitidos a los usuarios va creciendo, debido a que las listas de revocación deben ser consultadas en cada operación que involucre certificados y firmas digitales, si se desea una implantación seria y robusta de PKI. Bien es cierto que el esquema de confianza vertical, promulgado por las estructuras de certificación en árbol, resulta más escalable que los modelos de confianza horizontal, como el adoptado por PGP, cuya problemática es tan seria que no se prevé solución satisfactoria.

· Finalmente, la tecnología PKI es considerada un tanto esotérica por usuario final, que no terminan de entender del todo la jerga relacionada. Acostumbrado a autenticarse sin más que introducir su nombre y contraseña, puede sentirse fácilmente rebasado por la complejidad tecnológica de las firmas digitales y demás funciones criptográficas. Por demás, en la medida en que no se instauren las tarjetas chip, controles biométricos y otros dispositivos similares criptográficamente robustos, el problema de los usuarios anotando su contraseña (en este caso para acceder a su clave privada) en un post-it pegado en el monitor persistirá por mucho tiempo.

7.10. PASOS PARA EVALUAR SOLUCIONES PKI

7.10.1 Flexibilidad

Es esencial que todos los componentes de una PKI sean compatibles, ya que es improbable que todos provengan de un único proveedor. Por ejemplo, el CA deberá poderse interconectar con los sistemas existentes, como servidores de directorios

instalados previamente en la organización. La PKI debe emplear interfaces estándar abiertos como LDAP y X.500 (DAP) para garantizar que puede funcionar con todos los servidores de directorios que cumplen los estándares.

Asimismo, muchas organizaciones se han decantado por proveedores de tarjetas inteligentes y módulos de seguridad de hardware (HSM). También en este caso, las interfaces estándar, como el PKCS#11 (Cryptoki), la PKI tiene la flexibilidad necesaria para funcionar con una amplia gama de señales de seguridad. En muchos sistemas de PKI, el registro es necesario hacer el registro cara a cara, para proporcionar el nivel necesario de confianza. Sin embargo, tal vez esto no sea siempre apropiado, por lo que es posible que se necesite un registro desde un punto remoto. La PKI debe permitir a los usuarios solicitar certificados a través del correo electrónico, empleando un buscador web estándar, o automáticamente a través de dispositivos de comunicación en red para VPN.

Para algunas implementaciones a gran escala, los certificados deben emitirse por lotes, por ejemplo, para tarjetas de banco o documentos nacionales de identidad. En esos casos, la PKI exige la flexibilidad de un proceso automatizado de RA vinculado a la base de datos de tarjetas.

7.10.2 Sencillez de manejo

Aunque los principios con los que funciona un sistema de PKI pueden ser complicados, su gestión no debe serlo. La PKI debe permitir a personal no especializado, como administradores comerciales, manejarla con confianza. Estos operadores no tienen por qué entender las complicaciones de los algoritmos criptográficos, claves y firmas. Debe resultar tan fácil como pulsar iconos y dejar a la aplicación de software que se encargue del resto. La interfaz debe ser gráfica e

intuitiva, ayudando a la tarea de gestión, en lugar de dificultarla con complejos registros de la base de datos.

La flexibilidad y sencillez de manejo aportarán un gran rendimiento a la inversión en un sistema de PKI, ya que repercuten en aspectos como la formación, el mantenimiento, la configuración del sistema, la integración y, por supuesto, el futuro crecimiento en el número de usuarios. Estos aspectos pueden elevar el coste de una PKI muy por encima del coste inicial de implementación y, por lo tanto, se deben estudiar atentamente en la fase de evaluación.

La PKI se está convirtiendo en un elemento imprescindible en las estructuras de seguridad de las empresas y todo CA debe ser capaz de reflejar e implantar la política de seguridad de la organización.

Por este motivo, un sistema de PKI basado en políticas es crítico para garantizar que el proceso de gestión de certificados refleja con precisión los papeles de los Operadores de CA y RA y de los usuarios de certificados. Por ejemplo, el Operador de CA puede decidir delegar la revocación de certificados de usuarios finales en los Operadores de RA, al tiempo que retiene el derecho de revocación de los certificados de los Operadores de RA.

7.10.3 Crecimiento

A medida que una organización emplea y depende cada vez más de la PKI, es esencial que dicho sistema PKI pueda ampliarse para adaptarse a su crecimiento. Inicialmente, una PKI sólo puede soportar una sola aplicación.

Sin embargo, debe tener la suficiente versatilidad como para soportar más aplicaciones a medida que aparecen en línea.

También debe ser posible añadir componentes de CA y RA adicionales para soportar un número creciente de certificados a medida que crece la PKI. Asimismo, es posible que se necesiten diversos tipos de certificados y mecanismos de registros, a medida que la PKI se amplíe para incluir nuevos servicios.

7.10.4 Compatibilidad

La tecnología de PKI aún se encuentra en fase de desarrollo y resulta difícil predecir con cierto grado de acierto los usos y requisitos futuros para los sistemas de PKI. Los estándares para PKI aún están evolucionando y, en algunos casos, no existen todavía. Por lo tanto, para proteger la inversión y evitar futuros problemas de compatibilidad, es fundamental crear una PKI que sea totalmente abierta y construida para cumplir los estándares comerciales más comunes y avanzados. Esto debe estudiarse en la fase de diseño, para garantizar una integración armoniosa con el resto de la infraestructura de Tecnología de Información.

7.11. LA SEGURIDAD DE LA RA/CA

Los sistemas de CA/RA se encuentran en el núcleo de cualquier PKI. La seguridad de estos sistemas es de primordial importancia y si se pone en entredicho, correrá peligro toda la solución PKI.

En particular, la PKI debe garantizar lo siguiente:

· La clave privada del CA debe situarse en un módulo de seguridad a prueba de manipulaciones y se deben realizar copias de seguridad para la recuperación de desastres.

· El acceso a la CA y a la RA debe vigilarse muy atentamente, por ejemplo, empleando tarjetas inteligentes para garantizar una mejor autentificación de usuarios.

· También debe ser posible configurar el proceso de gestión de certificados de forma que un operador deba autorizar las solicitudes de certificación.

· Todas las solicitudes de certificación deben firmarse digitalmente mediante una fuerte autentificación criptográfica para detectar e impedir a los piratas informáticos que generen deliberadamente certificados falsos. Todas las acciones llevadas a cabo por el sistema de CA/RA deben registrarse en un registro de auditoria seguro, en el que cada entrada tenga asignada una fecha / hora y reciba una firma, para asegurar que las entradas no pueden falsificarse.

· La CA debe ser aprobada y verificada por un organismo independiente, por ejemplo al menos hasta ITSEC E2, pero preferiblemente hasta ITSEC E3 (Criterios de Evaluación de Seguridad de Tecnología de la Información). ITSEC es un estándar global reconocido para la medición de productos de seguridad y la evaluación E3 representa el mayor nivel de seguridad comercial de hoy día.

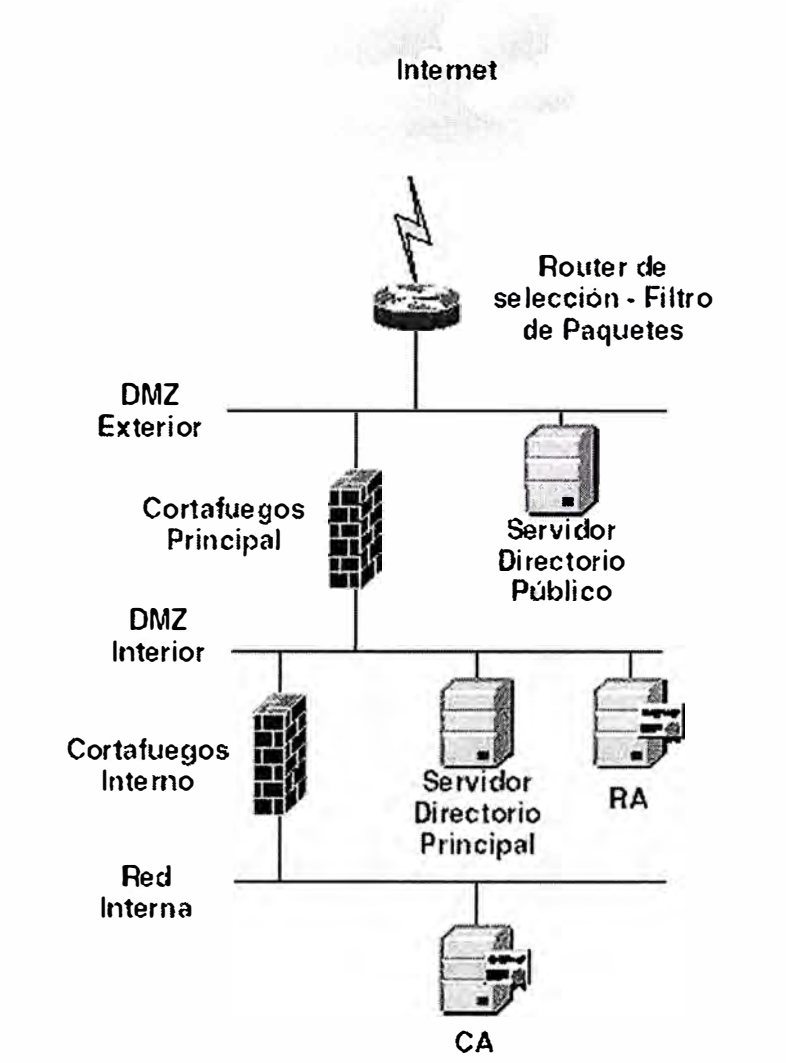


Figura 7.12 Topología Física de una PKI

7.12. APLICACIONES HABILITADAS POR PKI

Una PKI es un medio para conseguir un fin, que proporciona el marco de seguridad con el que se pueden distribuir las aplicaciones habilitadas por PKI para obtener ventajas finales.

Algunos ejemplos de aplicaciones pueden ser:

- Comunicaciones entre servidores en Internet

- Correo electrónico

- Intercambio Electrónico de Datos (EDI)

- Transacciones con tarjeta de crédito en Internet

- Redes Privadas Virtuales (VPN).

7.13. EJEMPLO DE APLICACIONES DE PKI

La PKI resulta ideal en una intranet, en la que se comparten documentos trabajo en grupo, se accede a recursos de red (servidores de archivos, bases de datos, etc.), se intercambia correo certificado entre los empleados, etc. PKI resulta mucho más ágil que los sistemas tradicionales de control basados en nombre y contraseña y listas de control de acceso.

En el caso de extranets o de Internet, PKI es de uso obligado. De hecho, es la única forma conocida actualmente de prestar confianza a los actores de las relaciones telemáticas que no se conocen entre ellos, tanto en el business-to-business entre empresas, como en el comercio al por menor, entre vendedores y compradores particulares por Internet. La confianza en un grupo de CA mundialmente reconocidas (como VeriSign) o localmente aceptadas permite que las entidades involucradas puedan fiarse unas de otras, a pesar de no existir contacto físico ni vínculo previo entre las partes. SSL y SET se están convirtiendo en estándares de facto que atestiguan el éxito de las tecnologías de clave pública en escenarios de seguridad descentralizados como Internet. Las últimas iniciativas de algunas empresa para cambiar sus procedimientos administrativos, realizados en papel y sometidos a la tramites burocráticos, hacia procesos digitales interactivos, hacen uso también de tecnología PKI.

Actualmente se están realizando distribuciones de PKI en todo el mundo, preparándose para el nuevo milenio de negocios digitales. El amplio abanico de organizaciones que implantan sistemas PKI refleja el hecho de que se trata de un

marco fundamental para permitir aplicaciones de comercio electrónico que repercutirá en todos nosotros.

CAPÍTULO VIII

DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA

8.1. INTRODUCCIÓN

El objetivo de asegurar una red es proteger la red y sus aplicaciones ante un ataque, asegurando la disponibilidad, la confidencialidad y la integridad de la información. Cuando las organizaciones diseñan sus arquitecturas de seguridad buscando lograr este objetivo, deben considerar muchos factores. No todas las redes y sus aplicaciones asociadas tienen los mismos riesgos de ataque o posibles costos de reparación antes un ataque. Por consiguiente, las compañías deben realizar análisis de costo-beneficio para evaluar los potenciales retornos de inversión para distintas tecnologías de seguridad en redes y otros componentes versus los costos de oportunidad de no implementar estas soluciones. Dentro de este proceso, las organizaciones deberían considerar sus implementaciones de seguridad como ventajas competitivas que pueden atraer más clientes, empleados y socios de negocios.

En una red empresarial la información juega un papel preponderante y cada vez las compañías son más dependientes de ella, lo que obliga a contar con elementos, recursos y herramientas que permitan tener acceso a dicha información sin importar

donde se esté. Además, bajo los nuevos esquemas de transformación comercial es de vital importancia para la empresa tener disponible sus recursos no solo a los usuarios internos sino también a sus clientes, proveedores y cualquier persona que esté interesada en sus productos y servicios.

Gracias al comercio electrónico las empresas podrán tener mayor facilidad y flexibilidad en el manejo de la información interna y otros recursos, pero al mismo tiempo implica una amenaza inherente al negocio, puesto que al estar conectados a Internet ya no se está aislado del mundo y de esta forma, desconocidos podrían tener acceso a los sistemas internos.

Los fundamentos de diseño y decisiones de implantación varían de acuerdo a las funcionalidades requeridas de la red, sin embargo, a continuación se muestran los objetivos de diseño que pueden ayudar en el proceso de decisión:

· Seguridad y mitigación de ataques basados en una política.

· Implementación de la seguridad a través de una infraestructura (no sólo en dispositivos especializados de seguridad).

· Administración de la seguridad y reportes.

· Autenticación y autorización de usuarios y administradores a los recursos de la red.

· Detección de intrusos a los recursos críticos y redes.

· Soporte para aplicaciones emergentes.

La arquitectura de seguridad debe ser confiable y escalable. La confiabilidad en la red incluye redundancia para proteger cualquier posible falla de algún dispositivo ya sea por mala configuración, falla física, o un ataque en la red.

Las corporaciones están en continua expansión de sus redes de misión crítica con nuevas aplicaciones de Intranet, Extranet y comercio electrónico, por lo que las

tecnologías de seguridad de la red deben estar en aumento para prevenir intrusos y eliminar vulnerabilidades de seguridad. Si no tienen precaución y conciencia de las amenazas, las corporaciones podrían experimentar grandes problemas, daños o pérdidas.

8.2. PRINCIPIOS DE DISEÑO DE UNA RED SEGURA

Antes de la implementación de una solución de seguridad en redes, se debe tener en consideración muchos temas fundamentales. Algunos de ellos son:

1) Integridad, significa que las medidas de seguridad se deben conservar y preservar. No debe existir información corrupta ni perdida de información. Estos deben proteger la información en forma consistente en todo tiempo. Estos deben proteger la confidencialidad y sensitividad de la información.

2) Disponibilidad, significa que las medidas de seguridad deben estar disponibles en todo tiempo, y que los sistemas de información que estos protegen deben estar disponibles en todo tiempo.

3) Protección Adecuada, significa que la infraestructura debe protegerse con un grado correspondiente con su valor. Sólo deben protegerse los componentes de la red hasta que pierdan su valor y deben protegerse a un grado consistente con su valor.

4) Efectividad, significa que cualquier control que se implemente debe ser efectivo en asegurar la red y las partes que lo componen. Sin embargo, estos deben ser eficientes, fáciles de usar y apropiados en tamaño al tipo de organización en el cual estarán operando.

5) Diligencia debida, significa que la seguridad en redes es un proceso continuo y evolutivo. La red debe ser continuamente monitoreada y gestionada par asegurar la seguridad.

8.3. FASES PARA ASEGURAR UNA RED

Se deben seguir las siguientes ocho fases en el diseño de una red segura.

8.3.1 Fase 1: Requerimientos del Sistema

La fase de requerimientos del sistema consiste en reconocer las necesidades de seguridad en su red y definir los objetivos de mejora de dichas necesidades. Esto incluye:

1) Evaluar la necesidad y el nivel de seguridad que la red requiere;

2) Evaluar el valor de la información en la red y determinar el nivel de seguridad necesario para proteger la información. Esta medición, junto con el paso 1, deberá satisfacer el principio de adecuada protección; y,

3) Medición de cualquier debilidad previsible en la situación actual de la red, por eso identificando parcialmente cualquier necesidad para una fuerte protección.

También, mientras se enfoque el principio de adecuada protección, los diseñadores de la red deben decidir si hay necesidad para el incremento del nivel de seguridad existente. La política de seguridad de la red deberá ser manejada y definida por necesidades cuantificables – no por miedo o pereza.

8.3.2 Fase 2: Formulación del Concepto

Esta fase considera los diferentes métodos para lograr los objetivos que se definieron en la fase de requisitos de sistemas. Se debe determinar los aspectos positivos y negativos de cada posible plan de acción. Finalmente, la elección del curso de acción deberá ser transformado en un plan detallado para proporcionar la seguridad en toda la red.

1) Análisis de Riesgo

El análisis de riesgo es una tarea crítica que ocurre durante las dos fases iniciales del modelo del proceso. El análisis de riesgo esta dividido en tres diferentes estados: valoración de la sensibilidad, valoración del riesgo, y la valoración económica.

· Valoración de la sensibilidad, define las varias necesidades definidas en la fase de requerimientos del sistema tal como ellos fueron relacionados en la valoración de los recursos de la red.

· Valoración del riesgo es la más importante y significativa actividad de todo el análisis de riesgo. Es usado para definir las amenazas contra de la red, vulnerabilidad de la red, y los niveles de riesgo que resulta de la explotación de las vulnerabilidades de la red por las amenazas definidas en contra la red. Ciertas preguntas simples facilitan la valoración de la susceptibilidad de la red a un riesgo que se vuelve en una realidad. Por ejemplo, los riesgos de la red incluyen la falta de un backup diario y un plan de recuperación de desastres, software de antivirus, métodos de detección de intrusos, software de control de acceso, cortafuegos, practicas de contraseñas, encriptación y fuerte autenticación.

· Valoración económica, calcula el valor esperado de una perdida, en el caso de que los riesgos definidos se vuelvan realidad y la seguridad de red sea comprometida.

8.3.3 Fase 3: Definición de los Sistemas

Durante esta fase, se crean las especificaciones del actual sistema con el detalle exacto de operación del sistema. Adecuada con las necesidades de la implementación de la red segura, esta fase explica el comportamiento de la red bajo cualquier circunstancia previsible. Usando la información recogida del análisis de riesgos, los diseñadores de red deben predecir sus acciones en un escenario no previsible. Basado en la información recolectada en las previas fases y las especificaciones de sistemas

diseñadas aquí, los diseñadores deben decidir proceder o descontinuar con la implementación de red segura.

8.3.4 Fase 4: Diseño de Ingeniería

Durante esta fase, las especificaciones producidas en las fases previas serán usadas para crear y diseñar la solución, eso explica en detalle cada una de las especificaciones que serán realizadas. Por ejemplo, el diseño de ingeniería debe detallar como la red debería repeler ante un "hacker" intentando un ataque de IP Spoofing por la utilización de gateways a nivel de circuitos, una amenaza cuyo efecto podría haber sido descrito en la fase de definición de sistemas.

8.3.5 Fase 5: Verificación del Diseño

El diseño debe ser probado en la fase de verificación del diseño. Esta fase constituye en un periodo de prueba, el cual verifique el uso del sistema, la seguridad, y el mantenimiento. Usando el ejemplo anterior de un hacker intentando realizar un ataque de IP spoofing, esta fase debería probar la viabilidad o la probabilidad de que el hacker engañe al gateway a nivel de circuito. Los diseñadores de la red deben elegir en descontinuar el proceso si el sistema es vulnerado, o proceder e implementar el diseño de la red.

8.3.6 Fase 6: Instalación y Puesta en Producción

Durante esta fase, la solución de red segura es instalada y preparada para operar. Antes de la puesta en producción, los diseñadores deben examinar la red para ver si todavía se reúne los objetivos planteados definidos en la fase de requerimientos del sistema. Con tal de que todas las fases se hayan completado, esta fase será la fase final en la cual el diseño y la implementación se vuelve realidad el resultado es que

una red puede ser considerada segura. No obstante, como se indico antes, el proceso de asegurar una red es evolutivo y de forma continua, así se plantea la siguiente fase.

8.3.7 Fase 7: Operación

En la fase de operaciones, los diseñadores de red y administradores gestionaran el sistema desarrollado y se enfocaran en identificar los puntos de mejora que se requiera, para que toda la red sea completamente segura. Usando prueba de penetración y varias herramientas de hacking e intrusión, periódicamente deben realizar búsqueda de nuevos puntos débiles y de vulnerabilidades. Una vez que las vulnerabilidades son descubiertas, se debe realizar actualizaciones en la red. Debido a que el número de nuevas amenazas se incrementa con el tiempo, el proceso debe ser continuo.

8.3.8 Fase 8: Retiro

Eventualmente, deben retirarse del diseño los sistemas que no logran los beneficios de mejora. La red, por ejemplo, que no puede ser mejorada para prevenir amenazas externas debe ser retirada. Es así que el ciclo natural del proceso retorna a la primera fase de requerimientos del sistema para reforzar la red y mantenerla controlada.

7.4. CICLO DE MANTENIMIENTO DE LA SEGURIDAD

El mantener un alto nivel de seguridad en la red requiere un ciclo continuo de esfuerzos que consiste en tres fases principales:

· Establecimiento de las políticas de seguridad que definen los objetivos de seguridad de la empresa.

· Implantación de tecnologías de seguridad en la red de una manera profunda y en partes, de manera que la empresa no deje sobre sólo un tipo de tecnología la solución de todos los problemas de seguridad.

· Auditar la red de forma recurrente para asegurar que las políticas de seguridad estén siendo aplicadas y reforzadas apropiadamente y que no se hayan desarrollado irregularidades mientras crece la red. Se deben utilizar los resultados de estas auditorias para modificar las políticas de seguridad e implementación de tecnología según se requiera.

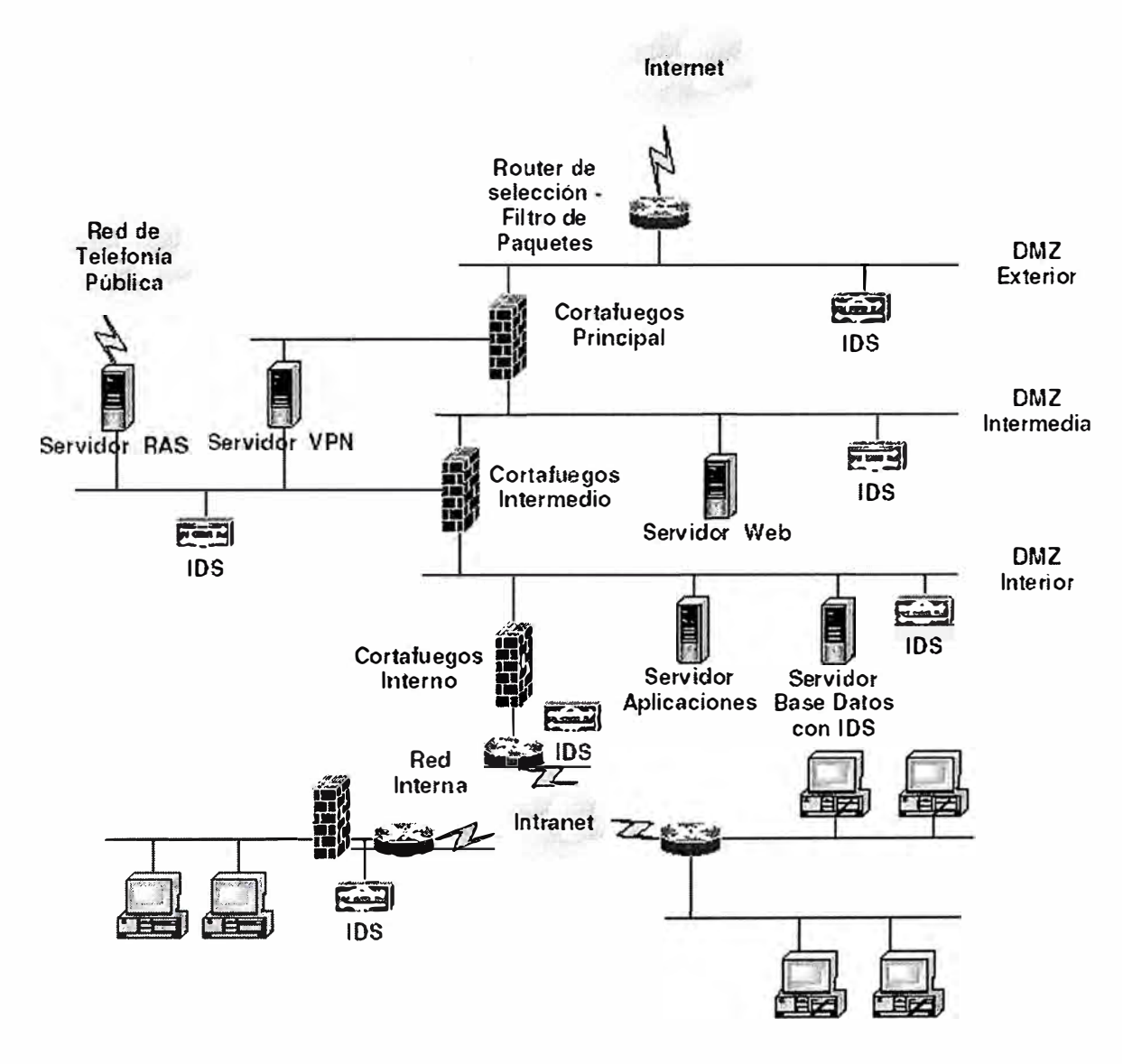


Figura 8.1 Ejemplo de diseño de una red segura

CONCLUSIONES

Entre las principales conclusiones que podemos obtener del presente informe se tienen:

1. En las redes de telecomunicaciones actuales, existe una serie de posibles ataques a la seguridad de las comunicaciones, entre los que destacan acceso no autorizado a recursos, modificación de mensajes o escuchas no autorizadas. Para contrarrestar estas amenazas es necesario ofrecer servicios de seguridad, que son los siguientes: autentificación, confidencialidad, control de acceso, integridad y no repudio.

2. La seguridad en IP (IPSec) tiene una arquitectura modular que brinda servicios independientes de autenticación y cifrado además posee una alta resistencia a estrategias de ataques, en la práctica se puede realizar distintas configuraciones que garantizan la calidad de servicios incluso servicios sensibles al tiempo como son voz y video.

3. La aplicación de Seguridad es indispensable en las redes públicas. IPSec tiene enfoque diferente a otros protocolos de seguridad más populares como SSH y SSL, que funcionan en la capa de transporte y están ligados con una aplicación particular. Con IPSec pueden establecerse comunicaciones seguras extremo a extremo, de forma flexible y bajo diversas configuraciones, sin importar la aplicación del nivel de usuario.

4. El Cortafuegos es uno de los elementos de seguridad más importantes para mantener nuestra red local aislada de los posibles ataques del exterior. Todo el tráfico exterior hacia nuestra red, debe pasar por dicho elemento, proporcionándose una seguridad casi ideal.

5. Las redes privadas virtuales son una solución real, barata y segura para las telecomunicaciones de las empresas actuales. Cada vez hay en el mercado más hardware y software para implementarlas y administrarlas, igual que aumenta el número de empresas que ofrecen estos servicios. La solución de VPNs está más orientada a grandes empresas que ha medianas o pequeñas ya que éstas dos últimas no suelen tener ni muchos trabajadores móviles, ni gran número de sucursales, menos aún repartidas por una amplia geografía y en la mayoría de los casos los datos que puedan intercambiar no serán de una importancia vital. En el futuro cercano, las empresas de todos los tamaños se comunicarán mediante Internet y realizarán contratos, operaciones compra-venta y otro tipo de transacciones económicas, con lo que la seguridad será muy importante y este tipo de redes se impondrá para poder utilizar Internet. Hasta entonces es una solución para empresas grandes o medianas en crecimiento.

6. La criptografía esta al alcance de la mano de todos, y cada vez es más fácil usarla e integrarla con aplicaciones ya existentes, sin tener complicaciones. Ante la inseguridad de un acceso ilimitado la criptografía es la solución única y fiable, que nos facilita el trabajo de cada día.

7. Los sistemas de detección de intrusión son elementos necesarios dentro de una red, sin embargo todavía existe la dificultad de configuración y operación que para un administrador de seguridad novato podría llegar a ser complicado.

ANEXO

ABREVIATURAS

ADSL	Asymmetric Digital Subscriber Line	Tecnología de Banda Ancha que permite el uso de la red de telefonía básica, transformándola en línea de alta velocidad, el término asimétrico se debe a que las velocidades para "downstream" y "upstream" son diferentes.
AH	Authentication Header	Protocolo de seguridad de tráfico utilizado para proveer servicios de integridad de datos y autenticación del origen de los datos
ATM	Asyncronous Tranfer Mode	Es una tecnología con conexiones dedicadas que organiza la información digital en celdas de 53 bytes que los transmite sobre el medio físico usando tecnología de señales digitales. Individualmente, una celda es procesada de forma asíncrona relativa a otras celdas y es encolada antes de ser multiplexado sobre la ruta de transmisión. Si bien la velocidades estándares son de 155.520 Mbps o 622.080 Mbps, las redes ATM pueden alcanzar velocidades de 10GBs.
BITS	Bump in the Stack	Implementación de IPSec a nivel de Sistemas Operativos, la cual trabaja insertando y extrayendo paquetes en la pila IP.
BITW	Bump in the Wire	Implementación de IPSec que usa un dispositivo externo para la encriptación.
CA	Certification Authority	Es una entidad o servicio que emite certificados.
CCA	Comercial Certificaction	Autoridad que emite certificados comerciales también conocidos como terceras partes seguras.

	Authority	
CERT	Computer Emergency Response Team	Equipo de Respuesta a Emergencias de Computadoras, conformado en su mayor parte por voluntarios expertos calificados con el único objetivo de brindar una respuesta rápida a los problemas de seguridad.
CHAP	Challenge Handshake Authentication Protocol	CHAP es ampliamente aceptado como estándar que usa el esquema usando el algoritmo MD5 de "hash" para encriptar la autenticación. Un esquema "hash" cambia la información de tal forma que sea único y no se puede retornar al formato original. Este protocolo no envía la contraseña actual por la red, en vez de esto, usa el mecanismo de orden-respuesta con el "hash" MD5 en forma unidireccional. CHAP usar tres verificaciones para proveer una autenticación encriptada. El equipo que autentica envía primero una cadena hacia el cliente. El cliente responde con un valor encriptado de la cadena que recibe. El equipo que autentica verifica el valor y aprueba la autenticación. CHAP periódicamente verifica la identidad del cliente. Este cambia la cadena cada cierto tiempo y elimina el mensaje, el cual lo protege contra los ataques "playback".
CPS	Certification Practice Statement	Es el documento en el que se detallan los procedimientos operativos sobre cómo ejecutar la política de seguridad y cómo aplicarla en la práctica.
CPU	Central Proccesing Unit	Parte de la computadora que controla todas las demás partes.
CRL	Certificate Revocation List	Listas publicadas por las autoridades de certificación donde se incluyen aquellos certificados que han sido revocados para que los clientes puedan comprobarlas.
DAP	Directory Access Protocol	Protocolo para el acceso a directorios con estándar X.500.
DES	Data Encryption Standard	Algoritmo de criptografía simétrica desarrollado por IBM en 1977 y adoptado por las oficinas gubernamentales estadounidenses para protección de datos.
DMZ	Demilitarized Zone	Zona Desmilitarizada, es la subred que se destina para ubicar ciertos servidores que brindaran servicios públicos.
DNS	Directory Name System	Protocolo que provee el servicio de traducción nombre a dirección IP para Internet. Existen servidores que brindan este servicio y traducen

		nombres del tipo x.y.z en direcciones IP, y viceversa.
DOI	Domain of Interpretation	Dominio de Interpretación de IPSec, son los parámetros que se negocian para establecer los canales seguros bajo políticas pre-establecidas.
DoS	Denial of Service	Ataque de negación de servicio, tiene como objetivo interrumpir el funcionamiento normal de un servicio de red impidiendo el uso o la gestión de recursos.
DQDB	Distributed Queue Dual Bus	Estándar de la IEEE para redes de área metropolitana.
DSA	Digital Signature Algorithm	Es un algoritmo estándar usado solo para la generación de certificados no puede ser usado para encriptación de datos.
DSS	Digital Signature Standard	Estándar que usa el algoritmo DSA como algoritmo de firma y el algoritmo SHA-1 para obtener el resumen del mensaje a encriptar.
EAP	Extensible Authentication Protocol	Es una extensión para el protocolo PPP, provee métodos de autenticación adicionales para usuarios RAS, tales como tarjetas inteligentes, Kerberos v5, y certificados. En forma similar a MS-CHAP, EAP es un protocolo de mutua autenticación, donde el cliente y el servidor verifica la identidad de cada uno. EAP abre la puerta a fabricantes de terceros para desarrollar esquemas de autenticación tales como el reconocimiento de voz, retina e identificación de huella digital.
EDI	Electronic Data Interchange	Estándar usado para la transferencia de información entre diferentes compañías en Internet, su uso se ha incrementado grandemente llegando a ser un importante mecanismo para las empresas de compra y venta de información.
ESP	Encapsulating Security Payload	Protocolo de seguridad de tráfico, además de proveer servicios de integridad de datos y autenticación del origen de los datos provee confidencialidad de datos.
FTP	File Transfer Protocol	Protocolo estándar para la transmisión de archivos, se considera inseguro debido a que transmite los datos de autenticación en texto claro por la red.
GRE	Generic Routing Encapsulation	Protocolo que realiza la encapsulación de un protocolo de red arbitrario sobre otro protocolo de red.
HSM	Host Security Module	Equipo de seguridad que provee funciones de criptografía para diferentes aplicaciones que requieran transacciones seguras.

ICMP	Internet Control Message Protocol	Es una extensión del Protocolo de Internet (IP) definido por el RFC 792. ICMP soporta paquetes conteniendo mensajes de error, control e información. Por ejemplo el comando PING, usa ICMP para diagnosticar la conectividad de una conexión a Internet.
ICV	Integrity Check Value	Parámetro que utiliza el protocolo AH para la verificación de integridad de la información.
IEEE	Institute of Electrical and Electronics Engineers	Instituto de Ingenieros Electrónicos y Eléctricos.
IETF	Internet Engineering Task Force	Grupo de personas que participa en el desarrollo de los estándares de Internet. La IETF está compuesta por más de 50 grupos de trabajo que desarrollan dichos estándares.
IDEA	International Data Encryption Algorithm	Algoritmo de criptografía simétrica que emplea llaves de 128 bits.
IDS	Intrusion Detection Systems	Sistemas automáticos de software o hardware que automatizan los procesos de monitoreo de eventos en una sistema de computadoras o red, analizando y buscando indicios de problemas de seguridad.
IKE	Interchange Key Exchange	Protocolo de manejo dinámico de llaves y asociaciones de seguridad (SA).
IPSec	IP Security Protocol	Es un conjunto de extensiones al protocolo IP. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad.
IPv4	IP version 4	Protocolo de la capa 3 versión 4
IPv6	IP version 6	Protocolo de la capa 3 versión 6
ISAKMP	Internet Security Association and Key	El protocolo ISAKMP esta definido en el RFC 2408. El cual prescribe los procedimientos para el formato de los paquetes para el establecimiento seguro, negociación, modificación y eliminación de la SAs y sus atributos, incluyendo llaves secretas. Provee una base para la implementación del manejo de llaves y es independiente de la generación de llaves, los protocolos de autenticación y encriptación y las definiciones de SA. ISAKMP puede ser implementado sobre la capa de transporte usando el puerto 500 udp conforme a lo indicado en el RFC.
ISP	Internet Service Provider	Proveedor de Servicios Internet.

ISO	International Organization for Standardization	Un grupo de estándares reconocido por la Unión Internacional de Telecomunicaciones de las Naciones Unidas y responsable de la promulgación de una variedad de estándares, incluyendo comunicación y procesamiento de datos.
ITSEC E2	Information Technology Security Evaluation Criteria Level 2	Estándar para evaluación de las características de seguridad de los sistemas de información o productos, examina y prueba para asegurar que trabajen correctamente y no muestren ninguna vulnerabilidad lógica. E2 significa nivel 2.
ITSEC E3	Information Technology Security Evaluation Criteria Level 3	Estándar para evaluación de las características de seguridad de los sistemas de información o productos, examina y prueba para asegurar que trabajen correctamente y no muestren ninguna vulnerabilidad lógica. E3 significa nivel 3.
ITU-T	International Telecommunications Union – Telecommunications Sector	Es uno de los tres sectores de ITU (International Telecommunication Union) Union Internacional de Telecomunicaciones cuya misión asegurar una eficiente producción de estándares (Recomendaciones) cubriendo todos los campos de las telecomunicaciones.
LAC	L2TP Access Concentrator	Dispositivo que físicamente termina una llamada L2TP.
LAN	Local Area Network	Una red de comunicación de datos con una extensión geográfica limitada, típicamente un solo edificio o un campus.
LDAP	Lightweight Directory Access Protocol	Protocolo diseñado para proveer a diversas aplicaciones una forma simple acceso de lectura/escritura a directorios X.500.
LNS	L2TP Network Server	Dispositivo que termina y autentica una sesión PPP.
L2F	Layer 2 Forwarding	Protocolo que soporta la creación de redes privadas virtuales (seguras) usando una línea serial sobre Internet.
L2TP	Layer 2 Tunneling Protocol	Protocolo que facilita el tunelaje de los paquetes PPP a través de una red de forma tal que sea lo mas transparente posible para los usuarios finales y para las aplicaciones.
MAN	Metropolitan Area Network	Red de comunicación de datos con una extensión geográfica que abarca una ciudad.
MD4	Message Digest Algorithm version 4	Algoritmo hash de un solo sentido desarrollados por los laboratorios RSA.
MD5	Message Digest	Algoritmo usado para la generación de

	Algorithm version 5	certificados digitales, procesa los mensajes de entrada en bloques de 512 bits y produce una salida de 128 bits.
MPPE	Microsoft Point to Point Encryption	Método de Encriptación propuesto por Microsoft para encriptar sesiones PPP. Usa el algoritmo RSA RC4 para proveer confidencialidad de la información.
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol	Es una versión propietaria de Microsoft del protocolo CHAP. Una ventaja de usar MS-CHAP es que al contrario de PAP y SPAP, este protocolo permite la encriptación de la información. La información se encriptará sobre el protocolo PPP o conexiones PPTP usando MPPE. Existen dos versiones MS-CHAP v1 y MS-CHAP v2. Una desventaja de MS-CHAP v1 es que soporta solo la autenticación unidireccional. Un cliente no puede determinar la autenticidad de 1 servidor RAS al cual se conectara. MS-CHAP v2 supera esta limitación permitiendo una autenticación mutua donde el cliente y el servidor pueden identificar el uno al otro.
NAS	Network Access Server	Servidor de Acceso Remoto a Red
NAT	Network Address Translation	Traslación de Direcciones de Red.
NIST	National Institute of Standards and Technology	Institución Norteamericana de Estándares y Tecnología, es una unidad del departamento de Comercio de EEUU. NIST promociona y mantiene estándares de medición. También tiene programas activos para asistencia a la industria y ciencia para el desarrollo y uso de nuevos estándares.
NNTP	Network News Transfer Protocol	Protocolo para la distribución, selección y consulta de nuevos artículos entre la comunidad de Internet. NNTP esta diseñado para que nuevos artículos sean almacenados en una base de datos centralizada, permitiendo al suscrito la selección de solo algunos que el necesite para leer. También se provee los servicios de indexación, referencias cruzadas y fechas de expiración de los mensajes.
NSA	National Security Agency	Es una organización estadounidense de criptología. Coordina directamente, y realiza actividades especializadas para proteger los sistemas de información de los EEUU, también

		produce inteligencia de información para otros países. Es una organización de alta tecnología, NSA esta en la vanguardia de las comunicaciones y procesamientos de datos. Es también uno de los centros de análisis de lenguas extranjeras e investigación del gobierno estadounidense.
NTP	Network Time Protocol	Protocolo que provee servicios de sincronización del tiempo.
OSI	Open System Interconnection	El área de ISO enfocada a los estándares de protocolos de comunicación de datos y sistemas distribuidos.
QoS	Quality of Service	Calidad de Servicio, es la capacidad de ofrecer uno o varios servicios de red sometidos a los criterios y acuerdos de calidad de la entidad receptora (basado en la Percepción Humana y/o Requerimientos Técnicos).
PAP	Password Authentication Protocol	PAP es el menos seguro de los protocolos de autenticación debido a que envía las contraseñas en texto claro. Generalmente, se debe usar este protocolo solo cuando intente conectar a Sistemas Operativos que no sea Windows que no soporten contraseñas encritadas o cuando se va a llamar a servidores SLIP, los cuales no soportan contraseñas encriptadas. Debido a que cualquiera que capture los paquetes de autenticación con un analizador de protocolos puede fácilmente leer las contraseñas que no están encriptadas, no se recomienda el uso de PAP.
PAT	Port Address Translation	Es una función facilitada por algunos ruteadores o cortafuegos los cuales permite a los equipos en una LAN comunicarse con el resto de la red (tal como Internet) sin revelar su verdadera dirección IP privada. Todos los paquetes salientes tienen su dirección IP traslada a la dirección IP externa del ruteador o cortafuegos. Los paquetes de respuesta hacia el ruteador o cortafuegos son trasladadas hacia el interior usando la dirección IP del equipo original.
PKCS7	Cryptographic Message Syntax Standard	Los estándares PKCS son un conjunto de protocolos estándares interfabricantes para hacer posible el intercambio seguro de información usando una infraestructura de clave publica. Estos estándares incluyen encriptación RSA, encriptación basada en contraseñas, sintaxis de certificado extendido y sintaxis de mensajes

		encriptados por S/MIME, el estándar propuesto para mensajería segura. Los estándares fueron desarrollados por los laboratorios RSA en cooperación de un consorcio que incluyo a Apple, Microsoft, DEC, Lotus, Sun, and MIT.
PKCS10	Certification Request Syntax Standard	Estándar que define la forma como deben realizarse los requerimientos al CA.
PKCS11	Cryptographic Token Interface Standard	Este estándar especifica una API (Application Programming Interface) llamada "Cryptoki"para dispositivos que almacenar información criptográfica y realizan funciones criptográficas.
PKI	Public Key Infrastructure	La infraestructura de clave publica habilita a los usuarios de una red insegura tal como Internet para asegurar el intercambio de información y dinero de forma privada a través del uso de un par de llaves criptográficas la publica y la privada que es obtenida y compartida a través de la autoridad de confianza, La infraestructura de clave publica proporciona un certificado digital que puede identificar de forma individual o de forma organizacional, en servicios de directorio que puedan almacenar y cuando sea necesario revoca los certificados.
PGP	Pretty Good Privacy	Es un programa popular para encriptar y desencritar correo electrónico en Internet. También puede ser usado para enviar una firma digital encriptada que permita al receptor verificar la identidad del que envía y conoce que el mensaje no fue cambiado en el camino. Esta disponible ya se como software gratuito y en versión comercial de bajo costo, PGP es un programa que es ampliamente usado para asegurar privacidad individual y también usado por muchas empresas. Desarrollado por Philip R. Zimmermann en 1991, PGP ha llegado a ser un estándar de facto para asegurar el correo electrónico. PGP también puede ser usado para encriptar archivos y luego ser almacenados para que sean ilegibles para otros usuarios o intrusos.
PMTU	Protocol Maximum Transfer Unit	Es la unidad de paquete o frame más grande, especificado en octetos, que puede ser enviado en una red basada en paquetes o frames tal como Internet. El TCP usa el MTU para determinar el máximo tamaño de cada paquete en cada trasmisión.
PoP	Point of	Es un punto de acceso a Internet. Una PoP

	Presence	necesariamente tienen una única dirección IP. Un proveedor de servicio Internet tiene un punto de presencia en Internet o probablemente mas de uno. Un PoP puede residir actualmente en un espacio arrendado por una empresa de telecomunicaciones al cual esta conectado el ISP. Un PoP usualmente incluye ruteadores, agregadores análogo/digitales, servidores, y frecuentemente switches frame relay o ATM.
PPP	Point to Point Protocol	Es un protocolo para comunicación entre dos computadoras usando la interfase serial, provee servicio en la capa 2 OSI.
PPTP	Point to Point Tunneling Protocol	Protocolo que permite encapsular paquetes PPP en datagramas IP para transmitirlos en una red IP como Internet. Es un protocolo que permite a empresas extender su red corporativa a través de túneles privados sobre redes publicas como Internet.
RA	Registration Authority	Una autoridad de registro en una red es la que verifica los requerimientos para certificados digitales y le indica a la autoridad de certificación que los procese. Las RAs son parte de la infraestructura de clave publica.
RAS	Remote Access Server	Servidor de Acceso Remoto.
RDSI	Red Digital de Servicios Integrados	Es un conjunto de estándares de la ITU para transmisión digital sobre líneas Telefónica de cobre así como de otros medios. Integra ambos, voz y datos juntos con información digital sobre la misma red. Existen dos niveles de servicio: BRI (Basic Rate Interface), dirigido a usuario de empresas pequeña y usuarios en sus hogares y el PRI (Primary Rate Interface), para empresas grandes. Ambos incluyen un numero de canales B y canales D. Cada canal B transporta datos, voz y otros servicios. Cada canal D transporta información de control y señalización. El BRI consiste de 2 canales B de 64 Kbps y un canal D de 16 Kbps asi como el BRI puede tener velocidades hasta 128 Kbps. EL PRI consiste de 23 canales B y un canal D de 64 Kbps en EEUU y 30 Canales B y 1 canal D en Europa.
RRAS	Routing and Remote Access Services	Servicio de Ruteo y Acceso Remoto, usado en productos Microsoft.
RFC	Request for	Es un documento formal de la IETF que es

	Comments	resulto por el comité encargado y seguido de la revisión de las partes interesadas. Algunos RFCs son de naturaleza informativa, estos son propuestos para llegar a ser estándares, la versión final de un RFC llega a ser estándar y no se permite otros comentarios o cambios. Los cambios pueden ocurrir, ya sea a través de subsecuentes RFCs que se elabora en conjunto de las partes previas de RFCs.
RSA	Rivest - Shamir – Adleman	El algoritmo de criptografía asimétrica más ampliamente conocido y patentado en Estados Unidos. Se utiliza para firmas digitales y distribución de llaves. Fue inventado en 1977 por Ron Rivest, Adi Shamir, y Leonard Adleman (RSA).
SA	Security Association	Es el contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los protocolos a utilizar, las transformaciones, las llaves y la duración de validez de dichas llaves.
SADB	Security Association Database	Es la base de datos donde son almacenadas las SAs.
SET	Secure Electronic Transaction	En un sistema para asegurar las transacciones financieras en Internet. Fue soportados inicialmente por Mastercard, Visa, Microsoft, Netscape, y otros. Con SET, un usuario entrega una billetera electrónica (certificado digital) y la transacción es conducida y verificada usando una combinación de los certificados y firma digitales entre el comprador, el vendedor y el banco del comprado de forma tal que se asegure la privacidad y confidencialidad. SET hace uso de SSL de Netscape, el STT (Secure Transaction Tecnology) de Microsoft y protocolo http seguro. SET usa algunas veces pero no todos los aspectos de una infraestructura de clave publica.
SHA-1	Secure Hash Algorithm Version 1	Un algoritmo no criptográfico que aplica una función hash de un solo sentido, fue diseñado para ser expresamente utilizado en DSA/DSS.
SKEME	Secure Key Exchange Mechanism for Internet	Es un protocolo para el intercambio de llaves, define un tipo de intercambio de llaves autenticados en el cual las partes hacen uso de encriptación publica de llaves para autenticar el uno al otro y compartir los componentes del intercambio.

SLIP	Serial Line Internet Protocol	Protocolo que provee la facilidad de transportar trafico TCP/IP sobre líneas seriales, tales como línea telefónica, entre dos computadoras.
SMTP	Simple Mail Transfer Protocol	Protocolo estándar para la transmisión de mensajes de correo electrónico.
SNMP	Simple Network Management Protocol	Es el protocolo para gestión de red y monitoreo de dispositivos de red y sus funciones.
SPAP	Shiva – Password Authentication Protocol	Es una versión propietaria de PAP, ofrece un poco mas de seguridad que PAP ya que tiene un mecanismo de encriptación reversible. Alguno que capture los paquetes de autenticación no podrá leer la contraseña SPAP, pero este protocolo es susceptible de ataque "playback" (por ejemplo, un intruso que grabe el intercambio y reproduce el mensaje de vuelta para ganar acceso no autorizado). Los ataques "playback" son posible debido a que SPAP siempre usa un método de encriptación reversible para enviar las contraseñas por la red.
SPI	Security Parameter Index	Es una parámetro de 32 bits que identifica de manera única una SA.
SPD	Security Policy Database	Es la base de datos de las políticas de seguridad, la cual es indexada por seleccionadores.
SSH	Secure Shell	Es una interface basada en Unix y protocolo para asegurar el ingreso remoto a una computadora. SSH es actualmente un conjunto de tres utilitarios slogin, ssh y scp que son versiones seguras de herramientas antiguas rlogin, rsh, y rcp. Los comandos SSH son encriptados y aseguradas de diversas formas. Ambos en cliente y servidor son autenticadas usando un certificado digital y las contraseñas son protegidas siendo encriptadas. SSH usa criptografía de clave publica para ambos, autenticación y conexión. Los algoritmos de encriptación incluidos son Blowfish, DES, e IDEA. IDEA es por defecto.
SSL	Secure Socket Layer	Es un protocolo usado comúnmente para gestionar la seguridad de la transmisión de mensajes en Internet. Fue desarrollado por Netscape, SSL usa sistema de encriptación de llave publica y privada de RSA el cual también incluye el uso de un certificado digital. SSL ha sido recientemente sucedido por TLS (Transport Layer Security) el cual es basado en SSL. SSL

		usa una capa de programa entre el protocolo HTTP y la capas TCP.
TCP	Transmission Control Protocol	Protocolo de transporte orientado a conexión utilizado en Internet y utilizado por muchas aplicaciones como: Telnet, FTP, SMTP y HTTP para establecer comunicaciones confiables.
TTL	Time To Live	Es el valor en un paquete de Protocolo IP que indica al ruteador cuando o no descartar el paquete. El valor incial del TTL es configurado por el origen por defecto y cada ruteador que recibe el paquete sustrae uno del campo TTL, cuando la cuenta llega a cero, el ruteador lo detecta, descarta el paquete y envia un mensaje ICMP de regreso al sistema originador.
TOS	Type of Service	Dentro del esquema de QoS (Calidad de servicio) es un campo de 8 bit con valores de 0 a 15 que son asignados para manejar de forma especial el trafico (por ejemplo, minimizar el retardo, maximizar el uso de la red).
TTP	Trusted Third Party	Es un sistema de confianza en una tercera parte que se encarga de certificar las claves públicas. También se le conoce como autoridad de certificación (CA).
UDP	User Datagram Protocol	Es un protocolo no orientado a conexión, es usado por aplicaciones de red que desean salvar el tiempo de procesamiento debido a que ellas envían unidades de información pequeñas para intercambio. UDP al igual que TCP trabajan en la capa de Transporte (capa 4 OSI).
VPN	Virtual Private Network	Una VPN trabaja usando una infraestructura publica compartida mientras se mantiene la privacidad a través de procedimientos y protocolos de tunelaje. Estos protocolos encriptan la información para enviarla y luego lo desencriptan al final en la recepción, enviando la información a través del túnel y no se puede ingresar otra información que no sea apropiadamente encriptada.
WWW	World Wide Web	La definición técnica es: Todos los recursos y usuarios de Internet que están usando el protocolo HTTP.
X.509	Estándar recomendado por ITU para el uso de certificados digitales	Es el mas amplio estándar para la definición de certificados digitales El X.509 es una recomendación del ITU, lo cual significa que no tiene aun un definición y aprobación. Como resultado, las compañías han implementado el estándar en diferentes formas. Por ejemplo

		ambos Netscape y Microsoft usan certificados X.509 para implementar SSL en sus exploradores de internet. Pero un certificado X.509 certificado generado por Netscape no puede ser leible por productos Microsoft y viceversa.
3DES	Triple Data Encryption Standard	Algoritmo para encriptación de información, es una mejora al algoritmo DES, usa tres estados del algoritmo DES con tres llaves por separado de 56 bits, la longitud total de la llave 3DES es de 168 bits.

BIBLIOGRAFÍA

1. Stallings, "Comunicaciones y Redes de Computadores", Editorial Pearson, 2000.
2. Tanenbaum, "Redes de Computadoras", Editorial Pearson, 3ra edición 1997.
3. Kent & Atkinson, RFC2401 "Security Architecture for the Internet Protocol", 1998.
4. Kent & Atkinson, RFC2402 "IP Authentication Header", 1998
5. Kent & Atkinson, RFC2406 "IP Encapsulation Security Payload (ESP)", 1998.
6. IP Security Protocol Working Group, EITF. http://www.ietf.org/html.charters/ipsec-charter.html.
7. Varios, "PPTP". http://www.microsoft.com.
8. Varios, "L2TP". http://www.cisco.com.
9. Varios, "SSH". http://www.ssh.com, http://www.openssh.org.
10. Wack, Cuttler & Pole, "Guidelines on Firewalls and Firewalls Policy", NIST Special Publication 2002
11. Varios, "Check Point Firewall-1". http://www.checkpoint.com.

12. Varios, "Firewalls & Perimeter Security", http://www.sans.org.

13. Varios, "IDS", http://www.iss.net.

14. Bace&Mell, "Intrusión Detection Systems". NIST Special Publication 2001.

15. Kuhn, Hu, Polk & Chang, " Introduction to Public Key Technology and the Federal PKI Infrastructure". NIST Special Publication 2001.

16. Varios, "PKI Solutions", http://www.rsasecurity.com.

17. Zimmerman, "Secure Infrastructure Design" http://www.cert.org.

18. Varios, "SAFE", http://www.cisco.com.