UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

POLÍTICAS DE SEGURIDAD EN INTRANET

T E S I S

QUE PARA OBTENER EL TITULO DE INGENIERO EN COMPUTACIÓN

P R E S E N T A :

SAÚL LORA ANAYA

DIRECTORA DE TESIS:
ING. GLORIA GUADALUPE MARTÍNEZ ROSAS

MÉXICO, D. F., ENERO DE 2010

Dedicatoria

Yo, sólo seguí los pasos por los que sabía
que la constancia, y el deseo de seguir
me llevarían hasta el fin del camino.

Tú, trazaste un sendero por el cual tus
pasos fueron nuevos, y en tu andar
la esperanza y fortaleza te permitieron seguir.

Con mucho cariño a mi hermana Erika,

porque no tengo más palabras para agradecer tú apoyo,

y todo lo que tú eres.

¡ Gracias a nombre de todos !

Índice

ÍNDICE

Introducción

INTRODUCCIÓN

Uno de los aspectos más importantes en el ámbito de las redes de computadoras es la seguridad, ya que de otro modo carecería de sentido el disponer de una red que no brinde el más mínimo rasgo de seguridad en los servicios con que cuenta.

El problema que se presenta al hablar de seguridad es muy grande y extenso debido a la forma, complejidad y variedad de ataques que se pueden presentar y a la manera en que han ido evolucionando, convirtiéndose hoy por hoy en una potencial amenaza difícil de combatir.

El contar con procedimientos de uso y manejo establecidos dentro de la red de manera táctica y lógica, y con la ayuda de herramientas de software y hardware, permiten implementar políticas de seguridad que nos ayudan a proteger, mantener y desarrollar redes seguras.

El tocar este tema de la seguridad nos lleva a la realización del presente trabajo que por la dimensión y complejidad que se presenta al abordarlo se ha acotado en su extensión más no en su contenido, ya que las redes privadas; Intranets, son una representación a escala de un universo más grande de redes: Internet, heredando así casi todas sus características y problemáticas. Y que en la actualidad son el pilar de cualquier empresa u organización que desee permanecer presente compitiendo por ofrecer mejores servicios y productos.

De esta forma nos adentraremos a analizar y plantear un sistema de seguridad que se adapte a las necesidades más comunes en Intranet, basado en políticas que nos ayuden a asegurar la información que viaja a través de esta, ofreciendo la integridad, confidencialidad y aseguramiento necesarios de este activo tan importante; como son los datos, del que se desea resguardar su valor intrínseco.

El análisis y exposición de los temas se hacen en dos vertientes para facilitar su comprensión, las cuales convergen en los métodos y aplicaciones de seguridad propuestas.

Por un lado se presenta el carácter técnico de los protocolos de comunicación TCP/IP, en los que se basa una Intranet, mostrando los aspectos más sobresalientes e importantes de su diseño, así como el factor de riesgo y vulnerabilidad inherentes a éstos. Además del uso de otros protocolos aplicados a la seguridad sobre este modelo de comunicación.

Por otra parte están los procedimientos y herramientas de software y hardware aplicados a la seguridad en los sistemas de comunicación mostrados, en base a los estándares internacionales más utilizados, disminuyendo los riesgos y vulnerabilidades, contribuyendo al uso y administración de recursos, de tal forma que una vez que se entiende la necesidad de contar con sistemas de seguridad, se muestran los métodos para prevenir y contrarrestar los posibles ataques.

En el primer capítulo se da un panorama general sobre las políticas de seguridad y su importancia, así como la forma que seguirán a lo largo de todos los capítulos. Todo esto aterrizado al campo de acción sobre el que se llevarán a cabo: Intranets.

Después en el segundo capítulo, defino y propongo las recomendaciones necesarias para prevenir el uso de software “malicioso” (malware) en sus distintas formas, además de medidas de seguridad físicas para el hardware y administración de archivos.

Una vez vistos los aspectos más relevantes a tratar fuera del ámbito de los protocolos de comunicación, en el tercer capítulo empezamos a introducirnos al mundo de las comunicaciones bajo el modelo TCP/IP, para tratar de entender el lenguaje que utilizan los distintos dispositivos que intervienen en el proceso de

comunicación en los sistemas basados en esta tecnología, y con base en esto poder entender por que existen “agujeros en la seguridad” y las técnicas de ataque más utilizadas, mostrando el beneficio que brindan los sistemas criptográficos en este aspecto.

En el cuarto capítulo hago referencia a los mecanismos de control de acceso a la red, aplicados a los diferentes tipos de usuarios y dispositivos que se presentan en los sistemas distribuidos, con base en los métodos de identificación y autenticación para los miembros de la red y subredes que la conforman.

Ya para el quinto capítulo se tienen los conceptos suficientes para explicar y utilizar un dispositivo de seguridad basado en tecnología UTM (Administración Unificada de Amenazas), con el que se aterrizan y aclaran varios de estos conceptos.

En el sexto y último capítulo resalto la importancia que tiene Internet como red mundial de comunicación y algunas de las aplicaciones más utilizadas, sin perder de vista el objetivo general de la seguridad, junto con algunas otras recomendaciones.

De esta forma se pretende el análisis, exposición y comprensión de estos temas, con la finalidad de generar una herramienta de apoyo para todos aquellos administradores de redes cuya responsabilidad es la de mantener y dar soporte a estos sistemas, sin perder nunca de vista la seguridad y operatividad necesarias a seguir, que garanticen las aplicaciones y servicios necesarios que se amolden a las necesidades particulares de cada red.

Capítulo 1

Panorama General e Importancia de las Políticas de Seguridad

CAPÍTULO 1 PANORAMA GENERAL E IMPORTANCIA DE LAS POLÍTICAS DE SEGURIDAD

1.1 ANTECEDENTES

Hoy por hoy los activos de una compañía u organización dependen principalmente del uso de la información que necesitan diariamente manejar, la globalización y automatización de servicios son puntos clave que nos llevan a utilizar tecnologías cada vez más sofisticadas.

Desde la aparición de la computadora personal hasta nuestros días se ha dado un enorme salto y hoy es casi imprescindible para cualquier tipo de empresa el uso de ésta para la movilización de datos. Y no hablamos sólo de una computadora, hablamos de varias, desde unas cuantas, hasta cientos y pueden llegar a ser miles, las que se conectan entre sí formando redes: Intranets, cuya finalidad es compartir toda clase de recursos, donde cada computadora actúa como una puerta al interior que nos permite penetrar de manera fácil y rápida a la información.

Actualmente podemos conocer el interior de una empresa gracias a estas puertas, es tan similar como cuando abrimos la puerta de una casa y en primera instancia podemos tener un panorama general de la organización y ubicación de cada lugar reservado dentro de ésta, el patio, la sala, la cocina, etc. Y cuando entramos y recorremos cuidadosamente cada uno de estos lugares, podemos ver con más detalle lo que hay particularmente en cada uno de ellos, pero no podemos así tan fácil entrar a cualquier casa como tampoco permitimos que entren a la nuestra porque lo que hay dentro es de valor para nosotros y no dejamos que alguien más llegue y se lo pueda llevar, lo pueda tomar o maltratar y para evitarlo implementamos medidas de seguridad como el poner chapas a las puertas, protecciones a las ventanas, cámaras de circuito cerrado, alarmas y toda clase de herramientas que nos permitan brindar seguridad a nuestros bienes. Inclusive

puede haber lugares en donde sólo nosotros podemos tener acceso y otros miembros de la casa no.

Pues de la misma forma una red de computadoras necesita ser resguardada y vigilada para evitar que alguien quiera entrar sin autorización; esto es, cuando el ataque proviene del exterior, o inclusive cuando se hace mal uso de los recursos; cuando el ataque viene del interior y pueda extraer, borrar o cambiar información lo cual pueda significar cuantiosas pérdidas para la organización.

El problema de una Intranet es que aunque es una red privada y bien definida no está exenta de ataques, ya que los más comunes provienen del interior de la red por los mismos usuarios y esto puede ser debido a tres causas principalmente:

1 Ignorancia
2 Negligencia
3 Malicia

A la par que los sistemas computacionales y las tecnologías evolucionan, los tipos de ataques también han ido evolucionando y perfeccionando, tanto, que inclusive hacen uso de estas mismas tecnologías para poder perpetuar sus actos y en muchos de los casos ni siquiera ser descubiertos ni dejar rastro.

Al inicio de la revolución tecnológica y el desarrollo de grandes redes de computadoras, los ataques internos consistían sólo en ataques físicos o aprovecharse de los permisos para obtener o alterar información y los externos en averiguar una clave válida.

En la actualidad los ataques operan contra la lógica operativa de todo el sistema tratando de encontrar y explotar vulnerabilidades en los programas, algoritmos de cifrado, protocolos, así como denegar los servicios que se prestan, pudiendo tomar control completo de los sistemas.

Son éstas y otras tantas las causas por lo cual es necesario establecer reglas de seguridad a manera de evitar posibles ataques a la red ya sea de forma consciente o inconsciente.

Pero antes de entrar de lleno al campo de la seguridad, tenemos que definir las características propias de una Intranet, ya que es en este terreno donde se aplicarán las políticas y por tal motivo debemos establecer nuestro punto de partida.

1.1.1 INTRANETS

Una Intranet es una red privada que se distingue de otras redes porque se apoya en el protocolo de comunicación TCP/IP (Transfer Control Protocol / Internet Protocol) que engloba a varios protocolos diferentes y se denominan a menudo “protocolos de Internet”, aunque pueda o no estar conectada a esta gran red, así que una Intranet puede considerarse como una reproducción a escala de Internet, administrada separadamente y configurada para cumplir políticas de seguridad local. La configuración de la red es responsabilidad de la empresa u organización a la que pertenece y puede ir desde una sola LAN (Local Area Network – Red de Área Local) en un único sitio, hasta un conjunto de éstas conectadas entre sí ubicadas en distintos sitios, separadas incluso por países.

El protocolo TCP/IP se encuentra estratificado en capas que se corresponden con el estándar de los protocolos de comunicaciones OSI (Open System Interconnection) diseñados por la Organización Internacional de Estandarización (ISO).

TCP/IP por sí mismo es independiente del estrato físico, aunque los protocolos más comunes que se utilizan en este nivel son el 802.3 del IEEE (llamado comúnmente Ethernet) y el X.25.

Los protocolos IP y TCP corresponden a las capas tres (Red) y cuatro (Transporte) del modelo OSI respectivamente, como se muestra en la figura 1.1. El primero se encarga del envío y recepción de paquetes por la red y el segundo se asegura de que los paquetes de datos lleguen a su destino ya que es un protocolo orientado a conexión.

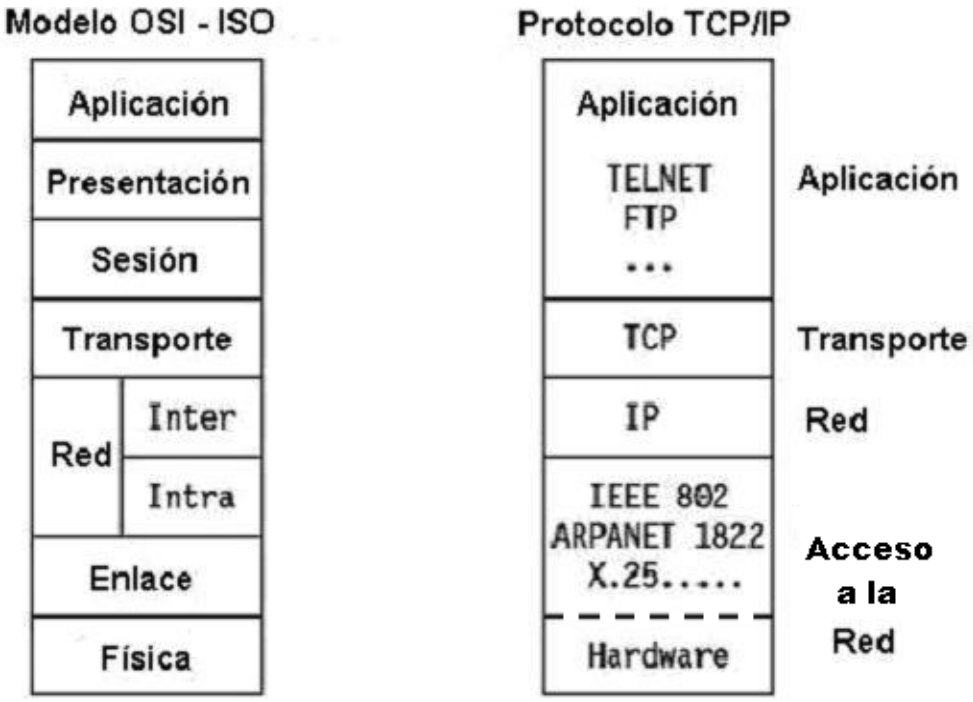


Figura 1.1 Analogía entre el modelo OSI y el protocolo TCP/IP

Es ésta una característica que hace que una Intranet sea vulnerable ya que el protocolo es en sí mismo una herramienta potencial de explotar y vulnerar, ya que sólo hace falta tener un conocimiento técnico básico para hacerlo.

Al ser Intranet una red basada en TCP/IP puede ofrecer los mismos servicios que Internet: FTP, HTTP, SMTP, TELNET, SNMP, NFS... Por tal motivo se debe asegurar que cada uno de estos servicios sea seguro y confiable.

Debemos tener presente que el concepto de red no está ligado al cableado utilizado para la comunicación entre los equipos, sino a la dirección IP que se le

asigna a un dispositivo y que identifica la red a la que pertenece. De tal modo que podemos tener varias redes dentro del mismo cableado pero solamente los equipos que pertenezcan a una misma red podrán comunicarse, de tal modo que una dirección IP no puede ser asignada dos veces dentro de una misma red.

Hay dos tipos de direcciones IP: públicas y privadas. Un dispositivo con IP pública es visible desde cualquier otro equipo que esté conectado a Internet, y las IP privadas son exclusivas dentro de las empresas u organizaciones. Estos equipos no pueden accederse desde Internet pero sí pueden salir a Internet por medio de un router o proxy que tenga una IP pública.

Las direcciones IP están formadas por números de 4 bytes y se representan de la forma a.b.c.d, donde cada letra es un número entre 0 y 255. Las direcciones se dividen en dos partes: el identificador para red y el identificador para host. De tal modo que hay tres tipos de direcciones: primarias (clase A, clase B y clase C), de grupo (clase D) y las reservadas que no se pueden utilizar actualmente (clase E). Como se muestra en las figuras 1.2 y 1.3.

Figura 1.2 Clases de direcciones IP

Clase	Formato (red-host)	Número de Redes	Número de Hosts X Red	Rango de Direcciones	Máscara de Subred
A	r.h.h.h	128	16,777,214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	r.r.h.h	16,384	65,534	128.0.0.0 - 191.255.0.0	255.255.0.0
C	r.r.r.h	2,097,152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	grupo	-	-	224.0.0.0 - 239.255.255.255	-
E	no permitidas	-	-	240.0.0.0 - 255.255.255.255	-

Figura 1.3 Rango de direcciones IP

Pero sólo algunas de estas direcciones IP están reservadas para redes privadas como se observa en la figura 1.4.

Clase	Rango de direcciones para redes privadas
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

Figura 1.4 Direcciones IP privadas

A excepción de las direcciones IP especiales (broadcast, loopback, indicador de red, etc.) y reservadas, el resto de las direcciones de las clases A, B y C, pertenecen a Internet.

Como ejemplo tenemos las figura 1.5 donde observamos una red privada conectada a Internet con direcciones IP públicas que van de la 194.143.17.8 a 194.143.17.13 (la dirección 194.143.17.8 es la dirección de red y la 194.143.17.13 es de broadcasting) donde se conectan 3 servidores (web, correo y proxy) y un router que da salida al resto de Internet. Y en la parte interna (privada) de la red, la dirección 192.168.1.0 donde se conectan 20 equipos y el servidor proxy.

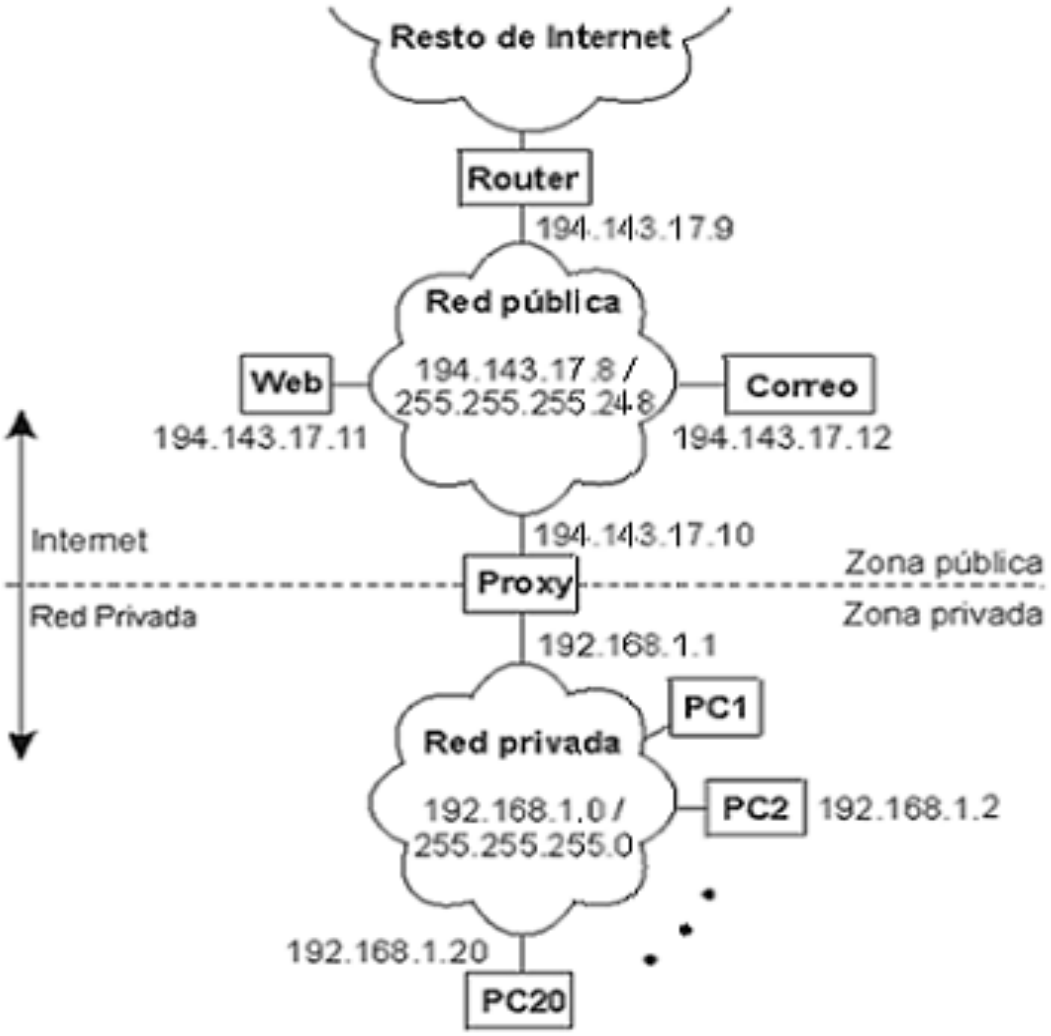


Figura 1.5 Red privada conectada a Internet

1.2 METODOLOGÍA PARA EL DESARROLLO DE LAS POLÍTICAS

Los problemas de seguridad en una red son cuantiosos y en ocasiones difíciles de detectar y corregir por la complejidad que en sí misma la red representa. No obstante, brindar la mayor seguridad es un reto para el administrador, ya que implica una organización bien estructurada en todos los niveles y alcances de la red y un constante esfuerzo por alcanzar esta meta.

Para ello es necesario implementar políticas de seguridad que brinden la mayor protección posible a la red tanto en sus componentes físicos como a la información que viaja en ella, permitiendo el envío seguro de datos entre usuarios y dispositivos, registrando los cambios o alteraciones en la red que pudieran resultar en una posible amenaza.

Cualquier tarea relacionada con la seguridad que pretenda formalizarse debe contemplar tres aspectos fundamentales:

1 Qué: lo que se quiere lograr o cumplir, (lo que hay que proteger).
2 Quién: responsable de que se cumpla, (encargado de realizarla).
3 Cómo: actividades para lograr el objetivo, (lo que hay que hacer).

Una política de seguridad debe permitir establecer las necesidades y medidas de protección que una organización necesita, de tal modo que describe qué tipo de gestión de seguridad se pretende lograr y cuáles son sus objetivos. Para ello es necesario determinar cuatro fases en la vida de una política:

1 Desarrollo: La política es creada, revisada y aprobada.
2 Implementación: Se pone en práctica, y se da a conocer.
3 Mantenimiento: Garantizar el cumplimiento (monitorear) y actualizar.
4 Eliminación: Por qué se cambia de tecnología o es reemplazada.

Las políticas de seguridad pueden apoyarse en otros documentos que sirvan para materializar los principios y objetivos de seguridad que se pretenden lograr. Estos documentos pueden ser: las normas, procedimientos, instrucciones técnicas y políticas de uso.

1.2.1 PROCEDIMIENTOS

Un procedimiento de seguridad establece las actividades o tareas detalladas en el desempeño de un proceso de seguridad, así como la, o las personas responsables de su ejecución.

Describe una serie de pasos a seguir en la ejecución de una actividad determinada, en los cuales se contempla cumplir con una norma o garantizar que mediante estas medidas se cubran aspectos de seguridad que se pretenden establecer. Un procedimiento debe ser claro y detallado para que sea fácil de interpretar. Un procedimiento no tiene que ser extenso ya que son las especificaciones pormenorizadas a ejecutar.

Los procedimientos pueden dividirse en tres grupos: de prevención, de detección y de recuperación. Los procedimientos de prevención aumentan la seguridad de la red en condiciones normales de funcionamiento previniendo la ocurrencia de violaciones en la seguridad, un ejemplo es la encriptación en la transmisión de datos. Los procedimientos de detección nos ayudan a detectar violaciones a la seguridad, un ejemplo son los programas de monitoreo o auditoría. Y por último los procedimientos de recuperación que nos ayudan a retornar el funcionamiento correcto del sistema una vez que se ha perpetrado una violación a la seguridad.

Aunque estos tres tipos de procedimientos son importantes, es claro que es más conveniente enfatizar y dar más atención a los mecanismos de prevención y detección, ya que evitar o detectar una violación a la seguridad es mucho mejor y menos comprometedor que restaurar el sistema, por eso haremos más hincapié en estos tipos de procedimientos.

Los procedimientos más comunes de prevención son:

1 **De identificación y autentificación.** Se basan en la identificación de entidades pertenecientes al sistema para saber si dicha entidad (usuario, programa, dispositivo, etc.) se reconoce dentro de la red, y una vez hecha la identificación, autenticarlas, para comprobar que dicha entidad es en realidad quien dice ser.

2 **De control de acceso.** Todo recurso dentro de la red ha de estar protegido mediante mecanismos de control de acceso para protegerlos de cualquier entidad que quiera acceder a ellos.

3 **De separación de objetos.** Los objetos con niveles distintos de seguridad deben evitar el flujo de información entre ellos a menos que exista una autorización del mecanismo de control de acceso, quedando agrupados los objetos dentro de niveles de seguridad distintos. Esta separación puede dividirse en cinco grupos: física, temporal, lógica, criptográfica y de fragmentación.

4 **De seguridad en las comunicaciones.** Consiste en proteger la integridad y la privacidad de los datos cuando viajan por la red, la mayoría de estos mecanismos se basan en la criptografía.

5 **De uso.** Se especifican las prácticas adecuadas sobre el uso y manejo de los equipos, sistemas o tecnologías, a manera de establecer una regulación en cuanto al uso de éstos por los usuarios. Deben documentarse las normas de comportamiento que los usuarios deben seguir en el uso de los recursos, considerando los usos autorizados y no autorizados.

En estos procedimientos se plasma de manera clara y concreta las decisiones hechas en materia de seguridad por parte de la organización con la finalidad de ser utilizadas por todos sus miembros como medidas de

protección para saber qué hacer con la información y los recursos del sistema.

1.2.2 INSTRUCCIONES TÉCNICAS

Las instrucciones técnicas de seguridad son las acciones necesarias para completar y llevar a cabo un procedimiento en particular dentro del sistema. Deben ser claras y detalladas, de tal forma que la persona que las ejecute no tenga que decidir sobre algún aspecto en el desarrollo de ésta. A mayor detalle, mayor garantía y precisión en su ejecución.

Generalmente este tipo de instrucciones están orientadas al uso y configuración de herramientas de software y hardware que permiten cubrir los aspectos específicos dentro de un procedimiento, dicho de otro modo, son los ingredientes que forman un procedimiento.

Para este tipo de instrucciones es necesario contar con manuales técnicos de los dispositivos a utilizar y/o configurar, manuales para la instalación de programas, asesoramiento y todo tipo de información que nos brinde un marco de referencia claro para poder empezar a documentar paso a paso las instrucciones y requerimientos necesarios para completar un procedimiento de seguridad, encaminado a resolver un problema específico dentro de una política de seguridad.

1.2.3 NORMAS

Una norma de seguridad define de manera concreta lo que hay que proteger, y bajo qué ambiente o situación específica se hace. Las normas se agrupan en diferentes áreas dependiendo el tipo de alcance que se pretenda obtener en cuanto a seguridad: normas de seguridad física, de seguridad en la información,

de control de acceso, etc. Una norma debe ser clara y no ambigua en su interpretación.

La Organización Internacional de Estandarización (ISO – International Organization for Standardization), y la Comisión Electrotécnica Internacional, han reservado la serie ISO/IEC 27000 para la seguridad de la información. Aunque la serie no se ha completado aún, se encuentran publicadas las normas:

ISO/IEC 27001:2005. Especifica los requisitos para la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en el ciclo de Deming (Plan-Do-Check-Act), la cual es certificable.

ISO/IEC 27002:2005. A partir del 2007, es el nuevo nombre de ISO 17799:2005, manteniendo su año de edición. Es un Código de buenas prácticas para la Gestión de la Seguridad de la Información. No es certificable.

ISO/IEC 27005:2008. Ayuda a la aplicación de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO/IEC 27006:2007. Requisitos para la acreditación de entidades de auditoría y certificación en Sistemas de Gestión de Seguridad de la Información.

Cabe mencionar que la serie ISO/IEC 27033 en fase de desarrollo y fecha de publicación prevista para el 2010 y 2011. Es una norma enfocada a redes que consiste de siete partes:

1 Gestión de seguridad en redes.
2 Arquitectura de seguridad en redes.
3 Referencia de redes.
4 Aseguramiento de las comunicaciones entre redes con Gateways.

5 Acceso remoto

6 Aseguramiento de comunicaciones en redes mediante VPNs.

7 Diseño e implementación de seguridad en redes.

Proviene de la ampliación, revisión y renumeración de la norma ISO 18028. Sólo algunas empresas especialistas en seguridad de la información pueden otorgar estos certificados una vez que la empresa u organización que se va a certificar es auditada y aprobada según los estándares aplicados.

Este proceso implica una inversión y cambios en el modo de funcionamiento pero que al final es redituable. Por ejemplo, un banco que ha sido certificado puede garantizar a sus clientes que cuando efectúan transacciones por Internet se hacen bajo un mínimo riesgo.

1.3 IMPLEMENTACIÓN

Cuando una política es creada, revisada y aprobada, el siguiente paso es la implementación. La implementación de las políticas de seguridad es un proceso técnico administrativo, a través del cual se utilizan herramientas de software y hardware que permiten cubrir los aspectos técnicos necesarios que den a la política un carácter práctico de uso. Eso es por un lado, y por el otro hay que difundir y dar a conocer dichas políticas a todos los miembros de la organización, los cuales deben acatarlas sin exclusión alguna, cabe mencionar que para esto es necesario el apoyo del sector directivo de la organización, para que de esta forma sea más sencillo llegar a todos los usuarios.

Dicho de otra forma la implementación es el acto de poner en práctica todos esos procedimientos y normas en que se basan las políticas de seguridad aplicadas a las entidades u objetos que se observaron era necesario resguardar en la fase de desarrollo de la política.

La información y capacitación del personal son puntos clave en la implementación de las medidas de seguridad, ya que finalmente son éstos los usuarios para los cuales se crean las políticas. También es necesario recabar información e interactuar con los usuarios de forma regular para que se tomen decisiones acordes a las necesidades de seguridad que se requieran, ya que de este modo sabremos y podremos detectar más fácilmente alguna falla en los sistemas debido al contacto directo que tenemos con ellos. De este modo tendremos un mayor control y conocimiento del funcionamiento de la red evitando en muchas ocasiones llegar al usuario sólo cuando levanta un reporte de fallas o hace una solicitud de servicio.

El implementar políticas de seguridad en la red no es sólo ponerlas en práctica y evitar que dejemos de preocuparnos o dejemos de trabajar en aspectos de seguridad. El siguiente paso es el mantenimiento donde se contemplan tareas como la actualización de programas, pruebas en los componentes de la red (cables, interfases de red, etc.), monitoreo de las cargas de trabajo, rendimiento y tiempo de respuesta, etc. Todo esto con la finalidad de tener un mayor control sobre la red y cuando sea necesario reestablecer el sistema de manera parcial o total debido a una falla técnica o de seguridad.

Hay dos aspectos que tenemos que contemplar al momento de una falla en la red: minimizar el impacto y qué debemos hacer cuando suceden. El objetivo después de una interrupción en el servicio es devolver el sistema a su estado de operación normal lo más pronto posible. Cuando se diseña la red se logran reducir los puntos posibles de falla, y donde existan o se crea que hay estos puntos si es económicamente viable y la situación es crítica, se debe contar con equipo de respaldo para afrontar este tipo de situaciones, un ejemplo sería el servidor de archivos perteneciente a un banco donde la situación se complica si se llegaran a perder datos o llegase a fallar el servidor, ya que el término “respaldo” engloba también este tipo de aspectos.

Capítulo 2

Seguridad de Software y Hardware

CAPÍTULO 2 SEGURIDAD DE SOFTWARE Y HARDWARE

2.1 INSTALACIÓN Y USO DE PROGRAMAS

Una de las bases más importantes en los sistemas de cómputo son los programas, ya que la parte del software es más importante para el administrador o el usuario que el hardware en sí, y aunque existe una relación de interdependencia entre ambos (“sin hardware no hay software”, y que no discutiremos), los programas son más fáciles de acceder y permiten un entorno de trabajo más amigable para el uso de los equipos y dispositivos.

Para ejemplificar lo anterior podemos pensar en dos computadoras con las mismas características técnicas (marca, modelo, memoria, procesador, etc.) pero con distintos sistemas operativos instalados provocando que la capacidad, funcionamiento, rendimiento y utilización de recursos en cada máquina dependa del sistema operativo en particular, además de que el usuario o administrador contará con las herramientas propias que le proporcione dicho sistema para mejorar o disminuir el desempeño de sus tareas.

Por tal motivo, es necesario que la primera regla para el software que utilicemos en nuestra red sea que esté perfectamente catalogado para saber qué programas se ejecutan en cada máquina y quién, o quiénes los utilizan para que de este modo sea posible tener una imagen escrita del equipo en cuestión. Esta medida es necesaria en caso de tener que restaurar los programas del equipo parcial o completamente y mantener un historial o antecedente como información de respaldo.

Debemos tener cuidado con los programas que instalamos sobre todo cuando provienen de fuentes no reconocidas o de dudosa procedencia ya que existen dos aspectos que tenemos que cuidar y tener en mente en cuanto a seguridad de software: “malware”, denominación que se le da a un conjunto de programas cuya

finalidad es violar la seguridad de los sistemas de manera hostil y desapercibida, y “bugs” o errores en los programas que son inherentes a la programación.

2.1.1 MALWARE

Este tipo de programas son creados con la intención de atacar la seguridad de los sistemas y es necesaria una buena concienciación por parte de los usuarios para evitar en la medida de lo posible ejecutar programas desconocidos sin previa consulta al administrador, ya que la propagación de estos programas es muy rápida y se corre el riesgo de afectar a toda la red. Los más comunes son:

1 **Virus:** la palabra virus utilizada en informática es una curiosa analogía, ya que en realidad proviene del acrónimo: “Vital Information Resources Under Siege” (recursos de información vital bajo acoso) y se trata de un código que se inserta en un fichero ejecutable capaz de reproducirse a sí mismo y modificarse. No es un programa independiente ya que necesita un programa donde hospedarse.

2 **Gusanos:** programas capaces de viajar a través de las redes cuya finalidad es alcanzar un equipo y una vez hecho instalar un virus, atacar como lo haría un intruso o consumir ancho de banda y recursos de la red en cuestión y seguir viajando.

3 **Conejos:** programas cuya característica es su auto reproducción de forma exponencial hasta que la cantidad de recursos (memoria, procesador, disco, etc..) son insuficientes llevando al sistema a la negación de servicios quedando inhabilitada.

4 **Caballos de Troya:** son programas capaces de engañar al usuario ya que mientras se piensa que realizan alguna función útil se está

ejecutando simultáneamente una aplicación dañina para el sistema sin que el usuario se percate de este evento.

5 **Bombas lógicas:** parecidos a los caballos de Troya sólo que éstos se ejecutan bajo ciertas condiciones específicas como una determinada fecha, la creación de un archivo con cierto nombre dado o un número determinado de ejecuciones del mismo programa que contiene la bomba lógica.

6 **Túneles:** se trata de un canal de comunicación que no forma parte del diseño original y que viola las políticas de seguridad entre un proceso receptor y un emisor para intercambiar información; sólo existen en sistemas con seguridad de tipo multinivel.

7 **Puertas traseras:** son programas que se utilizan para brincar los métodos usuales de autenticación que se utilizan para ejecutar una aplicación.

2.1.2 BUGS

Este tipo de problemas surgen a la hora de programar ya que es casi imposible no equivocarse dentro de miles de líneas de código y debido a esta situación hay programas que se crean para aprovechar esta vulnerabilidad en los sistemas y atacar.

Ya sea que se pueda presentar en una aplicación sencilla o en el mismo sistema operativo lo cual implica un grave riesgo, pero este tipo de errores existe y hay que cuidar. Uno de los más comunes por ejemplo, es el de “buffer overflow” o “stack smashing” desbordamiento de pila, el cual mediante una aplicación en C es posible desbordar la pila generando una violación de segmento sobrescribiendo la dirección de retorno. El problema radica en que si hacemos que esta nueva

dirección no sea aleatoria sino que apunte a la dirección de un programa en concreto provocando que se ejecute (en unix y en linux cuando alguien ejecuta un programa SUID o SGID lo hace con los privilegios de quien los creó y si éstos fueron creados por root, el atacante podría ejecutar un shell con estos privilegios).
Después de ver que existen programas capaces de dañar o poner en riesgo la integridad de la información y de los equipos como lo es el malware, o aprovechando errores en los programas; como lo son los bugs, es necesario tomar medidas para proteger nuestra red, independientemente de los programas antivirus y antiespía que existen y que se deben instalar en los equipos de la red, es necesario tomar medidas más contundentes que prevengan una intervención de este tipo.

2.1.3 VIRTUALIZACIÓN COMO MEDIDA DE PREVENCIÓN

Es conveniente que si se va a hacer algún cambio o instalación por vez primera de algún programa, sobre todo cuando dicho cambio involucra a varios equipos pertenecientes a una subred de nuestra Intranet, es conveniente probarlo anteriormente durante algún tiempo para comprobar su funcionamiento y cerciorarnos de que se ejecuta adecuadamente sin alterar el estado actual de la red.

Para ello será necesario contar con un equipo denominado “equipo piloto”, a través del cual probaremos previamente el software que deseemos instalar o reemplazar. La técnica recomendada es implementar en dicho equipo una máquina virtual (VM, “Virtual Machine”) creada a través de software, ya que permite gran flexibilidad y compatibilidad pero sobre todo aísla los procesos que se ejecutan sobre el espacio que ocupa la máquina virtual sin repercutir en el resto del sistema encapsulando los riesgos que se pudieran producir al ejecutar algún programa desconocido que contenga malware o bugs. Podemos citar cuatro ventajas para utilizar virtualización:

1 **Aislamiento.** Un fallo en una aplicación o máquina virtual afecta sólo a esa máquina virtual y no al resto de las máquinas virtuales o del sistema.

2 **Seguridad.** Cada máquina cuenta con clave de acceso independiente, por lo tanto, un ataque de seguridad a una máquina virtual sólo afecta a esa máquina.

3 **Flexibilidad.** Se pueden crear máquinas virtuales con las características de hardware que especifiquemos a través del monitor de la máquina virtual sin necesidad de comprar más equipo.

4 **Facilidad.** La creación de una máquina virtual es sencilla y nos permite convivir de manera separada con distintos sistemas operativos en un solo equipo físico sin tener que particionar el disco duro. De tal forma que si deseamos probar una aplicación dentro de un sistema operativo en particular sólo basta con ejecutar la máquina virtual que contiene a dicho sistema operativo.

Hay dos caminos para virtualizar y de ello depende la abstracción de la máquina virtual: instalar la máquina virtual directamente sobre el hardware como sistema operativo, o instalar la máquina virtual sobre un sistema operativo denominado “host”, como lo muestra la figura 2.1.

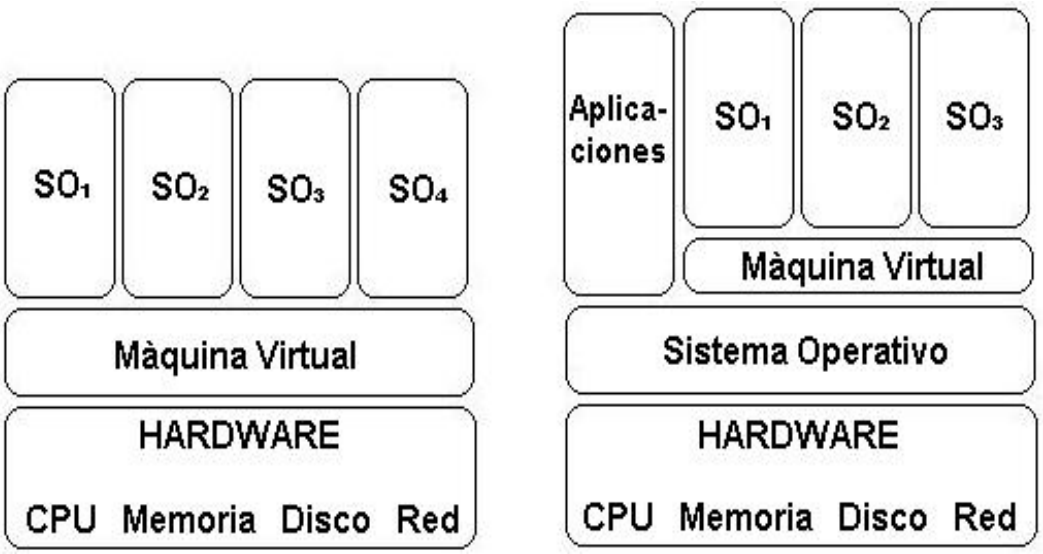


Figura 2.1 Abstracción de la máquina virtual

En este caso que sólo necesitamos la máquina virtual para probar programas y no para hacer aplicaciones más robustas hacemos la instalación sobre un sistema operativo ya instalado; host, y montaremos otro o varios sistemas operativos más sobre la máquina virtual dependiendo de los recursos que disponga la máquina que usaremos como piloto y las necesidades que se requieran satisfacer.

Las características de la máquina que usaremos como piloto deberán satisfacer las siguientes necesidades:

1 Procesador Pentium III (700 MHz o más recomendado).

2 La memoria RAM se calculará a partir de la necesaria para el sistema operativo “host”, la máquina virtual y el o los sistemas operativos virtuales que se instalen.

3 Disco duro de 20 GB, para brindarle a cada sistema operativo espacio suficiente (la máquina virtual requiere menos de 500 MB).

4 Adaptador ethernet.

El software que necesitaremos es el siguiente:

1 Sistema operativo host, que puede ser cualquier versión de windows o linux que satisfaga nuestras necesidades.

2 Programa de virtualización; en este caso VMware Server 1.0.4.

3 Sistema o sistemas operativos para ser instalados en la máquina virtual (windows o linux).

El programa VMware Server es una aplicación fácil de instalar ya que utiliza un menú de ventanas que nos van guiando a través del proceso como se muestra en la figura 2.2, y nos permite instalarlo sobre plataforma windows o linux en cualquiera de sus versiones.

Figura 2.2 Instalación de VMware Server

Ya una vez instalado en nuestro equipo piloto nos permite montar sistemas operativos en forma virtual y conectarnos de manera local o remota ya que está diseñado para trabajar en el ambiente cliente-servidor lo que le da un punto más a su favor. El programa nos ofrece una interfaz amigable y un menú a través de su consola mediante el cual podemos crear las siguientes aplicaciones:

1 Crear una máquina virtual para instalar un sistema operativo.

2 Abrir una máquina virtual existente.

3 Conectarnos con otro servidor VMware y abrir una máquina virtual en forma remota.

4 Configurar el servidor VMware que tenemos instalado en nuestro equipo, como se observa en la figura 2.3.

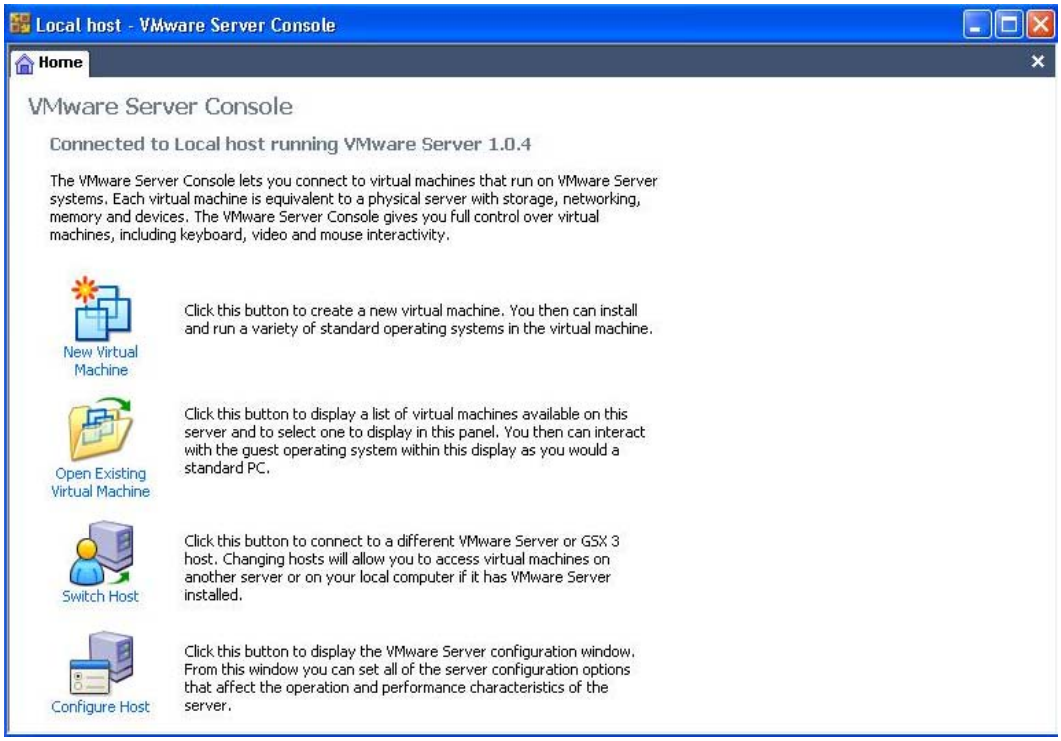


Figura 2.3 Consola de VMware Server

El proceso para instalar el sistema operativo que hayamos elegido montar sobre la máquina virtual es el mismo que haríamos habitualmente sobre el disco duro o cualquier partición de éste. En este aspecto VMware Server tiene un mayor margen de aplicación ya que permite instalar sistemas operativos Windows y linux en cualquiera de sus versiones y también algunas versiones de Novell y Solaris, como se ve en la figura 2.4.

Figura 2.4 Instalación de Sistema Operativo en VMware Server

Una vez que tengamos trabajando nuestro sistema operativo en la máquina virtual podremos probar cualquier tipo de software que queramos ya sea que lo instalemos desde un disco o de Internet sin el mayor riesgo a comprometer otros equipos o recursos de la Intranet.

2.2 SEGURIDAD FÍSICA Y MANEJO DE EQUIPOS

La seguridad física y el manejo de los equipos es un aspecto que en ocasiones queda olvidado y que hay que tener en cuenta, ya que toda medida de seguridad en los servicios y aplicaciones que se brinden en la Intranet queda neutralizada si por ejemplo, el atacante pudiera filtrarse hasta el centro de control y acceder físicamente a los sistemas, ésta sería una situación verdaderamente peligrosa para la red toda vez que un atacante opte por preferir una vulnerabilidad física a una lógica. Los motivos pueden ser muchos desde robar equipo como lo puede ser un simple mouse (para venderlo o utilizarlo), hasta acceder a la información confidencial que hay en el sistema (como una cinta de backup o disco duro).

Por tal motivo he destinado este apartado dentro del presente trabajo para definir las medidas de seguridad básicas para proteger los recursos físicos de la red, esto con la finalidad de brindar seguridad a los equipos de la Intranet.

En este aspecto se pueden implementar dichas medidas como procedimientos de control de acceso físico a las diferentes áreas de la organización, esquematizadas como una serie de cuatro círculos concéntricos que forman estratos de protección donde la seguridad aumenta a medida que nos acercamos al centro del círculo más interior, y en donde el área de cada círculo es directamente proporcional al número de personas que se pueden alojar en cada uno de estos círculos.

Cada uno de los cuatro estratos define los diferentes tipos de áreas físicas que se deben proteger para mantener el hardware de la red seguro mediante mecanismos de control de acceso. Figura 2.5.

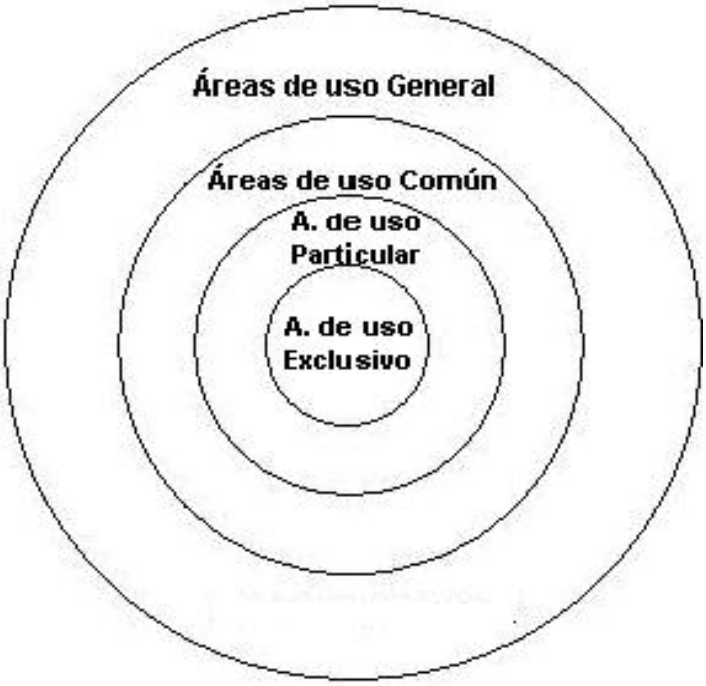


Figura 2.5 Estratos de seguridad física

La descripción de cada una de estas áreas es la siguiente:

1 **Áreas de uso general.** Son los lugares que el personal interno y externo comparten, generalmente son áreas de recepción, pasillos, salas de espera, etc., y el riesgo no es muy grande ya que los equipos se encuentran generalmente lejos de estas áreas.

2 **Áreas de uso común.** Son lugares donde el personal interno se agrupa en función de las actividades que desarrolla. En estos lugares es donde se encuentra a la mayoría del personal de la organización y el riesgo es medianamente alto ya que existe contacto directo con los equipos por parte del personal interno y ocasionalmente con el personal externo, aunque el tipo de información que se maneja en este estrato no es muy relevante. Este tipo de áreas generalmente

están agrupadas en departamentos (compras, contabilidad, recursos humanos, etc.).

3 **Áreas de uso particular**. En estos lugares se sitúa el personal con alto rango o jerarquía como lo son directores, gerentes, coordinadores, responsables de área, etc., y generalmente se trata de oficinas privadas. En estas áreas existe poco personal pero el riesgo es alto ya que los equipos e información que manejan son exclusivos e importantes.

4 **Áreas de uso exclusivo**. Estas son áreas dedicadas a resguardar los sistemas e información crítica del sistema, como servidores, cintas de respaldo, switches, routers, bases de datos, etc. Generalmente estos lugares forman parte del departamento de cómputo donde la seguridad debe ser máxima ya que el riesgo es muy alto debido al equipo tan costoso que se maneja ya que aquí se concentra toda la información crítica de la red y de la empresa u organización y cuyo mecanismo de control de acceso debe permitir sólo la entrada a él, o a los administrador(es), y/o al personal que él designe.

2.2.1 CONTROL DE ACCESO PARA ÁREAS DE USO GENERAL

Para este tipo de áreas que regularmente son espacios abiertos dentro de la organización o empresa y de mucha concurrencia, bastará con aplicar medidas de seguridad comúnmente típicas:

1 Llevar un registro de entradas que permita identificar al personal externo a la organización que se encuentra dentro de las instalaciones justificando su presencia. Inclusive aplicar esta medida

al personal interno cuando exista la necesidad de entrar en horarios o días que están fuera de sus labores

2 Contar con cámaras de vigilancia alrededor de estos lugares que permitan el monitoreo constante.

3 Si existe equipo de cómputo de uso público en estas áreas será necesario protegerlo (sobre todo de vandalismos), dejando al alcance del usuario sólo los elementos necesarios para utilizarlo. En la actualidad es muy común y recomendable que se utilicen pantallas inteligentes o táctiles para estos fines.

4 No dejar cables de red sueltos ni a la vista o tomas de red olvidadas en algún rincón.

Estas sencillas medidas pueden prevenir y ayudar en mucho a la seguridad en estas áreas ya que en muchas ocasiones basta con utilizar el sentido común para aplicarlas y que el atacante note que existe un control y una preocupación por la seguridad por parte de la organización que hagan que decline su interés, porque en la mayoría de los casos se trata de ataques casuales propiciados por las circunstancias y la facilidad que se presenta para ejecutarlos.

2.2.2 CONTROL DE ACCESO PARA ÁREAS DE USO COMÚN

Estas áreas generalmente están divididas en departamentos donde encontramos a la mayoría de usuarios de la organización y por tal motivo los accesos deben ser más restringidos. Las medidas recomendadas son las siguientes:

1 Concienciar al usuario de la responsabilidad que debe asumir por el equipo que está utilizando y sancionar cualquier alteración, avería o

pérdida del mismo por acciones que éste emprenda sin previa consulta al administrador o encargado.

2 Los accesos a estos lugares son controlados mediante chapas de seguridad y uno o varios responsables pertenecientes a la misma área encargados de abrir y cerrar el lugar.

3 Verificar cotidianamente el estado de los equipos de cada área y anotar en una bitácora la información que se recabe.

4 El personal ajeno a estás áreas; ya sea interno o externo, deberá mantenerse al margen de los equipos y la información.

2.2.3 CONTROL DE ACCESO PARA ÁREAS DE USO PARTICULAR

Por tratarse de áreas donde la información y equipos que se utilizan son más delicados se debe tener cuidado con el personal autorizado a estos lugares implantando mecanismos de control de acceso que brinden mayor seguridad y que permitan recabar información o alertar de la entrada y salida a estas áreas. Este mecanismo puede implantarse de la siguiente forma:

1 Si las condiciones técnicas y requerimientos de la organización ameritan utilizar características biométricas de él, o los usuarios, autorizados a permanecer en determinada área se puede llevar a cabo. La más común es la huella digital.

2 Utilizar lectores de tarjetas o lectores de códigos de barra en las puertas que al momento que el usuario desliza su tarjeta o código de barras a través del lector se verifica en la base de datos la existencia de dicho usuario y los lugares a los que tiene permitido acceder. El inconveniente de este sistema surge cuando un usuario olvida o

extravía su tarjeta sin percatarse inmediatamente de ello quedando expuesta a que alguien más la tome.

3 Utilizar puertas con sistema de claves de acceso; que ya es muy común encontrar actualmente, y su funcionamiento es similar que los lectores del punto anterior.

4 Otra medida en caso de no aplicar las anteriores es colocar sensores en las puertas con lo que se enviaría una señal alertando al administrador del área o personal de vigilancia cuando un usuario entra o sale. Este sistema se pude hacer más extensivo inclusive a áreas en otros niveles ya que su implantación es más económica.

En este estrato los mecanismos de seguridad dependerán en gran medida del valor de los activos que la organización haya fijado en estas áreas y de las facilidades técnicas y geográficas para implementarlas. De tal modo que la implantación de las medidas de seguridad quedarán sujetas al estudio de estos factores.

2.2.4 CONTROL DE ACCESO PARA ÁREAS DE USO EXCLUSIVO

Por tratarse del área más importante de la red desde el punto de vista técnico-administrativo, la implantación de medidas de seguridad alcanzan su nivel máximo en esta área. Los mecanismos de seguridad en este nivel dependerán de la distribución geográfica que se tenga del área y la cantidad de recursos que se deban proteger implementado una serie de medidas basadas en la utilización de algunos de los métodos citados anteriormente o la combinación de ellos, aún así es recomendable asumir las siguientes reglas:

1 Utilizar dos controles de acceso: uno para el área en general del departamento de cómputo y otro para el área exclusiva de él, o los

administradores; utilizada generalmente para acceder a los sistemas críticos de la red como servidores.

2 Mantener la temperatura adecuada para los equipos y revisar periódicamente el estado de las instalaciones donde éste se encuentra.

3 La configuración y cambios en los equipos se deberá hacer por el administrador o bajo la supervisión o instrucción del mismo, algo que siempre resulta práctico y muy importante es consultar los manuales.

4 Cualquier violación a la seguridad o alteración en los equipos deberá ser atendida inmediatamente y emprender las acciones necesarias para corregirlas y sancionar, si es el caso, al responsable.

Son muchas las amenazas al hardware, pero también son muchas y muy variadas las soluciones que podemos asumir dependiendo de las necesidades de cada organización y de cada área, tomando en cuenta que el costo de estos mecanismos de seguridad nunca deben ser más caros que lo que queremos proteger, porque de lo contrario estaríamos en un error y lejos de convertirse en buena una inversión para la organización, se convertiría en una pérdida para la misma.

Por último, no hay que pasar por alto que normas y hábitos tan elementales como cerrar las puertas con llave al salir, no prestar equipo sin previa consulta o autorización, mantener limpio el lugar donde se encuentran los equipos, son necesarias y en muchas ocasiones suficientes para evitar ataques y daños al hardware.

2.3 SEGURIDAD DE ARCHIVOS

Anteriormente la información que una organización o empresa generaba estaba depositada en papel ya que era la única fuente de almacenamiento disponible. Estos documentos eran resguardados y organizados en archivos, de tal modo que era preciso llevar un control de seguridad para toda esta cantidad de papeles a manera de mantener la integridad de la información que en ellos se encontraba. Estas medidas de seguridad consistían en evitar la pérdida, robo, alteración, manipulación y todas aquellas actividades que conllevan a cambiar el estado en que se encuentra la información dentro de estos archivos dañándolos y atentando en contra de su prevalencia, repercutiendo en la operatividad de los procesos que dependen de estos datos dentro de la organización.

En la actualidad el uso del papel ha sido sustituido por medios de almacenamiento mucho más sofisticados desde la aparición de la computadora. Estos medios de almacenamiento van desde cintas magnéticas, discos duros, cd´s, usb´s, blu-ray, etc., hasta clusters y arreglos más estructurados que permiten una gran capacidad de almacenamiento de datos y facilidad de manejo.

Pero aunque los medios de almacenamiento han cambiado sigue siendo necesario utilizar medidas de seguridad que permitan mantener la integridad de la información y de los archivos que es, a final de cuentas, el medio lógico que permite la agrupación de la información de manera ordenada para ser leída, modificada, o transportada según se necesite. Pero no se trata sólo de mantener resguardada toda esa pila de información sea cual sea el dispositivo elegido, sino además evitar pérdidas de información cuando se encuentra en tránsito y que aún no ha sido guardada ya que la susceptibilidad de una falla en el sistema es inevitable e impredecible.

Por tal motivo una organización que maneje información de valor crítico, y no sólo eso sino que requiera mantener la información del sistema al día, deberá contar

con un sistema de respaldo de archivos que brinde la protección necesaria ante la pérdida de información y brinde el soporte necesario para recuperarse ante situaciones de fallo.

Mantener copias de seguridad o “back-up”, es un proceso de respaldo de archivos que se utiliza para guardar información creando imágenes exactas de los discos de los servidores, bases de datos, aplicaciones, archivos, etc., que sirven para la restauración total o parcial de información ya sea desde el mismo equipo donde se realice el back-up o en otro, para migrar servicios a otros equipos, o clonar la imagen de un servidor en otros evitando la instalación del sistema operativo, programas y actualizaciones en cada uno de ellos.

2.3.1 MODELOS DE ALMACENAMIENTO DE ARCHIVOS PARA BACK UP

Las técnicas que se utilizan para organizar la información y establecer los criterios con base en un modelo que permitan el almacenamiento de las copias de seguridad pueden ser las siguientes:

1 **Desestructurado.** Es la forma más fácil pero menos efectiva ya que sólo consiste en hacer copias en algún dispositivo de almacenamiento (p.e. cd´s), con información mínima del sistema o datos que se pretendan guardar.

2 **Completo.** Se hace una copia completa de la información cada que se active el proceso de respaldo. El inconveniente es el tiempo que tarda y la cantidad de espacio que se requiere.

3 **Incremental.** Se basa en hacer varias copias sobre la misma fuente de información que se desea guardar. Una vez que hacemos una copia completa de la información en un instante dado, posteriormente se

realizan copias sólo de los archivos o ficheros nuevos o modificados ya sea de manera completa o redundante de forma incremental, ya que podemos hacer una copia incremental sobre otra ya existente. La restauración del sistema consiste en obtener una copia completa de la información y las copias incrementales posteriores a la fecha o instante que se desea recuperar la información. La ventaja de este modelo es la rapidez para efectuar las copias de respaldo, su desventaja es que el número de copias incrementales pude ser muy grande.

4 **Diferencial.** Consiste en hacer una copia completa de la información y generar copias de los ficheros o archivos que han sido creados o modificados pero siempre a partir de la última copia completa, la última copia diferencial sustituye a la anterior la cual puede guardarse en un proceso incremental inverso. Su ventaja es que para restaurar el sistema sólo se necesita la última copia completa del sistema que se haya efectuada y la última copia diferencial, la desventaja es que el proceso de respaldo es lento debido a que la copia diferencial va aumentando de tamaño.

Para ilustrar lo anterior podemos pensar que un día “X” hacemos una copia completa del sistema (Xc), sí el día siguiente, es decir X+1, hacemos una copia incremental (X+1i), sólo se copian las modificaciones hechas a la copia Xc, y al siguiente día, es decir X+2, volvemos a hacer otra copia incremental (x+2i), sólo se copian las modificaciones hechas a la copia X+1i, y no a la Xc, de tal forma que la restauración completa del sistema consiste en tomar la última copia completa y las incrementales:

Restauración Completa Incremental = Xc + X+1i + X+2i

Si decidiéramos hacer lo mismo pero ahora utilizando el método diferencial el día X+1 tendríamos una copia diferencial (X+1d) con las modificaciones de los

archivos o ficheros a partir del día X que es la fecha de la última copia completa (Xc), y el día X+2 tendríamos una copia diferencial (X+2d), con las modificaciones a partir de la última copia completa (Xc) también, de tal forma que las copias diferenciales reflejan los cambios desde un mismo punto fijo en el tiempo, lo que permite que una copia diferencial nueva sustituya a la anterior, con lo que en realidad tenemos una copia actual del sistema separada en la última copia completa del sistema (Xc) y la ultima copia diferencial (X+2d). Con lo que obtenemos la siguiente deducción:

Restauración Completa Diferencial = Xc + X+2d

2.3.2 APLICACIÓN DEL MODELO INCREMENTAL-DIFERENCIAL CON ACRONIS IMAGE SERVER

Como ya vimos, la necesidad de respaldar la información que manejamos en una red es indispensable independientemente de las necesidades particulares que tengamos que satisfacer como: volumen de información a respaldar, frecuencia del proceso de respaldo, tiempo de recuperación, plataforma, sistema de archivos y medios de almacenamiento compatibles, etc., de tal modo que hemos buscado una solución integral que se adapte a las necesidades de la red y a las políticas de administración, brindando un entorno seguro y transparente.

Acronis Image Server en su versión Enterprise 9.0, es un sistema de recuperación, clonación y respaldo de archivos basado en los modelos incremental-diferencial, para una plataforma heterogénea de servidores físicos, de red, virtuales y autónomos basados en Windows y linux, que permite movilidad de la información. Con esta herramienta podemos programar las tareas de respaldo en determinados momentos o eventos, o inclusive personalizarlos con la creación de comandos.

Este sistema es compatible con la mayoría de los dispositivos de almacenamiento utilizados: unidades de disco duro, almacenamiento en red NAS y SAN, bibliotecas de cintas, cargadores automáticos, cintas SCSI, controladoras IDE y SCSI RAID, usb, cd, dvd, pc card y fire wire (IEEE 1394). Además reconoce la mayoría de archivos y los que no son copiados sector a sector.

2.3.3 COMPONENTES Y REQUISITOS DEL SISTEMA PARA INSTALAR ACRONIS IMAGE SERVER

La instalación del programa se hace a través de una interfaz gráfica que muestra los seis diferentes componentes con que cuenta el sistema y que se pueden instalar, tal como se muestra en la figura 2.6. Cada uno de los componentes se instala por separado iniciando por Acronis License Server y todos se incluyen en el mismo kit de instalación.

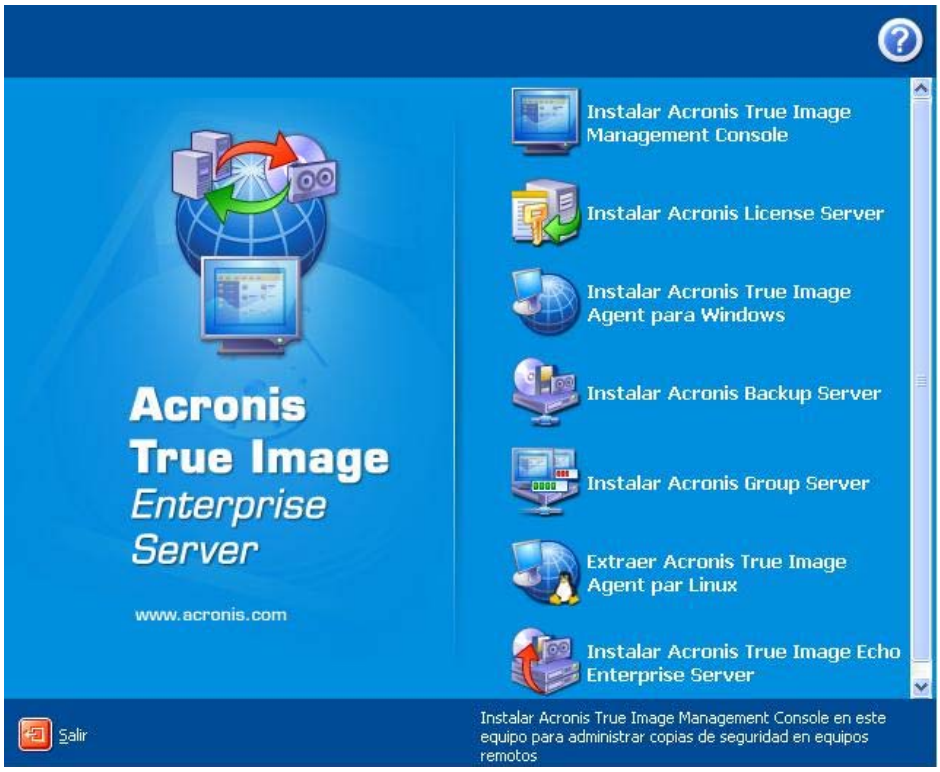


Figura 2.6 Menú de Instalación de Acronis Image Server

Los componentes se adaptan a las necesidades más comunes de respaldo que se necesitan en una Intranet, y son:

1 **Management Console.** Esta es una consola de acceso remoto que permite al administrador la instalación, configuración y control de los componentes instalados en otros equipos vía remota.

2 **Agent para Windows.** Es la aplicación tipo cliente para los equipos que se acceden vía remota bajo ambiente windows.

3 **Agent para Linux.** Es la aplicación tipo cliente para los equipos que se acceden vía remota sobre plataforma linux.

4 **Group Server.** Con esta herramienta se pueden programar, controlar y gestionar tareas de respaldo aplicadas a grupos a través de los agentes instalados en las máquinas.

5 **Back Up Server.** Es una aplicación para el almacenamiento centralizado y administración de copias de seguridad que se instala en un servidor en red con gran capacidad de almacenamiento en disco duro, pudiendo crear un espacio por separado para cada usuario o equipo, o crear un servidor espejo.

6 **Enterprise Server.** Es una herramienta de aplicación local para gestión del servidor y recuperación de datos en caso de fallas. Puede realizar copias de archivos y carpetas seleccionadas, así como de discos duros y particiones enteras.

Los requisitos mínimos del hardware para su instalación son los siguientes:

1 Procesador Pentium I.

2 Memoria de 256 MB.

3 Unidad de CD-RW o FDD para discos de arranque.

Los sistemas operativos compatibles para la instalación de los componentes de Acronis Image Server se listan a continuación; (excepto agent para linux):

1 Windows Profesional 2000 SP4/XP Professional SP2.

2 Windos Server 2000/Advanced Server 2000/Server 2003.

3 Windos XP Professional x64 Edition y Windos Server 2003 x64.

4 Windows Vista todas las versiones (excepto algunos componentes remotos).

La instalación de Agent para linux es soportada por las siguientes versiones:

1 Linux 2.4.18 o kernel posterior.

2 SuSE de la 8.0 a la 9.3, Red Hat 9.0, Advanced Server 2.1, 3.0 y 4.0, Fedora Core 2, 3 y 4, Enterprise Server 3.0, Mandrake 8.0, 9.2, 10.0 y 10.1, Slackware 10, Debian estable e inestable (sarge), ASPLinux 9.2, 10, 11 y II, ASPLinux Server IV, Virtuazzo 2.6.x, Gentoo, UnitedLinux 1.0, Ubuntu 4.10, TurboLinux 8.0 y 10.0. Y todas las versiones x64 de estas distribuciones.

En la siguiente figura 2.7 podemos ver la pantalla de Enterprise Server y el menú que muestra las herramientas de configuración, respaldo y recuperación de archivos.

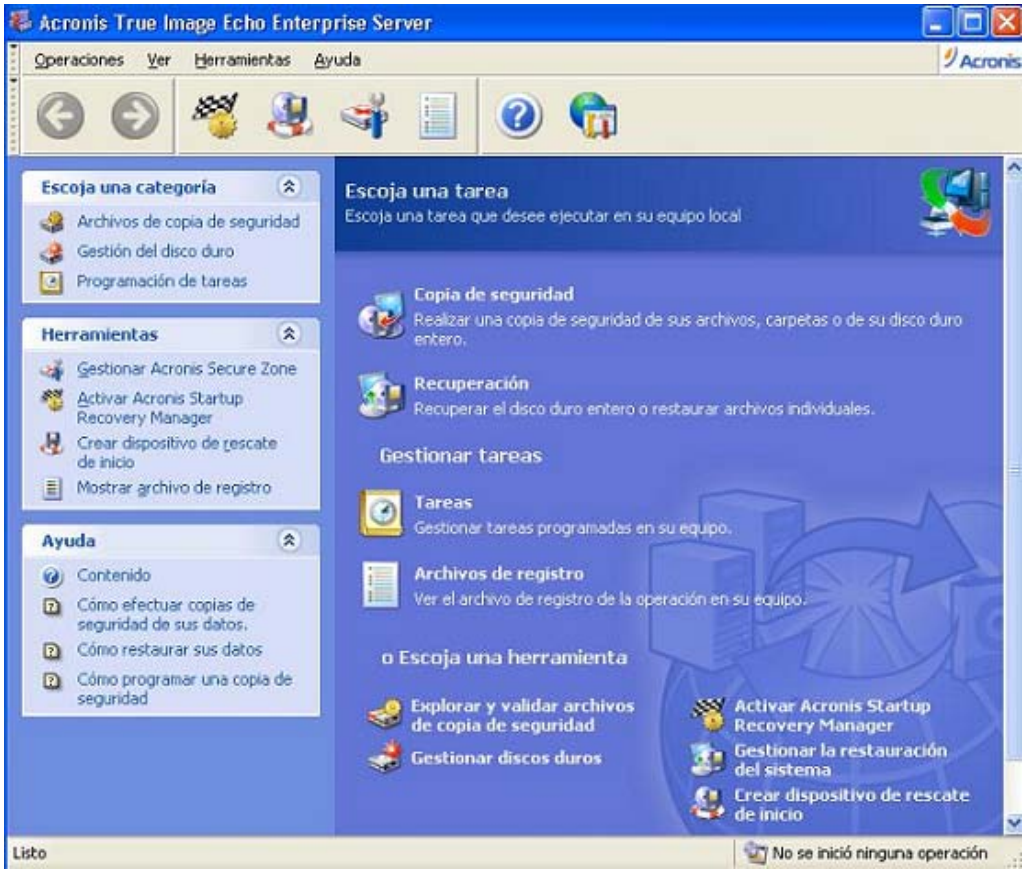


Figura 2.7 Menú de Enterprise Server

Por ejemplo, si queremos hacer una copia de seguridad de algún archivo tenemos que hacer lo siguiente:

1 Seleccionamos la opción Copia de Seguridad y enseguida abrirá un asistente y le damos “siguiente”.

2 Se abre una nueva ventana y pregunta qué elementos queremos copiar y seleccionamos “Mis datos”, como se muestra en la figura 2.8, y le damos “siguiente”.

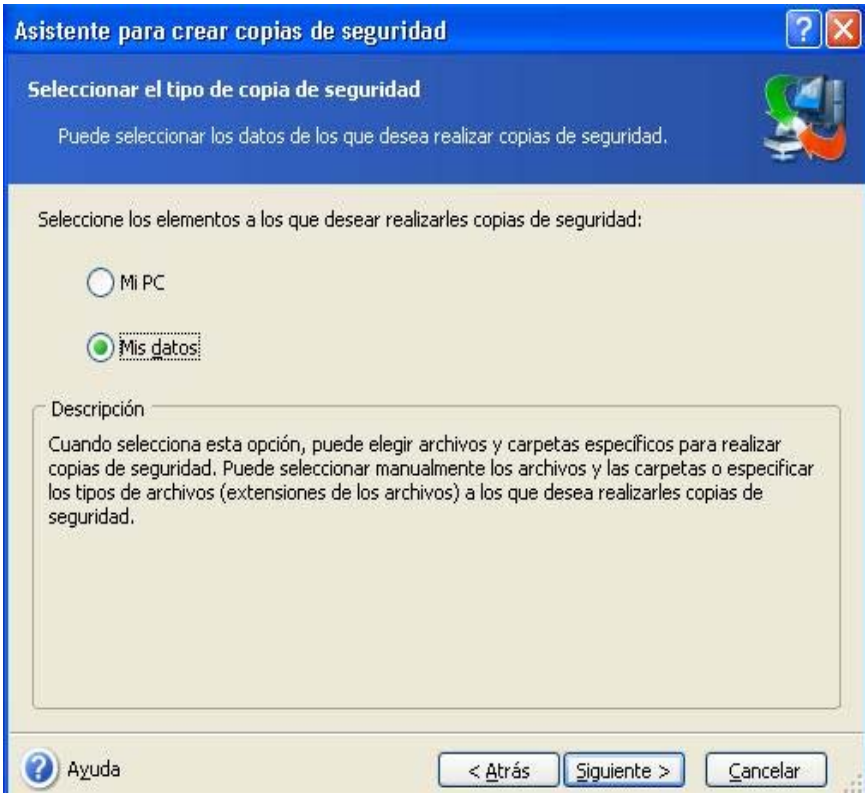


Figura 2.8 Ventana del asistente para copias de seguridad

3 Ahora se abre otra ventana donde podemos especificar la ruta donde se encuentra el archivo y lo seleccionamos. Una vez hecho le damos “siguiente”. Podemos seleccionar más de un archivo o carpeta si así lo deseamos.

4 Se nos presentará una ventana donde podemos excluir archivos por su extensión o característica para que no se incluyan en nuestra copia de seguridad, como se muestra en la figura 2.9.

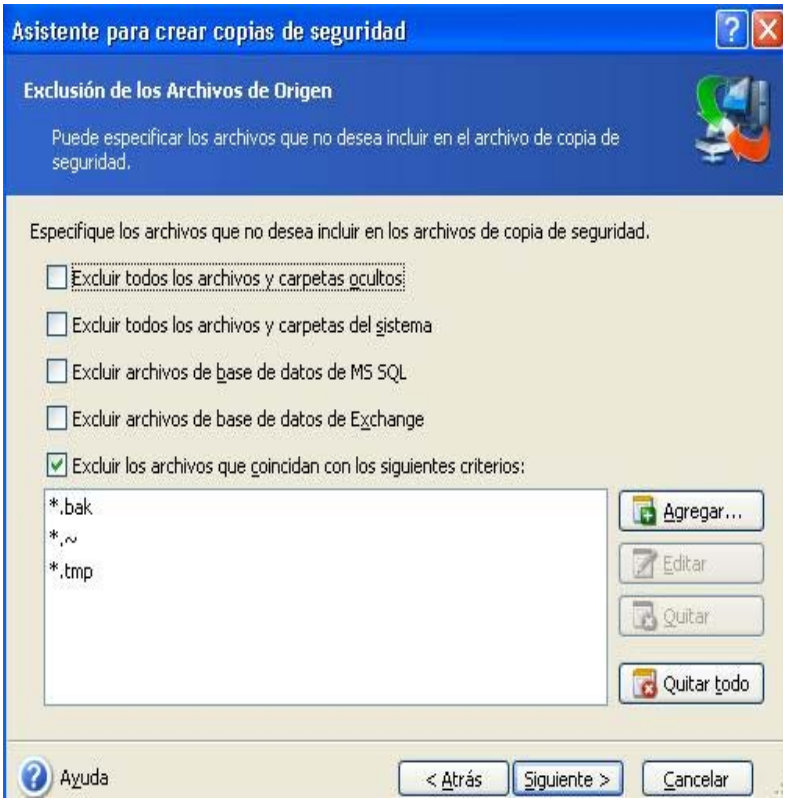


Figura 2.9 Exclusión de archivos en la copia de seguridad

5 Ahora elegiremos en dónde queremos guardar el archivo. Podemos elegir cualquier ubicación, pero es recomendable guardarlo en Acronis Secure Zone ya que es una partición protegida del disco duro y que no es accesible por otras aplicaciones, tal como se ve en la siguiente figura 2.10. Dicha partición debe ser configurada por separado antes de usarla.

Figura 2.10 Selección de la ubicación de la copia de seguridad

6 Hay que tomar en cuenta que si es la primera vez que se respalda el archivo será necesario hacer una copia de seguridad completa, posteriormente las copias podrán elegirse ya sea de modo incrementales o diferenciales como se muestra en la figura 2.11

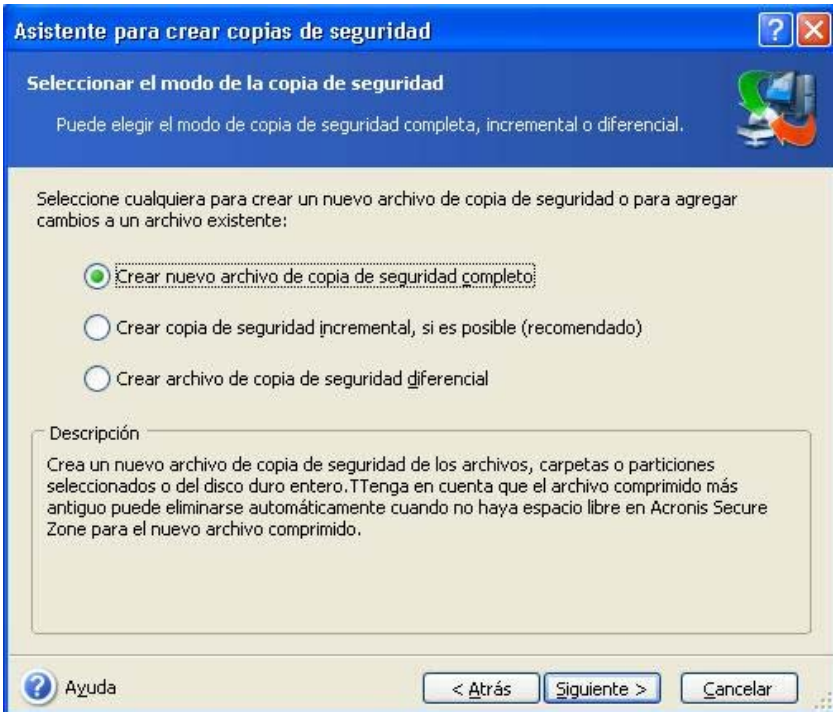


Figura 2.11 Modelos de copias de seguridad

7 Una vez elegido el tipo de copia de seguridad que se desea, el sistema hace el respaldo y una vez terminado el proceso se despliega un mensaje avisando que ha concluido satisfactoriamente si así es el caso.

En este momento ya contamos con una copia de seguridad guardada en Acronis Secure Zone, y cuyo proceso de respaldo podrá ser programado posteriormente a través de la opción “Tareas” del menú principal, ahorrando así el hacerlo manualmente a través del modelo incremental o diferencial, como se muestra en la figura 2.12

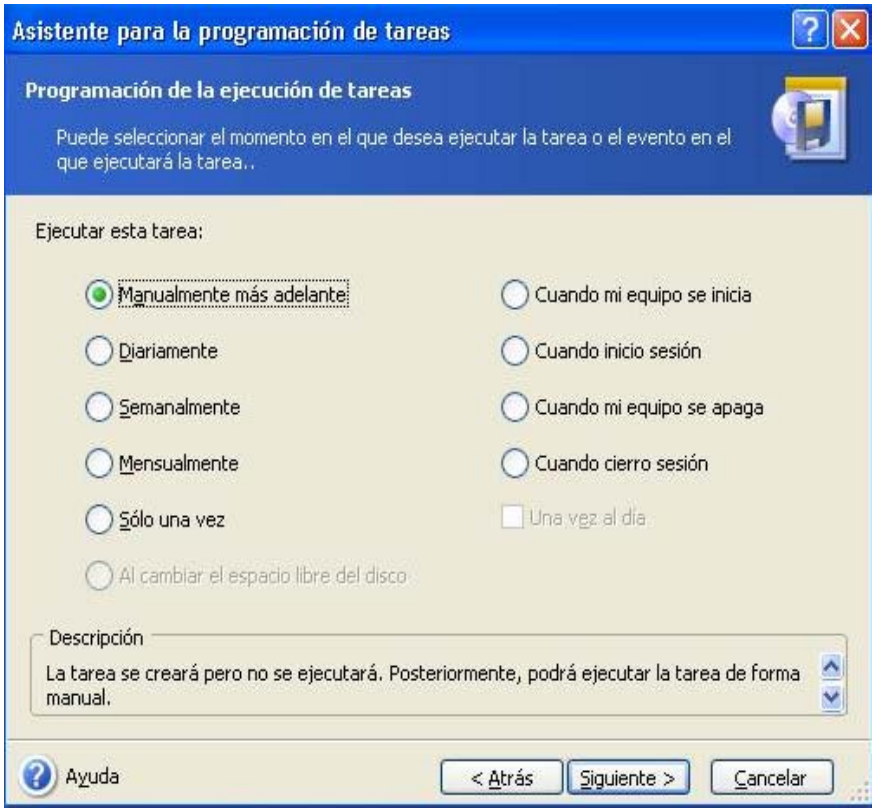


Figura 2.12 Asistente para programar tareas de respaldo

La ventaja de crear una partición Acronis Secure Zone, es que permite la recuperación de información aún cuando el sistema operativo falle ya que se pude arrancar el equipo a través de System Recovery, que es una herramienta que permite arrancar el equipo con esta opción y reconocer dicha partición donde se encuentra nuestra información respaldada para de este modo poder recuperarla.

2.4 ACTUALIZACIONES

Las vulnerabilidades y riesgos en el software, el hardware y la información en muchas ocasiones son inherentes e inevitables, propios del entorno donde se encuentran, de tal manera que se convierten en factores con los que día a día tenemos que tratar de prevenir. Muchas ocasiones contamos con el equipo y el

software adecuado para implementar nuestras políticas de seguridad, pero debido precisamente a estas características propias de los sistemas de tender a fallas debido a errores propios (bugs en el caso del software, y obsolescencia extrema o daños en el caso del hardware), la labor se dificulta.

Para ello es que en este apartado contemplamos las actualizaciones como una medida de seguridad y prevención, ya que puede establecerse como un procedimiento más dentro de las políticas de seguridad para la Intranet.

2.4.1 ACTUALIZACIÓN DE SOFTWARE

Es claro que las vulnerabilidades propiciadas por software existen y que las compañías que desarrollan estos productos trabajan para corregirlos lanzando “parches de seguridad”, que es el nombre que se da comúnmente a una porción de código que se inserta sobre otro para corregir errores o cambiar a una nueva versión del producto, o en el caso de los antivirus las vacunas contra las nuevas amenazas de virus y que en su conjunto forman parte de la actualización de software. Y aunque periódicamente se lanzan nuevos parches también se descubren nuevas vulnerabilidades de tal modo que se convierte en una cadena interminable por tratar de contrarrestar estos males.

Las recomendaciones en cuanto a actualización de software son las siguientes:

1 **Consultar.** Revisar periódicamente las páginas oficiales de los productos que se tienen instalados en los equipos de la Intranet para mantenerse al tanto de las últimas noticias, novedades y parches disponibles.

2 **Instalar**. Los parches y actualizaciones disponibles siguiendo los procedimientos e indicaciones dadas con el producto o desde los sitios oficiales.

3 **Informarse**. Tomar en cuenta la información de los CERT Advisories (Technical Cyber Security Alerts), que se encuentran en la página oficial de la organización CERT (Computer Emergency Response Team), donde se publican oportunamente los detalles técnicos asociados a las vulnerabilidades encontradas y las medidas que se pueden tomar para corregirlas.

Éstas son las reglas básicas que podemos considerar en cuanto a mantener las actualizaciones del software instalado en nuestra red pero también tomar en cuenta aquellas que se adapten más a las necesidades propias del sistema donde trabajemos.

Y por último, mencionar que la organización CERT fue creada en 1988 por el departamento de defensa estadounidense y el proyecto ARPA (Advanced Research Project Agency), cuyas funciones principales es alertar sobre violaciones de seguridad descubiertas en los sistemas y en evitar o minimizar el impacto que éstos puedan producir tratando de mantener al día la información más reciente que se tenga concerniente a seguridad informática y comunicaciones.

2.4.2 ACTUALIZACIÓN DE HARDWARE

Al igual que el software el hardware debe mantenerse actualizado como medida de prevención y de seguridad para la Intranet. Los factores más comunes que hay que evitar son los siguientes:

1 **Obsolescencia.** Evitar que los equipos con el pasar del tiempo se vuelvan incompatibles con la mayoría de las aplicaciones existentes ya que es muy común encontrar por ahí equipos olvidados que corren bajo sistemas ya obsoletos que por olvido, descuido o porque la aplicación que aún corre en ese equipo con el pasar de diferentes

administraciones no se ha podido actualizar y entre más pasa el tiempo más se olvida, pero no nos percatamos que es precisamente ahí donde se van creando hoyos de seguridad para la red.

2 **Deterioro.** Reemplazar el equipo que se considere que ya está en condiciones de renovarse antes de que falle, evitando la pérdida de información y funcionalidad de la red.

Tomando estas consideraciones empezamos a crear la base de un sistema de seguridad para Intranet, en un entorno de trabajo fácil de administrar ya que gran parte del trabajo que se lleva a cabo dentro de la red es la administración de recursos y servicios. Por tal motivo nos enfocamos a que las estrategias tomadas en cuanto a seguridad cumplan con este requisito por un lado, y por el otro sean transparentes al usuario y a los demás procesos dentro de la Intranet.

Capítulo 3

Seguridad de la Información

CAPÍTULO 3 SEGURIDAD DE LA INFORMACIÓN

3.1 TIPOS DE DATOS

Antes de adentrarnos en el contexto de este capítulo debemos analizar algunos aspectos que hay que tener claros en cuanto a las diversas formas en que los datos son originados. El hecho es que los datos que se guardan en un equipo; llámese estación de trabajo, servidor o computadora, pueden ser de diversa índole debido a que se originan y se emplean por los múltiples y diversos programas de aplicación que en cada uno de estos equipos se ejecutan, y según el programa dependerá el formato que se le dé a los datos.

Este formato consiste en un arreglo muy particular de ordenar los bits de información que determinan la procedencia del programa que originó el patrón de los datos, y que en su conjunto forman un archivo, el cual puede ser reconocido en otro equipo distinto de donde se originó gracias a esta característica lógica de acomodar la información, de tal forma que los datos pueden ser leídos o modificados siempre y cuando se tenga instalado el mismo programa de aplicación para que los pueda interpretar.

De tal modo que el compartir información entre diferentes equipos no involucra mayor complejidad que contar con los programas adecuados en cada uno de ellos. Pero en cambio lo que hay que considerar es la manera de cómo hacer llegar la información entre los diversos equipos, en otras palabras, el medio que utilizamos para transportar los datos de una máquina a otra, y por otro lado brindar la seguridad necesaria durante el transporte, haciendo de éste un servicio seguro al momento que la información se encuentre viajando de un equipo a otro.

Recordemos que por tratarse de una Intranet la manera en que viaja la información a través de la red es por medio de protocolos de comunicación basados en el modelo TCP/IP, de manera que la comunicación entre los diversos equipos de la red se hace mediante las distintas capas de protocolos dentro de la

familia TCP/IP; figura 3.1, la cual también muestra el RFC (Request For Comments – Petición de Comentarios), correspondiente a cada uno.

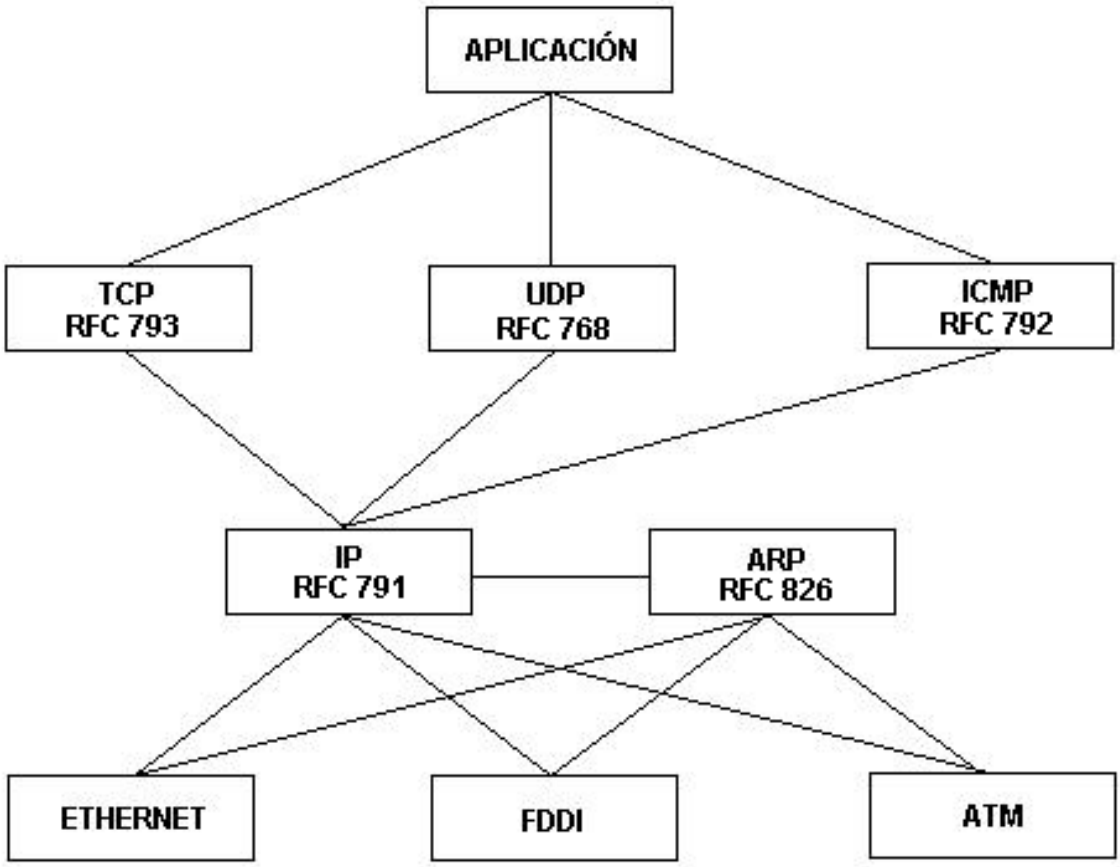


Figura 3.1 Familia de Protocolos TCP/IP

Esta estructura de comunicación plantea un problema de seguridad doble respecto a la información que viaja por la red de manera inherente a su diseño. Por un lado tenemos la propia información que deseamos transportar la cual es empaquetada por distintos protocolos, que por la naturaleza de su contenido ya es valiosa por tratarse de datos que revelan algún valor para la organización o empresa en cuestión. Y por el otro, el modo de funcionamiento de los protocolos y formato de los paquetes hacen que la información que utilizan para comunicarse entre las distintas capas y equipos de la red se convierta en una fuente valiosa de información como se muestra en la figura 3.2.

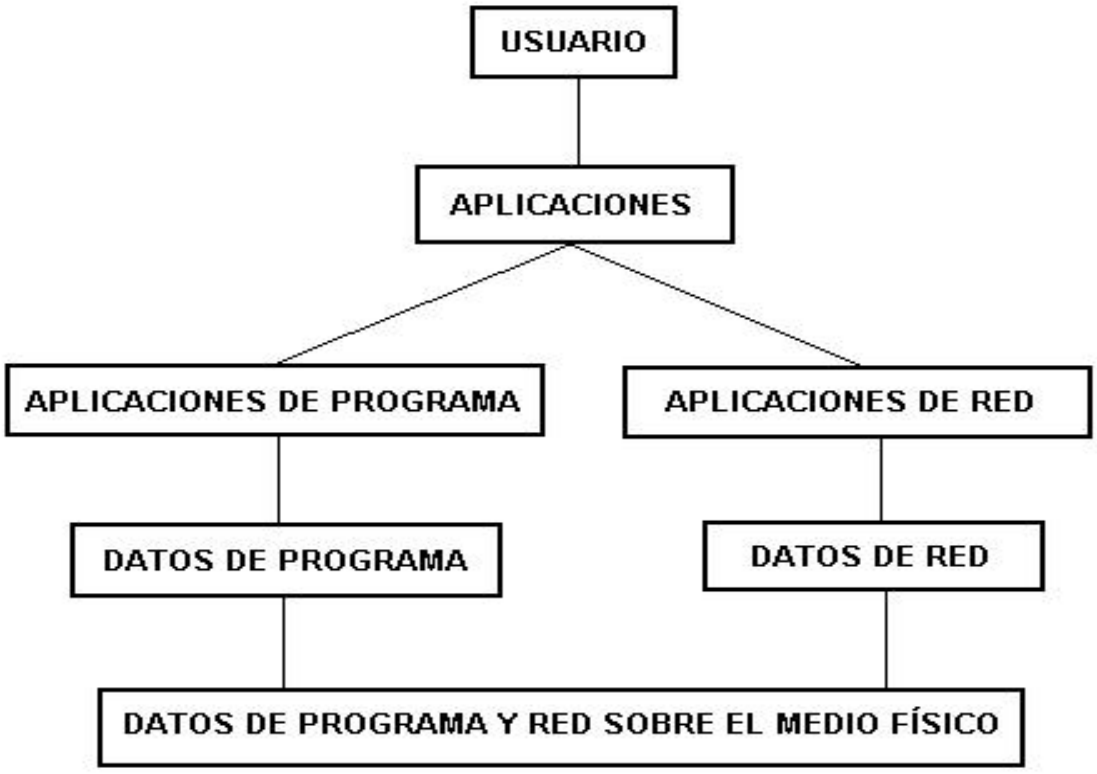


Figura 3.2 Datos que viajan por la red

3.1.1 RFC – PETICICIÓN DE COMENTARIOS

Las características técnicas de cada uno de los protocolos en TCP/IP, están fuera del alcance de este trabajo ya que su comprensión y análisis requiere de un estudio de investigación completo, pero hago mención de ellos en su concepto básico y queda a consideración del lector el profundizar en estos temas en los RFC's, los cuales desde 1969 y con la evaluación de IETF (Internet Engeenering Task Force – Grupo de Trabajo de Ingeniería en Internet); cuya organización contribuye a la normalización de Internet, decide si una propuesta puede convertirse realmente en un RFC oficial, entre otras cosas.

Un RFC se define mediante un título y un número específico de forma única, el cual no puede repetirse ni eliminarse aunque el RFC sea substituido o quede obsoleto.

La descripción de cada RFC se hace en inglés y en formato ASCII, siguiendo una estructura específica que deben cumplir, y antes de convertirse en un RFC oficial, debe pasar por un proceso muy estricto, para que pueda ser interpretado e implementado sin ambigüedades. Ya una vez aprobado el RFC se convierte en un protocolo formal, por lo que el sentido de su nombre “petición de comentarios (RFC)” queda en segundo plano.

Cada uno de los protocolos que existen en Internet tienen asociado un RFC que los define y en ocasiones algunos otros adicionales que los amplían.

3.1.2 FORMATO DE LOS DATOS EN LA RED

El proceso para establecer una conexión entre dos equipos empieza cuando la aplicación desea transmitir datos haciendo una llamada al módulo TCP, el cual es un protocolo fiable y orientado a conexión encargado de recibir buffers de datos provenientes de las aplicaciones que solicitan el envío de datos empaquetándolos en segmentos, a la vez que establece un canal de comunicación bidireccional con el equipo remoto (vía puerto-proceso).

Una vez hecho esto se hace una llamada al módulo IP ya que es un sistema de entrega de paquetes llamados datagramas, y es a través de la dirección IP destino del equipo remoto que se sabe a quién va dirigido dicho paquete, estos paquetes viajan a su vez por tramas físicas (tramas ethernet, u otra(s) si se tuviera que cruzar alguna red con distinta configuración) a través del medio físico de comunicación, y las cuales necesitan la dirección física MAC (Media Access Control, Control de Acceso al Medio) origen y destino de los equipos. La primera dirección es conocida pero la segunda no y es aquí cuando actúa el protocolo

ARP (Address Resolution Protocolo, Protocolo de Resolución de Direcciones), el cual envía un mensaje ARP-Request, a todas las máquinas de su red preguntando la dirección física de la máquina con determinada dirección IP, si la dirección IP está asociada a alguna máquina dentro de la red, ésta responderá advirtiendo que la pregunta es para ella y enviará una trama ARP-Replay con su dirección física, de lo contrario será necesario consultar algún otro dispositivo (router) para saber si al otro lado de la red existe está dirección IP. Este proceso pude repetirse varias veces por distintas redes saltando los datagramas por distintas tramas físicas hasta encontrar o no el equipo asociado a esta dirección IP llegando al último punto posible de acceso para saberlo.

Ya que se conocen ambas direcciones físicas, el equipo de origen envía los datagramas IP sobre las tramas físicas con las direcciones IP y físicas de origen y destino incluidas dentro de los campos de las tramas, a la vez que los datagramas IP pueden seguir rutas distintas ya que el mismo protocolo se encarga de buscar la ruta óptima en todo momento, y los paquetes pueden ser nuevamente reordenados por la información de secuencia que en ellos se encuentra. Tal ilusión es creada por el protocolo TCP el cual implementa un circuito virtual de comunicación creando la idea de que todos los paquetes viajan uno tras de otro por una misma vía de comunicación. Además las direcciones MAC son guardadas en una tabla de direcciones (ARP caché), así la próxima vez que se desee acceder a la misma dirección IP del equipo remoto ya no se tendrá que preguntar por su dirección física puesto que esta ya está almacenada en la tabla.

Debido a que el protocolo IP es no fiable y no orientado a conexión se utiliza el protocolo ICMP (Internet Control Message Protocol, Protocolo de Mensajes de Control y Error), para el control de errores pero sin tomar ninguna decisión, los cuales viajan dentro del campo de datos de un datagrama IP.

.

El protocolo UDP (User Datagram Protocol, Protocolo de Datagrama de Usuario), es un protocolo simple de intercambio de datagramas sin seguridad ya que se

envían sin confirmación de recibido ni garantía de entrega, por lo que se denomina no fiable y no orientado a conexión. Se utiliza cuando se requiere enviar información como en el TFTP (Trivial File Transfer Protocol, Protocolo de Transferencia de Archivos Triviales), en el menor tiempo, ya que por no manejar confirmaciones ni control de errores la información puede viajar más rápido.

La figura 3.3 muestra como son empaquetados los datos por las distintas capas de los protocolos TCP/IP cuando se establece una conexión entre dos equipos y viajan por la red a través de las tramas ethernet sobre el medio físico.

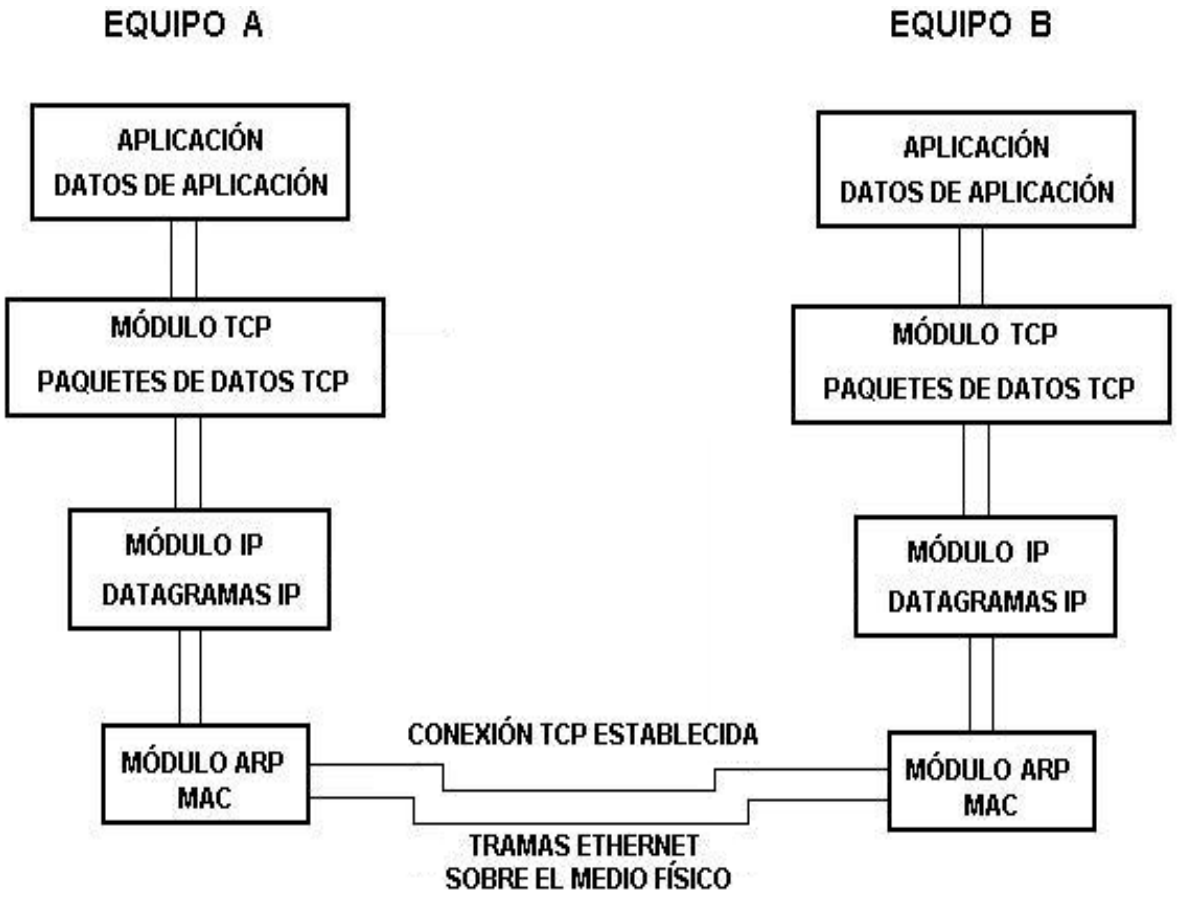


Figura 3.3 Conexión TCP/IP entre dos equipos

La conexión se establece por medio de los módulos TCP y sin importar quién haga la petición se logra una vía de comunicación full-duplex. El tamaño de las tramas o

paquetes de cada uno de los protocolos es de 32 bits, los cuales se dividen en campos de diferentes tamaños que indican distintas aplicaciones o estados, o inclusive en el caso del protocolo TCP se hace uso de un campo de 6 bits para el uso de banderas.

Excepto para las tramas de acceso al medio las cuales dependen del tipo de red que se trate, por ejemplo ethernet maneja un MTU (Unidad Máxima de Transferencia), de 1500 bytes como máximo y un mínimo de 64 bytes para el campo de datos (no para el tamaño de la trama ya que esta va de 64 a 1518 bytes debido a los campos de control y cabeceras que utiliza), además de que el esquema de acceso a ethernet mediante el cual los equipos pueden monitorear el estado del medio para saber si está libre o no para transmitir y evitar colisiones es conocido como CSMA/CD (Carrier Sense Multiple Access with Collision Detect, Acceso Múltiple con Detección de Portadora y Detección de Colisiones), con una velocidad de transmisión de 10 Mbps. (aunque en la actualidad existe fast ethernet que transmite a100 Mbps y giga ethernet). El medio físico utilizado es el cable UTP categoría 5 y 5e, en distancias menores a 100 metros y capacidad de transmisión de 100 Mbps y 1 Gbps respectivamente, con un ancho de banda de 100 MHz para ambas categorías.

Todo este proceso se realiza llevando en todo momento información valiosa del sistema por la red de un lado hacia otro y transportando los datos de usuario de la misma manera, cruzando por un sin fin de equipos, redes y sistemas de manera libre hasta llegar al equipo destino donde se desea enviar y/o recibir información.

La figura 3.4 muestra cómo viaja la información entre equipos pertenecientes a una misma red, y en particular a un mismo segmento ya que no intervienen dispositivos de interconexión.

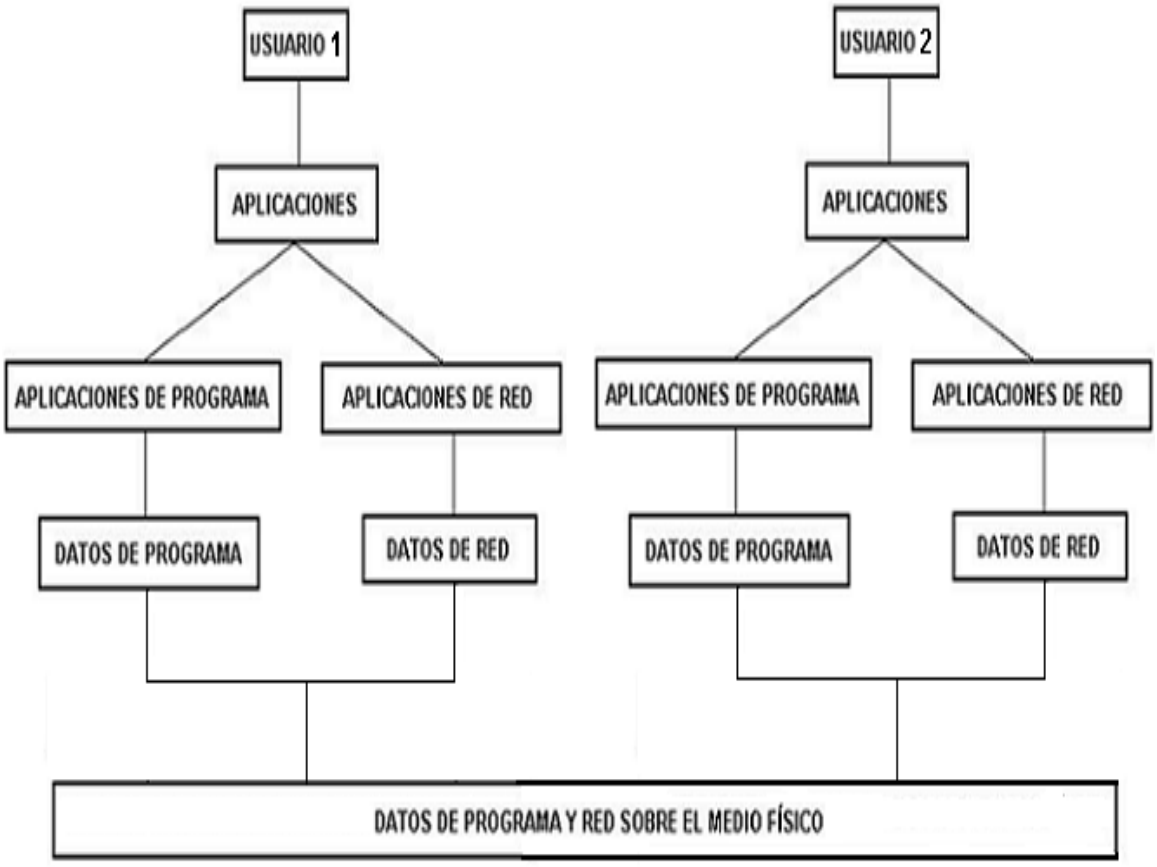


Figura 3.4 Comunicación entre equipos de la misma red

Si los equipos pertenecieran a segmentos de red distintos, la configuración mostrada en la figura anterior se vería modificada en la capa perteneciente al medio físico, ya que no se vería como un único segmento que une ambos equipos, sino que serían dos segmentos unidos por un dispositivo de red para interconectar los dos equipos. Y en general este modelo de comunicación se aplica para los “n” equipos pertenecientes a la red y los “m” segmentos de la misma.

3.2 MANEJO DE LA INFORMACIÓN

Como ya vimos existe información viajando a través de la red, ya sean datos de usuario y/o datos de la red utilizada para la comunicación entre protocolos, pero el flujo de información siempre es constante en una Intranet, la cual cruza por varios dispositivos, y si ésta cuenta con salida a Internet la información tendrá que cruzar

por un número mayor de dispositivos haciendo que los datos que van viajando sean aun más vulnerables al pasar por distintas redes lo que ocasiona un problema de seguridad desde el momento que la información es puesta sobre las tramas ethernet para alcanzar su destino.

Debemos tener cuidado de contar con las medidas necesarias para asegurar que la información que recorre la red está protegida, tomando en cuenta que la posibilidad de que ocurra un intento de ataque de seguridad en nuestro sistema es posible en todo momento. Lo que nos lleva a pensar en cómo se podría llevar a cabo dado el modo de operación de la red explicado anteriormente, y el valor y naturaleza de la información que se expone al momento que viaja por la red y se encuentra de alguna manera presente en los cables, circuitos y componentes que atraviesa, de tal modo que debemos seguir ciertos modos en que operan los tipos de ataques más comunes que tratan de explotar cierto tipo de vulnerabilidades que se encuentran ligados al mecanismo y funcionamiento de los protocolos de comunicación en la red.

Este tipo de planteamiento nos lleva a tratar de saber hasta dónde es segura la red una vez que hemos aplicado procesos y herramientas que nos lo demuestran, permitiendo tener un mayor control y conocimiento de las funciones en la Intranet.

De tal forma que la información que viaja por la red puede ser analizada por el atacante siguiendo un orden lógico de acción en cuanto a la recopilación de datos y ejecución del ataque. Acciones que lo lleven a penetrar y burlar los distintos métodos de reconocimiento que se hacen en la red para crear una conexión que le permitan establecer una vía de comunicación hacia el interior de la red, enmascarando las técnicas empleadas para evitar ser sorprendido o dejar el menor rastro, y segundo, escalar privilegios como usuario dentro de la misma para obtener control sobre el objetivo planeado y perpetuar su ataque. La figura 3.5 muestra las distintas etapas que completan la estructura de este ataque.

Figura 3.5 Etapas de un ataque

Cada una de las etapas mostradas en la figura anterior, utilizan métodos y técnicas específicas para la recopilación de información necesaria en la identificación del objetivo de ataque, mismas que a continuación se describen así como las recomendaciones necesarias para evitarlas.

3.2.1 INFORMACIÓN DE ATAQUE Y ESTRATEGIAS DE DEFENSA

Las etapas que comprenden un ataque de seguridad en la red están caracterizados por el uso y manejo de información que en cada una de ellas se utiliza para adentrarse hasta alcanzar el objetivo deseado, dichos ataques podemos decir que son *"planificados"*, ya que se sabe la secuencia de pasos a seguir, al mismo tiempo que se pude predecir la etapa siguiente a partir de la

etapa actual y proponer con base en esto un sistema de seguridad acorde a las necesidades que a continuación se mencionan.

3.2.1.1 RECONOCIMIENTO

Esta etapa comienza por establecer y definir el objetivo de ataque dentro de la organización o empresa, ya sea la misma red, algún servidor, equipo o proceso en particular. Posteriormente se trata de recopilar toda la información posible acerca del objetivo, empezando por la organización o empresa a la que pertenece y todo lo referente a ella, así como del propio objetivo. La información de la empresa u organización se puede obtener de diferentes fuentes como Internet, empleados, revistas, etc., o a través de ICANN (Internet Corporation for Asiggned Names and Numbers, organismo sin fines de lucro que a nivel internacional regula los nombres de dominios en Internet y las direcciones numéricas IP), para obtener el rango de redes asociado a la organización.

La técnica empleada para obtener información de la red se denomina “Footprinting”, la cual consiste en explorar la red para la adquisición de cualquier tipo de datos que permitan determinar e identificar procesos y vulnerabilidades a explotar para ingresar dentro del sistema. Para ello se hace uso de herramientas propias de sistema como de otras que se utilizan con fines particulares.

Dentro de las herramientas estándar que se encuentran incluidas en los sistemas están los comandos de red que se utilizan para analizar y detectar fallas como: ping, tracert, nslookup, finger o netstat para sistemas Windows, y sus equivalentes en sistemas Linux: ping, traceroute, whois y finger, las cuales permiten obtener información de usuarios y equipos de la red, ya sea desde el interior de la misma o del exterior por Internet.

Por otro lado existe otro tipo de utilidades que no forman parte del sistema, las cuales son de uso específico y pueden extraer más información como: nmap,

queso, smartwhois, y otras similares cuya finalidad es la misma, pero con un enfoque más profundo al tratar de obtener la mayor cantidad de información posible.

Este tipo de herramientas ya sean propias del sistema o no, utilizan los datos proporcionados por el sistema emisor o receptor dentro de los paquetes TCP/IP, por ejemplo el comando nslookup trabaja sobre la capa IP traduciendo las direcciones IP a nombres de máquinas obteniendo la relación que existe entre los diversos sistemas de la red.

Por otro lado el comando tracert (Windows) o traceroute (Linux), permite determinar la topología tanto física como lógica de una red y los sistemas existentes entre dos equipos.

El funcionamiento de tracert se basa en el campo TTL (Time to Live 8 bits, que determina el número de saltos que pude hacer un paquete en la red, si su valor es cero el paquete se destruye), en la cabecera de los datagramas IP determinando uno a uno los saltos que hace un paquete a través de la red hasta llegar a su destino ya que su valor se ve decrementado en uno cada vez que el paquete es reenviado por un router, siendo el valor del primer datagrama en el campo TTL=1 y con una petición del tipo ICMP “Echo Replay” al primer router que encuentre (en respuesta el “Echo Request” del equipo donde se envía la petición), el cual contesta y se decrementa TTL, ahora TTL=0 (“TTL Extinguido”), al llegar al primer router enviando la dirección IP origen de la interfaz del router al host fuente mediante un mensaje ICMP “destination unreachable”, de tal manera que el siguiente datagrama alcanzará un salto más ya que TTL ahora valdrá 2, y la dirección IP del siguiente router es enviada de nuevo al host de origen cuando TTL vuelva a ser cero de este modo se realiza la traza entre dos equipos, (este procedimiento se repite hasta un máximo de “n” saltos que se especifiquen). El formato de estos paquetes se ilustra en la figura 3.6.

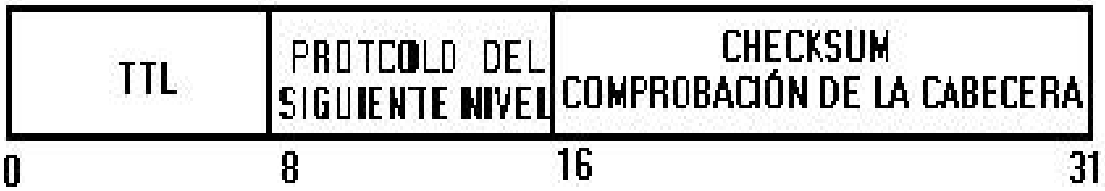


Figura 3.6 Formato de los paquetes IP para TTL

El comportamiento de esta herramienta dependerá del sistema operativo donde se ejecute ya que mientras en sistemas Linux se utiliza el protocolo UDP (o ICMP opcional), en Windows se utiliza sólo el protocolo ICMP. La sintaxis es la siguiente:

[instrucción] [-opción(1),...-opción(n)] [nombre del host / IP]

tracert –h (# de saltos) –w(tiempo en ms) www.hostindicado.com

El formato de los paquetes ICMP y UDP se muestra en las figuras 3.7 y 3.8 respectivamente.

Figura 3.7 Formato de los paquetes ICMP

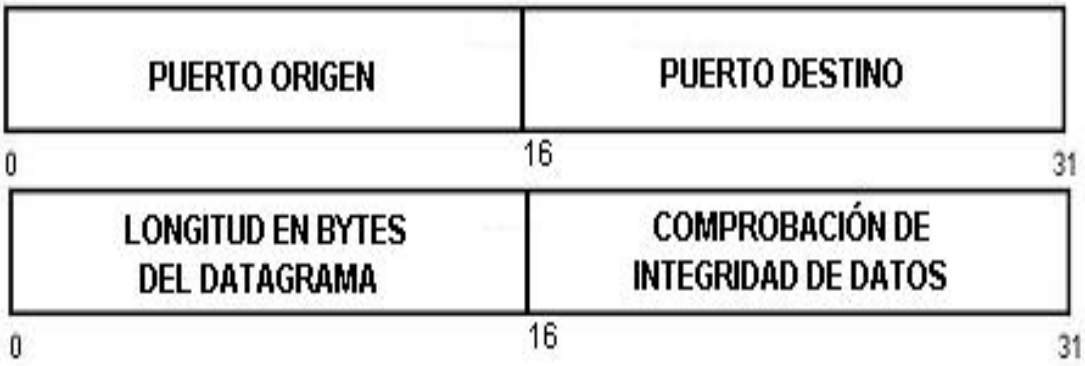


Figura 3.8 Formato de los paquetes UDP

Si por el contrario la aplicación es utilizada mediante UDP, se construye un paquete UDP a un número de puerto alto (puerto 33434 predeterminado) que se crea desocupado a un host indicado, el cual se incrementa en uno por cada salto lo que hace difícil saber el número de puerto conque llega finalmente al destino especificado, y precisamente lo que intentamos saber son los saltos que el paquete hace a través de distintas redes, por tal motivo se implemento una herramienta que permite setear (-s), un puerto de manera fija para que no cambie su valor, de lo contrario sería difícil saber a qué número de puerto llega la petición del host local. La sintaxis es la siguiente:

[instrucción] [-opción(1),...-opción(n)] [nombre del host / IP]

traceroute –p(# de puerto) www.hostindicado.com

El problema con los paquetes UDP o ICMP son los firewalls, ya que los paquetes pasarán por distintos puertos y filtros de paquetes, dependiendo la configuración del firewall rechazará o permitirá dichos paquetes, lo más habitual es utilizar puertos habituales, así mismo existe una herramienta denominada “Rotorouter” cuyo objetivo es defender la red ante este tipo de amenazas basadas en traceroute, generando respuestas falsas a este tipo de peticiones.

En el caso del comando ping utiliza paquetes ICMP del tipo “Echo Request” en el host local (el que hace la petición) y “Echo Replay” para el host remoto (al que se

haya lanzado la petición de respuesta). De tal modo que si obtenemos respuesta del host remoto podremos averiguar dos cosas: primero saber sí una determinada dirección IP existe dentro de la red, y segundo que hay un equipo a la escucha de dichas peticiones. El formato para utilizar este comando es similar a la utilizada en tracert:

[instrucción] [-opción(1),...-opción(n)] [nombre del host / IP]

ping –r (#de rutas) www.hostindicado.com

La funcionalidad de estas herramientas está orientada a brindar una interfaz de ayuda para detectar problemas de conexión en la red. La forma en que trabajan con base en los protocolos TCP/IP hace posible aprovechar las características que éstos tienen para obtener información acerca de las conexiones y paquetes disponibles en la red, ya sea desde el interior (Intranet), convirtiéndose en una herramienta útil para el administrador al momento de detectar fallas en la red, o del exterior (Internet), donde la situación puede resultar en una posible amenaza.

Estas instrucciones como tales no implican mayor riesgo desde el punto de vista para el que fueron creados, lo que sí es una amenaza es la profundización que hacen cierto tipo de implementaciones que adoptan la misma filosofía de funcionamiento y la llevan un paso más adelante tratando de obtener información más sensible del sistema a atacar con base en la utilización de peticiones de paquetes TCP/IP, derivando en una técnica llamada “Fingerprinting” la cual tiene como finalidad obtener la huella de identificación del sistema en particular, en otras palabras se trata de averiguar el sistema operativo que corre en el equipo objetivo de ataque para en base a esto saber sí existen vulnerabilidades a explotar y puertos disponibles.

El uso de estas herramientas permiten desde otro punto de vista averiguar de forma pasiva hasta donde una red puede ser vulnerable, ya que uno de los

métodos más efectivos para protección es simular un ataque con las mismas herramientas que podrían ser utilizadas por cualquier atacante.

Una de las herramientas por excelencia al ser muy completa es el programa “nmap”, utilizada en sistemas Windows, Linux y Mac, la cual utiliza como base el mismo funcionamiento que hacen tracert y ping de los paquetes (ICMP, UDP), pero además robustece esta idea haciendo un análisis de los paquetes que recibe como respuesta del host remoto, logrando identificar ciertas características propias del sistema estudiado en particular. Y por otro lado aumenta las opciones con las que puede ser usado conformando un set de herramientas más completo en base al grado de información que es capaz de manipular en los paquetes TCP/IP.

La técnica Fingerprinting utiliza como fuente de información los datos insertados en los paquetes del protocolo TCP y la forma en que se establece la comunicación entre el cliente y el servidor en tres pasos denominada *“TCP three way handshake”*, la cual se ilustra en la figura 3.9, ya que la interpretación de los RFC’s varía dependiendo del sistema en cuestión.

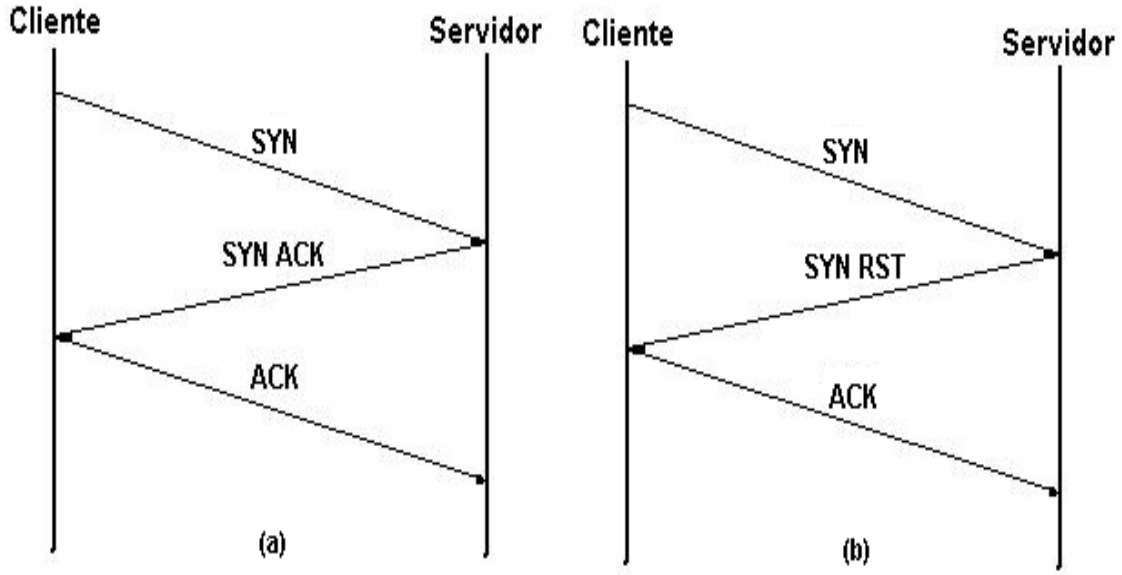


Figura 3.9 Enlace de comunicación TCP en tres pasos.
3.9(a) Conexión a un puerto abierto. 3.9(b) Conexión a un puerto cerrado

El inicio de una conexión siempre empieza por un paquete de sincronización (SYN) por parte del cliente, el servidor deberá responder con una confirmación de que la petición enviada puede ser atendida (SYN ACK) o no (SYN RST) y el cliente deberá responder a esta para confirmar de recibido (ACK). La finalización de la conexión se lleva a cabo mediante un paquete de fin (FIN) por parte del sistema que desea terminar la conexión, el cual deberá ser respondido por el otro equipo mediante una confirmación (ACK) y un paquete de fin (FIN) también, a lo que el equipo que desea terminar la conexión confirmará de recibido (ACK) y terminara la comunicación. El formato de este tipo de paquetes se ilustra en la figura 3.10.

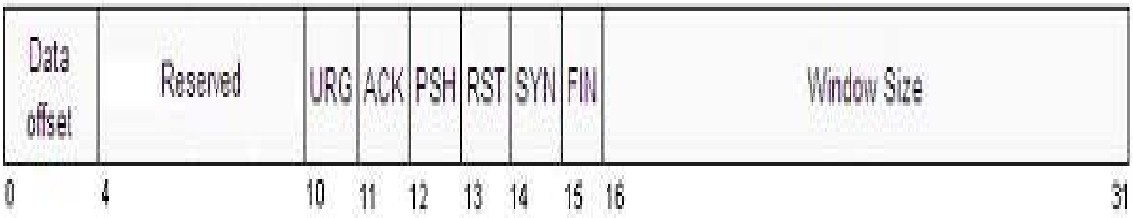


Figura 3.10 Campos TCP

Los tipos de comprobaciones más frecuentes sobre estos campos para averiguar el sistema operativo en particular son los siguientes:

1 **WINDOW SIZE.** El tamaño de ventana utilizado por cada sistema ayuda a identificarlo ya que en cada caso es muy particular. Este campo indica el número de bytes que el receptor puede recibir y cuya secuencia de inicio (primer byte) está indicado en el campo Acknowledgment Number (Número de reconocimiento) del formato TCP, siempre y cuando el valor del campo ACK este activado, figura 3.11. Cuando la secuencia es la del primer byte de datos del segmento esta se encuentra en el campo Sequence Number (Número de Secuencia, e igual que Acknowledgment Number es de 32 bits) si el valor del campo SYN está activado.

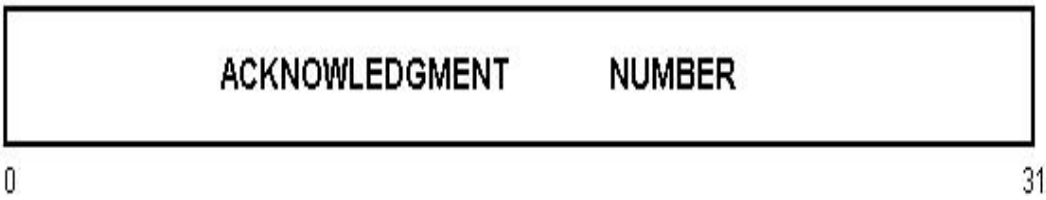


Figura 3.11 Formato del paquete Acknowledgment Number del Protocolo TCP

2 **ACK.** El número de secuencia asignado a este campo es devuelto, y mientras que algunos sistemas devuelven el mismo valor recibido otros lo incrementan en uno haciendo de esta una característica que permite identificar al sistema en cuestión.

3 **FIN.** La forma en que se lleva a cabo el término de una comunicación también permite identificar de que sistema se trata.

Estas son las técnicas más utilizadas para exploración de paquetes en la red basadas en TCP que permiten extraer información (Fingerprinting). Pero también existen otras alternativas de búsqueda en base a la utilización de otro tipo de paquetes.

Como ya lo mencioné, dentro de las primeras técnicas a utilizar en contra de estos ataques es tratar de usar la misma ideología y herramientas que emplearía un atacante, y en base a los resultados obtenidos hacer un análisis en cuanto a las posibles vulnerabilidades detectadas (en cuanto a la información disponible en los paquetes TCP/IP), pudiendo seguir como referencia las recomendaciones del RFC 2196 “Site Security Handbook” (Manual de Sitios Seguros), cuyo propósito es establecer una guía práctica a los administradores de sistemas para asegurar la información y servicios que ofrecen en Internet (aunque es aplicable también para aquellos sitios sin conexión a Internet).

Los sistemas IDS (Instrusion Detection Systems, Sistema de Detección de Intrusos), pretenden contemplar todas las posibles intrusiones basadas en vulnerabilidades del modelo TCP/IP tomando acciones de acuerdo a su configuración (mensajes de alerta, o reset de conexiones), algunos IDS´s permiten la actualización de la base de datos de reconocimiento de patrones de búsqueda de información sin esperar a que el fabricante lance los parches.

La forma más directa de protegerse ante ataques basados en el comportamiento de los paquetes TCP/IP para obtener información acerca de la topología de la red y los sistemas que se encuentran, consiste en establecer filtros de paquetes y para ellos se utilizan los firewalls, cuya clasificación depende del nivel o niveles en que trabaje sobre el modelo TCP/IP, siendo los siguientes los más usados:

1 **PACKET FILTERING** (Filtro de Paquetes). Trabaja a nivel de red (IP).

2 **PROXY SERVER** (Servidor Proxy). Trabaja en los niveles de Aplicación (“Application Gateway”), y Transporte (TCP o UDP “Circuit Level Gateway”).

3 **STATEFUL MULTILAYER INSPECTION** (Estado de Inspección Multicapa). Trabaja en las capas de Aplicación, Transporte y Red.

Las figuras 3.12, 3.13 y 3.14 muestran los diferentes niveles de aplicación de estos tipos de firewalls.

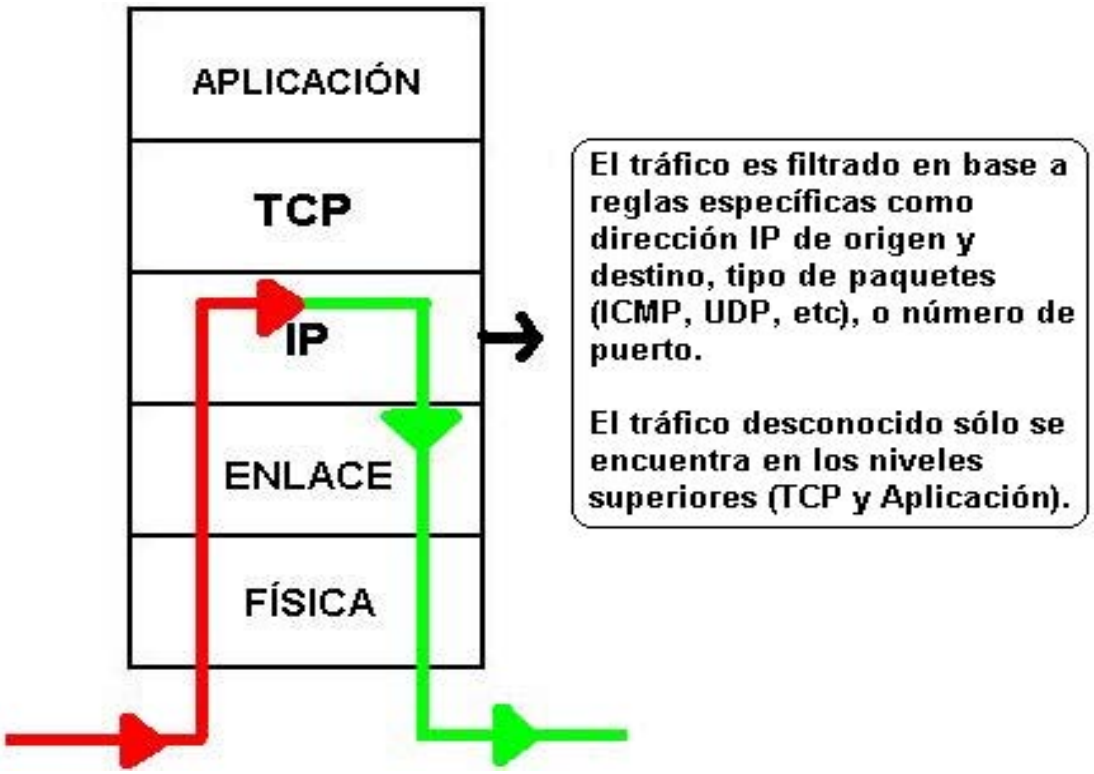


Figura 3.12 Packet Filtering

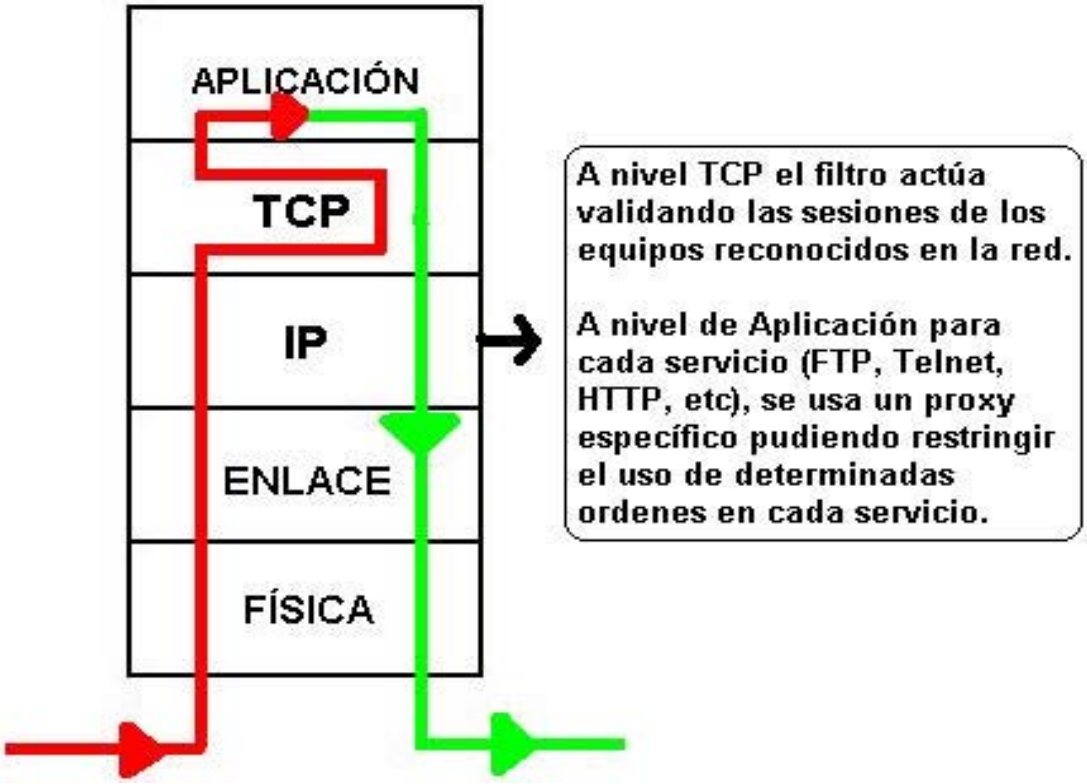


Figura 3.13 Proxy Server

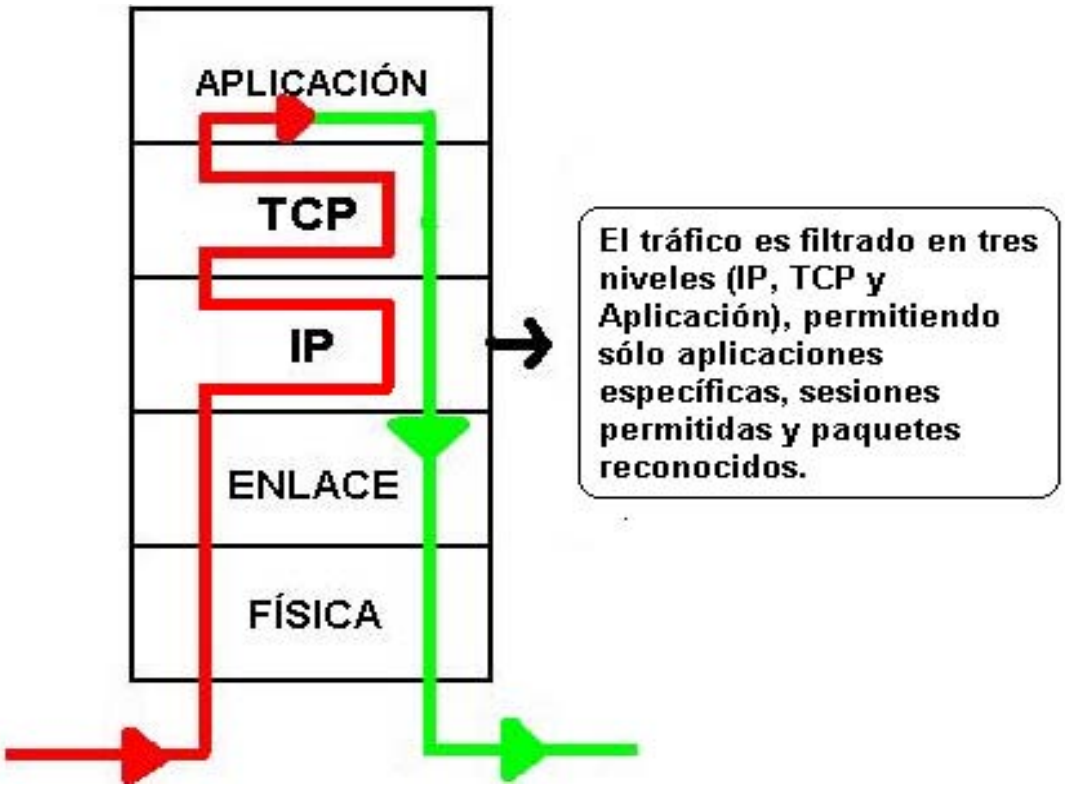


Figura 3.14 Stateful Multilayer Inspection

Como vemos en las figuras anteriores un firewall permite examinar el tráfico de la red tanto entrante como saliente con base en ciertas reglas específicas, y mientras que un firewall de filtrado de paquetes generalmente se implementa mediante un router, el proxy server (aplicación software) se ejecuta sobre un Gateway o Bastión Host, como se muestra en la figura 3.15.

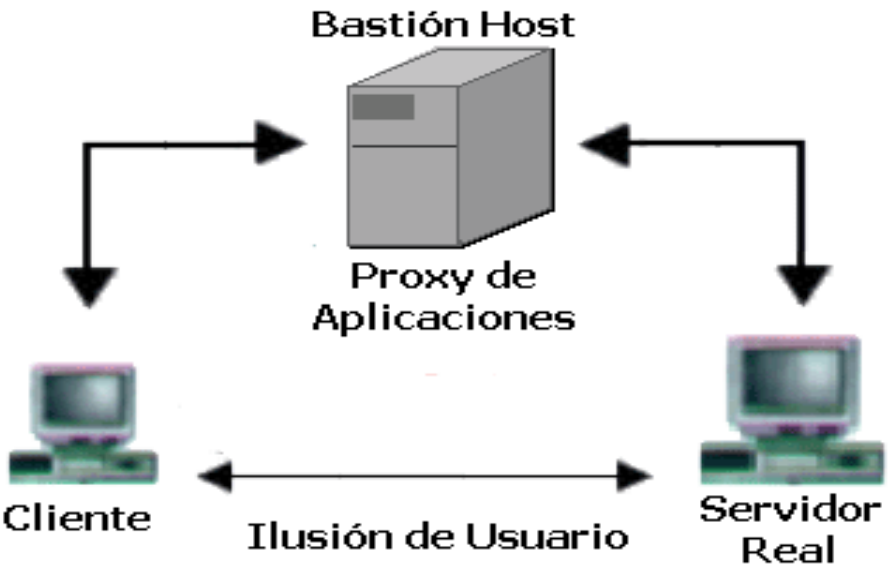


Figura 3.15 Aplicación de un Servidor Proxy

Un Servidor Proxy implementa mayor protección y servicios, ya que permite conectar con una sola dirección pública varias máquinas de la red (NAT, Network Adress Translation) ocultando las direcciones de red verdaderas, pero es más costoso y en ocasiones su rendimiento no es justificable, además que no es transparente como en el caso del firewall de filtrado de paquetes que sí lo es, la desventaja de éste es que las direcciones de la red son visibles desde el exterior y las reglas de filtrado pueden evadirse o engañarse a causa de errores en las mismas, pero su costo es más bajo.

En la práctica los firewall utilizan dos o más técnicas de filtrado a la vez para aumentar su eficacia, permitiendo una inspección multicapa.

El siguiente paso en nuestro sistema de protección es analizar y evitar las técnicas de exploración y enumeración.

3.2.1.2 EXPLORACIÓN Y ENUMERACIÓN

Estas técnicas son empleadas con el fin de obtener el rango de direcciones IP empleadas en la red (exploración), y cuentas de usuario para tratar de escalar privilegios en el entorno de red o grupo de trabajo (enumeración).

La exploración o escaneo de puertos consiste en aprovechar las características utilizadas por el protocolo TCP para el enlace de comunicación (figura 3.9), los ataques más comunes de escaneo son los siguientes:

1 **TCP.** El cliente realiza el proceso completo de conexión (SYN - SYN ACK – ACK), por tal motivo es muy fácil de detectar.

2 **SYN.** El cliente inicia la comunicación enviando un SYN, si el servidor responde con SYN ACK, el cliente envía un RST, y por lo tanto sabemos que el puerto está abierto pero no establecemos conexión.

3 **FIN.** El cliente envía un paquete tipo FIN para iniciar la conexión (algo que no es común ya que la comunicación debe empezar con SYN), de tal modo que el servidor responde con un RST para todos los puertos cerrados, y por conclusión podemos saber cuáles puertos están abiertos.

4 **XMAS TREE.** Es similar a la anterior pero un poco más sofisticada ya que el paquete enviado por el cliente además de llevar activada la bandera de FIN, también activa las banderas URG y PUSH.

5 **NULL.** El cliente envía un paquete con todas las banderas desactivadas provocando que el servidor envíe un RST en todos los puertos cerrados.

Las pruebas basadas en UDP dependen de varios factores, ya que por ser un protocolo no orientado a conexión no es muy confiable, la respuesta común a este tipo de peticiones es a través de mensajes ICMP (ejem. “puerto inalcanzable”, con lo que se determina que el puerto no está activo). Una forma de comprobar que existe un sistema de filtrado dentro de la red es enviar un paquete UDP al puerto cero, lo que debería provocar una respuesta ICMP como en el ejemplo anterior, sí no hay respuesta quiere decir que existe un dispositivo filtrando el tráfico hacia la red.

La enumeración o acceso se lleva a cabo a través de técnicas de crackeo de cuentas de usuarios mediante comprobaciones en línea y la ayuda de herramientas específicas empleadas para este fin, aunque también existe la posibilidad de hacer este tipo de pruebas fuera de línea una vez que se obtengan los archivos de cuentas y contraseñas, aplicando técnicas de diccionario, fuerza bruta o criptoanálisis, como las empleadas por los programas: Caín y Abel, Hydra, Jhon the Ripper, etc. sobre los archivos de contraseñas (SAM en Windows, passwd y shadow en Linux). La penetración en la red es el siguiente paso a seguir para llevar a cabo esta tarea.

Para ello es necesario aprovechar los *”exploits”* en el sistema, que no son otra cosa que las vulnerabilidades o agujeros propios del sistema los cuales pueden ser utilizados para infiltrarse, de tal modo que la información recabada durante el proceso de reconocimiento es de gran ayuda en esta fase.

Una vez identificado el exploit a utilizar para el sistema en particular se ejecuta el *“payload”* adecuado, el cual consiste en la aplicación de un proceso dentro de otro proceso, es decir se inyecta dentro del proceso remoto el proceso local que pretende vulnerar la seguridad del equipo en cuestión para comprometerlo, y según sea el payload utilizado se podrán realizar diferentes operaciones entre ambos hosts. Dependiendo del exploit, la conexión y el resultado de la explotación

del sistema atacado, dependerá el número de payload's a utilizar. La figura 3.16 ilustra el exploit y el payload de un sistema.

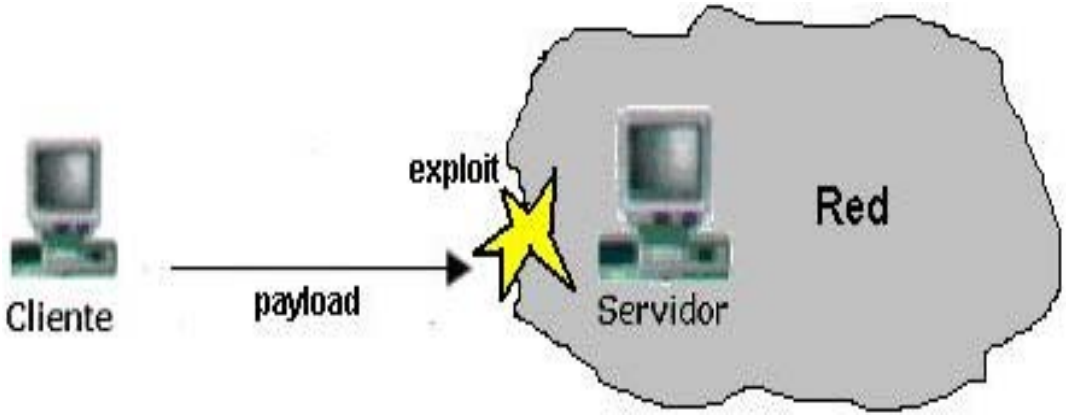


Figura 3.16 Exploid y payload

Como ejemplo citaremos el exploit encontrado en los sistemas Windows (hasta julio del 2003 que se lanzó el parche), en el servicio RPC (Remote Procedure Call, Llamadas a Procedimientos Remotos), en particular el servicio DCOM (Modelo de Objetos de Componentes Distribuidos), el cual presentaba un error al momento de controlar las solicitudes que le llegaban, con lo cual, mediante un payload era posible apuntar al puerto 135 (puerto utilizado para este servicio), del host remoto y provocar un desbordamiento de memoria provocando la falla en el servicio dejando la posibilidad de ejecutar código arbitrario y obtener privilegios dentro del sistema.

Los programas orientados a este tipo de técnicas cuentan con una base de datos que contiene los exploits reconocidos para los sistemas operativos soportados y los payload´s que se pueden introducir por el exploit especificado, de tal forma que cada exploit reconocido dentro de la base de datos está asociado a un conjunto de payload´s el cual puede contener uno o varios payload´s que aprovechan el exploit en el sistema en particular. Tal es el caso de la herramienta Metasploit utilizada en

Windows y Linux, la cual hace uso de esta técnica, tal como se observa en la figura 3.17.

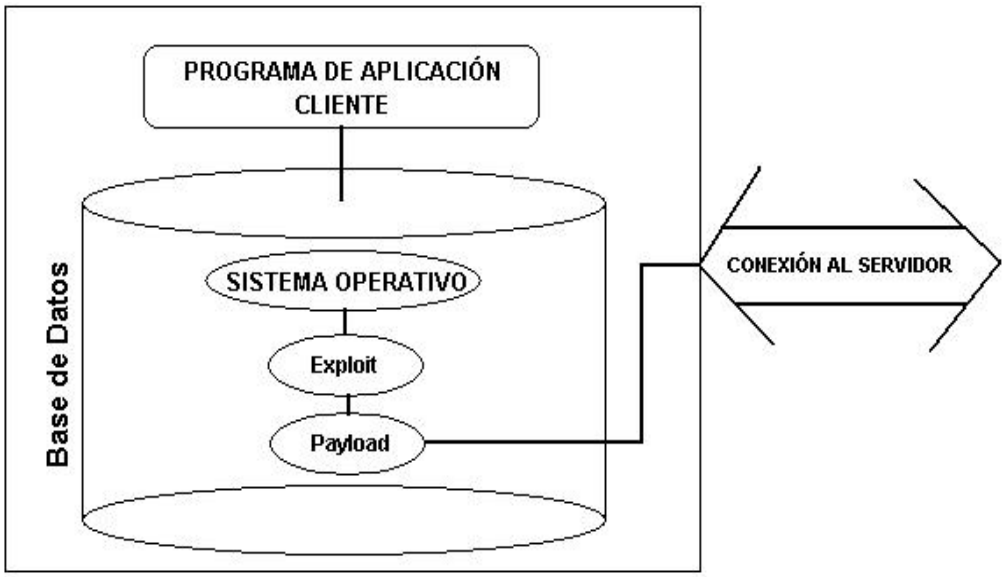


Figura 3.17 Utilización de la base de datos de exploit´s y payload´s

Por eso una de las recomendaciones al momento de llevar a cabo la implementación de políticas de seguridad es deshabilitar todos los servicios TCP/IP que no sean necesarios, y mantenerse al tanto en cuanto sean descubiertas nuevas vulnerabilidades para los sistemas que estemos utilizando en la Intranet.

Como ya lo había mencionado, las actualizaciones forman un aspecto importante dentro de este proceso porque permiten la instalación de los parches necesarios en el momento que se descubren nuevas vulnerabilidades y contrarrestar el efecto de los exploits.

3.2.1.3 ACESSO

Hasta este punto, el ataque ha consistido en averiguar la configuración de la red y de los sistemas que se encuentran operando, y se ha encontrado la forma de introducirse dentro del sistema objetivo de ataque o algún otro, a través del cual se pueda llegar hasta el host remoto deseado aprovechando los hoyos de seguridad que existen dentro de la red, logrando evadir los firewall`s, IDS's/IPS's, y utilizado una variedad de herramientas como las que ya se han mencionado para lograr penetrar hasta el punto deseado y/o permitido.

Una vez que el atacante ha logrado llegar al objetivo y ha alcanzado privilegios dentro del sistema comprometido, se instala un programa "backdoor" para ocultar el acceso y ejecutar todo tipo de herramientas necesarias para extraer información confidencial, tales como: keyloggers, spayware y rootkits entre otros.

En esta fase el ataque ha comenzado y el sistema se encuentra comprometido, de tal forma que el administrador ha perdido el control del mismo, y probablemente en un principio esta acción pase desapercibida debido a los programas introducidos dentro del equipo para ocultar la infiltración, porque aunque se tenga un monitoreo constante del tráfico, servicios y de los principales equipos dentro de la Intranet, estos programas tienen la capacidad de falsear la información que se obtiene de las herramientas administrativas y de supervisión, dando la impresión de que todo está en orden.

Lo más prudente ante esta situación es deshabilitar de la red el equipo en cuestión, y evaluar los daños producidos por el ataque para enmendar las fallas encontradas y cubrir los aspectos de seguridad que dieron origen a dicho ataque, para ello se podrá recurrir en ocasiones a técnicas de análisis forense en sistemas de cómputo.

3.2.1.4 MANTENER EL ACCESO

Cuando se descubre una vulnerabilidad dentro de un sistema que se pretende atacar, la primera regla a seguir es no apresurar dicha acción, sino evaluar la situación a modo que el ataque no sea descubierto antes de concluirse. Para ello se hace uso de “troyanos” para crear puertas traseras (backdoors), los cuales se instalan dentro de la víctima disfrazados dentro de alguna aplicación solicitada por el usuario al momento de descargar algún programa, un correo, o algún otro medio electrónico, sin que se percate de ello ya que la aplicación solicitada está infectada con el fragmento del programa malicioso y al ejecutarse ésta, se ejecutará también el troyano que a su vez puede invocar y desencadenar otros programas de manera remota, “enganchándose” al host desde el cual se pretende llevar a cabo el ataque, permitiendo una vía de comunicación oculta (backdoor).

La finalidad y acciones de este malware dependerá de la idea en particular para el que hayan sido creados, y permitirán al atacante encubrir muchas de sus acciones mientras se encuentre en el sistema afectado.

3.2.1.5 ENCUBRIMIENTO

Una vez perpetuado el ataque el siguiente reto es borrar todo rastro de las acciones realizadas dentro del equipo atacado, así como de las herramientas y programas utilizados para que no se descifren las técnicas empleadas a manera de no dejar ninguna pista que pueda conducir al culpable. Los pasos a seguir son los siguientes:

1 Deshabilitar los sistemas de auditoría dentro del equipo en cuestión.

2 Borrar log´s y aplicaciones utilizadas que hayan servido para comprometer al sistema.

3 Borrar la evidencia de las herramientas y programas usados, en este caso se puede utilizar la “esteganografía” (técnicas que permiten ocultar información o programas dentro de otro; generalmente inmersas en imágenes o sonido, de manera que su misma existencia sea inadvertida).

La forma y variedad con que se puede llevar a cabo un ataque son tan diversas como las herramientas que se pueden utilizar, además de las circunstancias y características particulares de la red, pero hemos podido establecer un marco de referencia general que permita la creación de un modelo de seguridad orientado a garantizar la comunicación entre los protocolos TCP/IP, dando una breve introducción de éstos para poder entender su funcionamiento, al mismo tiempo que se muestran las fallas de seguridad inherentes a su diseño y comportamiento, entrando ahora al campo de la información que viaja dentro de esta vía de comunicación (TCP/IP), y que son finalmente los datos de aplicación del usuario.

3.3 ENCRIPTACIÓN DE DATOS

El enlace de comunicación entre dos dispositivos dentro de la arquitectura cliente-servidor TCP/IP, tiene como finalidad el compartir información de diversas aplicaciones creando una ruta bidireccional entre ambos equipos para el envío y recepción de datos. Una vez listo el canal de comunicación, estos datos hacen su recorrido a través de esta vía hasta llegar a su destino, de tal forma que podríamos hacer una analogía de este servicio con el servicio postal convencional, donde la dirección contiene los datos del destinatario a donde se quiere hacer llegar la carta; lo que equivale a la dirección física y lógica (MAC e IP).

El cartero es el medio de transporte; equivalente al protocolo TCP, y la carta son los datos o información que queremos hacer llegar al destinatario, de tal forma que si nuestra carta se extraviara, fuera robada, llegará a una dirección equivocada, o simplemente fuera leída por alguien más antes de llegar a su destino final,

cualquiera de estas situaciones podrían repercutir en graves consecuencias si la información que contiene revela información confidencial e importante acerca de nosotros, de una empresa u organización. De la misma forma sucede con la información que enviamos a través de una red y debemos asegurar que bajo las circunstancias ya mencionadas la información se mantenga a salvo.

La criptografía es la técnica utilizada para garantizar el contenido e integridad de la información en la comunicación entre dos entidades permitiendo la autentificación de ambas para una mayor seguridad.

Para ello la información original denominada información en claro o plana, se somete a un proceso de cifrado a través de un algoritmo el cual utiliza una clave, convirtiéndolo en galimatías ilegible llamado criptograma, el cual contiene la misma información que los datos en claro, sólo que ahora podrán ser entendidos únicamente por las entidades que conozcan el algoritmo de cifrado (clave).

El uso de estas técnicas se remonta a miles de años, y a través del tiempo se han ido sofisticando y volviéndose más complejas con la ayuda de los avances tecnológicos disponibles en cada época.

3.3.1 ALGORITMOS DE CIFRADO

Los algoritmos de cifrado pueden clasificarse en dos grandes grupos: simétricos y asimétricos. Los primeros utilizan únicamente una clave; llamada privada, para cifrar y descifrar la información, por tal motivo son conocidos también como sistemas de clave privada, y los segundos utilizan dos claves distintas, la clave privada y otra clave; llamada pública, el remitente utiliza la clave pública del destinatario para cifrar el mensaje y sólo la clave privada del destinatario podrá descifrarla, estos sistemas son también llamados de clave pública.

Para ejemplificar utilizaremos el sistema RSA, el cual fue descrito a finales de la década de los años 70 y debe su nombre a las iniciales de sus creadores: Ron Rivest, Adi Shamir y Len Adleman. Utiliza un algoritmo asimétrico, y que en la actualidad es uno de los más utilizados en los sistemas de seguridad basados en encriptación de datos. El algoritmo es el siguiente:

1 Escogemos dos números “p” y “q”, tal que p y q sean primos.

2 Obtenemos el valor de un número “n” igual al producto de p por q:

$$n = p \times q$$

3 Obtenemos una función de n:

$$f(n) = (p-1)(q-1)$$

4 Obtenemos la clave pública “e”, tal que:

$1 < e < f(n)$; y “e” sea número primo relativo de f(n)

de modo que (f(n) / e) No es número entero

5 Obtenemos la clave privada “d”, tal que:

$d = ((X * f(n)) + 1) / e$; X = {1,2,3... } hasta obtener un número entero en la expresión.

Una vez calculadas las claves públicas y privadas podemos utilizarlas para la encriptación/desencriptación de datos a partir de las siguientes expresiones:

Cifrado: $C = M^e \bmod(n)$

Descifrado $M = C^d \bmod(n)$; donde M = Mensaje plano

La complejidad del algoritmo depende del número de bits que se utilicen en los cálculos. Ilustraremos el algoritmo con dos números pequeños p y q.

1 Sea p = 3 y q = 11

2 n = p x q
n = 3 x 11 = 33

3 f(n) = (p-1)(q-1)
f(n) = (3-1)(11-1) = 20

1 e = 3 ; ya que 20 / 3 = 6.6666 , y no es entero

5 d = ((X * f(n)) + 1) / e
d = ((1 x 20) +1) / 3 = 7

Supongamos que queremos cifrar el número 2.

Cifrado C = M^e mod(n) ; M = 2, ya que es el mensaje a enviar
C = 2^3 mod(33)
C = 8 mod(33) = 8 ; Ahora nuestra cifra es 8

Y para obtener nuevamente el mensaje utilizamos la siguiente expresión:

Descifrado M = C^d mod(n)
M = 8^7 mod(33)
M = 2097152 mod(33) = 2 ; y obtenemos nuevamente el mensaje plano.

Podemos observar que pese a que p y q fueron elegidos de tal forma que tuvieran valores pequeños, las operaciones arrojan números que crecen considerablemente. Gracias a esta peculiaridad la complejidad del algoritmo hace que sea difícil descifrar la información, y aunque se conozca el algoritmo utilizado sin las claves es muy difícil intentar hacerlo.

En el siguiente ejemplo (figura 3.18), utilizaremos los mismos valores de p y q; 3 y 11 respectivamente, para cifrar mensajes de texto asignándole a cada letra del alfabeto (a,b,c,..,z) los valores (1,2,3...,26), mediante un programa escrito en C, mostrando el valor numérico tanto del cifrado como del descifrado y posteriormente obtener de nuevo el mensaje plano original.

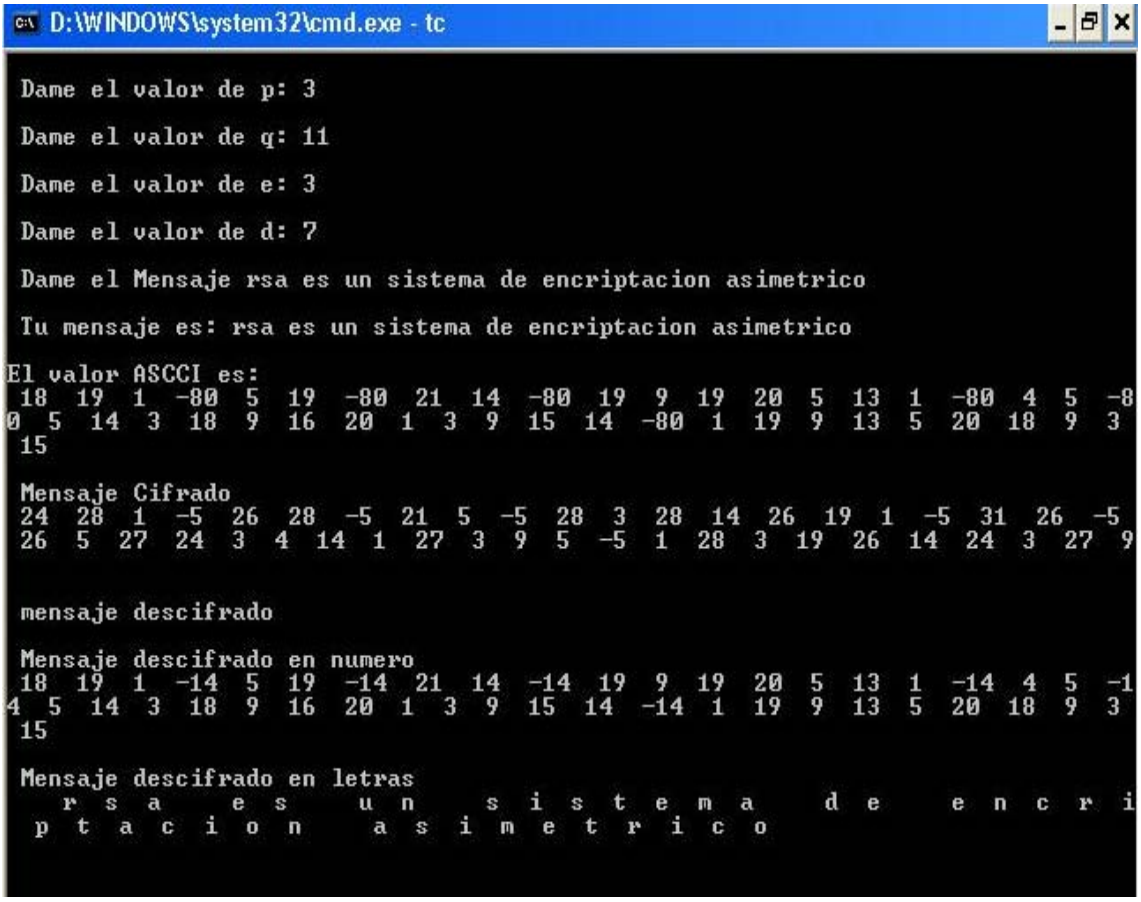


Figura 3.18 Programa en C que cifra texto ASCII en RSA

Ahora cambiaremos los valores de p y q, asignándoles los valores 17 y 23 respectivamente, sobre el mismo texto plano para observar las diferencias, figura 3.19.

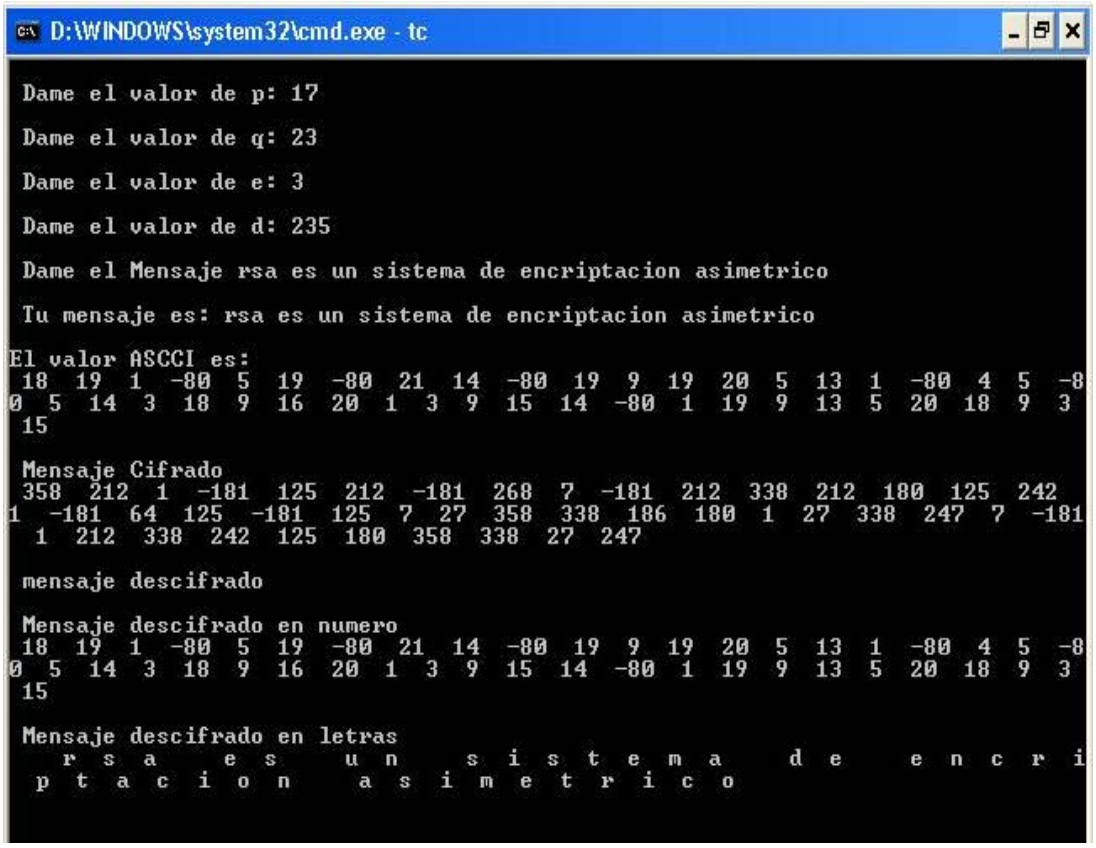


Figura 3.19 Cambiando los valores de p y q del ejemplo en la figura 3.18

Como podemos observar en las figura 3.18 y 3.19 las claves de cifrado dependen de los valores de p y q, y sin importar qué valores tomen se podrán cifrar y descifrar mensajes sin que esto afecte al resultado siempre y cuando cumplan con las condiciones dentro del algoritmo especificado.

3.3.2 PROTOCOLOS DE ENCRIPTACIÓN EN TCP/IP

Del mismo modo la información que circula por la red en claro puede ser protegida frente a vulnerabilidades y técnicas como el sniffing, robo de sesiones, paswords y contraseñas, utilizando protocolos de seguridad basados en la encriptación de datos mediante algoritmos asimétricos en las capas del modelo TCP/IP.

A grandes rasgos estos protocolos se diferencian según la capa TCP/IP en la que trabajen, y además de proporcionar un método de confidencialidad en el envío de la información, también ejecutan otro tipo de funciones como: compresión, autenticación e integridad de los datos. Entre los más destacados están:

1 **SSL.** (Secure Socket Layer – Capa de Conexión Segura), para comunicación entre navegadores y servidores web.

2 **PGP.** (Pretty God Privacy – Privacidad Bastante Buena), encriptación de correos electrónicos.

3 **S/MIME.** (Secure Multipurpose Internet Mail Extensions – Extensiones de Correo Internet Multipropósito Seguras), para envío y recepción de mensajes electrónicos de todo tipo (multimedia).

4 **SSH.** (Secure SHell – Interfaz Segura), establece sesiones de tipo seguro para la transmisión de datos.

5 **IPSec.** (IP Security – IP Segura), para comunicación segura entre dispositivos de red, y establecimiento de redes privadas virtuales (VPN´s).

Cada una de estas herramientas implementa un modelo de seguridad distinto en función de las necesidades propias a satisfacer y características de la Intranet, es decir, si la red que tenemos no tiene conexión a Internet no es muy necesario instalar SSL, ya que éste trabaja sobre las capas de aplicación y trasporte TCP de Internet (FTP, HTTP, Gopher,...), y más concretamente tenemos HTTPS (Hypertext Transfer Protocol Secure – Protocolo Seguro de Transferencia de Hipertexto), que mediante SSL asegura el protocolo HTTP para navegación segura. Es utilizado principalmente por entidades bancarias, tiendas virtuales de compras en línea y todo tipo de servicios que requieran el envío de información

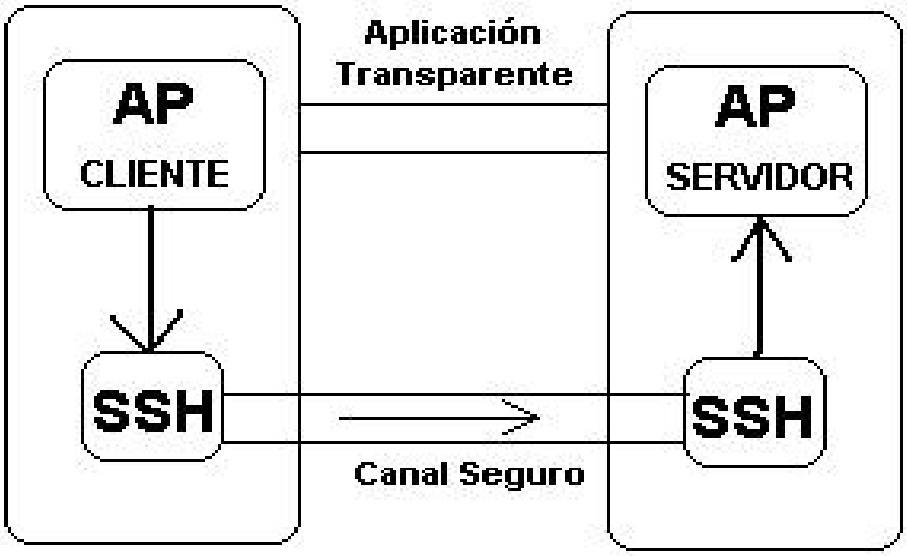
confidencial a través de Internet, ya que crea un canal independiente de cifrado entre el servidor y el cliente.

Por otro lado, la utilidad de una red se basa en la facilidad para compartir recursos e información, de modo que podemos lograr un intercambio de archivos entre equipos de forma segura a través de SSH por medio de conexiones remotas, ya que permite la transmisión segura de cualquier tipo de datos, el cual al igual que HTTPS, crea un canal de comunicación segura encriptando los datos que viajan a través de éste, sustituyendo los habituales servicios de Telent o FTP.

Para tener una idea más clara sobre estos protocolos de encriptación analizaremos con más detalle SSH.

3.3.3 SSH

Como mencionamos anteriormente SSH es un protocolo que facilita la comunicación segura entre equipos bajo el modelo cliente-servidor a través de un túnel de comunicación (tunneling), de tal forma que los datos son tomados de la aplicación (cliente) que requiere enviarlos y los reenvía por un canal seguro, el servidor recoge los datos al otro lado del túnel y los envía a la aplicación que se hará cargo de procesarlos. Esto permite generar conexiones de servicios inseguros (http, ftp, smtp, pop3, etc.) sobre SSH (portforwarding), tal como se ilustra en la figura 3.20.



3.20 Port Forwarding en SSH

El protocolo SSH se establece en tres niveles:

1 **Nivel de Transporte.** Se realiza la autentificación del servidor, se establece un canal seguro de cifrado, integridad de datos e identificador único por sesión.

2 **Nivel de Usuario.** Se realiza la autentificación del usuario por medio de claves públicas y privadas, de contraseña o basada en la procedencia del host.

3 **Nivel de Conexión.** Encargado de realizar sesiones simultáneas.

Existen dos versiones de SSH: SSH1 y SSH2, los cuales son incompatibles entre sí, y solo diremos que SSH2 es un protocolo más confiable que SSH1, ya que reestructura la implementación, y utiliza el algoritmo DSA (Digital Signature Algorithm – Algoritmo de Firma Digital), que es más moderno y soluciona defectos que se encuentran en RSA.

3.3.4 CONFIGURACIÓN BÁSICA DE SSH

La configuración que realizaremos está basada en OpenSSH 3.8.1 y plataforma Windows. Una vez que los hayamos instalado de la manera habitual por medio de un menú interactivo de ventanas procedemos a la configuración (figura 3.21).

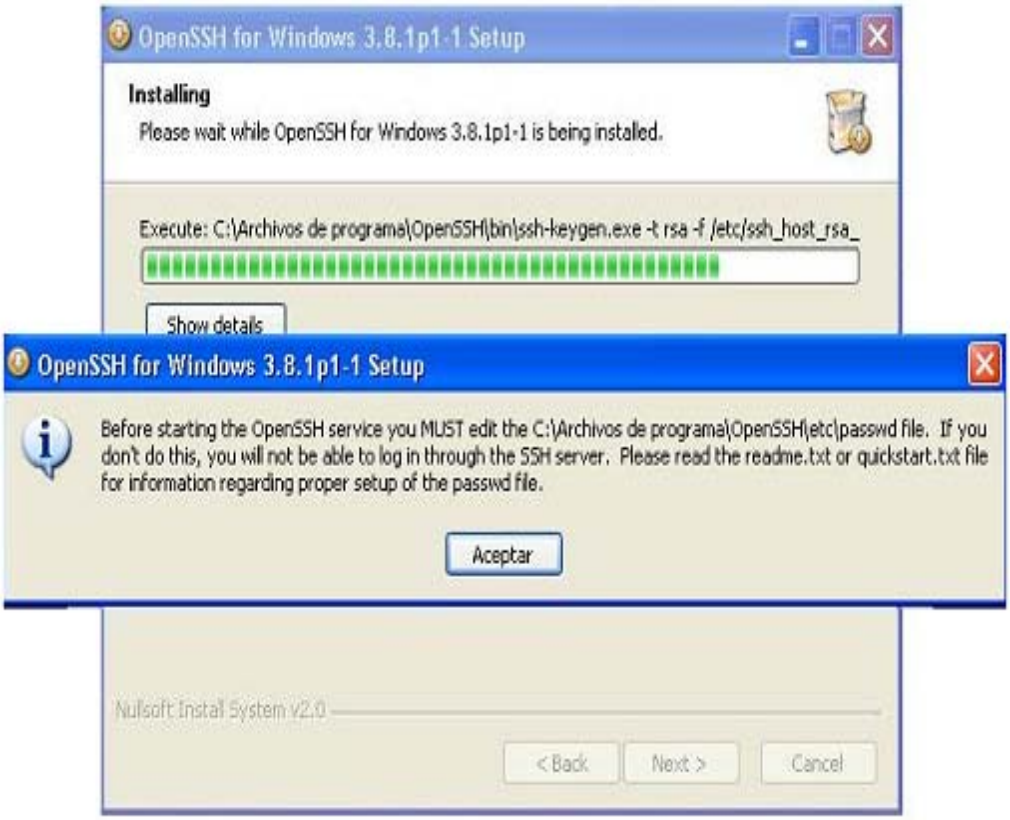


Figura 3.21 Instalación de SSH

Al observar la figura anterior aparece un mensaje de advertencia que indica que se debe editar el archivo “passwd” para poder acceder al servidor SSH. Este archivo debe contener los usuarios locales y de dominio que se conectarán a este servidor, ya que como acabamos de instalar SSH este archivo está vacío, o no existe en cuyo caso tendremos que crearlo.

Para hacerlo tenemos que ir a la carpeta “bin” que se encuentra en el archivo “OpenSSH”, en la ruta que hayamos elegido durante la instalación; generalmente

“C:\Archivos de Programa\OpenSSH\bin”, y desde el símbolo del sistema de Windows tecleamos lo siguiente:

mkpasswd –l –u usuario >> ..\etc\passwd

Con esta instrucción hemos logrado dos cosas, primero crear el archivo passwd dentro de la carpeta “etc.” del directorio OpenSSH, y segundo dar de alta a un usuario (-l –u usuario), donde “-l”, significa que es local y “-u” para dar de alta al usuario que sustituiremos por el nombre real del usuario. Para los usuarios de domino se utiliza:

mkpasswd –d –u usuario >> ..\etc\passwd

La siguiente figura 3.22, muestra la instrucción.

Figura 3.22 Alta de usuarios en el archivo passwd e SSH

Los nombres de usuarios que demos de alta en el archivo “passwd”, deben ser los mismos que se utilizan tanto para equipos locales como para acceder a la red, de lo contrario aparecerá un mensaje diciendo que no se ha encontrado el nombre de usuario, y casi de la misma forma creamos el archivo “group”, para asignar permisos a los usuarios mediante la siguiente instrucción:

mkgroup –l >> ..\etc\group

Posteriormente hay que configurar las variables del sistema, para ello vamos al icono de “Mi PC” y hacemos click con el botón derecho y seleccionamos la opción “propiedades”. Aparecerá una nueva ventana con varias pestañas en la parte superior, de las cuales seleccionamos la que dice “Opciones Avanzadas”, entonces seleccionamos la casilla “Variables de entorno” dentro de ésta.

Una vez que estemos ahí tenemos que hacer dos cosas: una, es verificar que el valor (ruta) de la variable “Path” sea la del archivo “bin” (“C:\Archivos de programa\OpenSSH\bin”), para ello podemos elegir la casilla “Modificar”. Y segunda es crear la variable “HOME” con la opción de la casilla “Nueva” con el valor “C:\Archivos de programa\OpenSSH”, tal como se muestra en la figura 3.23.

Figura 3.23 Configuración de las variables de entorno de SSH

Ahora procederemos a crear los archivos con las claves públicas y privadas que utilizaremos para el envío y recepción de mensajes encriptados. La instrucción es la siguiente:

ssh-keygen –t rsa

El resultado lo podemos observar en la siguiente figura 3.24.

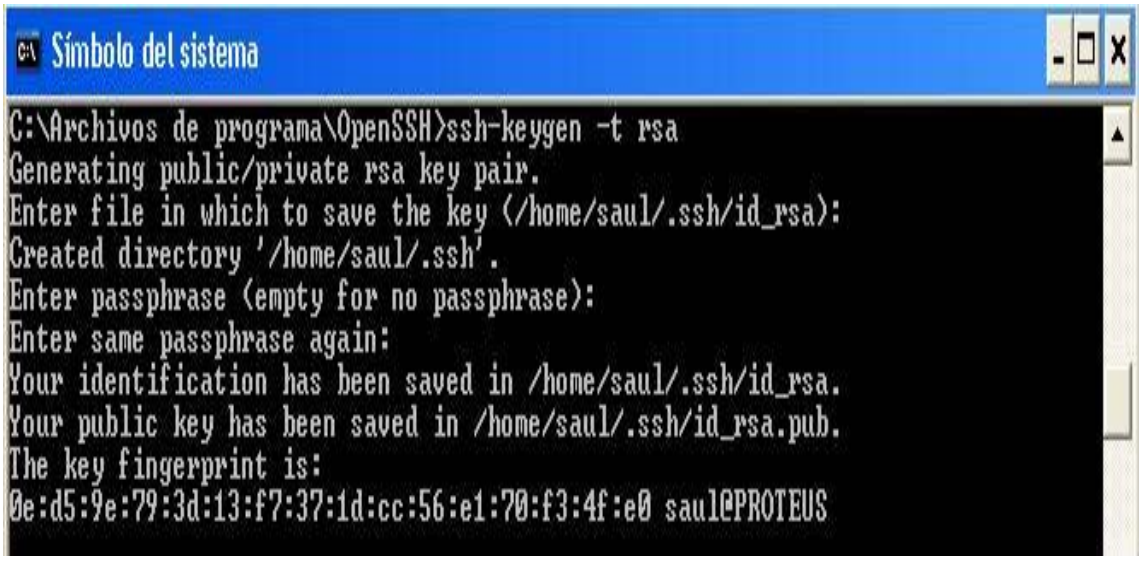


Figura 3.24 Creación de la llave pública y privada (RSA) en SSH

Las llaves se guardan dentro de la carpeta “.ssh” en la ruta “D:\Documents and Settings\Adminisrador”, donde “Administrador” es el nombre del usuario con privilegios de administrador, este archivo se crea al momento de ejecutar dicha instrucción. También se pueden crear claves “dsa” cambiando “rsa” por “dsa” en la instrucción anterior.

En la figura 3.25 podemos ver el contenido del directorio “.ssh” donde se encuentran el archivo “id_rsa” que contiene la clave privada, así como el archivo “id_rsa.pub” con la clave publica; las claves tienen una longitud de 1024 bits.

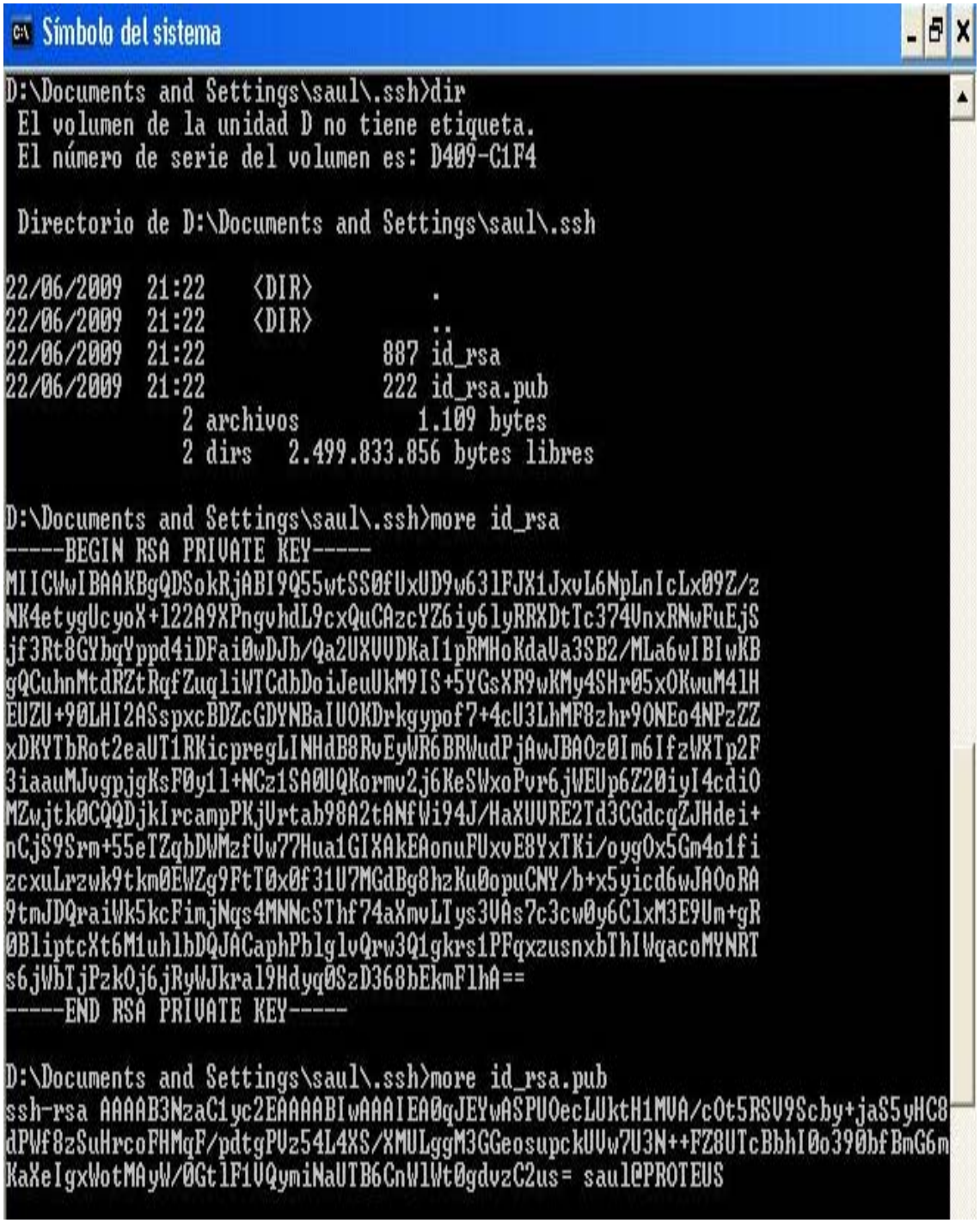


Figura 3.25 Valor de la clave privada y la clave pública del servidor SSH

Una vez que hemos comprobado que ya contamos con las claves de cifrado tenemos que crear el archivo "authorized_keys" (sí es que no se ha creado

durante la instalación) donde se ingresarán todas las llaves públicas de los clientes incluyendo la del servidor para el intercambio de datos, así que tecleamos lo siguiente desde la ruta donde está el archivo ".ssh":

more id_rsa.pub >> "C:\Archivos de programa\OpenSSH\etc\authorized_keys"

La figura 3.26 muestra la ejecución de la instrucción.

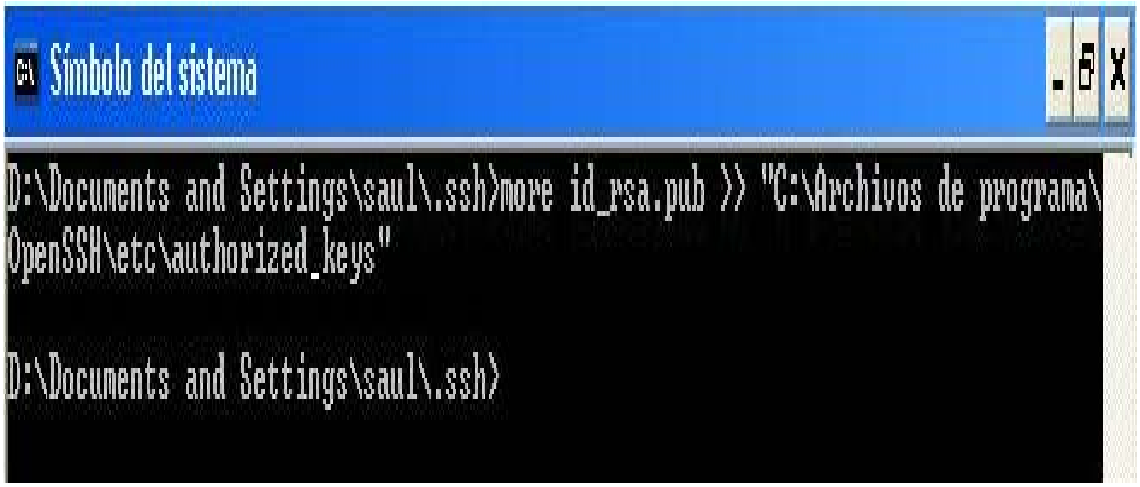


Figura 3.26 Creación del archivo "authorized_keys" de SSH

Hay que observar que el archivo "authorized_keys" se creó en la carpeta "etc." dentro de OpenSSH, y debemos de considerar esta misma ruta para el archivo de configuración "sshd_config" (dentro de la misma carpeta "etc."), el cual debemos editar para verificar que todos los parámetros sean los correctos para que el servidor autentifique por medio de claves públicas, figura 3.27.

Figura 3.27 Archivo “sshd_config” de SSH

Este archivo de configuración permite establecer los distintos parámetros bajo los que correrá el servidor de SSH, como son el puerto de escucha (22 por default), las rutas de los directorios donde hay que buscar las claves, tiempo de espera para que los usuarios se autentifiquen, versión de SSH, utilizar compresión, etc.

Una vez que hemos realizado la configuración básica del servidor podemos iniciarlo, para ello usamos la siguiente instrucción: net start opensshd, desde la carpeta “etc.”, figura 3.28:

Figura 3.28 Iniciando el servidor de SSH

Como podemos observar en la figura anterior el servidor se ha puesto en marcha, y la conexión de los usuarios se pude hacer desde programas cliente con entorno gráfico facilitando así la tarea del envío y recepción de archivos, los cuales el administrador puede especificar en una ruta determinada para el acceso de cada usuario en particular. Para ello se deberá modificar el archivo passwd para indicar cuál será dicha ruta, además de dar los permisos necesarios de escritura y/o lectura.

3.4 RESPALDO DE LA INFORMACIÓN

3.4.1 COPIAS DE SEGURIDAD Y TOLERANCIA A FALLOS

En éste modelo de seguridad trato de establecer las medidas básicas de prevención y corrección para enfrentar los distintos tipos de amenazas para los activos más importantes que conforman una red: los datos, ya que por poner un ejemplo pensemos que la posibilidad de que se produzca un fallo en los sistemas ya sea a nivel de hardware o software por cualquier causa: virus, error humano, desastre natural, etc., existe. Aunque es cierto que la fiabilidad de estos sistemas ha aumentado, y si nos vamos al extremo de suponer la pérdida tanto de software como de hardware diremos que la pérdida de información es probablemente más

valiosa que el propio equipo, ya que el equipo por muy costoso que sea puede ser reemplazado pero la información perdida ya no.

Para enfrentar este tipo de situaciones existen dos técnicas que pueden implementarse en una red para protección de datos y fallos: las copias de seguridad y los sistemas tolerantes a fallos.

Las copias de seguridad sugieren un esquema de duplicidad de datos, es decir, mantener toda aquella información relevante en copias duplicadas por si se pierde el original ya sea total o parcialmente sin importar por que causa, convirtiéndose ésta en una práctica necesaria.

Los sistemas tolerantes a fallos por otro lado son aquellos capaces de soportar determinados tipos de fallos en la medida en que puedan soportarlos y para los cuales fueron pensados o diseñados, de tal forma que puedan seguir trabajando sin interrupción ni pérdida de información, ya que se basan prácticamente en la redundancia de componentes físicos.

3.4.2 DIFERENCIA ENTRE COPIAS DE SEGURIDAD Y TOLERANCIA A FALLOS

Ambas técnicas están ligadas desde el punto de vista conceptual para el fin con que son usadas: brindar un soporte ante alguna pérdida, solo que las copias de seguridad se basan en duplicar componentes lógicos (datos), y los sistemas tolerantes a fallos basan su funcionamiento en duplicar componentes físicos (hardware), como son: discos, cintas o incluso un servidor completo.

Una copia de seguridad hace posible seguir trabajando tras una pérdida de información una vez que se haya recuperado la información borrada de alguna de las copias, solo que para ello habrá de transcurrir un tiempo considerable para poder reanudar el sistema a su estado normal de trabajo.

Un sistema tolerante a fallos hará posible el seguir trabajando sin que exista interrupción alguna sin que haya inactividad en el sistema, pero si pensamos en un desastre natural o un evento que ocasionara la destrucción total del equipo indiscutiblemente una copia de seguridad sería la alternativa adecuada.

Como hemos visto ambas técnicas pueden ser complementarias dentro de una red en la que sea relevante el respaldo y protección de la información, siendo el carácter y volumen de los datos que se manejen un factor determinante en él, o los modelos a seguir para implementar las técnicas de respaldo.

Las copias de seguridad, la forma y los procesos para llevarse a cabo se trataron en el capítulo dos (2.3.1. “Modelos de Almacenamiento de Archivos para Backup”), así que ahora me enfocaré en los sistemas tolerantes a fallos. Sólo añadiré al respecto que el medio de almacenamiento a elegir para realizar las copias de seguridad dependerá de factores como: volumen de la información, tiempos de acceso de lectura/escritura requeridos, y por supuesto el costo.

3.4.3 IMPLEMENTACIÓN DE SISTEMAS DE TOLERANCIA A FALLOS

Estos sistemas pretenden un funcionamiento de manera continua sin interrupciones, aunque se susciten determinados fallos afectando en lo más mínimo su funcionamiento, claro ejemplo de lugares donde se utilizan son bancos, centrales telefónicas, y todas aquellas empresas u organizaciones que requieran ofrecer un servicio ininterrumpido y cuyas fallas resulten en pérdidas cuantiosas.

Este tipo de sistemas se basan en el concepto de redundancia, formados por diversos tipos de mecanismos y dispositivos que en conjunto hacen posible la tolerancia a fallos.

La redundancia consiste básicamente en la duplicación de determinados componentes, de tal forma que si uno de ellos falla, se active automáticamente el otro para que el sistema siga trabajando, los más utilizados son los siguientes:

1 **REDUNDANCIA DE DISCOS.** Consiste en mantener un duplicado del disco primario, de manera que los procesos de escritura se realicen simultáneamente en ambos; el disco primario y la copia, y en caso de fallo en el disco primario se conmute automáticamente la actividad al disco duplicado, a esta técnica se la conoce como “disk mirroring” (disco espejo), figura 3.29.

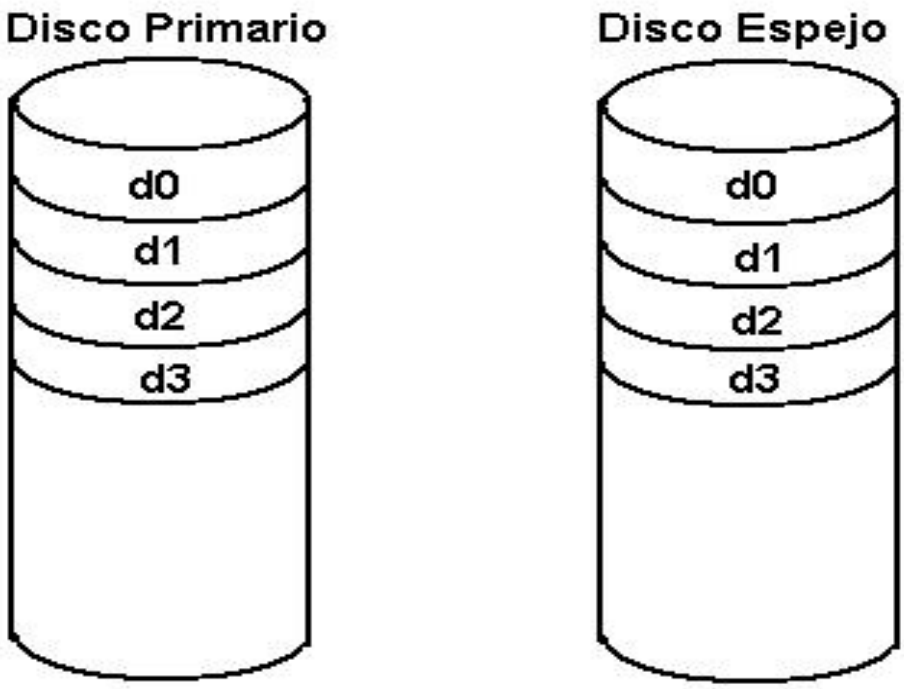


Figura 3.29 Disk Mirroring (Disco Espejo)

En ambientes donde se requiere mayor seguridad también se duplica la tarjeta controladora de manera que cada disco cuenta con su propia tarjeta, a esta técnica se le conoce como “disk duplexing” (disco duplicado).

2 **SISTEMAS RAID:** (Redundant Arrays of Inexpensive Disk – Arreglo Redundante de Discos Económicos), es una técnica de almacenamiento de datos que utiliza varios discos duros pero que son vistos como si se tratase solo de uno dentro del sistema.

Dependiendo de la configuración RAID utilizada llamada comúnmente “nivel”, estos sistemas son capaces de ofrecer mayor tolerancia a fallos, mayor rendimiento, mayor integridad y mayor capacidad, ya que los datos a almacenar son divididos en fragmentos (sectores, bytes o incluso bits), y son distribuidos entre los distintos discos, registrándose además la información de paridad de cada fragmento (en algunos niveles RAID).

Como los datos son fragmentados al momento de que el sistema lee o escribe sobre los discos por medio de varias cabezas trabajando en paralelo, se produce un aumento en la velocidad con que se llevan a cabo estas operaciones.

En esta técnica se utiliza una única unidad adicional de almacenamiento para dos o más unidades primarias, logrando un grado de seguridad aceptable para la mayoría de los casos, suponiendo una ventaja económica sobre el “disk duplexing” y “disk mirroring”, ya que requieren de una unidad adicional por cada unidad primaria.

3 **OTRAS REDUNDANCIAS.** En ambientes donde se requiere de mayor seguridad se cuenta además de las técnicas ya mencionadas, con redundancia de otro tipo de componentes como pueden ser las líneas de comunicación o los servidores en cuyo caso se les conoce como servidores espejo.

Otro factor que hay que considerar al momento de implementar sistemas de tolerancia a fallos, es la pérdida de información por fallas en el suministro de energía eléctrica por subidas, bajas, picos de tensión o pérdida total del suministro.

Para ello hay que considerar los sistemas UPS (Uninterruptible Power Systems – Sistemas de Alimentación Ininterrumpida), que se emplean precisamente para este tipo de situaciones de falla en el suministro eléctrico.

Estos sistemas están formados por baterías auto recargables y pueden trabajar en dos formas distintas: en modo espera (standby) o modo continuo (online). Los primeros solo entran en funcionamiento automáticamente cuando se produce una falla del suministro eléctrico, y los segundos trabajan de manera constante. El tiempo que brindan de energía puede ser poco pero suficiente para que se reanude el servicio eléctrico o se tomen las medidas para salvar los datos en los equipos.

Para determinar la potencia del UPS a utilizar hay que tomar en cuenta la potencia de todos los equipos que están conectados a la red, aunque no toda la potencia se consume, para ello existe un factor de potencia que depende del equipo que se trate, ya haciendo uso de la siguiente fórmula podemos calcular la potencia requerida por cada equipo:

Potencia = (Voltaje Suministrado) x (Corriente del equipo) x (factor de potencia)

Por ejemplo, en una PC el factor de potencia de la fuente de alimentación es de 0.6 aproximadamente, la corriente de 1.5 A y el voltaje suministrado de 127 V, con lo que tenemos una potencia de:

Potencia PC = (127 V) x (1.5) x (0.6) = 114.3 W

Como hemos visto los sistemas tolerantes a fallos se basan esencialmente en la redundancia, y pueden implementarse mediante la utilización de una sola técnica o la combinación de varias, dependiendo del nivel de seguridad que se pretenda alcanzar y se necesite satisfacer.

3.4.4 SISTEMAS DE ALMACENAMIENTO SAN Y NAS

Ahora bien, si hablamos de volúmenes muy grandes de información y entornos de trabajo donde las copias de seguridad pueden quedar obsoletas en cuestión de horas o inclusive minutos debido a la desbordante carga de datos en cambio constante, se necesita de una arquitectura con gran capacidad de almacenamiento como la que emplea el modelo SAN (Storage Area Network – Red de Área para Almacenamiento), se trata de una infraestructura planeada para la administración de un gran cantidad de unidades de almacenamiento, permitiendo que varios servidores accedan a estas unidades de modo compartido.

Un sistema de almacenamiento SAN permite conectar cientos de discos duros en el rango de los terabytes, esta arquitectura se considera una extensión del modelo DAS (Direct Attached Storage – Conexión de Almacenamiento Directo), donde la conexión entre el servidor y el sistema de almacenamiento es directo, o sea, punto a punto, pero en ambos casos las peticiones de datos al sistema de ficheros se hace de manera directa por las aplicaciones en los servidores, sólo que en DAS el almacenamiento es local y en SAN el almacenamiento es remoto, SAN utiliza dos protocolos de acceso: FC (Fibre Channel – Canal de Fibra Óptica), y/o Gibabit Ethernet, más recientemente iSCSI (internet Small Computers System Interface – Sistema de Interfaz de Internet para Pequeñas Computadoras) para acceder al sistema de ficheros.

Existe otro tipo de arquitectura que se amolda más fácilmente a volúmenes de información en un rango medio, (Network Attached Storage - Conexión de Almacenamiento en Red), en este sistema de almacenamiento las peticiones de

datos generadas por las aplicaciones acceden de manera remota al sistema de ficheros utilizando los protocolos CIFS (Common Internet File System – Sistema de Archivos Comunes para Internet), y NFS (Network File System – Sistema de Archivos en Red). Las figuras 3.30 y 3.31 ilustran las arquitectura SAN y NAS respectivamente

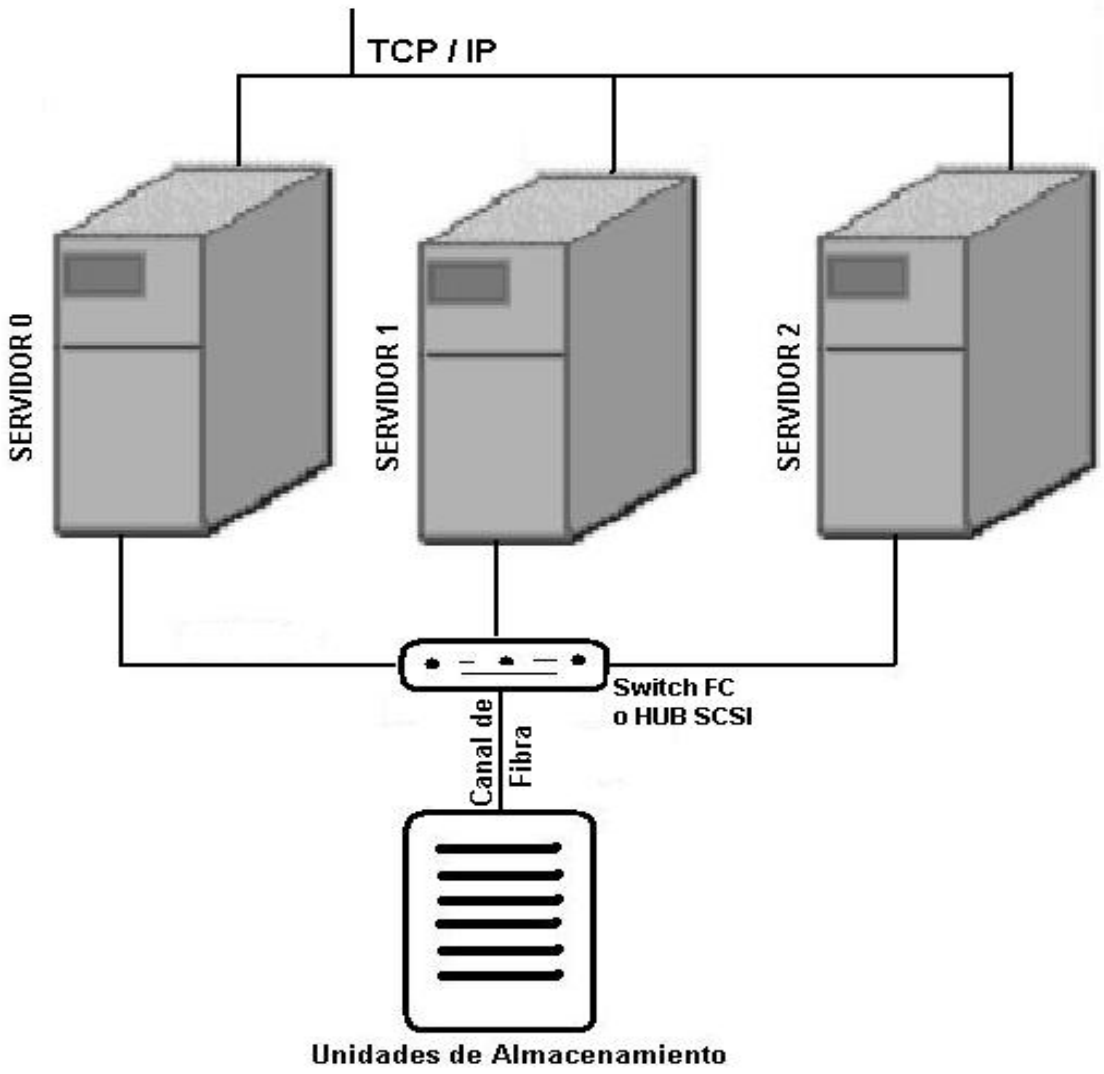


Figura 3.30 Modelo de Almacenamiento SAN

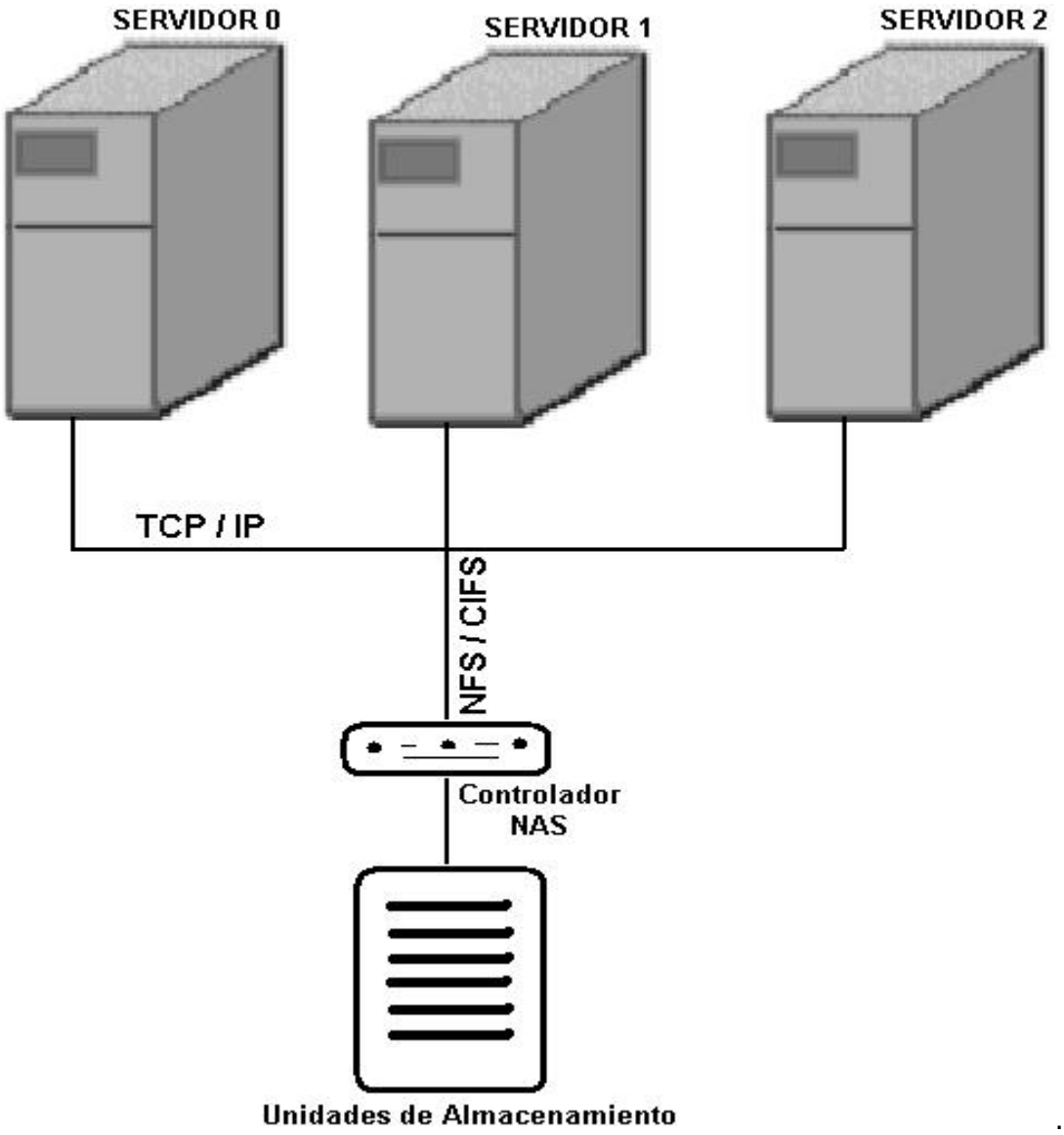


Figura 3.31 Modelo de almacenamiento NAS

Como podemos observar en las figuras 3.30 y 3.31, la diferencia entre ambos modelos radica en que en la arquitectura SAN las aplicaciones que se encuentran dentro de los servidores acceden a los datos de manera directa; aunque dichas aplicaciones sean llamadas de manera remota por los usuarios a través de la red TCP/IP, mientras que en la arquitectura NAS el acceso a los datos por parte de las

aplicaciones de los servidores se hacen de manera remota a través de la red TCP/IP, de manera que los servidores y los dispositivos de almacenamiento pueden estar físicamente muy separados, inclusive por ciudades.

Por eso es necesario un estudio del entorno de operación para el que se disponga adoptar un sistema de seguridad de datos como medida de protección y prevención contra la pérdida, avería o fallo en los sistemas encargados de llevar a cabo la tarea del almacenamiento de datos.

Capítulo 4

Control de Acceso

CAPÍTULO 4 CONTROL DE ACCESO

4.1 TIPOS DE USUARIOS

En este capítulo abordamos el tema de la seguridad en el ámbito de usuarios, ya que es necesario mantener un control de cada uno de los usuarios que accede a la red y establecer los permisos y derechos entre lo que está y no está permitido que hagan, de tal forma que puedan realizar su trabajo sin problemas y se pueda preservar la seguridad de la red.

En los sistemas operativos que se utilizan para el trabajo en redes parte de la seguridad se basa en la autenticación de usuarios, por eso es indispensable que se fijen los mecanismos y las reglas a través de las cuales se llevará a cabo este proceso, y cuya tarea compete entre otras, al administrador de la red.

4.1.1 ADMINISTRADORES

Cuando se tienen equipos trabajando bajo un entorno de red, se reparten recursos y se comparten servicios e información, de tal forma que existe una cantidad de usuarios; que varia según el entorno del que se trate, pero todos conectados simultáneamente a la red, de tal forma que si no existen los mecanismos de control necesarios para distribuir y compartir los recursos y servicios que cada uno de ellos consume y utiliza, no será posible mantener la estabilidad y seguridad dentro de la red, y por el contrario entorpecerá los procesos de administración que se necesitan llevar a cabo para el resguardo de la misma.

Y sin lugar a duda, el administrador de la red (que puede ser uno o varios), es el usuario más importante desde el punto de vista operacional, ya que es el encargado de que todo funcione de acuerdo con lo previsto y bajo las mejores condiciones para lograr un óptimo desempeño en la red, es como si se tratara de un mecanismo al que hay que ajustar cada uno de los engranes que lo conforman, sin perder de vista el más mínimo de los detalles, ya que una falla por muy

pequeña que sea en cualquiera de los engranes repercute en la totalidad del sistema.

Bajo este punto de vista el administrador posee todos los privilegios dentro de la red, pero al mismo tiempo es el responsable de todo lo que suceda en ella, y ha de cuidar el más mínimo de los detalles en todas las tareas que realiza como parte de su labor cotidiana.

Son múltiples las tareas que debe llevar a cabo el administrador de la red como parte esencial en el mantenimiento, funcionamiento y seguridad de la red, pero entre todas ellas, las que se refieren de forma general a la administración de cuentas de usuarios están:

1 **ADMINISTRACIÓN DE CUENTAS (Identificación y Autenticación).** Esta medida de defensa permite prevenir el acceso de usuarios no autorizados a la red; es la base para el control de acceso. Para que un usuario pueda utilizar los recursos debe contar con una "identificación" única, que le permitirá acceder a la red una vez que su identificación sea "autenticada" por el sistema, verificando que la identificación aportada por el usuario sea válida, y así el sistema pueda reconocer dicha identidad. Las técnicas más utilizadas para llevar a cabo la autenticación de un usuario son: a través de un nombre de usuario y contraseña, tarjeta de banda magnética, características biométricas, entre otras, y en cuyos casos sea necesario se puede implantar un modelo de autenticación basado en la combinación de estas técnicas.

2 **ASIGNACIÓN DE PERMISOS** Una vez que se le asigna a un usuario su identificación, también será necesario definir los recursos a los cuales va a tener acceso, tales como directorios, impresoras, programas, etc., y los permisos sobre dichos recursos. Los permisos

deben establecer las condiciones en las que un usuario podrá hacer uso de los recursos, es decir, definir hasta dónde se le permitirá al usuario manipular dicho recurso. Los permisos pueden ser de lectura, escritura, borrado, ejecución, modificación, etc., sobre los recursos, o inclusive procesos más avanzados como conexión remota a ciertos programas o bases de datos, planificación de copias de seguridad, entre otras.

3 **DEFINIR GRUPOS DE TRABAJO.** Los grupos de trabajo son conjuntos de usuarios que comparten los mismos permisos y derechos dentro del sistema, de tal modo que permiten simplificar las tareas de administración cuando el número de usuarios es muy grande y la definición para los nuevos usuarios que se agreguen.

4 **RESPALDO DE INFORMACIÓN.** Como ya lo mencionamos en el capítulo tres, éste es un proceso muy importante, ya que la información es el valor más preciado que hay que asegurar, y los datos de usuario son como los granos de arena, que vistos conjuntamente pueden formar una inmensa montaña, la cual puede desvanecerse si dejamos que poco a poco se vayan perdiendo los granos.

5 **ACTUALIZACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS.** La actualización y configuración correcta de los equipos permite cerrar espacios que pudieran ser utilizados como agujeros de seguridad, a la vez que permiten el óptimo desempeño y rendimiento en los equipos, generando un entorno de trabajo confiable y seguro para el usuario; tal como se expuso en el capítulo dos.

4.1.2 USUARIOS

Los usuarios en general son cada una de las personas que tienen acceso a los recursos de la red, los cuales son vistos por el sistema como una entidad que posee una identificación que les permite ser reconocidos, y tienen la responsabilidad de acatar las medidas establecidas dentro de las políticas de seguridad para ayudar al mantenimiento, conservación, utilización y manejo de los recursos y servicios con que cuenta la red, asumiendo cada uno de ellos su correspondiente papel en el seguimiento de dichas reglas.

Y aunque varios de los usuarios pueden estar representados bajo grupos de trabajo, también existen usuarios que permanecen fuera de estos grupos debido a la exigencia de la labor que desempeñan y que generalmente requieren de un mayor número de privilegios dentro de la red, es aquí donde hay que tener más cuidado con los procedimientos que elegiremos para mantener la seguridad global de la red.

De la misma forma en que los servidores pueden agruparse lógicamente en grupos o dominios, separados cada uno en función de los servicios que prestan y tipo de actividad que se realiza en dicho dominio, las cuentas de usuario también pueden ser agrupados en “grupos de trabajo” debido a que los propietarios de esas cuentas (usuarios) comparten los mismos recursos y necesidades bajo un dominio en particular.

Este planteamiento permite la administración de las cuentas de usuario de manera eficaz bajo un mismo esquema, ya que los atributos confinados para un grupo de trabajo son heredados a cada uno de sus miembros sin tener que redefinir dichos atributos cada que se ingrese un nuevo usuario. Facilitando el manejo y control por parte del área administrativa.

La definición de estos grupos de trabajo no es sólo exclusiva para los dominios, sino que también pueden ser creados bajo otro tipo de características más específicas como puede ser un grupo de usuarios desarrollando un proyecto, investigación u otro tipo de actividad que amerite su creación.

4.2 CUENTAS DE USUARIO Y CONTRASEÑAS

El método más común para la identificación y autenticación de un usuario dentro del sistema se basa en la utilización del nombre de usuario y contraseña de manera unívoca, es decir que solo debe existir un nombre de usuario y una contraseña única que identifican de manera exclusiva a cada uno de los usuarios de la red y que llamaremos “cuenta de usuario” cuando la información de un usuario en particular (nombre de usuario y contraseña) es almacenada en un servidor dedicado a esta tarea dentro de la red o dentro de un equipo de forma local; a la primera se le llama cuenta de dominio y a la segunda cuenta local.

La principal diferencia entre una cuenta de dominio y una cuenta local es que en el primer caso el usuario puede identificarse desde cualquier equipo conectado a la red o un dominio en particular y acceder a los recursos bajo las políticas globales de seguridad que se aplican a la red, y en el segundo caso sólo sirve para identificarse en el equipo donde existe la cuenta (sin tener necesariamente que acceder a la red), bajo las políticas establecidas solo para ese equipo en cuestión.

Una vez que el sistema ha autenticado al usuario, éste podrá acceder a los recursos que este autorizado, independientemente del equipo o sistema donde estos se encuentren ya que generalmente si se trabaja dentro de un dominio en particular, los usuarios solo tienen que ser autenticados una sola vez por un host de confianza (trusted host), de manera que los demás equipos bajo el mismo dominio confiarán en la veracidad de dicha identidad.

La administración de las cuentas de usuario se basa en gran parte en llevar a cabo las siguientes tareas:

1 **TIEMPO DE VIDA DE LA CUENTA.** Que empieza desde el proceso de solicitud hasta el cierre o baja de la cuenta, pasando por las etapas de establecimiento (alta de la cuenta), manejo y seguimiento, y durante el cual se deberá seguir un lineamiento a seguir en cada etapa.

2 **HOMOGENEIDAD.** Establecer patrones para la identificación y autenticación de usuarios de manera general para facilitar los procesos de administración ejecutándose de manera práctica. Emprender un modelo de directivas de seguridad en todos los dominios de la red.

3 **ACTIVIDAD DE LA CUENTA.** Ésta fase corresponde a la etapa de seguimiento la cual resulta ser en sí la más larga, y por tal motivo es donde se enfocará la mayor parte del tiempo y esfuerzo desde el punto de vista administrativo, y en cuanto seguridad se refiere. Las revisiones periódicas ayudan a tener un mayor control y adecuación de los permisos otorgados a las cuentas en función de las necesidades directas del usuario, tomando nuevas consideraciones que se relacionen con el cambio de funciones de algún miembro de la organización.

4 **BAJA DE LA CUENTA.** Esta es la última etapa del ciclo de vida de una cuenta, y consiste en eliminar las cuentas del sistema asignadas al personal; que por la razón que sea, se desvincula de la organización.

Es a través de las cuentas de usuario el medio por el que el administrador controla todo lo que un usuario puede hacer en un dominio, fijando las restricciones, permisos y derechos a su cuenta.

Los permisos definen los accesos a los recursos de la red como impresoras, archivos, programas, etc., incluyendo permisos para escribir, leer, modificar o inclusive borrar. Los derechos establecen acciones que un usuario puede llevar a cabo y se aplican por encima de los permisos, tales como: conexión remota, realizar copias de seguridad, llevar control de auditoria, etc. Y las restricciones son todas aquellas acciones que no se contemplan dentro de los permisos y los derechos asignados a una cuenta. La asignación de estos atributos que se dan a una cuenta se logra a través de los controladores de dominios cuya tarea principal es la centralización de la gestión de cuentas de usuario, recursos y los permisos sobre dichos recursos.

4.2.1 CONTROLADORES DE DOMINIO

La información que proviene de los usuarios debe ser depositada en sistemas de almacenamiento que faciliten los procesos de gestión y seguridad de la red en forma centralizada, pero sobre todo que permitan el mayor control de las actividades que se realizan como parte de los procesos administrativos que se llevan a cabo para con los usuarios.

Esta labor es realizada por los controladores de dominio o PDC (Primary Domain Controller). Un controlador de dominio es un servidor dedicado cuya labor principal es almacenar información de las cuentas de dominio para la identificación y autentificación de usuarios así como de aplicar las políticas globales de seguridad sobre dichas cuentas que se encuentran en la base de datos del directorio maestro del controlador; figura 4.1.

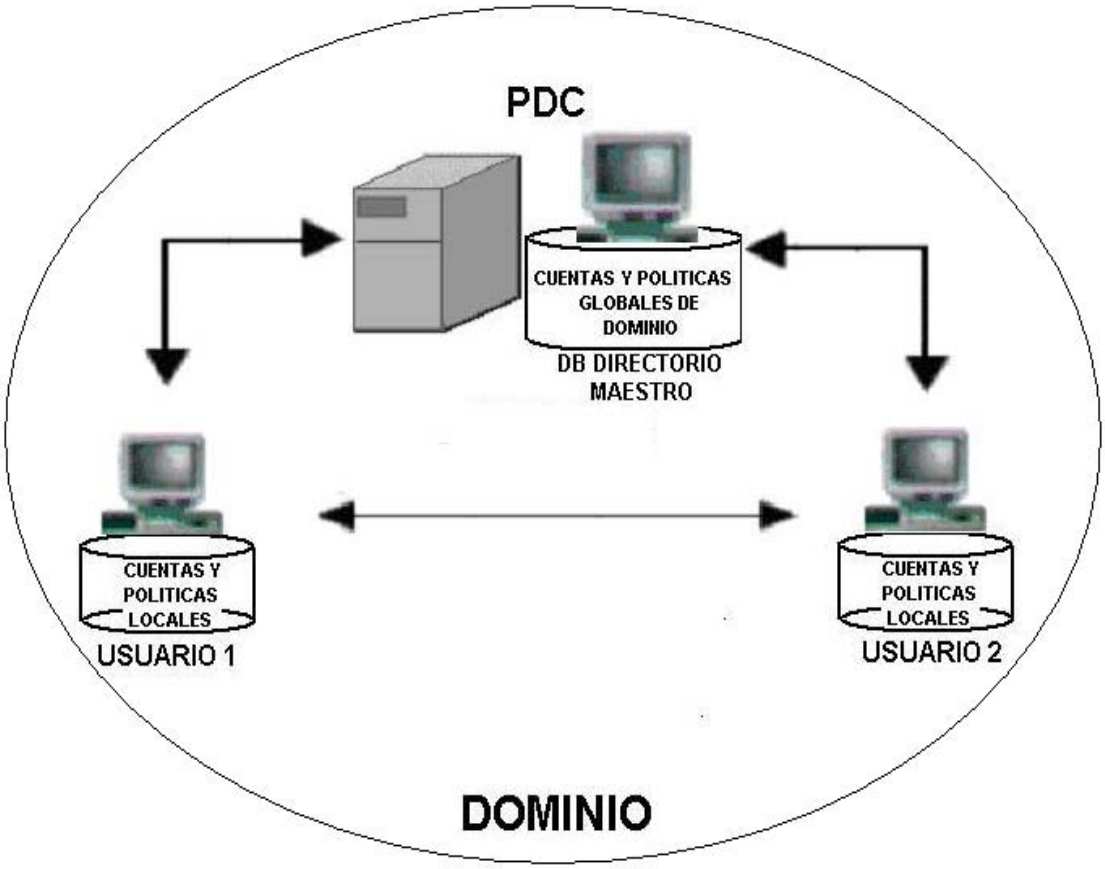


Figura 4.1 Controlador de Dominio PDC

Controlador de dominio es el nombre genérico utilizado para el servidor encargado de administrar y compartir recursos en una red, tal como se observa en la figura anterior. Gracias a los protocolos utilizados a nivel de aplicación dentro del modelo TCP/IP se pueden integrar diferentes plataformas en una red, ya que mientras Windows utiliza el Directorio Activo (Active Directory) a través del protocolo SMB (Server Message Block – Servidor de Bloques de Mensajes), renombrado recientemente como CIFS (Common Internet File System – Sistema de Archivos Comunes de Internet), diseñado para compartir recursos en una red, SAMBA es la versión libre para linux que engloba varios protocolos incluyendo SMB (soportado también por sistemas unix y Mac OS), al igual que la implementación de Sun Microsystem, NIS (Network Information Service – Servicio de Información de Red) para sistemas unix.

Las principales funciones que realiza un controlador de dominio referente a las cuentas de usuario son las siguientes:

1 Administrar cuentas de usuario y contraseñas de forma centralizada, así como los cambios que se realicen en ellas.

2 Actualizar los cambios que se realicen a una cuenta tanto en el controlador local como en la del resto de los controladores que existan en la red.

3 Autenticar la entrada de usuarios en la red.

El proceso de validación de una cuenta de dominio se realiza enviando desde la máquina cliente el nombre de dominio al que se quiere conectar, el nombre de usuario y la contraseña al controlador de dominio. Lo primero que realiza el controlador de dominio es la comprobación del dominio que sea correcto para posteriormente autenticar el nombre de usuario y la contraseña comparándolas con el directorio donde se almacenan las cuentas de usuarios.

Durante este proceso pueden ocurrir tres cosas:

1 Si el dominio existe y la identificación del usuario es correcta, el controlador de dominio notifica al cliente el acceso, figura 4.2.

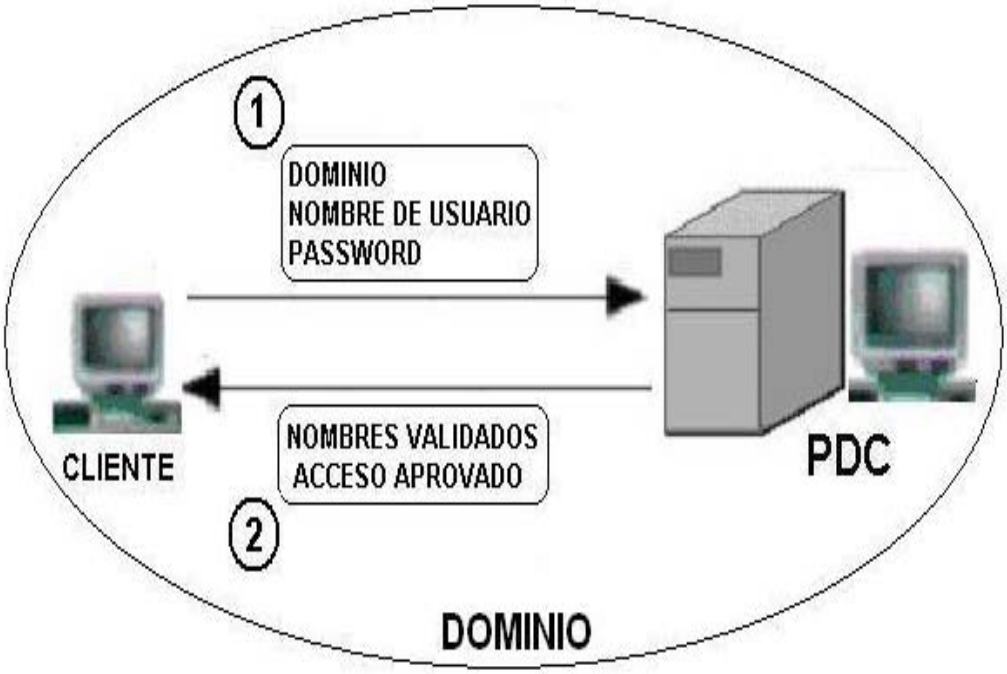


Figura 4.2 Autentificación de cliente de dominio

2 Si el nombre de dominio no existe para el controlador al que se hace la petición de acceso, pero reconoce que el dominio se refiere a otro controlador con el que mantiene una relación de confianza, la información del cliente es enviada a este otro controlador el cual autenticará los datos y si son correctos notificará la validación al primer controlador el cual a su vez la reenviará al cliente, figura 4.3.

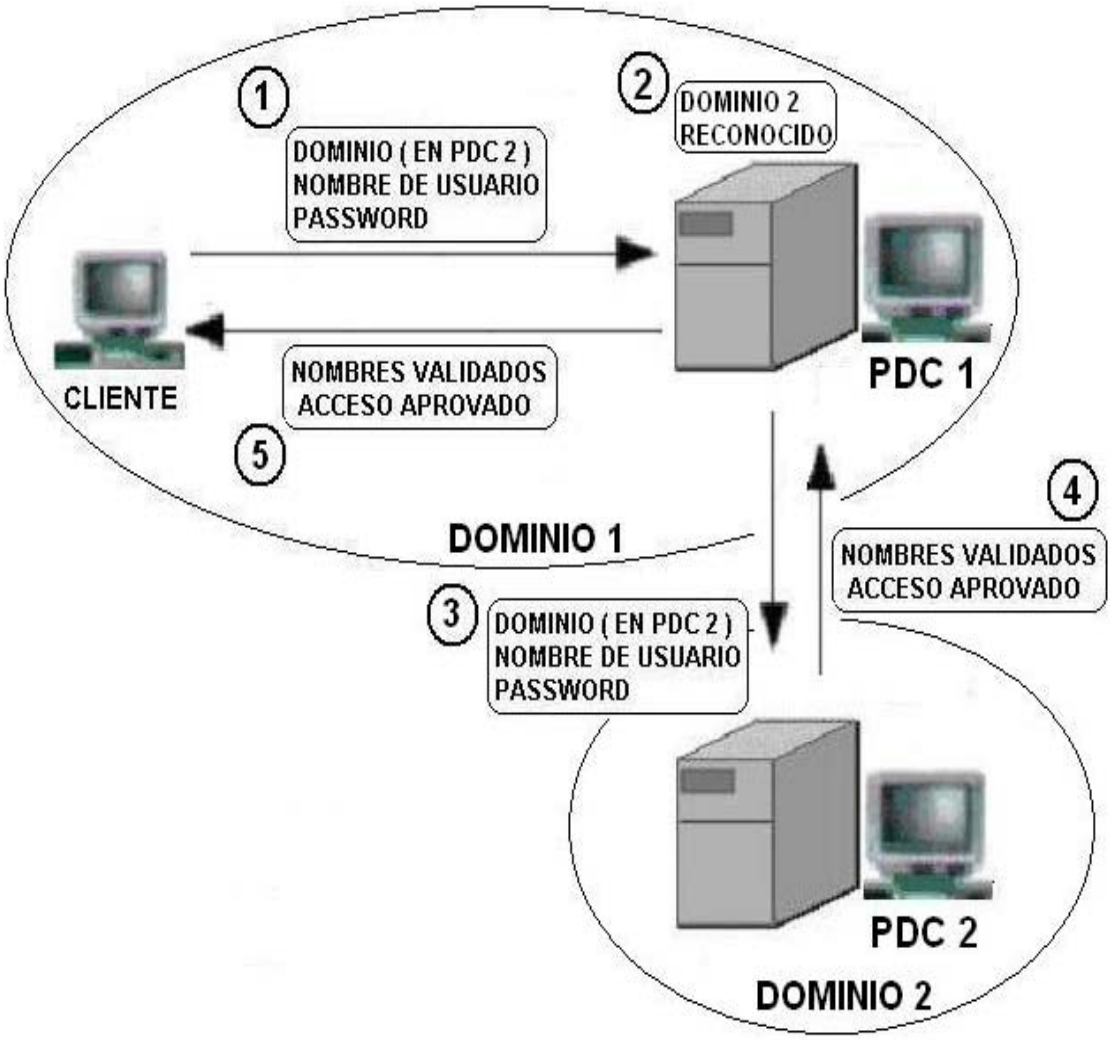


Figura 4.3 Autenticación de cliente de otro dominio

3 Si cualquiera de los datos enviados por el cliente para su autenticación no son correctos el controlador negará el acceso a dicho cliente.

Por tal motivo es indispensable asegurarse que los controladores principales de dominio estén siempre en función y que los directorios donde se encuentra la información de usuarios y de red en general se mantenga actualizada inclusive si se cuenta con controladores de reserva BDC (Backup Domain Controller –

Respaldo del Controlador Dominio), de tal modo que cualquier falla que se produjera en el PDC permitiría promover un BDC a PDC, figura 4.4.

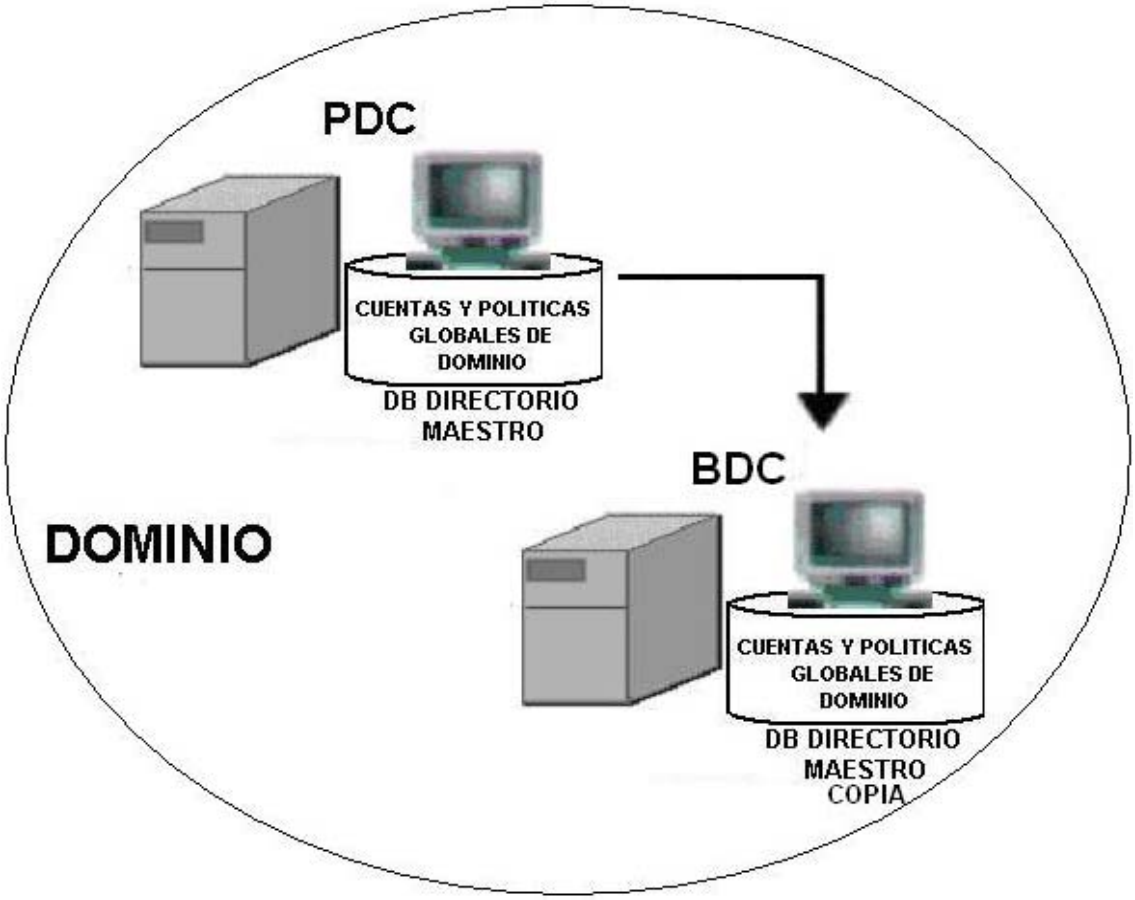


Figura 4.4 Respaldo de PDC mediante BDC

4.2.2 SERVICIO DE DIRECTORIO

La búsqueda de usuarios y recursos sobre la red se hace por medio del “servicio de directorio” ya que éstos son vistos como objetos organizados de manera lógica y jerárquica con atributos propios almacenados en la base de datos del directorio. Por medio del servicio de directorio es posible llamar un recurso por su nombre y no por su dirección de red, por tal motivo un intento de acceso a un recurso puede

retornar a una referencia en otro servidor que aloja el recurso (parte del árbol del directorio), dando respuesta a la petición del cliente que solicitó dicho recurso, ya que los servicios de directorio utilizan un sistema distribuido de almacenamiento de información entre los servidores que conforman el directorio mismo. Un servicio de directorio proporciona la interfaz para acceder a los datos contenidos en los espacios de nombres.

Inicialmente se publicaron los estándares X.500 por la UIT (Unión Internacional de Telecomunicaciones) en los años 80 para el servicio de directorio, los cuales fueron adoptados por el protocolo DAP (Directory Access Protocol – Protocolo de Acceso a Directorio) a través del modelo OSI, y posteriormente surgió LDAP (Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorio) para el modelo TCP/IP actualmente más difundido.

En concreto podemos analizar brevemente el Directorio Activo que utiliza Windows, el cual se implemento siguiendo estándares y protocolos que facilitan la comunicación con otros servicios del directorio, de los cuales sobresalen:

1 **DHCP.** (Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Servidor), ofrece servicio de direcciones de red a los equipos (clientes) en forma desatendida.

2 **DNS.** (Domain Name Server – Servidor de Nombres de Dominio), provee a los clientes un nombre que equivale a la dirección IP.

3 **SNTP.** (Simple Network Time Protocol – Protocolo Simple de Tiempo de Red), para administrar el tiempo en servicios distribuidos.

4 **LDAP.** (Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorio), mediante este protocolo las aplicaciones pueden acceder y modificar la información contenida en el directorio.

5 **Kerberos.** Protocolo de seguridad para la autentificación de usuarios y equipos en general.

6 **X.509.** Estándar que permite la certificación de información con clave publica para mayor seguridad en la red.

Es debido a que el Directorio Activo de Windows, SAMBA y NIS para sistemas linux y unix, se basan en estos protocolos (entre otros), se puede integrar una red con diversas plataformas, ya que en su acepción más simple un servicio de directorio es un componente esencial de todo sistema operativo en red para administrar, compartir y localizar fácilmente los recursos de la red como deposito central de información para toda la infraestructura de la red.

Ahora bien y siguiendo con el análisis del Directorio Activo, un dominio es un conjunto de equipos que comparten una base de datos en un directorio común y que se identifica mediante un nombre particular DNS que equivale a una dirección IP única dentro del dominio.

Los dominios pueden ser organizados en forma jerárquica, ya que en algunas ocasiones es necesario disponer de varios dominios dentro de una misma organización, los cuales pueden ser:

1 **ÁRBOLES DE DOMINIO.** Existe un nombre de dominio raíz al cual se denomina “principal” y/o subdominios “secundarios” que comparten el sufijo del DNS principal. Ejemplo: cartelera.com, como dominio principal y cinecartelera.com, teatrocartelera.com, como dominios secundarios.

2 **BOSQUES DE DOMINIO.** Está formado por el conjunto de árboles de dominio, ya que dentro de una organización puede haber más de un nombre de dominio raíz. Ejemplo: cartelera.com, como dominio

principal y cinecartelera.com, teatrocartelera.com, como dominios secundarios forman un árbol de dominio, y viajes.com, como dominio principal y nacviajes.com, internacviajes.com forman otro árbol de dominio.

De esta forma la información contenida en el Directorio Activo es accesible para todo el bosque de dominios, asignando a cada objeto atributos únicos garantizando la homogeneidad en toda la red, figura 4.5.

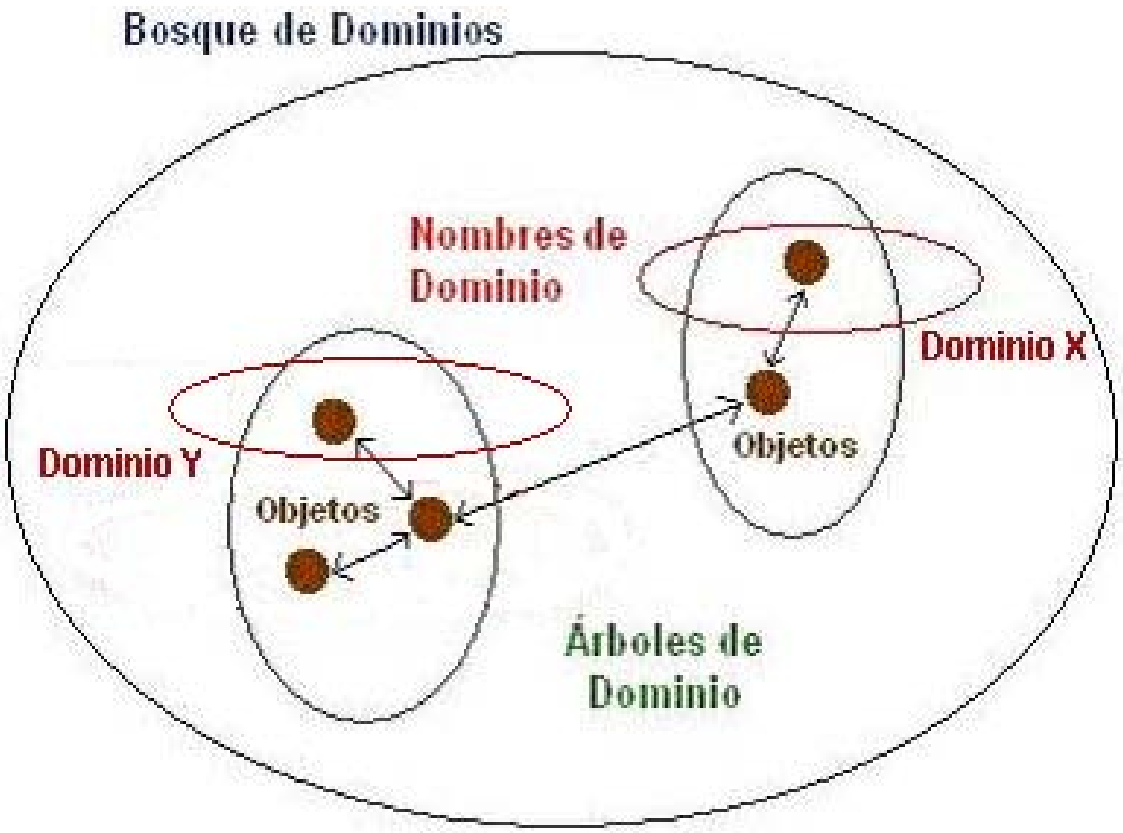


Figura 4.5 Organización jerárquica para un dominio dentro del Directorio Activo de Windows

Ésta es a grandes rasgos la estructura lógica que presenta una red conformada por un conjunto de dominios y subdominios los cuales son organizados

jerárquicamente para englobar a cada uno de los objetos que forman estos conjuntos, de tal forma que es posible tratar a cada uno de estos objetos individualmente, y que junto con sus atributos pueden ser organizados y almacenados dentro de un directorio a nivel de red para facilitar el control y administración de recursos como parte fundamental en el ciclo de vida de las políticas de seguridad implantadas.

4.3 FUNCIONES HASH

Siguiendo con la parte administrativa y el control de acceso de usuarios se analizará con mayor profundidad el método más comúnmente utilizado que es por medio de nombre de usuario y contraseña el cual se basa en la utilización de funciones de tipo “hash”, para garantizar la confidencialidad de los datos que introduce el usuario desde su teclado cada vez que se identifica en la red.

Como su nombre lo indica más que un código de encriptación, una función hash es una función matemática con un dominio y un codominio relacionados por medio de una función, la cual debe cumplir las siguientes condiciones:

1 **HOMOGENEIDAD.** Los elementos del codominio de la función deben ser homogéneos en su tamaño o longitud, es decir, dada una entrada A, con k bits de longitud variable del tipo (A0, A1, A2, ..., Ak-1), donde Ak-1 es el último elemento y $k \in (0, 1, 2, ..., n)$, al aplicar la función hash (H(A)) sobre dicha entrada tendremos como salida una B con m bits de longitud fija:

$$H(A) = B \;;\; \text{donde B es siempre de “m” bits de longitud fija}$$
$$(B0, B1, B2, ..., Bm-1), \text{ donde } m=n$$

Dicho de otra manera si fijamos el tamaño de la salida B de la función en 50 bits y aplicamos la función a dos entradas de distinta

longitud, por ejemplo 20 y 100 bits respectivamente, en ambos casos la longitud del resultado será de 50 bits ya que ese es el tamaño que fijamos para todas las salidas, por tal motivo a este tipo de funciones se les conoce como “función resumen”, porque a partir de un texto base que podría ser de miles de bits de longitud, el resultado será seguramente mucho más pequeño que la entrada.

2 **INYECTIVIDAD.** Se pretende que para cada entrada A perteneciente al dominio de la función se tenga una sola imagen B en el codominio figura 4.6, de tal forma que si:

$$H(A) = H(A') \Rightarrow A = A'$$

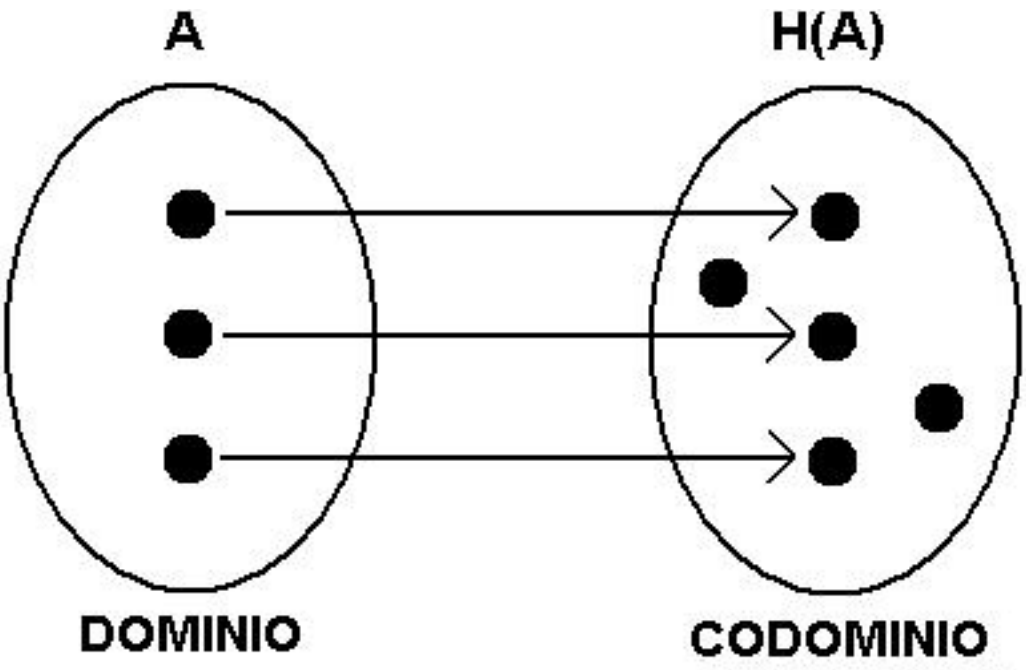


Figura 4.6 Funciones Inyectivas

Lo cual es una mera idealización que más adelante explicaremos.

3 **“ONE WAY HASH FUNCTION” (Irreversibilidad).** Esta propiedad hace referencia al hecho de que es imposible reconstruir el texto

original a partir del resultado, ya que no existen operaciones inversas para tal efecto, por eso se dice que este tipo de funciones son de un solo sentido, y esta característica es precisamente la que diferencia este tipo de funciones de los algoritmos de cifrado los cuales pueden encriptarse y desencriptarse.

4 **RESISTENCIA A COLISIONES.** Dado que la primera propiedad nos dice que el tamaño de la salida de una función hash es constante se puede romper la segunda propiedad que establece que para cada entrada distinta debe existir sólo una salida distinta, ya que si el tamaño de la salida es “m” el número de salidas distintas será de 2^m, pero como el número de entradas es mucho mayor (infinito), se rompe con esta condición ya que para que se cumpliera el número de entradas tendría que ser también “m”, esto es lo que se conoce como colisiones.

Por tal motivo es posible utilizar ataques de fuerza bruta para obtener el texto original, ya que dadas las características propias de la función que ya se explicaron, existe la probabilidad de encontrar dos entradas distintas que proporcionen la misma salida.

Aunque las colisiones son un hecho irrefutable, las funciones hash deben ser capaces de soportar los ataques de fuerza bruta a colisiones suaves y colisiones fuertes. Las primeras se basan en resistir a ataques sencillos donde dada una entrada A se encuentre A’, tal que H(A) = H(A’), y el segundo tipo pretende resistir ataques más fuertes donde sea fácil encontrar entradas distintas que produzcan las mismas salidas.

Dadas las características de estas funciones podemos encontrar dos aplicaciones donde su uso se ha vuelto imprescindible:

1 **FIRMAS DIGITALES.** Supongamos un documento X que queremos enviar, y dado que este pude ser muy extenso para ser cifrado, primero se divide y se aplica la función Hash a cada una de las partes obteniendo una H(X) para cada una de las partes en que se dividió el texto, posteriormente se aplica el algoritmo de cifrado correspondiente a la firma digital (clave privada) sobre H(X) (generalmente al menor valor de H(X)) obteniendo C(H(X)) (firma digital), y lo enviamos al destinatario junto con el texto original X.

El destinatario descifrara el mensaje C(H(X)) con la clave pública del propietario para obtener H(X), y aplicará la función hash al texto original X para comparar el valor del resultado H(X) que obtuvo con el que recibió, si ambos coinciden quiere decir que el texto original no sufrió ninguna modificación o alteración en su trayecto, por el contrario se puede saber que el texto presenta errores generando así un escenario de firma digital.

2 **CONTRASEÑAS.** Las contraseñas de usuario no son almacenadas como texto claro porque plantearía un grave problema de seguridad, lo que en realidad se guarda es el valor de la función hash obtenido al aplicar la función directamente a la contraseña suministrada por el usuario, ya que desde el punto de vista conceptual es más seguro que utilizar algún método criptográfico (dada la propiedad de irreversibilidad).

En este caso lo que nos interesa saber es como se lleva a cabo la encriptación de contraseñas a través de funciones hash, para tener una mayor idea de los niveles de seguridad que se manejan en este ámbito.

4.3.1 ALGORITMO MD5

El algoritmo MD5 (Message Digest Algorithm – Algoritmo de Resumen de Mensaje 5), es otro de los algoritmos desarrollados por el profesor Ronald Rivest a principio de la década de los 90 en sustitución de la versión anterior (MD4), y es el más utilizado para la encriptación de contraseñas.

De manera general podemos decir que este algoritmo se basa en tomar una entrada A, con k bits de longitud variable del tipo (A0, A1, A2, ..., Ak-1) y salida de 128 bits, donde Ak-1 es el último elemento y $k \in$(0, 1, 2,..., n), a la cual aplicaremos los siguientes pasos:

1 **AÑADIR BITS.** La longitud de la entrada (k), tiene que ser congruente con: 448 mod(512), de modo que k – 448 sea múltiplo de 512, para ello habrá que añadir bits al mensaje original comenzando con un bit “1”, seguido de tantos bits “0” como sea necesario, este paso se realiza inclusive si k ya cumple con esta condición obteniendo una k ‘ para el nuevo valor de k.

2 **REPRESENTACIÓN DE LOS PAQUETES.** La longitud del mensaje (antes de ser extendido) se representa con 64 bits, de modo que si k > 2^64, se usarán los 64 bits menos significativos, los cuales se concatenan al mensaje obtenido en el paso anterior, figura 4.7.

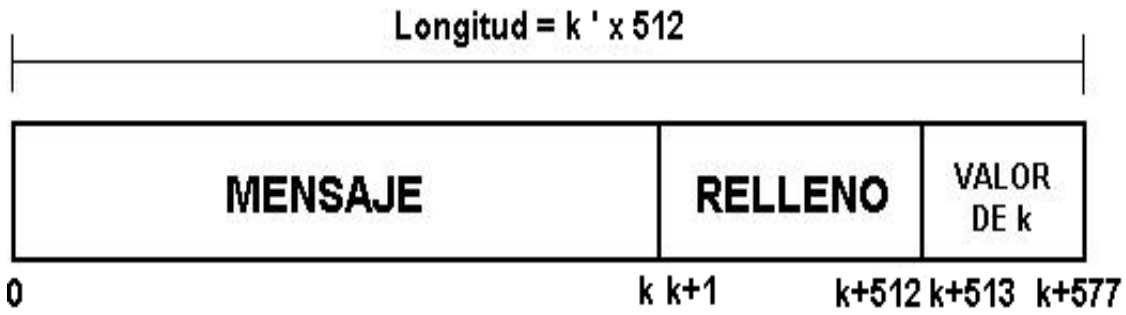


Figura 4.7 Mensaje modificado

De este modo se obtiene un nuevo mensaje cuyo tamaño en bits es múltiplo de 512.

3 **INICIALIZAR BUFER.** Un búfer auxiliar de 128 bits es inicializado con ciertos valores, el cual a su vez puede ser visto como 4 registros (A, B, C, D) de 32 bits cada uno.

4 **APLICAR ALGORITMO.** El paquete que representa al mensaje modificado se divide en bloques de 512 bits de longitud, y los procesa juntos con los 128 bits del búfer mediante el uso de cuatro funciones establecidas. Este proceso continúa hasta que todos los bloques de 512 bits han sido procesados.

5 **RESULTADO.** Por cada bloque de 512 bits procesado se obtiene un resultado de 128 bits que se almacena en el búfer, los cuales son nuevamente procesados hasta terminar con el último bloque. El resultado final se encuentra en el búfer al procesar el último bloque del mensaje, siendo el registro A el menos significativo y D el más significativo.

De esta forma es como se calcula la función hash de un texto usando el algoritmo MD5; y aunque es muy utilizado no es el único, por mencionar existe otro algoritmo que utiliza un concepto muy parecido: SHA (Secure Hash Algorithm –

Algoritmo Hash Seguro), desde la primera publicación en 1993 llamada SHA-0, actualmente está en pie la versión SHA-2 que engloba varias versiones que se diferencian en los rangos de salida.

El más difundido es SHA-1, el cual produce una salida de 160 bits de un mensaje de hasta 2^64 bits de longitud.

Dada la propiedad de irreversibilidad que presentan este tipo de algoritmos por basarse en el principio de las funciones hash, fue que se eligieron para la encriptación de contraseñas y su almacenamiento, y aunque desde su desarrollo se sabía de la existencia de colisiones se creía que era computacionalmente imposible obtener los valores que provocarán la colisión del algoritmo.

El razonamiento utilizado para romper el algoritmo se denomina “ataque de cumpleaños”, ya que parte de la probabilidad de calcular cuántas personas se necesitan para que dentro de un margen de probabilidad comprensible (mayor al 50%), al menos una de ellas cumpla años el mismo día en que nosotros cumplimos.

Si denotamos con “n” el número de personas tenemos que:

$$n (1 / 365) > 0.5 \Rightarrow n > 182$$

Lo cual muestra que el número de personas tendría que ser mayor a 182; en el mejor de los casos, pero podrían llegar a ser 365 lo cual no ayudaría en mucho si de tratar en disminuir los cálculos fuera necesario.

Es lo mismo que pensar en la probabilidad de encontrar una entrada B’ para una función hash tal que H(B) = H(B’), ahora bien si la entrada B es de 64 bits

$$n (1 / 2 ^ 64) > 0.5 \Rightarrow n > 2 ^ 32$$

Lo cual es computacionalmente imposible dada la cantidad de años que tardaríamos en encontrar la entrada B' deseada, ya que si pensamos en el peor de los casos en que tuviéramos que calcular todas las combinaciones posibles, esto es 2 ^ 64 intentos; en números grandes se vería así:

$$2 \wedge 64 = 18, 446, 744, 073, 709, 551, 616 \text{ combinaciones}$$

Una máquina dedicada sólo a probar cada una de las posibles combinaciones a una velocidad de procesamiento de un millón de combinaciones por segundo (lo que da un total de 31536000000000 combinaciones al año), tardaría alrededor de:

$$2 \wedge 64 / 31536000000000 = 584, 942 \text{ años}$$

Ahora bien y regresando al punto anterior, si pensamos en la posibilidad de que dos personas cualesquiera cumplan años en el mismo día la situación cambia, ya que como en un grupo de n personas tenemos n (n-1) / 2 parejas distintas resulta que:

$$(n (n - 1) / 2) (1 / 365) > 0.5 \Rightarrow n > 20$$

Lo cual representa una cantidad mucho menor que en el caso anterior, ya que en un grupo de 20 personas la probabilidad de que dos de ellas tengan el mismo cumpleaños es del 50 %. Y del mismo modo podemos probar que para una función hash con 2 ^ 64 entradas distintas la probabilidad de que dos de ellas generen el mismo resultado es:

$$(n (n - 1) / 2) (1 / 2 \wedge 64) > 0.5 \Rightarrow n > 2 \wedge 32 / 2$$

Lo que reduce significativamente los cálculos ya que ahora sólo tenemos que probar en un rango de 2^32 combinaciones como máximo para tener una probabilidad más acertada de encontrar dos entradas que generen el mismo hash,

lo cual sólo tardaría un par de horas en calcularse, ya que con la misma velocidad de procesamiento planteada se probarían 3600000000 entradas por hora tardando aproximadamente:

2 ^ 32 / 3600000000 = 1.2 horas

Ésta es una de las formas más comunes como se logra “romper” la función y violar accesos de seguridad que utilizan este tipo de algoritmos, encontrando por ejemplo, programas que se encuentran prácticamente al alcance de cualquier persona y que pueden realizar este tipo de ataques utilizando técnicas de diccionario, por tal motivo es recomendable establecer ciertas medidas y recomendaciones para uso y elección de contraseñas para que sean lo más “robustas”, ya que aunque no lo parezca este tipo de medidas contribuyen al fortalecimiento de las políticas de seguridad.

Las recomendaciones que se hacen en cuanto a la elección de contraseñas son las siguientes:

1. Debe contener al menos ocho caracteres.
2. Los caracteres deben ser alfabéticos, numéricos y especiales.
3. No pueden ser palabras comunes ni derivarse de éstas.
4. No deben relacionarse con información personal del usuario.
5. Deben crearse de tal forma que puedan recordarse fácilmente, ya sea de forma directa o a través de reglas nemotécnicas.

De esta forma ayudaremos a que el descubrir una contraseña no sea tan sencillo o de manera instantánea, ya que no es igual probar con combinaciones en las que sólo intervienen caracteres del mismo tipo: numéricos o alfabéticos en mayúscula o minúscula. Y en cuanto a las recomendaciones sobre los usos y prácticas de las contraseñas son las siguientes:

1. Cambiar periódicamente las contraseñas; con mayor frecuencia las de administrador o aquellas que sirvan para la administración de aplicaciones.
2. No utilizar una misma contraseña para varias cuentas o servicios.
3. Si se trata de sistemas o servicios delicados limitar el número de intentos para acceder.
4. Cambiar inmediatamente el perfil de la cuenta o contraseña en caso de sospecha de haber sido comprometida.
5. No divulgar, compartir o escribir las contraseñas para evitar su mal uso.

Así es como podemos fortalecer la administración de cuentas de usuario y prevenir riesgos en el ámbito de la ingeniería social que se da dentro de las organizaciones o empresas, que aunque no lo parezca, es una más de las amenazas de seguridad que podemos encontrar.

Capítulo 5

Seguridad en la Red

CAPÍTULO 5 SEGURIDAD EN LA RED

5.1 DISPOSITIVOS DE SEGURIDAD

Actualmente existe una tendencia para la integración de servicios en los dispositivos de seguridad que se implantan como parte de una estrategia de seguridad en cuanto a prevención y control de los diversos tipos de amenazas que hay al interior y exterior de una red, de tal forma que permiten en un solo punto centralizar su administración, del mismo modo que un PDC actúa en la administración y gestión centralizada de cuentas de usuarios en la red, es decir, este modelo permite fijar en un solo punto de la red los controles de seguridad y satisfacer las exigencias demandadas para la misma sin repercutir en su funcionalidad.

Este enfoque es conocido como UTM (Unified Threat Management – Administración Unificada de Amenazas), los sistemas basados en UTM han logrado consolidar varios sistemas de seguridad en uno solo, los cuales pueden variar de acuerdo al tipo de sistema UTM elegido y las necesidades propias de la red que se deseen cubrir, pero todos se basan en el mismo principio y características que comúnmente se pueden encontrar en este tipo de tecnologías, figura 5.1.

Figura 5.1 Servicios Unificados en los sistemas UTM

Como se observa en la figura 5.1, este tipo de dispositivos están diseñados para combatir varios tipos de actividades maliciosas en la red en diferentes capas, además de facilitar la administración y aplicación de políticas de seguridad a nivel de grupo o a nivel de usuario.

Las funciones de un sistema UTM generalmente se basan en las siguientes aplicaciones:

1 **FIREWALL.** En el perímetro de la red o en segmentos de la misma, ya sea filtrando a nivel de paquetes o a nivel de aplicación.

2 **IPS/IDS.** Para controlar el tráfico de la red basándose en patrones distintivos de ataques o de tráfico fuera de lo común de actividades no autorizadas, además de poder tomar medidas en caso de detectarse.

3 **ANTIVIRUS Y ANTISPAYWARE.** Detectando patrones dentro de los archivos indicativos de software malicioso.

4 **ANTISPAM.** Detectando y bloqueando el correo no deseado evitando que llegue a los servidores disminuyendo la carga por este tipo de mensajes.

5 **FILTROS WEB.** Bloqueando las direcciones con contenidos inapropiados o sin un fin justificable en las actividades de la organización.

6 **MONITOREO.** Proporciona información sobre el estado de la red según las políticas de seguridad del UTM.

Aparte de considerar las aplicaciones dadas en un sistema UTM, es necesario considerar otras cuestiones operacionales para la implantación de estos sistemas, tales como:

1 **FUNCIONALIDAD.** Esto con la finalidad de evaluar los servicios que se necesitan y el lugar donde se necesitan, por ejemplo, los sistemas IDS son especialmente útiles en segmentos de red donde se encuentren servidores con aplicaciones críticas.

2 **RENDIMIENTO.** Dada la combinación de servicios en un solo dispositivo es necesario entender la interdependencia que existe entre cada uno de ellos, y en caso de que alguno de estos servicios fallara saber en qué medida afectaría al resto.

3 **BALANCE DE CARGA.** Hay que asegurar dada la cantidad de usuarios en la red, el control de tráfico de manera lógica para optimizar el balance de carga en la red.

4 **ADMINISTRACIÓN Y MANTENIMIENTO.** La complejidad con que operan estos dispositivos no debe reflejarse en las labores administrativas o de mantenimiento, ya que de lo contrario entorpecerían estas tareas, tomando en cuenta que las modificaciones que pueda tener la red no impliquen una mayor complejidad en la re-configuración de estos dispositivos.

Otro de los beneficios que incorporan estos sistemas es que pueden ser administrados de forma remota, y de esta forma facilitar su implantación ya que de otro modo la falta de personal especializado dejaría a un lado el uso de estos dispositivos.

En general las reglas de filtrado utilizadas en estos dispositivos son las condiciones obligadas a seguir por un usuario, equipo o paquete de datos en la red, para que las políticas de seguridad cumplan con la labor de garantizar la seguridad para la utilización de los recursos de ésta a través de medios seguros, facilitando la gestión y administración de los recursos y servicios en la red.

Un ejemplo de tecnología UTM es el utilizado por el sistema operativo RouterOS de la compañía Mikrotik, el cual está basado en el kernel de Linux, y se encuentra en la tarjeta del router de la compañía, o puede ser instalado de forma independiente en una PC "común" compatible con procesadores x86 y capacidad mínima en disco de 64 MB, la cual trabaja de forma dedicada.

Las aplicaciones que ofrece este sistema se orientan a la seguridad, control y conectividad entre redes LAN, las cuales se mencionan a continuación:

1. Firewall (NAT).
2. Router.
3. Web Proxy.
4. Servidor SNMP
5. VPN (IPsec, PPTP, VLAN, MPLS).
6. Redes Inalámbricas (IEEE 802.11 a/b/g/n) y protocolos de encriptación (WEP, WPA, WPA2).
7. Hotspot.
8. QoS (Calidad de Servicio) y control de ancho de banda.

Además cuenta con un set de herramientas completo para optimizar las funciones diarias de control y monitoreo. La figura 5.2 muestra la pantalla de inicio desde la consola del RouterOS Mikrotik instalado en una PC.

Figura 5.2 Pantalla de inicio en la consola del RouterOS Mikrotik

5.2 MONITOREO DE PUERTOS

5.2.1 PUERTOS Y PROCEDIMIENTOS REMOTOS

Antes de empezar analicemos la necesidad de un usuario por acceder a información o aplicaciones que se encuentran en otro equipo, y bajo este esquema se necesitan dos cosas. Primero generar la petición de forma local preparándola para su transporte, y segundo transportar la petición hasta su destino, de tal forma que en vez de implementar un solo módulo de alta complejidad, esta labor pueda ser dividida en submódulos (técnicas y protocolos) independientes cada uno encargado de resolver distintas tareas.

De modo que por un lado tenemos el mecanismo RPC (Remote Procedure Call – Llamada a Procedimiento Remoto), utilizado en el esquema cliente – servidor, y encargado de iniciar la petición por el cliente solicitando al servidor que ejecute cierto proceso o aplicación, sin preocuparse por la comunicación entre ambos.

Ésta es una forma de abstracción del mecanismo de peticiones remotas entre sistemas en red.

Y por otro lado están los protocolos TCP/IP, encargados de la conexión y comunicación entre el cliente y el servidor para transportar las peticiones y las respuestas que el servidor envía de vuelta al cliente.

La interacción y modo de trabajo de los protocolos en forma general es la siguiente: supongamos que un cliente desea solicitar un proceso remoto que está en un servidor, y que el proceso emisor del cliente genera un bloque de datos listos para enviarse con ayuda del mecanismo RPC, los cuales son pasados al protocolo TCP/IP a través de un “puerto”. El protocolo RPC añada la información necesaria al bloque de datos para que el servidor pueda interpretar la solicitud hecha por el cliente, y el protocolo TCP/IP adhiere la información de control para que el bloque de datos pueda viajar por la red hasta su destino.

Una vez que el bloque de datos llega al conjunto TCP/IP, éste pasa por el protocolo TCP, el cual divide el bloque si es necesario, y añade a cada parte instrucciones de control (cabecera TCP) formando segmentos, posteriormente TCP entrega cada segmento al protocolo IP, que añada también información de control (como la dirección de red) a cada segmento, formando datagramas IP. Por último los datagramas pasan al nivel inferior de acceso a la red añadiendo su propia cabecera para que pueda ser transmitido por la red o subred hasta su destino. Cuando la petición llega a su destino este proceso se repite de manera inversa hasta que el bloque de datos queda nuevamente desenvuelto y es entregado al servidor a través de un puerto, figura 5.3.

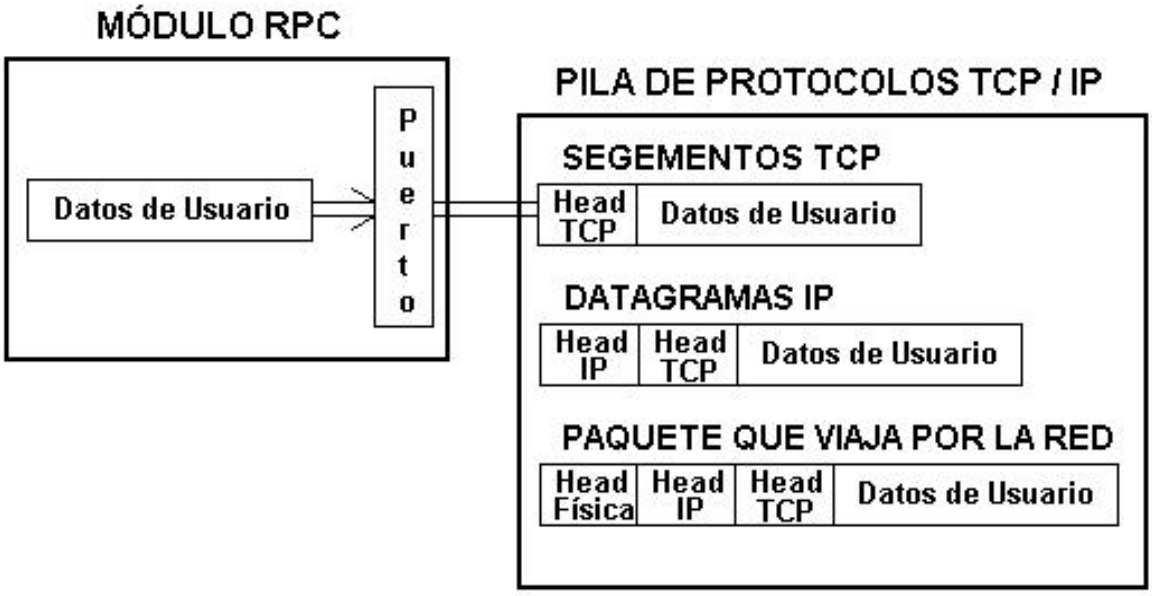


Figura 5.3 Relación RPC – TCP/IP

De esta forma la única conexión que hay entre el RPC y TCP/IP se hace por medio de un puerto, que no es más que una representación lógica identificada por un número particular que diferencia a cada una de las aplicaciones o servicios que presta un equipo en la red, y que se incluye al principio de un bloque de datos, así, un proceso remoto puede dirigir sus mensajes al puerto indicado, del mismo modo que una dirección IP sirve para comunicar con un equipo específico.

Para que el módulo RPC del cliente pueda solicitar la aplicación requerida al servidor, es necesario que éste conozca el puerto del servidor donde se encuentra dicha aplicación, ya que hasta el momento en que se hace la solicitud esta información es desconocida, porque ninguno de los dos equipos tienen información suficiente uno del otro.

Existen dos formas en la que el cliente puede saber el puerto de la aplicación remota. La primera es decidirlo con antelación, es decir, con direcciones de puerto fijas asociadas a cada una de las peticiones RPC disponibles para un cliente, así cada llamada RPC mantendrá el puerto correspondiente a la aplicación requerida en el servidor.

La segunda es utilizar una aplicación concertadora en el servidor (demonio de encuentros), para que el cliente envíe a éste un mensaje con el nombre de la RPC que necesita ejecutar, la cual es atendida por la aplicación concertadora, y una vez que se identifica la aplicación requerida se envía el número de puerto del servidor al cliente, para que la llamada a RPC sea enviada con ese número de puerto.

A su vez el protocolo TCP ofrece una conexión segura para el intercambio de datos entre aplicaciones, ya que la cabecera con una longitud mínima de 160 bits incluye información necesaria para ello, figura 5.4.

Figura 5.4 Formato de la cabecera TCP

Los campos puerto origen y destino sirven para identificar las aplicaciones que existen a través de esta conexión en los equipos origen y destino, así como, número de secuencia, de aceptación y ventana son para control de flujo y errores, ya que cada segmento es numerado para detectar su pérdida y determinar mediante el campo ventana la cantidad de datos que el receptor puede aceptar. El campo validez se usa para detectar errores en el segmento TCP.

El protocolo del siguiente nivel IP, ha sido la base de la arquitectura TCP/IP. La longitud mínima de la cabecera es de 160 bits igual que la cabecera TCP. La figura 5.5 muestra su formato.

Figura 5.5 Formato de la cabecera IP

El campo versión especifica si se trata de IPv4 o IPv6, IHL (Internet Header Lenght - Longitud de Cabecera de Internet) determina la longitud de la cabecera en palabras de 32 bits (se requieren 5 palabras como mínimo en una cabecera sin opciones, 160 bits), tipo de servicio se refiere a parámetros asociados con el paquete como retardo y capacidad de salida asociadas a éste, longitud total es para representar el tamaño del datagrama medido en bytes, identificación es usado para asociar a cada emisor los paquetes que este envía de forma unívoca, el campo indicadores consiste de 3 bits utilizados como banderas; el primero (MF - More Fragment) es usado para determinar la existencia de paquetes en camino, el siguiente (DF – Don´t Fragment) cuando se trata del último paquete, y el tercero no está en uso. El campo desplazamiento de fragmento sirve para ubicar la posición que ocupa un fragmento dentro del paquete original, TTL indica la cantidad de saltos que el paquete puede dar en la red ya que su valor se va decrementando en cada salto; si es cero el paquete se destruye (su valor por

default es 64). Protocolo indica el protocolo de nivel superior usado (TCP o UDP), control de cabecera sirve para comprobar la integridad de la cabecera exclusivamente, ya que hay campos de ésta que van cambiando en su recorrido (como TTL), dirección de origen y destino identifican al emisor y receptor mediante la dirección IP de cada uno.

Los campos de opción y relleno aseguran que la cabecera sea múltiplo de 32, tanto para TCP como para IP, ya que después de la cabecera se ingresan los datos, siendo de 64 Kbytes la capacidad máxima del campo de datos para IP, y en caso de ser menor debe ser múltiplo de 8.

Por último se añade la cabecera que permite a todo el paquete viajar a través de la red, asociando un dispositivo que a nivel lógico se identifica por una dirección IP, con un dispositivo de red que a nivel físico cuenta con una dirección (MAC) de 48 bits. La figura 5.6 muestra el formato que presenta la cabecera ARP.

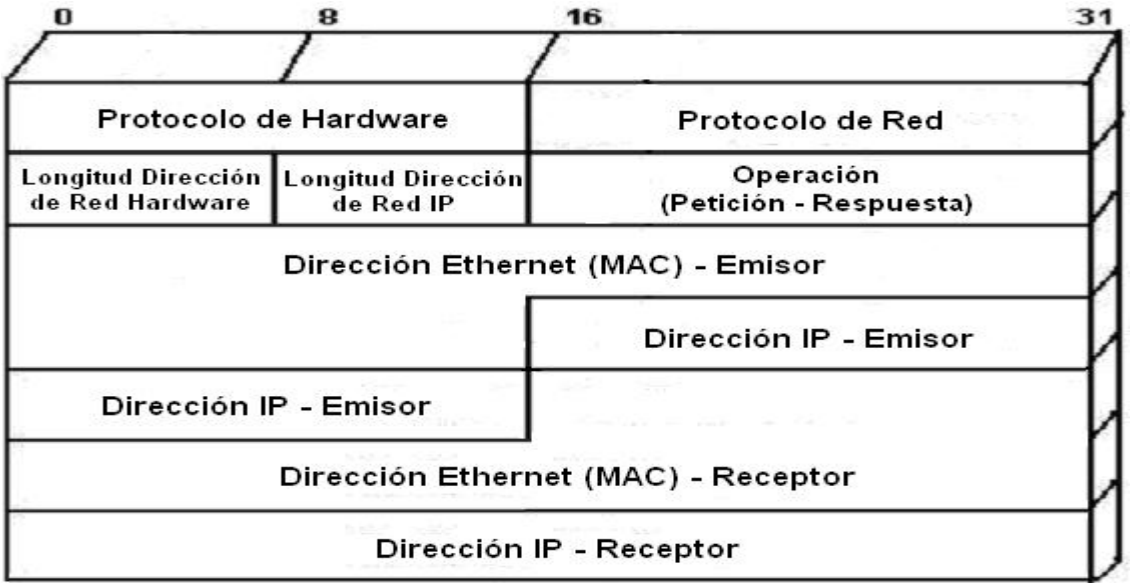


Figura 5.6 Formato de la cabecera ARP

Como se observa en la figura 5.6, los campos dentro de esta cabecera se utilizan en su mayoría para la asociación de direcciones IP con direcciones MAC, a

excepción de los campos protocolo de hardware y de red, que se utilizan para identificar los protocolos de la capa física y de red respectivamente, ya que ARP puede asociarse a protocolos diferentes a TCP/IP, pero se definen los campos con base en éste. El protocolo RARP es la función inversa del protocolo ARP.

Después de que se han añadido las cabeceras correspondientes a cada uno de estos protocolos el paquete está casi listo para enviarse a través de la red, sólo falta fragmentar el paquete en caso de ser necesario, debido a que el medio físico (ethernet) tiene un MTU (Maximum Transfer Unit - Unidad Máxima de Transferencia) de 1500 bytes, pero considerando que la cabecera IP tiene una longitud de 20 bytes, sólo quedan 1480 bytes disponibles.

La fragmentación se basa en la división del mensaje en paquetes menores o de igual tamaño que el MTU de la red en que se este trabajando. Para el caso de redes ethernet la fragmentación utiliza las banderas MF y DF, así como el campo desplazamiento de fragmento de la cabecera IP. La figura 5.7 muestra la fragmentación de un paquete de 3000 bytes a través de una red ethernet.

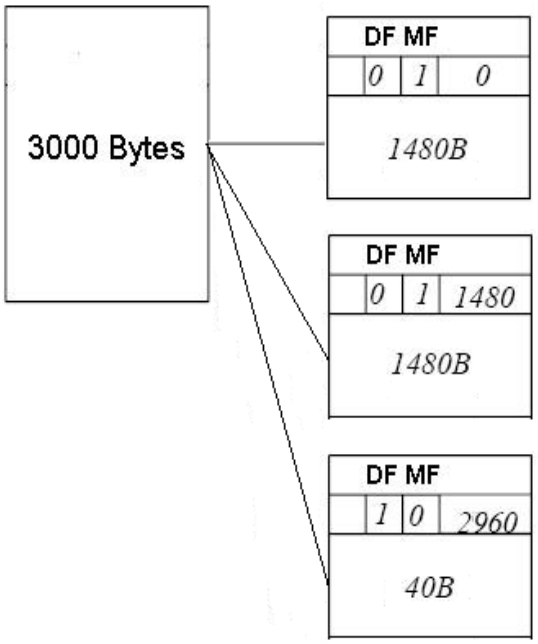


Figura 5.7 Fragmentación de paquetes sobre ethernet

Cuando el paquete por fin llegue a su destino el dispositivo de capa física recibirá el paquete, y éste irá pasando por los protocolos de nivel superior hasta llegar al protocolo TCP, el cual se comunicará a través del número de puerto indicado en la cabecera del paquete con la aplicación relacionada a éste, para que los datos lleguen a su destino en un proceso inverso al que se origino en el equipo emisor.

5.2.2 TIPOS DE PUERTO

Aunque un sistema se identifica en la red por una dirección que permite reconocerlo de manera unívoca, mediante la utilización de puertos es posible que una computadora pueda establecer simultáneamente varias conexiones provenientes de una misma máquina o de varias.

Para representar el número de puerto se utilizan 16 bits, por lo que tenemos 65536 puertos distintos que van del 0 al 65535, los cuales se dividen en tres categorías según la organización IANA (Internet Assigned Numbers Authority – Agencia de Asignación de Números para Internet), con el fin de establecer la asignación de puertos que utilizan las aplicaciones en Internet:

1 **WELL KNOWN PORTS – PUERTOS BIEN CONOCIDOS.** Que son los puertos más comunes y están comprendidos entre 0 y 1023, donde las aplicaciones son ejecutadas con privilegios de “root”.

2 **REGISTERED PORTS – PUERTOS REGISTRADOS.** Van del 1024 al 49151, y las aplicaciones asignadas a estos puertos son ejecutadas por usuarios o procesos con pocos privilegios.

3 **DYNAMIC y/o PRIVATE PORTS – PUERTOS DINÁMICOS y/o PRIVADOS.** Que corresponde al resto de los puertos y cuyas aplicaciones son particulares.

El monitoreo o escaneo de puertos es una técnica que permite establecer qué puertos se encuentran disponibles en una computadora, de esta forma es posible saber que aplicaciones se están ejecutando en dicha máquina al asociar el número de puerto con su aplicación.

Esta técnica puede ser utilizada para dos fines totalmente opuestos: mejorar la seguridad y control de servicios en la red, o para encontrar vulnerabilidades en las aplicaciones que se encuentran tras los puertos, lo cual resulta muy peligroso si se desconoce por completo la existencia de puertos “abiertos” por donde la información pasa a través de ellos sin control ni vigilancia, convirtiéndose en fácil punto de acceso para un atacante.

Para evitar este tipo de ataques es necesario filtrar los datos que pasan hacia los puertos a través de dispositivos dedicados conocidos como firewalls, y la falta de ellos o una mala configuración repercute en el tipo de situaciones ya mencionadas, figura 5.8.

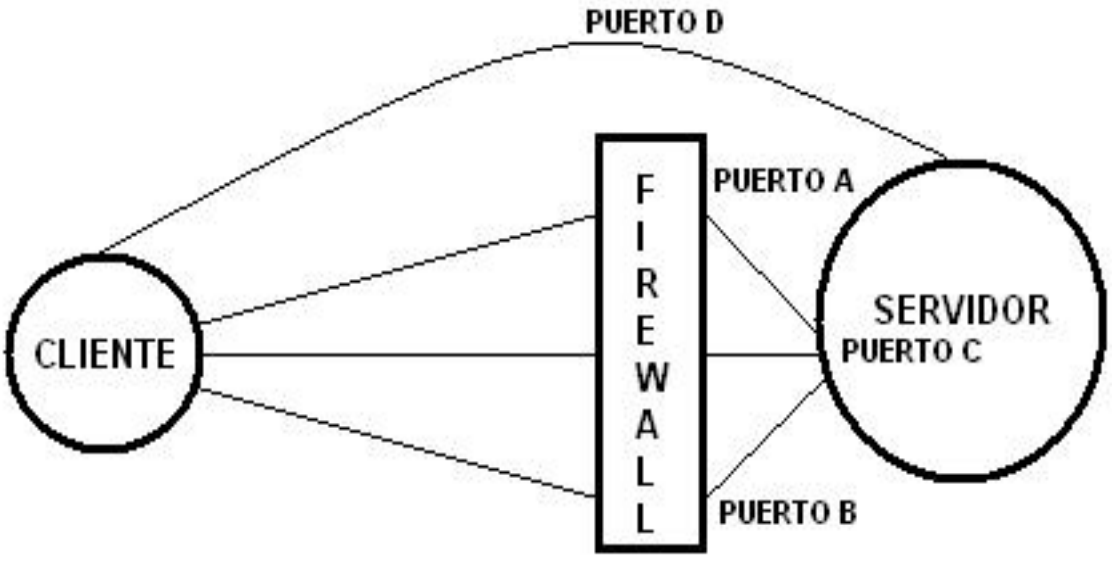


Figura 5.8 Vulnerabilidades en los puertos

Generalmente los ataques dirigidos hacia los puertos, lo hacen tratando de averiguar si existe algún puerto que no está filtrado, y es a través del envío de paquetes erróneos que es posible averiguarlo, ya que si el puerto, o puertos al que se envían dichos paquetes son filtrados, el firewall no permitirá su paso y no se obtendrá respuesta alguna, pero si no, el paquete llegará hasta su destino y el firewall responderá con un mensaje ICMP indicando el tipo de error que se trate, con lo que se concluyen dos cosas: que el puerto no es filtrado y que está abierto.

Un ejemplo de comunicación cliente – servidor a través del puerto 80; utilizado para la transmisión de páginas web por Internet y el protocolo http, se muestra en la siguiente figura 5.9.

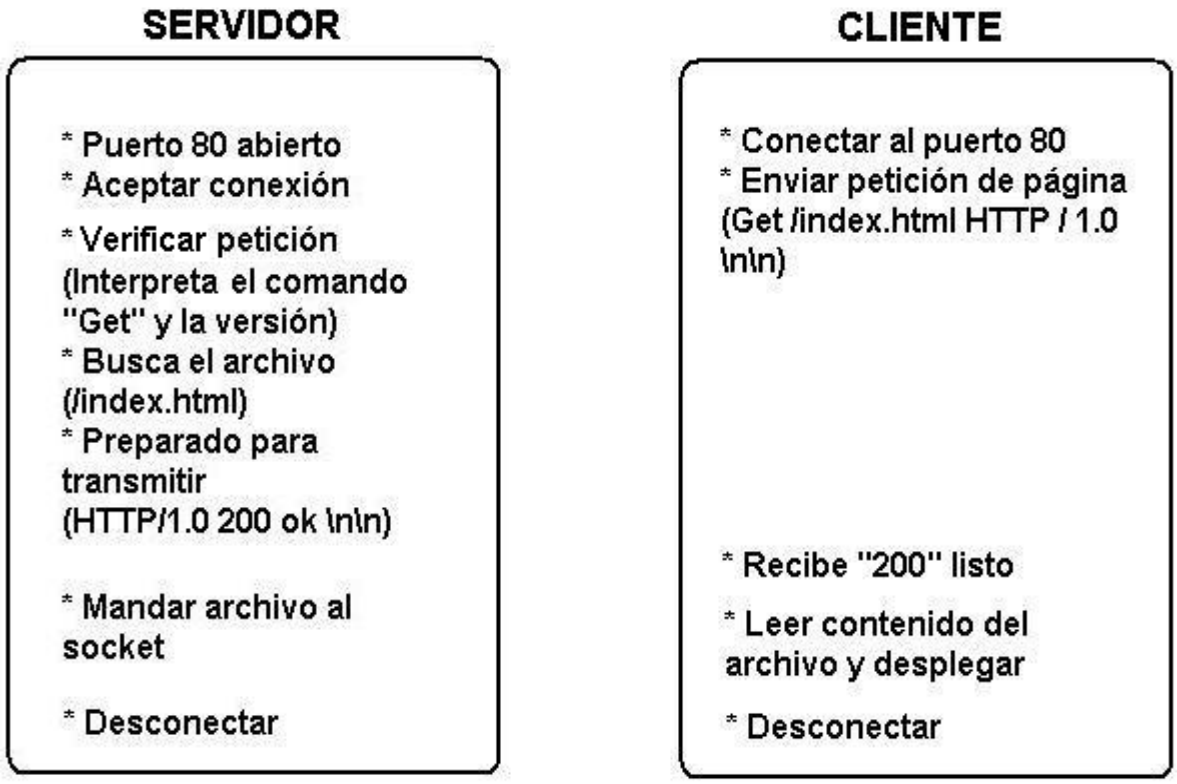


Figura 5.9 Conexión Cliente–Servidor al puerto 80

La configuración de los dispositivos utilizados para filtrar el paso de paquetes hacia o desde la red, es un modo de prevenir y controlar accesos sin autorización generados por la transferencia de datos que en su contenido puedan tener algún

tipo de malware y/o generar exceso de tráfico indeseado. Este tipo de situaciones son tratadas con mayor profundidad en la siguiente sección con un enfoque práctico.

5.3 RESTRICCIONES A SITIOS SEGUROS

Las Intranets son redes de computadoras que utilizan el protocolo TCP/IP para comunicarse, al igual que la red global de Internet, de modo que es posible encontrar el mismo tipo de aplicaciones (servidores WEB, FTP, E-MAIL, Bases De Datos, . . .), y problemas en ambas redes; aunque en un factor de escala menor para una Intranet.

De tal modo que las políticas de control de acceso a las aplicaciones que se prestan en la Intranet, deben establecer los filtros adecuados que aseguren el paso de los paquetes de datos una vez que se haya verificado su contenido, a los equipos donde se encuentran dichas aplicaciones para preservar la integridad de los sistemas y la red en general.

Las reglas de filtrado deben permanecer transparentes a las aplicaciones y usuarios por los dispositivos encargados de esta labor, que generalmente son firewalls.

El filtrado consiste en reglas que permiten establecer la aceptación o negación de un paquete de manera bidireccional, es decir, tanto para los paquetes de entrada como para los de salida a través de las interfaces de red de los dispositivos involucrados en esta tarea.

Las reglas son una lista compuesta de cadenas que sirven para comparar cada uno de los paquetes que pasan a través del mecanismo de filtrado para permitir la entrada, salida o reenvío de paquetes. Debido a que el paquete a analizar se compara con cada una de las cadenas de la lista hasta encontrar una regla que

cumpla, de otro modo si no se encuentra ninguna regla para el paquete se aplica la directiva de seguridad establecida para tal caso, la cual puede ser rechazar o ignorar el paquete, definiendo así las reglas del firewall. Cuando se rechaza un paquete se notifica mediante un mensaje de error (ICMP) a la dirección de donde proviene, y si se descarta no existe ninguna notificación, el paquete se elimina, siendo generalmente ésta la mejor opción, ya que cualquier respuesta además de generar tráfico en la red, ofrece información potencial que podría utilizarse con fines de ataque (fingerprinting).

Las reglas de filtrado en el firewall pueden tomar los siguientes criterios como base para permitir la entrada de paquetes:

1 Dirección de origen, lo que garantiza que el paquete proviene de algún sitio conocido.

2 Dirección de destino, para controlar el tráfico hacia equipos específicos, que se sabe ofrecen algún servicio.

3 Puerto de origen, para establecer la relación con la aplicación requerida que garantiza su aceptación.

4 Puerto destino, para restringir el acceso únicamente a los puertos permitidos por ciertas aplicaciones que se tengan, y justificar de este modo el acceso.

5 Aceptar paquetes de conexiones iniciadas por el propio equipo local con otros servidores, y rechazar las peticiones de conexión en los paquetes TCP entrantes (SYN activado y ACK desactivado).

Del mismo modo la salida de paquetes puede tomarse de la siguiente forma:

1 Dirección de origen, para permitir los paquetes que salen desde una dirección específica.

2 Dirección destino, para garantizar que existe un equipo receptor cuya dirección es conocida y de confianza.

3 Puerto de origen, para restringir la salida de paquetes por puertos en los que se conoce existe un servicio de aplicación, que justifica la salida del paquete.

4 Puerto destino, que garantiza la entrega del paquete para aplicaciones permitidas.

5 Responder a los servidores cuyas conexiones TCP fueron establecidas por los equipos locales de la red (ACK activado y SYN desactivado).

5.3.1 POLÍTICAS DE SEGURIDAD MEDIANTE FIREWALL MIKROTIK

Para ejemplificar uso un RouterOS de Mikrotik, para simular la configuración de las reglas de seguridad del firewall para una red en la cual se desea bloquear ciertas aplicaciones como parte de las políticas de seguridad adoptadas, y que por lo general se consideran innecesarias para el desempeño de las funciones que se realizan.

El RouterOS de Mikrotik está instalado en una PC compatible con el sistema. Las características del firewall-RouterOS son las siguientes:

1 Redireccionamiento (NAT), para prevenir accesos directos a los equipos sin autorización y al mismo RouterOS.

2 Inspección de paquetes y monitoreo de conexiones.

3 Filtro por dirección IP, o rango.

4 Filtro por puerto, o rango.

5 Soporte para el protocolo IPv6.

La red en la que se aplican las políticas es la mostrada en la figura 5.10. El RouterOS cuenta con tres interfaces Gigabit Ethernet montadas en un socket pci. La interfaz pública está conectada con el proveedor de Internet (ISP), las otras dos interfaces privadas sirven para conectar con las subredes cómputo y contabilidad.

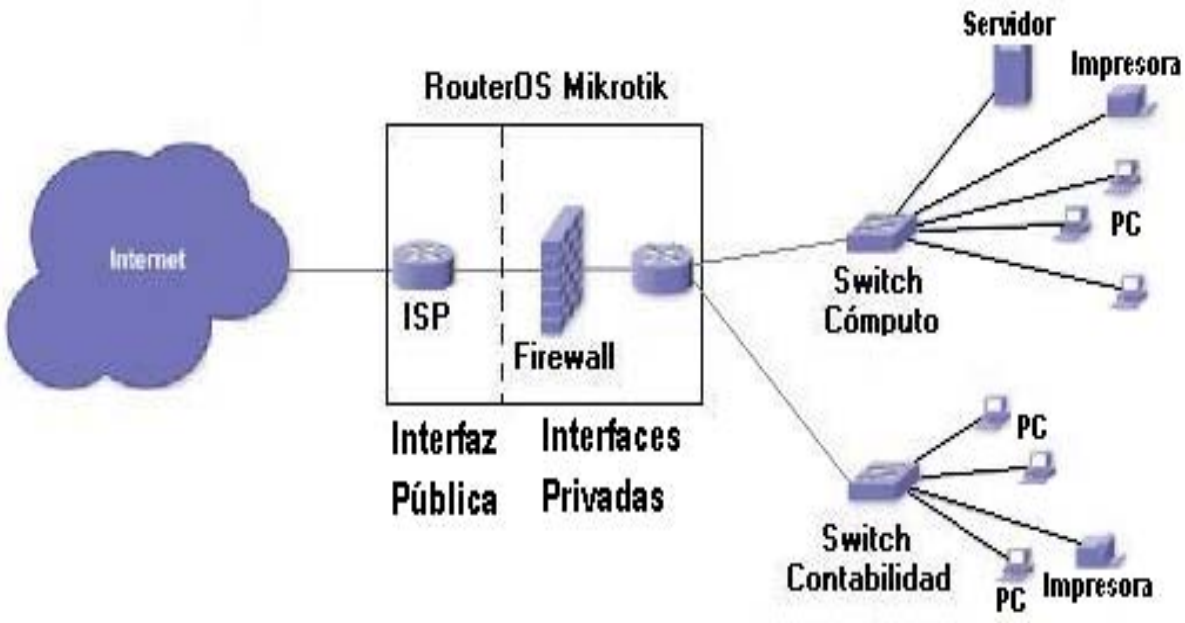


Figura 5.10 Red configurada con Mikrotik RouterOS

En este ejemplo todas las interfaces se encuentran físicamente juntas pero separadas lógicamente, ya que cada una se configura de forma independiente con sus propios atributos: nombre, dirección de red IP, dirección física MAC, interfaz interna o externa dependiendo si trabaja como privada o pública, etc.

Para este caso sólo se cuenta con dos subredes: cómputo y contabilidad; aunque generalmente suelen ser más. Inclusive no siempre es factible que tener todas las interfaces de red juntas en un solo dispositivo, existen varios factores que delimitan esta posibilidad, pero suponemos para este ejemplo que así es.

Para acceder al RouterOS y configurar el firewall, utilizamos la interfaz gráfica “WinBox” figura 5.11, instalada en una PC, por medio de la cual se accede al RouterOS de forma remota y amigable para el usuario.

Figura 5.11 Conexión al RouterOS con WinBox

Para entrar en la configuración del RouterOS tenemos que introducir la dirección IP o MAC de la tarjeta de red donde se encuentra instalado el sistema Mikrotik, y escribirla en la casilla “Connect To” de la figura anterior, o bien, podemos dar un click sobre el icono con los tres puntos (...) que se encuentra adelante, para que de este modo WinBox las detecte automáticamente.

Las restricciones a la red mediante el firewall son las siguientes:

1 **Bloquear Windows Live Messenger.**

2 **Bloquear conexiones P2P para una subred.**

5.3.1.1 BLOQUEO DE WINDOS LIVE MESSENGER

Las reglas de filtrado se aplican a los puertos utilizados por el servicio Windows live messenger versión 8.1, los cuales se listan a continuación junto con la aplicación relacionada a cada uno de ellos:

Característica	Puerto utilizado
Iniciar sesión en el servicio de Messenger	TCP 80, 443, 1863
Detección de la red	TCP 7001 UDP 9, 7001
Audio	TCP 80, 443, 1863 TCP/UDP 30000 - 65535
Audio (programa heredado) *	UDP 5004 – 65535
Conversaciones de vídeo y con cámara Web	TCP 80 TCP/UDP 5000 - 65535
Transferencia de archivos	TCP 443, 1863 TCP/UDP 1025 - 65535
Transferencia de archivos (programa heredado) *	TCP 6891 - 6900
Uso compartido de carpetas	TCP 1863 TCP/UDP 1025 – 65535
Pizarra y uso compartido de aplicaciones	TCP 1503
Asistencia remota	TCP 3389 TCP/UDP 49152 – 65535
Windows Live Call	TCP 443, 5061 UDP 5004 - 65525
Juegos	TCP 80, 443, 1863 TCP/UDP 1025 - 65535

* Para versiones anteriores a Windows live messenger 8.1, u otras versiones como msn.

Aunque la lista de puertos es extensa no es necesario bloquearlos todos, sólo los más indispensables como los que se utilizan para el inicio de sesión, ya que por ende las demás aplicaciones requieren que se haya establecido antes una sesión. Para mostrar este proceso y como parte del ejemplo, quedará bloqueado el puerto 443 utilizado para inicio de sesión entre otras aplicaciones, y el rango de puertos 6891 – 6900 utilizados para transferencia de archivos.

Una vez establecidas las reglas de filtrado y dentro de la interfaz WinBox, procedemos a configurar el firewall desde el menú principal, en el cual se muestran del lado izquierdo los módulos instalados en el menú de configuración, figura 5.12.

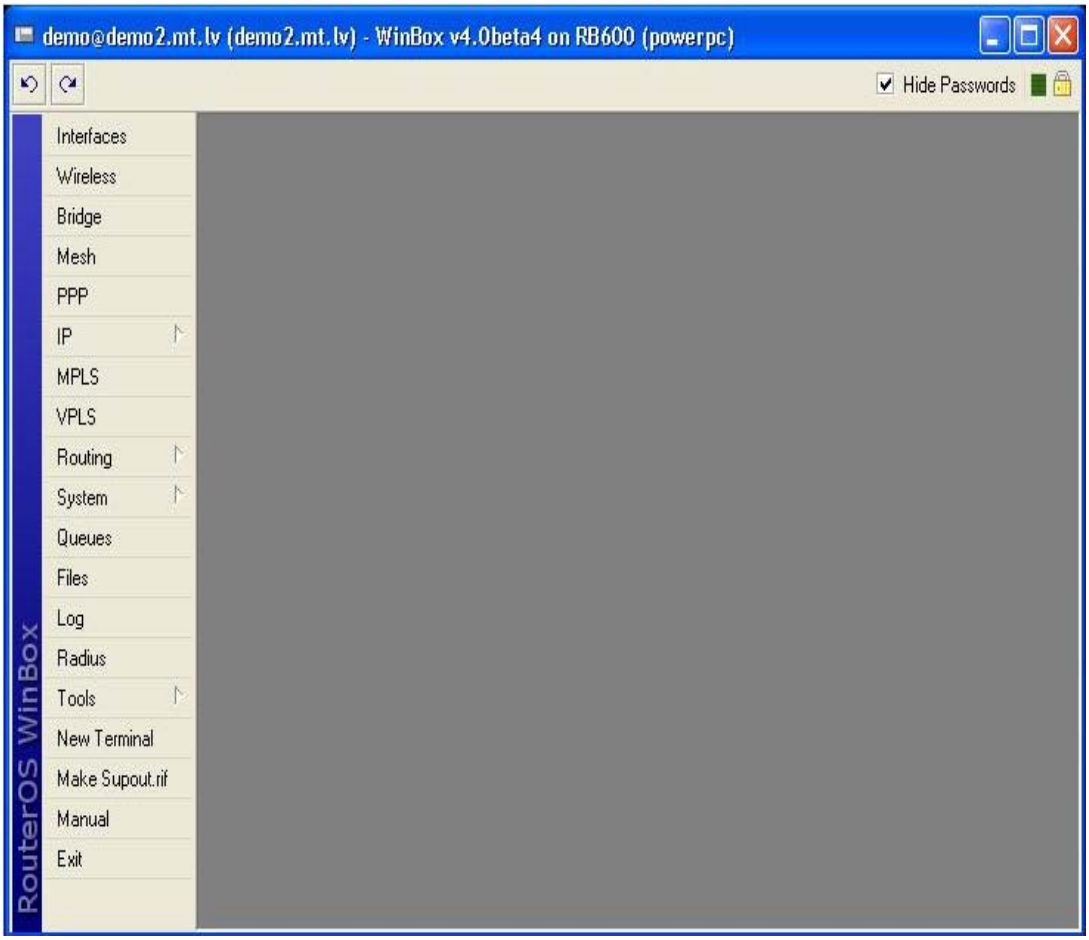


Figura 5.12 Menú principal de WinBox

Del menú que aparece en la parte izquierda de la pantalla elegimos la sexta opción; “IP”, para que se despliegue un submenú, y elegimos Firewall, con lo que se abrirá la ventana de configuración del firewall y la pestaña “Filter Rules” (Reglas de Filtrado), de forma predeterminada, figura 5.13. Hacemos click en el icono de signo “+” para añadir nuevas reglas.

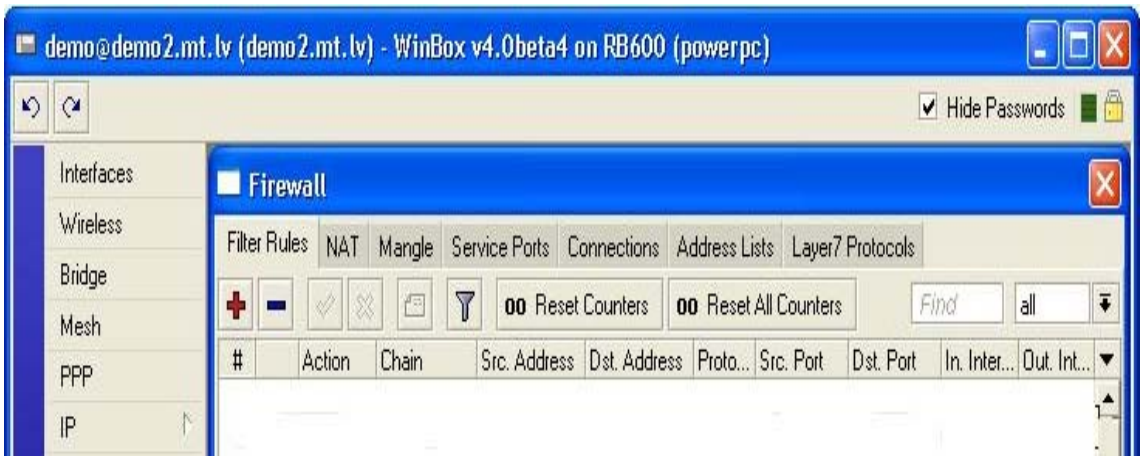


Figura 5.13 Configuración de las reglas del firewall

Ahora aparece una nueva ventana desde la que procedemos a bloquear los puertos utilizados por el Windows live messenger. En la pestaña “General” se dan a conocer los puertos sobre los que se aplicarán las reglas de filtrado, y en la pestaña “Action”, la acción, que en este caso es bloquearlos, figuras 5.14 y 5.15. Este proceso se repite para cada uno de los puertos que se desee bloquear.

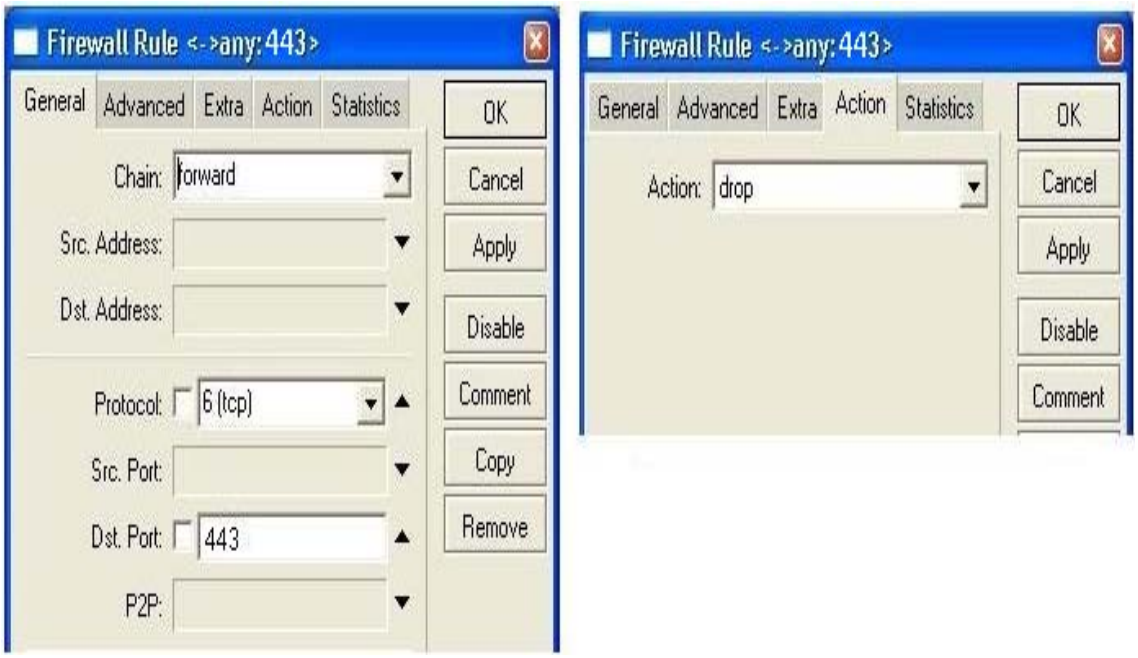


Figura 5.14 Reglas de filtrado puerto 443

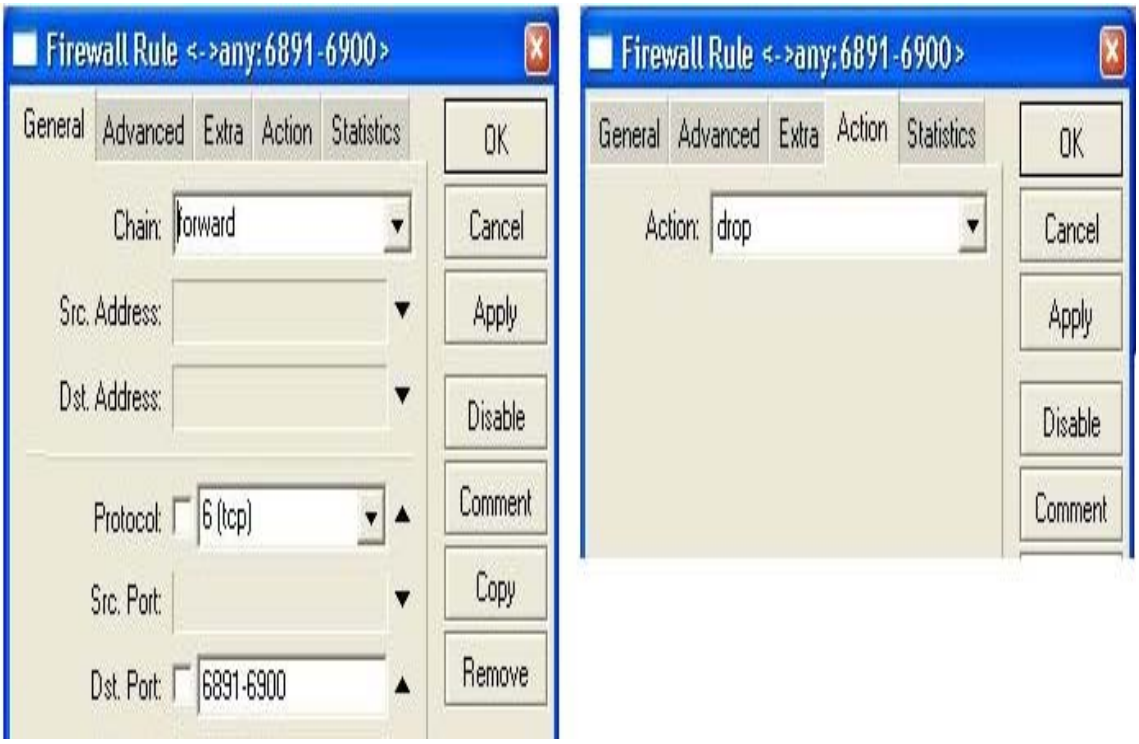


Figura 5.15 Reglas de filtrado puertos 6891 – 6900

Como se observa en las figuras anteriores son cuatro los parámetros que se configuran: cadena (Chain) para reenvío de paquetes (forward), puerto destino (Dst.Port.), protocolo (Protocol), y acción (Action), que es la regla a ejecutar sobre los parámetros dados.

Ahora bien, si se desea también es posible bloquear la dirección IP del servidor Windows live messenger (login.live.com), ubicado en USA propiedad de Microsoft Corp., con la misma dinámica con que se bloquearon los puertos que utilizan esta aplicación, la IP es: 65.54.186.79, figura 5.16.

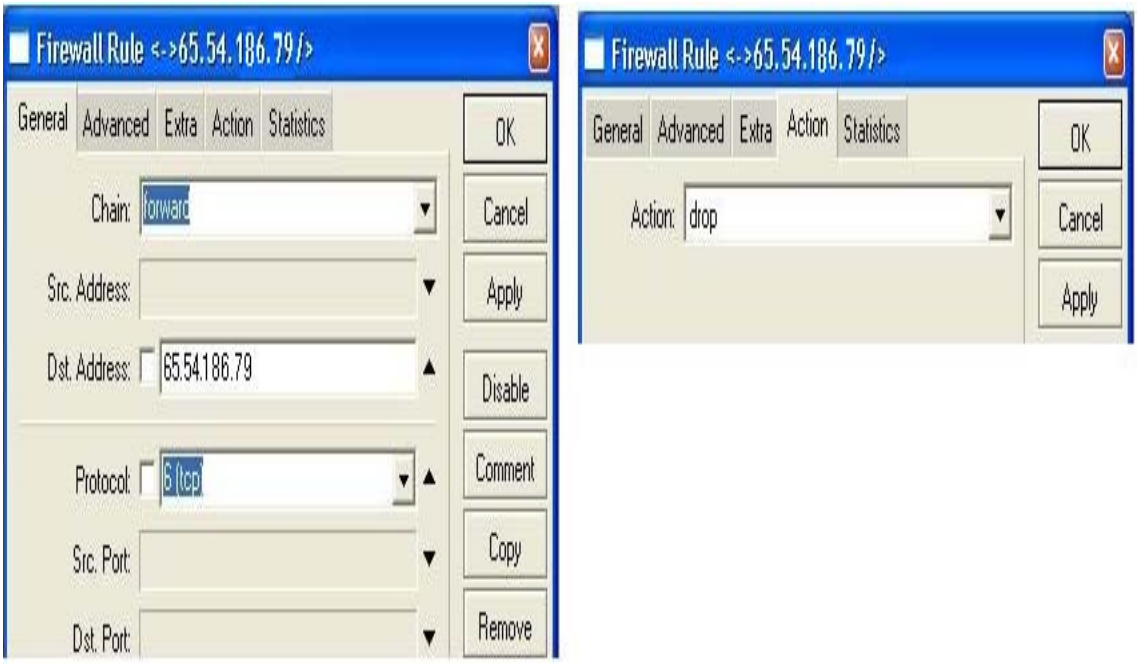


Figura 5.16 Reglas de filtrado IP de Windows live messenger

Con este último paso se han establecido las reglas del firewall RouterOS Mikrotik para bloquear Windows live messenger, evitando así utilizar recursos de la red de forma innecesaria. Ahora falta aplicar la segunda política establecida para bloquear las conexiones P2P (Peer to Peer).

5.3.1.2 BLOQUEO DE CONEXIONES P2P

El proceso es muy parecido al anterior sólo que ahora en vez de especificar el número de puerto, se establece el tipo de conexión que se desea bloquear, en este caso conexiones “Peert to Peer”, y la tarjeta de red del RouterOS Mikrotik sobre la que actuará esta política, figura 5.17.

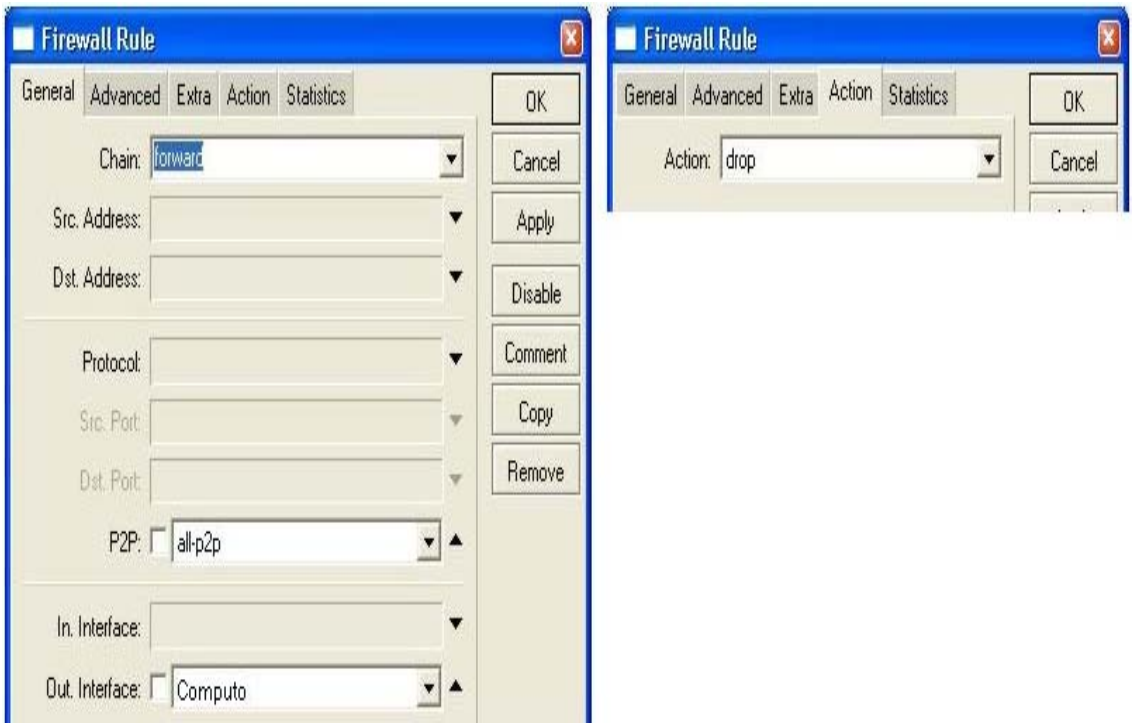


Figura 5.17 Reglas de filtrado para conexiones P2P

Los parámetros a configurar sobre esta regla también son cuatro como en el caso anterior, cadena y acción se repiten, mientras que protocolo y puerto son sustituidos por P2P (all-p2p), e interfaz de salida (Out. Internase), que en este caso se llama cómputo, y permite mantener aislada esta área como una subred dedicada exclusivamente al departamento de cómputo, donde por la sensibilidad de la información manejada, se evita tener conexiones de este tipo utilizando un RouterOS Mikrotik para su protección y administración.

Al final todas las reglas aplicadas al firewall pueden verse desde el menú principal donde se está la lista de todas las políticas que se hayan aplicado. En la figura 5.18 se muestran los puertos bloqueados para Windows live messenger y las conexiones P2P para la subred de cómputo.

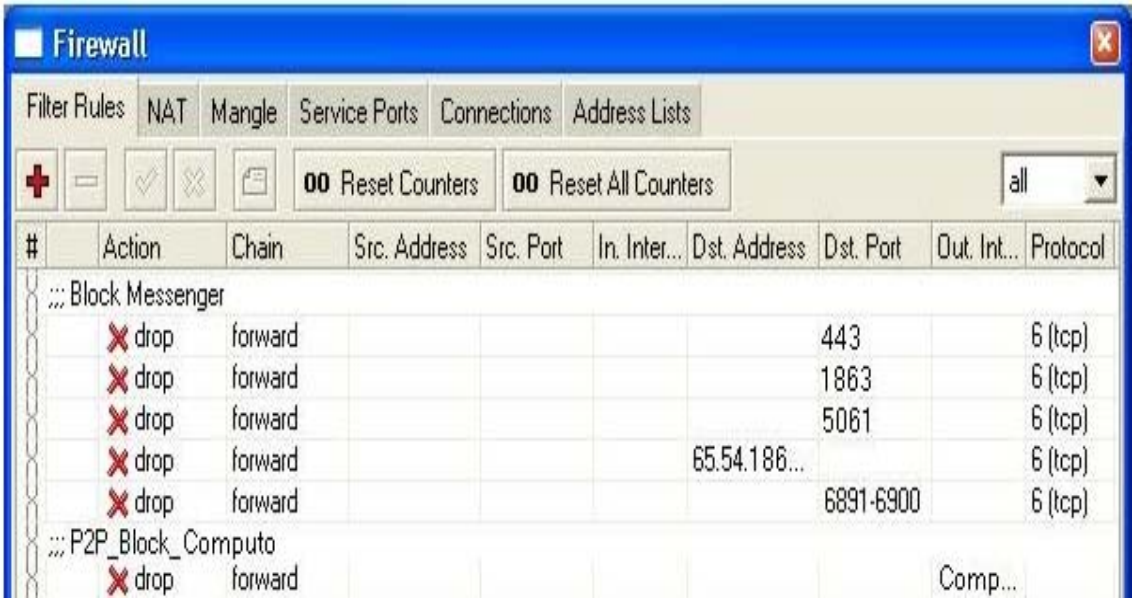


Figura 5.18 Reglas aplicadas al firewall

5.3.2 POLÍTICAS DE SEGURIDAD USANDO PROXY Y NAT CON MIKROTIK

Para reforzar las políticas y mostrar la utilización del servidor web proxy, y NAT del mismo RouterOS, ejemplifico aplicando las siguientes reglas como parte de la política de seguridad a seguir dentro de una red:

1 **Bloquear páginas web de messenger.**

2 **Bloquear páginas web con contenido pornográfico.**

3 **Descartar paquetes ICMP.**

Las características del servidor proxy son las siguientes:

1 Configuración de acceso por URL, origen o destino.

2 Configuración de Caché para optimizar ancho de banda.

3 Listas de acceso directo o acceso a través de otro proxy.

4 Transparente al usuario.

5.3.2.1 CONFIGURACIÓN DEL SERVIDOR PROXY Y NAT

Primero hay que configura el servidor proxy, y para ello en la ventana principal del WinBox figura 5.12, seleccionamos IP y posteriormente Web Proxy, figura 5.19.

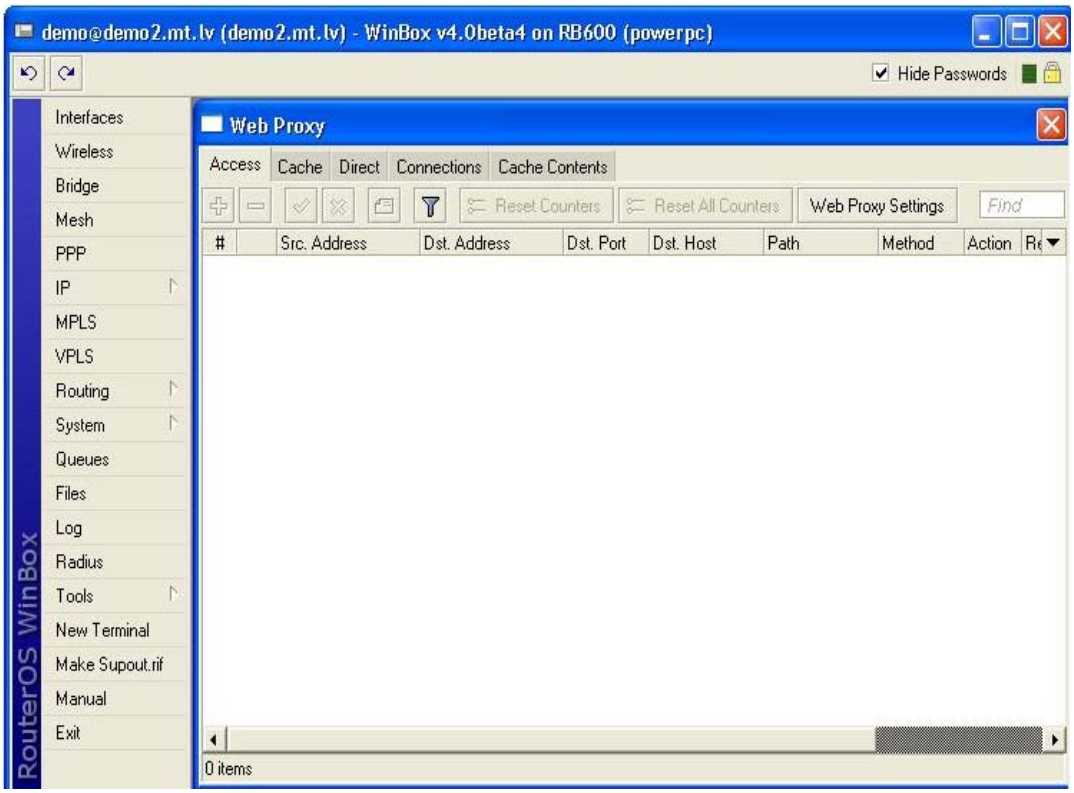


Figura 5.19 Menú de configuración del servidor web-proxy

Para iniciar la configuración hacemos click en la casilla “Web Proxy Settings”, que se muestra en la parte superior derecha de la figura anterior, con lo que se abre una nueva ventana donde se introducen los parámetros a configurar, figura 5.20.

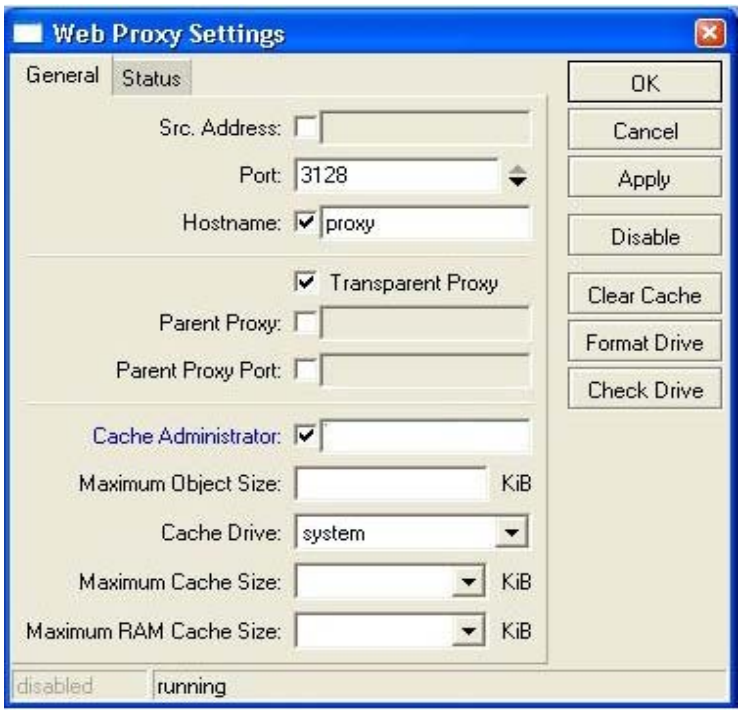


Figura 5.20 Configuración del servidor web-proxy

En la ventana mostrada en la figura anterior, se especifican los parámetros a configurar, tales como: Puerto (Port) que corresponde a la aplicación del proxy a través del cual el servidor escucha, nombre del host (Hostname), la opción para que sea transparente el servidor (Transparent Proxy) y el caché de administrador (Cache Administrator), en el cual se debe especificar un usurario como administrador del sistema cache que se ubica en el sistema (Cache Drive), además de asignar memoria a los objetos (Maximum Object Size) que se procesan, y al cache en disco y RAM (Maximum Cache Size y Maximum RAM Cache Size) que se utilizarán para este servicio. Se proponen los siguientes valores:

Maximum Objet Size	5120 KiB
Maximun Cache Size	2500000 KiB
Maximun RAM Cache Size	128000 KiB

Una vez terminada esta parte de la configuración hacemos click en la casilla “OK” para aceptar. Ahora falta redireccionar el puerto 80 que corresponde a la transmisión de páginas web, para que las peticiones y solicitudes que se hagan desde, o hacia la red pasen primero por el proxy a través del puerto 3128 y sean redirigidas. Para ello recurrimos nuevamente a la configuración del firewall y elegimos la opción NAT para definir las reglas para la traducción de direcciones. En la ventana que aparece asignamos los valores que se muestran en la figura 5.21.

Figura 5.21 Configuración de NAT

Los parámetros configurados se muestran en la pestaña “General” de la figura anterior, donde queda especificado que las reglas para la traducción de

direcciones se aplican al puerto 80 de la interfaz llamada “Computo”, aunque aún no se define la política, es decir, la acción sobre los parámetros ya establecidos. Por lo tanto en la pestaña “Action” definimos esta regla, figura 5.22. La regla deberá aplicarse para cada una de las interfaces internas que haya. Para la red de nuestro ejemplo esta interfaz pertenece a la subred “Contabilidad”.

Figura 5.22 Reglas de NAT

En esta regla la acción tomada es redirigir las conexiones del puerto 80 al puerto 3128 del servidor proxy instalado, y para que en todas las subredes que haya se reconozca el ruteo, en la pestaña “General” y “Action” se especifica la regla mostrada en figura 5.23.

Figura 5.23 Enmascaramiento NAT

Ahora hay que redireccionar aquellos puertos que son filtrados por el servidor proxy para que el tráfico entrante obtenga respuesta, es decir, como las peticiones al puerto 80 que pasan a través del proxy, es necesario indicarle a éste la dirección IP del servidor web donde serán atendidas.

Para configurar esta regla nos vamos al menú principal del firewall y hacemos click en la pestaña NAT, al abrirse la ventana de configuración en la pestaña “General” se definen los parámetros a configurar, figura 5.24.

Figura 5.24 Regla NAT para redireccionar el proxy al servidor web

Una vez establecida la regla NAT pasamos a la pestaña “Acción” para especificar hacia donde hay que redirigir el tráfico para el puerto 80, figura 5.25.

Figura 5.25 Estableciendo la dirección IP del servidor web

5.3.2.2 BLOQUEO DE WEB MESSENGER

Una vez configurado el servidor proxy el siguiente paso es bloquear las páginas web messenger. Por lo que regresamos al menú principal elegimos IP y después Web Proxy, en la ventana que aparece seleccionamos la pestaña “Access” que generalmente está dada por default, figura 5.26.

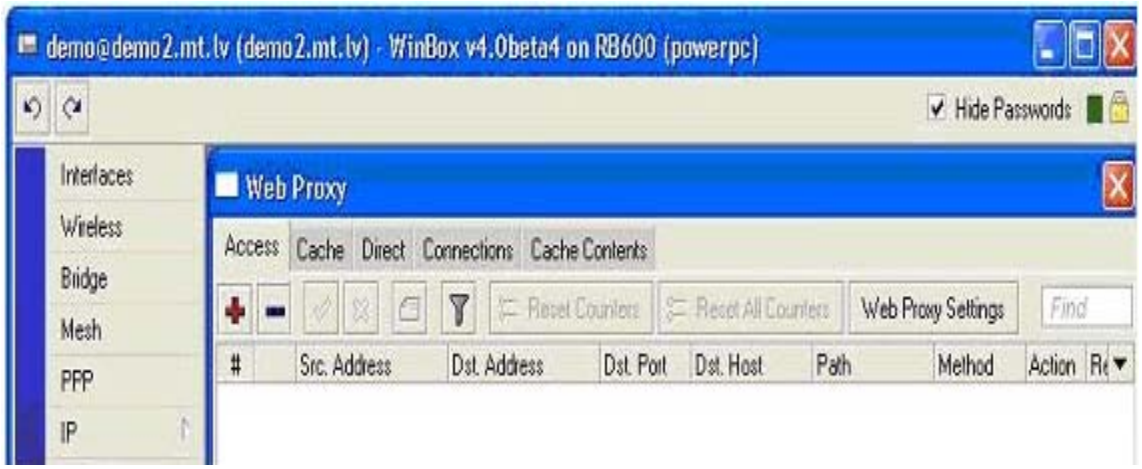


Figura 5.26 Menú de configuración del servidor web-proxy

Ahora haciendo click en el icono de signo más “+” que está debajo de esta pestaña, aparece una nueva ventana donde se configuran los parámetros deseados para la política que se desea implementar, figura 5.27.

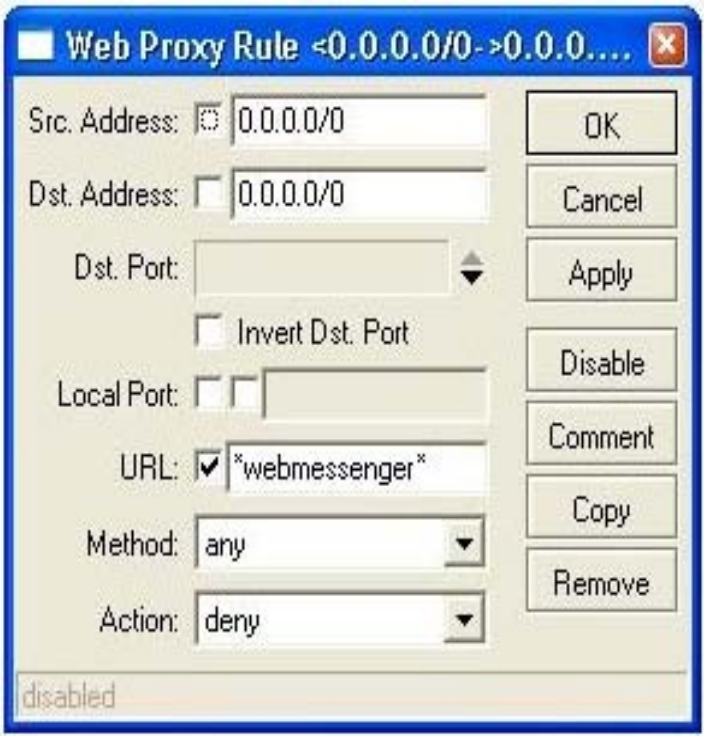


Figura 5.27 Bloqueo de web messenger a través del proxy

Como se observa en la figura anterior el parámetro principal es la URL, donde se especifica la cadena a buscar dentro de las páginas web, y posteriormente la acción que emprenderá la regla, que en este caso es rechazar “deny”.

5.3.2.3 BLOQUEO DE CONTENIDO PORNOGRÁFICO

De igual forma bloqueamos las páginas que contengan pornografía, figura 5.28.

Figura 5.28 Bloque de pornografía a través del proxy

Como en el caso anterior, lo más importante es especificar la cadena a buscar dentro de la página web, y al aplicar la regla “deny”, la URL será bloqueada automáticamente. Este proceso debe repetirse para buscar cadenas relacionadas con el mismo tema (sex, xxx, etc.), y del mismo modo puede hacerse para bloquear cualquier otra aplicación web como descargas de archivos, juegos, u otra clase de entretenimientos que están fuera de las funciones de una red organizativa.

Al final todas las políticas de seguridad aplicadas en el proxy pueden verse en la pantalla principal de configuración donde se lista cada una de las reglas

emprendidas, tal como se observa en la figura 5.29, donde también se muestra que se bloquearon archivos con formato mp3 y avi, así como descarga de archivos rar, zip o exe.

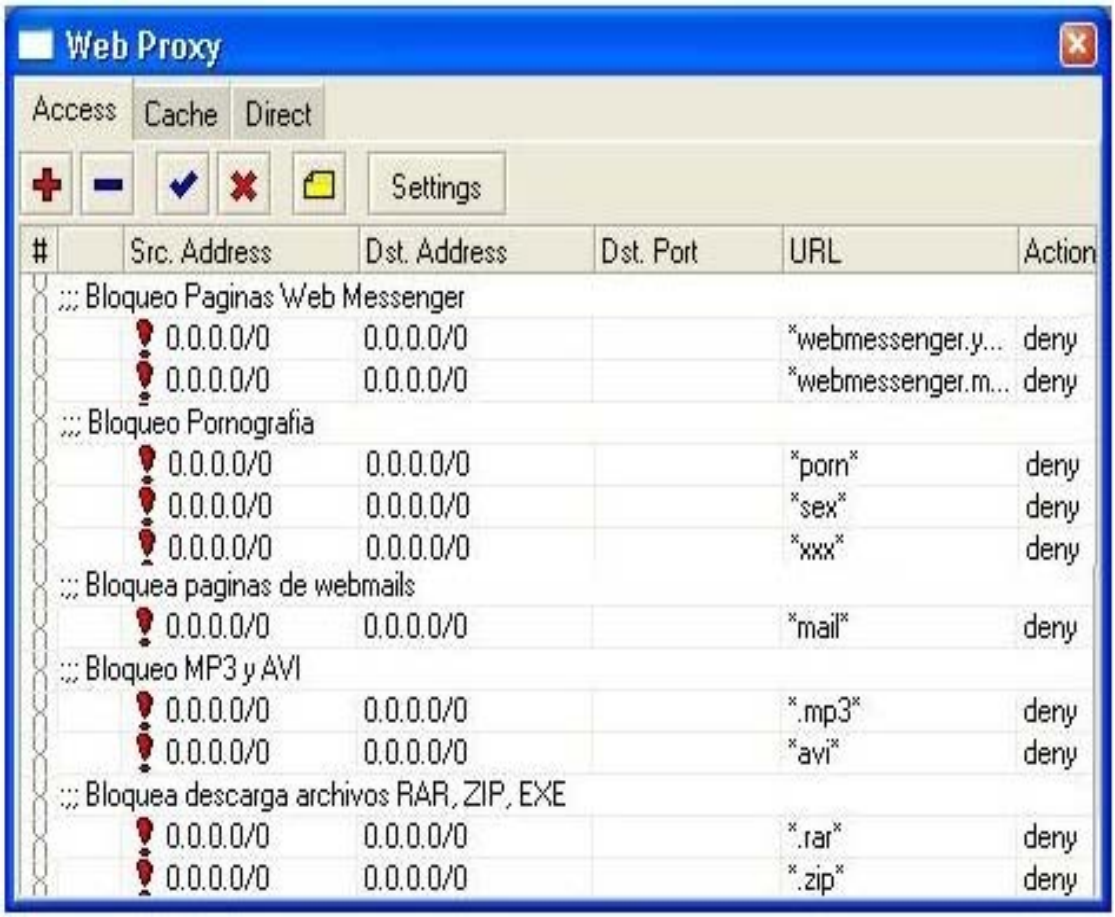


Figura 5.29 Reglas configuradas en el servidor proxy

Del mismo modo es posible definir nuevas políticas para el firewall y el servidor proxy (descartar conexiones invalidas, limitar paquetes ICMP, aceptar tráfico UDP,...), dependiendo de los servicios que se ofrezcan y necesidades de la red, siguiendo la misma dinámica que en los ejemplos anteriores.

5.4 REDES PRIVADAS VIRTUALES (VPN)

Las redes privadas virtuales (VPN – Virtual Private Network), son una infraestructura de red que permite la conexión de equipos de distintas redes privadas de forma remota; las cuales por lo general pertenecen a una sola organización como extensiones de la misma; VLAN (Virtual Local Area Network – Red Virtual de Área Local), para compartir recursos sobre una red pública como lo es Internet, creando una transmisión segura de datos utilizando técnicas de tunelling, encriptación y calidad del servicio (QoS – Quality of Service), logrando aprovechar los recursos de una red pública existente convirtiéndola en un medio seguro de enlace y transporte de datos de manera virtual, figura 5.30.

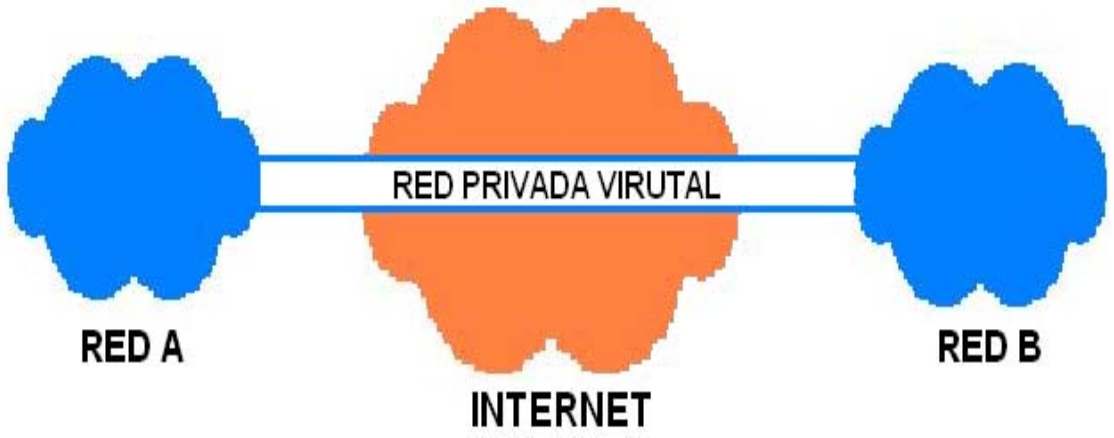


Figura 5.30 Red Privada Virtual VPN

Las causas por el que este tipo de redes son usadas se basa principalmente en dos factores determinantes:

1 **BAJO COSTO.** Debido a que utilizan la infraestructura existente de las redes públicas, disminuyendo en un alto porcentaje el costo de alquilar líneas dedicadas o en su defecto hacer un tendido de cableado propio; lo cual resulta totalmente ilógico cuando las distancias a cubrir son entre ciudades o incluso entre países.

2 **FÁCIL DE IMPLEMENTAR.** No requieren de mucha tecnología para su implementación, y su mantenimiento no es complicado.

La perspectiva que tienen los usuarios que se conectan desde fuera de la red a través de la VPN vía Internet, es similar a que si lo hicieran desde adentro de la misma, logrando que la conexión sea transparente para el usuario, ya sea que se trate de accesos remotos (desde oficinas externas, hoteles, hogar, etc.), o conexiones permanentes entre dos redes (punto a punto), como cuando se desea conectar varias sucursales de una organización con la oficina central.

Existen dos formas de implementar una VPN: por software o por hardware. En el primer caso el costo es mucho menor, con el inconveniente de que su rendimiento y configuración no son tan óptimos como cuando se hace a través de hardware, que por tratarse de equipos especialmente dedicados se logran mejores resultados, ya que todos los procesos son exclusivos para el manejo de la red pero con la desventaja de que el costo es mayor.

Ya sea que se implemente por software o por hardware una VPN, lo más importante a considerar son los protocolos a utilizar para que la VPN cumpla con los siguientes servicios en cuanto a seguridad se refiere:

1 **TUNNELING.** Esta técnica es utilizada para crear el canal de comunicación a través de la red pública, dando la ilusión de un túnel entre los extremos de los equipos involucrados que se desean conectar.

2 **CONFIDENCIALIDAD (Encriptación).** Para que los datos que viajan por la red pública lo hagan lo más seguro posible.

3 **AUTENTICACIÓN.** Para saber que usuario/equipo es el que intenta conectarse, y en caso de que su identificación no sea válida negar el acceso a la red.

4 **INTEGRIDAD.** Garantizar la información que viaja a través de la VPN.

El protocolo más utilizado para la creación de redes virtuales es IPsec (Internet Protocol Security – Protocolo de Seguridad para Internet), el cuál es un estándar en el IETF (Internet Engineering Task Force – Grupo de trabajo de Ingeniería en Internet), pero también existen otros como L2TP (Layer 2 Tunneling Protocol – Protocolo de Túnel Capa 2), sucesor de los protocolos PPTP (Point to Point Tunneling Protocol – Protocolo de Túnel Punto a Punto) y L2F (Layer 2 Forwarding – Transporte de Capa 2), los cuáles debido a sus deficiencias han sido reemplazados paulatinamente.

5.4.1 IPsec

IPsec es una extensión del protocolo IP que cumple con los servicios de tunneling, encriptación autenticación e integridad. Es considerado el protocolo ideal para las redes de la siguiente generación dada su relación con el protocolo IPv6, ya que IPsec está implementado en éste de forma obligatoria.

El protocolo IPsec, se apoya a su vez en dos protocolos principalmente para su funcionamiento; además de otros, éstos son: AH (Autentication Header – Autenticación de Encabezado) y ESP (Encapsulating Security Payload – Seguridad de Encapsulado de Carga Útil). Estos protocolos logran que se genere información extra para identificar asociaciones de seguridad añadiendo un encabezado extra entre las capas de red y transporte.

El protocolo AH se encarga de autenticar y contener las direcciones de origen y destino, ESP encripta y autentica y mantiene un flujo de tráfico limitado. En la figura 5.31 podemos ver la arquitectura de funcionamiento del protocolo IPsec.

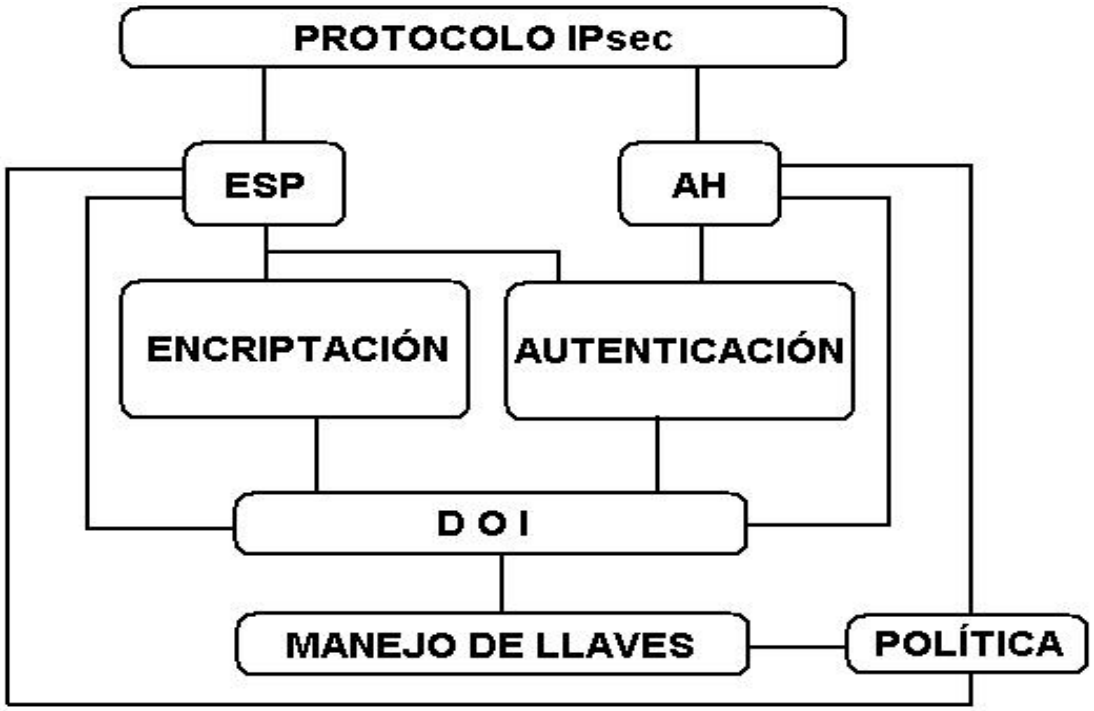


Figura 5.31 Arquitectura de IPsec

En la figura anterior se presentan de forma general cada una de las capas que intervienen para que IPsec sea un protocolo seguro. La comunicación entre dos entidades bajo este esquema, se hace a través de asociaciones de seguridad (SA – Security Asociations), determinando de esta forma los protocolos a utilizar, llaves, y duración de éstas entre otros parámetros. Dichas asociaciones son creadas de manera unidireccional, es decir, cada entidad mantiene una SA por separado para el tráfico de entrada y para el de salida, además de mantener SA independientes para cada protocolo; una para AH y otra para ESP. Estas SA son almacenadas en una base de datos que contiene toda esta información.

Los parámetros que se utilizan para establecer una comunicación segura con IPsec y entablar las Asociaciones de Seguridad se llaman DOI (Domain Of Interpretation – Dominio de Interpretación), a través de políticas definidas manualmente de forma estática, o asignadas de forma dinámica utilizando protocolos para el intercambio de llaves; IKE (Interchange Key Exchange – Intercambio y Cambio de Llave). Mediante este protocolo se crean las SA al momento de tratar de entablar una comunicación segura y no existir la SA, de tal forma que se negocia la SA con el destino y se crea la SA en la base de datos (SADB).

Las Asociaciones de Seguridad son referidas mediante un SPI (Security Parameter Index – Índice de Parámetros de Seguridad), en un campo de 32 bits que identifica a cada una de las SA, de esta forma tanto el emisor como el receptor saben que política aplicar para asegurar la información que se envía, y para verificar la información recibida. Este registro se incluye en las cabeceras de los protocolos AH y ESP.

Los parámetros que se utilizan para establecer las Asociaciones de Seguridad son los siguientes:

1 **NÚMERO DE SECUENCIA.** Es un campo de 32 bits que se incrusta en las cabeceras de los protocolos AH y ESP en los paquetes de salida. Inicia en 0 y se incrementa en uno cada que la SA es utilizada, con lo que se consigue detectar paquetes retransmitidos (replay).

2 **SOBREFLUJO DEL NÚMERO DE SECUENCIA.** Se activa para prevenir fallas por sobre flujo, en este caso la política establecida definirá que hacer.

3 **VENTANA ANTI-RESPUESTA.** Se utiliza durante el procesamiento de los paquetes de entrada para detectar y descartar paquetes retransmitidos por equipos desconocidos.

4 **TIEMPO DE VIDA.** Es el tiempo especificado en bytes para que una Asociación de Seguridad sea válida. Para evitar la pérdida de conexión se manejan dos tipos de alertas: soft y hard. La primera es una preventiva que indica que la SA está a punto de expirar y se pueda negociar una nueva SA antes de que esto suceda, de otra forma expirara cuando se llegue al límite; hard, y se pierda la conexión.

5 **MODO.** IPsec maneja dos modos de funcionamiento: túnel o transporte.

6 **DESTINO DEL TÚNEL.** Dirección IP agregada en el encabezado exterior del paquete IPsec en modo túnel.

7 **PMTU (Protocolo de Unidad Máxima de Transferencia).** Son utilizados debido a que IPsec no fragmenta ni reensambla paquetes.

Los algoritmos criptográficos que se utilizan en IPsec son: funciones hash (SHA) para integridad mediante certificados digitales, y ·AES (Advanced Encryption Standard – Estándar de Encriptación Avanzado) sucesor del algoritmo DES (Data Encryption Standard – Estándar de Encriptación de Datos) para confidencialidad.

5.4.2 TRASNPORTE Y TÚNEL CON IPsec

IPsec puede funcionar en dos modalidades: transporte y túnel. El modo transporte es utilizado para conexiones punto a punto entre hosts a través de la VPN, y el modo túnel es aplicado para la conexión no sólo de hosts, sino entre redes

enteras. Para ello los protocolos AH y ESP son configurados para funcionar en estas dos modalidades (AH y/o ESP en modo transporte – AH y/o ESP en modo túnel).

Bajo el modo transporte los paquetes provenientes de la capa superior (TCP o UDP) son tomados por el protocolo IPsec y se aplican las políticas de seguridad definidas, de tal forma que sí la política establece que los paquetes sólo deben ser autenticados se utiliza AH, pero sí es necesario mantener la confidencialidad de los paquetes se utiliza ESP, la figura 5.32 muestra la comunicación en modo transporte entre dos hosts.

Figura 5.32 IPsec en modo transporte

En modo transporte la seguridad proporcionada por IPsec se aplica sólo a la "carga útil" dentro del paquete proveniente de la capa superior (TCP), y no al paquete completo. El protocolo IPsec añade las cabeceras AH y/o ESP, para que por último la capa de red agregue la cabecera IP. La figura 5.33 muestra el encapsulado de los paquetes.

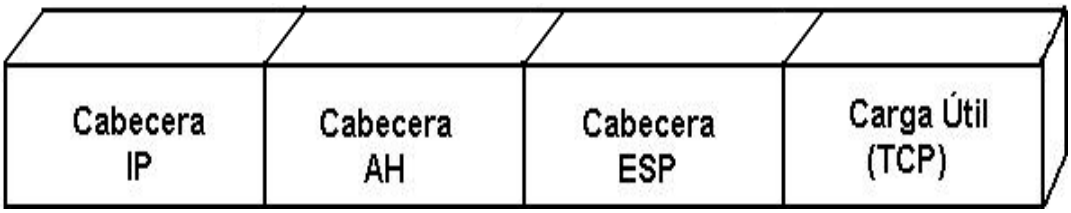


Figura 5.33 Formato de los paquetes IPsec en modo transporte

La figura anterior también muestra el orden con que se aplican los protocolos AH y ESP cuando ambos son utilizados, y la dirección IP (cabecera IP), donde se dirige el paquete permanece intacta, ya que a ésta no se le aplica ninguna seguridad extra, por lo que las tablas de enrutamiento permanecen intactas.

El otro modo de funcionamiento de IPsec; túnel, es utilizado cuando la seguridad del protocolo es proporcionada por un dispositivo externo independiente del equipo que genera los paquetes, es decir, en una comunicación segura host a host en modo transporte, los paquetes son enviados a su destino directamente por éstos, y el protocolo IPsec es implementado como una aplicación más, o como parte del sistema operativo.

En el modo túnel existe un dispositivo extra que toma los paquetes provenientes del host y aplica el protocolo IPsec, para ello deben existir Asociaciones de Seguridad entre el host y el dispositivo, y entre los dispositivos. Generalmente los dispositivos utilizados para generar una comunicación en modo túnel son los routers, la figura 5.34 muestra esta configuración.

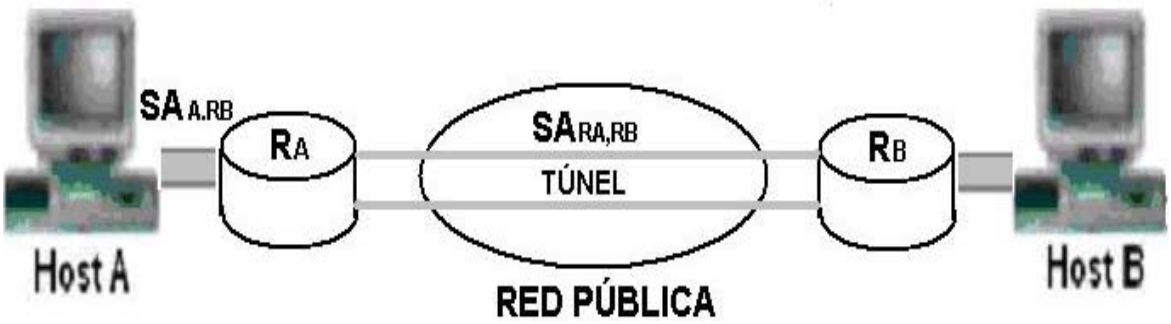


Figura 5.34 Configuración modo túnel con IPsec

En la figura 5.34, se ilustra la comunicación entre dos host, A y B, utilizando IPsec a través de dos routers, RA y RB, que proporcionan la seguridad y el canal virtual de comunicación (túnel) entre ambos hosts. La SA para que el host A pueda

establecer una conexión con el host B pude ser entre el host A y RB, o entre ambos routers, de esta forma se crea un canal seguro.

Este tipo de configuración es la que permite la creación de VPN's, ya que los routers son dispositivos capaces de soportar mayor tráfico, con lo que se logra no solo conectar un host, sino que se puede dar salida a varios equipos a la vez o incluso a toda la red, y con la configuración adecuada permiten una mayor granularidad en la seguridad de la red, ya que los equipos que se conectan a la VPN por la red pública no se exponen directamente a ésta.

En el modo túnel IPsec asegura paquetes de la capa de red, todo el paquete IP proveniente del host es encapsulado por las cabeceras IPsec que agrega el dispositivo que proporciona los servicios de seguridad, además de un encabezado IP extra que encapsula todo el paquete, para que sea posible enrutar los dispositivos y crear el túnel, la figura 5.35 muestra el formato de los paquetes.

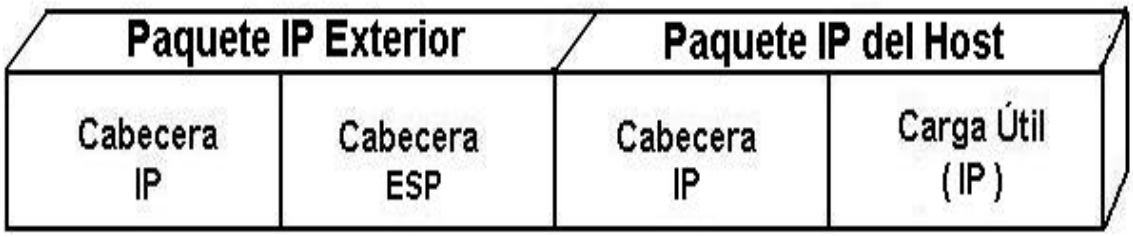


Figura 5.35 Formato de los paquetes IPsec en modo túnel

Como se observa en la figura 5.35, el host envía el paquete IP intacto al dispositivo externo el cuál adhiere cabeceras de seguridad de IPsec que envuelven todo el paquete, por lo que el paquete original viajará por el túnel con la dirección IP origen-destino que corresponde al dispositivo (router).

De este modo con el protocolo IPsec, es posible utilizar una red pública de poca seguridad para conectar equipos de una red privada a otra de modo seguro, ya

que éste protocolo se encarga de asegurar los paquetes a través de la red pública, en base a los servicios de seguridad que proporciona y las políticas de seguridad establecidas sobre direcciones IP (destino y origen), usuario, o puertos específicos donde haya que aplicar las políticas.

Por último mencionar que existen otros protocolos para la creación de VPN´s, tal es el caso de MPLS (Multi Protocol Label Switching – Conmutación de Etiquetas Mltiprotocolo) estándar creado por el IETF, el cual se basa en adherir etiquetas en los paquetes entre las capas de red y enlace (para cualquier protocolo utilizado en estas dos capas, de aquí el nombre “Multiprotocolo”), de tal forma que la trayectoria del paquete se hace en base al contenido de las etiquetas en los paquetes (Conmutación en función de Etiquetas), de modo que no es necesario el enrutamiento tradicional ni túneles punto a punto. Aunque ofrece mayor escalabilidad, requiere de una mayor complejidad técnica para su in

Capítulo 6

Riesgos y Vulnerabilidades en la Red

CAPÍTULO 6 RIESGOS Y VULNERABILIDADES EN LA RED

6.1 TIPOS DE ATAQUES Y VULNERABILIDADES

Para que un ataque se produzca deben existir una serie de condiciones que hagan factible su realización, dicho de otra forma, un ataque no puede perpetrarse si no existen las vulnerabilidades asociadas a estas condiciones como son: usuarios, equipos, sucesos e ideas, que de forma accidental, imprudencial o deliberada, puedan poner en riesgo la seguridad de los sistemas dentro de la red en el momento que se presente la condición apropiada.

Los ataques dentro de una red, son actividades encaminadas a violar la seguridad. Estas actividades son representadas con un conjunto de técnicas que facilitan y permiten al atacante alcanzar sus objetivos. Por tal motivo la finalidad de este apartado, es dar a conocer las técnicas más utilizadas para que sean consideradas al momento de la planeación y/o implementación, de las medidas de seguridad tomadas como parte de las políticas de seguridad encaminadas a proteger la red mediante la prevención, detección y respuesta.

Las redes informáticas tienen características que las hacen especialmente vulnerables debido a que no existe un canal de comunicación físico directo entre el emisor y el receptor, haciendo que la comunicación entre ambos sea insegura. Los ataques relacionados con este sistema de comunicación, se pueden clasificar en cuatro categorías:

1 **INTERRUPCIÓN.** Se produce cada que un sistema o servicio de la red son obligados a finalizar de forma abrupta.

2 **INTERCEPCIÓN.** Cuando algún ente (equipo o usuario), accede sin autorización a la información o equipos de la red.

3 **MODIFICACIÓN.** Se logra después de haber hecho una intercepción, y el contenido de la información o equipos son alterados en su forma original.

4 **SUPLANTACIÓN.** Se basa en falsificación de identidades para conseguir entrar en algún sistema bajo otra identidad.

Para prevenir este tipo de ataques las redes deben contar con un sistema de seguridad que incorpore mecanismos que proporcionen los tipos y niveles de seguridad requeridos. Tales mecanismos pueden clasificarse en:

1 CONFIDENCIALIDAD
2 INTEGRIDAD
3 AUTENTICACIÓN
4 NO REPUDIO
5 CONTROL DE ACCESO
6 DISPONIBILIDAD

Las vulnerabilidades en una red también están asociadas a los protocolos utilizados, debido a dos factores: primero son el medio a través del cual la información viaja, y segundo al nivel de penetración, ya que recorren las vías de comunicación pasando por varios dispositivos y redes, llegando a cruzar ciudades, estados, países y continentes.

Los protocolos de comunicación establecen los procedimientos bajo los cuales se realiza una comunicación, y para un atacante resulta muchas veces más fácil atacar a éstos que a los métodos de seguridad aplicados a los datos que llevan, tales como algoritmos de cifrado, ya que atacar un algoritmo requiere más tiempo y dedicación debido al cálculo que se necesita hacer, y por el contrario atacar un protocolo sólo requiere de cierta técnica por parte del atacante.

Y aunque los métodos de ataque pueden clasificarse en categorías, éstos pueden estar relacionados entre sí, ya que el uso de un método facilita o permite el uso de otros, de forma que se pueda complementar el ataque. Desde este punto de vista las técnicas de ataque pueden clasificarse en dos grupos:

a Por el número de paquetes a emplear en el ataque:
   i. **Atomic.** Si se utiliza un sólo paquete.
   ii. **Composite.** Cuando se usan varios paquetes.

b Por la información necesaria para llevar a cabo el ataque:
   iii. **Context.** Cuando se utiliza solo información de la cabecera del protocolo.
   iv. **Content.** Se necesita además de información de las cabeceras, el campo de datos.

En la siguiente figura 6.1, se muestra algunos ejemplos de ataques clasificados según las definiciones anteriores

	Atomic	**Composite**
Context	ping of death land attack	port scan SYN flood
Content	DNS attack RPC	sniffing SMTP attack

Figura 6.1 Ejemplo de ataques y su categoría

La mayoría de estos ataques están descritos en el capítulo tres, por ejemplo, según la tabla de la figura, “land attack” utiliza sólo un paquete (SYN) y la información en la cabecera IP (dirección origen y destino idénticas), por el contrario “SYN flood” está en la categoría de ataques DoS (Deny of Services – Negación de Servicios), la técnica que utiliza es enviar mensajes de forma masiva TCP del tipo SYN (para establecer conexión), las cuales son contestadas por el

servidor (SYN-ACK), a espera de que el cliente confirme la conexión mediante un ACK, y como nunca es enviado el sistema atacado consume memoria y recursos por cada una de las conexiones falsas, provocando la saturación y anulación de los servicios.

6.2 CLAVES DE ACCESO Y SEGURIDAD

Dada la importancia que tiene la seguridad en las redes de comunicaciones es necesario establecer una política sobre la gestión de claves, debido a tres factores:

1 **USO.** Cada que se utiliza una clave queda expuesta y se ve cada vez comprometida entre más tiempo pase y se utilice. Por tal motivo es necesario limitar el tiempo de uso y renovar periódicamente las claves.

2 **CANCELACIÓN.** Es necesario que las claves utilizadas por usuarios que se han apartado de la organización sean canceladas inmediatamente, ya que no deben tener más acceso a la información.

3 **CLASIFICACIÓN.** Es conveniente utilizar claves diferentes para distintas aplicaciones, minimizando la utilización de claves de administrador. Se puede utilizar una clasificación en forma piramidal, donde el vértice de la pirámide esté ocupado por la clave más importante de la red: “clave de seguridad maestra”. El número de niveles de la pirámide puede ser variable dependiendo de las necesidades y tamaño de la red en particular, pero el mínimo se aconseja de tres.

6.2.1 CICLO DE VIDA DE LAS CLAVES DE USUARIO

En el capítulo cuatro hice referencia a las cuentas de usuario y a la labor administrativa relacionada al mantenimiento de las mismas. Pero dada la importancia de esta tarea como parte de una política de seguridad vinculada con esta actividad, abordo nuevamente el tema desde un punto de vista práctico donde se esquematiza el ciclo de vida conveniente para una clave de usuario.

La siguiente figura 6.2 presenta el ciclo de vida habitual para las claves de usuario dentro de una red.

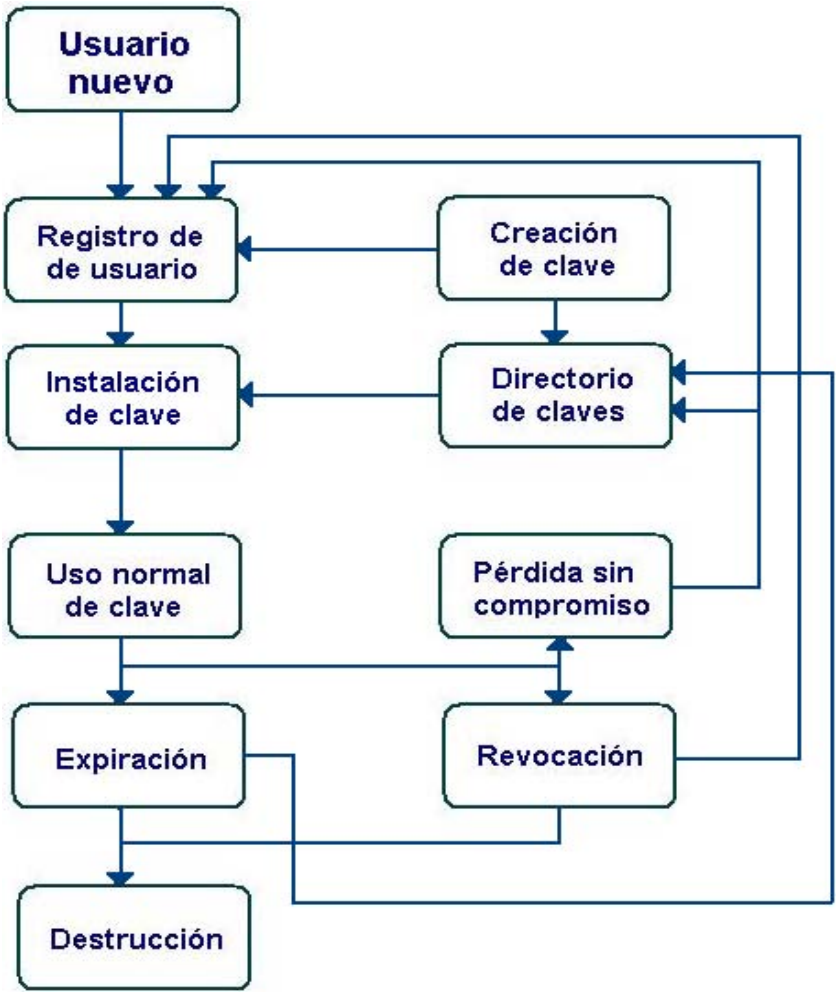


Figura 6.2 Ciclo de vida de las calves de usuario

La primera operación es registrar al usuario nuevo por parte del administrador o encargado, tras la autorización explícita de la dirección o gerencia de la organización que dan prueba fehaciente de la identidad del nuevo usuario que será registrado. Una vez terminado este proceso se procede a la creación de la clave del usuario.

A partir de este momento el usuario puede hacer uso de la clave de forma normal, hasta el momento que concluya el período de validez de ésta, y se proceda a su destrucción y sustitución por una clave nueva.

La clave queda almacenada en un directorio para que en caso de pérdida, sin que la clave haya sido comprometida, se pueda recuperar del directorio de claves, además de facilitar el control de éstas. Si la clave ha sido comprometida por algún motivo del que se sospeche, o bien el usuario se ha deslindado de la organización, la clave es revocada y destruida.

6.3 SEGURIDAD EN INTERNET

Las redes de computadoras, o también dicho redes de datos, tienen como finalidad el intercambio de información, pero no sólo deben satisfacer esta necesidad, sino que también deben cubrir otras características para considerarse eficientes. En otras palabras se debe asegurar que los datos que viajan por la red, estén protegidos a modo de evitar: fallas o errores en la recepción, pérdida o alteración de la información, y puntualidad en la entrega.

Esta serie de factores se engloban dentro de una política de seguridad para hacer de una red, un sistema fiable y seguro de comunicación, tanto que hoy en día las empresas y organizaciones se han vuelto dependientes de esta tecnología como recurso indispensable en el desarrollo de sus labores cotidianas, de modo que el establecer medidas de seguridad concretas y con buenos resultados se ha vuelto preponderante, sobre todo cuando se ofrecen servicios a través de Internet, ya

que al mismo tiempo se expone la información hacia el exterior, donde las condiciones hacen que se genere un riesgo inminente, al permitir que otros equipos/usuarios tengan acceso a dichos datos.

6.3.1 El World Wide Web

En las últimas dos décadas el desarrollo de Internet ha sido de forma exponencial, de modo que ha sobrepasado las espectativas por dos motivos: el flujo de información masiva, y las posibilidades de comunicación. El Internet que hoy conocemos no es el mismo que aquél cuando surgió a finales de los años 60. En ese entonces no existían interfaces gráficas ni amigables como las que hoy existen que facilitan el uso y manejo de este potencial recurso, sólo existían programas (como telnet y ftp), que se manejaban a base de comandos en modo texto, y una interfaz arcaica que poco a poco fue cambiando, hasta que aparece el World Wide Web (www), en el centro europeo de investigación nuclear (CERN) en Suiza (1989), desarrollado por Tim Berners y Robert Cailliau.

Aunque el Internet ya existía, no fue sino hasta la aparición del web que cambió por completo la experiencia del usuario, donde el entorno gráfico es fundamental, ya que detrás de estos o en una parte del texto, se encuentran inmersos enlaces a otros documentos (páginas electrónicas) y recursos, que le permiten al usuario interactuar de manera más sencilla e inmediata, olvidándose por completo de todo lo que hay detrás en la ejecución de una instrucción, aunque ésta tenga que pasar por varios procesos diferentes. Esto se debe a que se basa en tres características técnicas básicas:

1 **HTML.** (Hypertext Markup Language – Lenguaje Etiquetado de Hipertexto), que especifica el contenido y diseño de las páginas electrónicas para ser interpretadas por el programa cliente (navegadores).

2 **URL.** (Uniform Resource Locator – Localizador Uniforme de Recursos), para identificar otros documentos electrónicos o recursos, ya sea en el mismo servidor u otro distinto.

3 **HTTP.** (HyperText Transfer Protocol – Protocolo de Transferencia de Hipertexto), establece la forma en que los navegadores (clientes) y servidores se comunican.

La interconexión de redes unas con otras, ha dado auge a que cada día esta gran red crezca, y hoy en día sea uno de los medios de comunicación más importantes y trascendentes, ya que podemos acceder a él desde la comodidad de nuestro hogar y sumergirnos en este mundo de información como parte de nuestras actividades.

Por tal motivo la necesidad de conectar redes privadas a Internet es cada vez mayor, ya sea con fines de negocio, educativo, público, informativo, etc., convirtiéndose en un medio masivo de comunicación de gran alcance.

6.3.2 RED PERIMETRAL Y DMZ

Cuando una red privada ofrece servicios de correo, ftp, web u otros, hacia el exterior, es necesario ubicar los servidores para ser accedidos por otras redes generalmente Internet, de modo que se pueda tener control sobre el tráfico que fluye entre ambas redes, la pública y la privada.

Como parte de la seguridad en la red interna, es necesario implementar un modelo a seguir a manera de aislar los servidores y/o equipos que están expuestos a la red pública, ya que de lo contrario se corre el riesgo de que la red interna sea accedida a través de estos equipos en caso de un ataque que pudiera traspasar la seguridad de los equipos expuestos, la cual consiste generalmente en un firewall o proxy, que permite aislar ambas redes controlando el tráfico con base en la política

de seguridad escogida. Pero esta configuración no garantiza la seguridad de la red interna ya que ésta consiste en un único punto de control centralizado, figura 6.3.

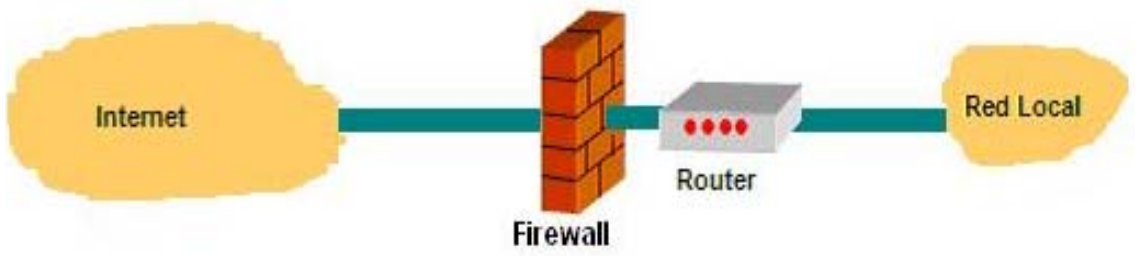


Figura 6.3 Enfoque tradicional firewall-router

La figura 6.3 muestra la acción de un solo firewall controlando el tráfico entre la red local e Internet, este enfoque es completamente tradicional utilizando una conexión simple entre dos redes a través de un router que posee dos interfaces de red. Para asegurar una red privada tanto de ataques externos como internos, se deben definir otro tipo de políticas de seguridad que sean capaces de establecer un perímetro de red, el cual consiste en una capa de seguridad adicional donde todo el tráfico tanto entrante como saliente, sea filtrado y aislado del resto de la red interna, de modo que si un atacante logra penetrar y entrar en la red sólo lo haga en la porción perimetral donde no se corre mayor riesgo, ya que el tráfico de la red interna no puede ser escuchado desde este punto.

Desde este punto de vista se puede establecer una red perimetral de protección, desde la cual se expongan diversos servicios en Internet a través de servidores, aceptando el tráfico proveniente del exterior sin comprometer la seguridad de la red completa.

Esta porción aislada de la red es conocida como *"Zona Desmilitarizada"* (DMZ – Demilitarized Zone), y es utilizada para generar redundancia en la seguridad y colocar servidores que se acceden desde Internet, de tal modo que todo el tráfico

entrante y saliente pasa por este punto de la red, permitiendo sólo las conexiones hacia, o desde Internet, a través de esta zona, ya que no están permitidas las conexiones de la DMZ hacia la red interna.

La arquitectura DMZ se consigue colocando dos firewalls: uno interno y otro externo. El primero se coloca entre la red perimetral y la red interna, el otro entre la red perimetral y la red externa, justo en esta zona delimitada por ambos firewalls se colocan los servidores que estarán disponibles desde Internet, aislando cualquier ataque que pueda provenir del exterior a la red local, tal como se muestra en la siguiente figura 6.4.

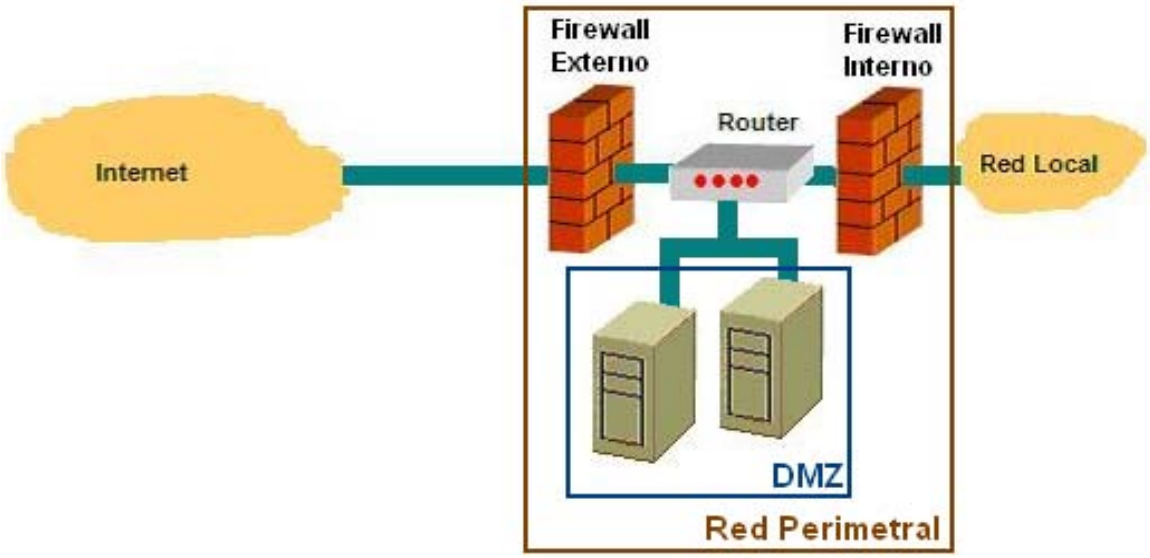


Figura 6.4 Red perimetral con zona desmilitarizada

La zona desmilitarizada provee una doble protección, y aunque físicamente puede consistir en un solo dispositivo (como se observa en la figura anterior), se utilizan distintas interfaces de red para aislar los firewalls y los servidores, la protección que proveen los firewall pueden verse como una capa que envuelve al router, figura 6.5.

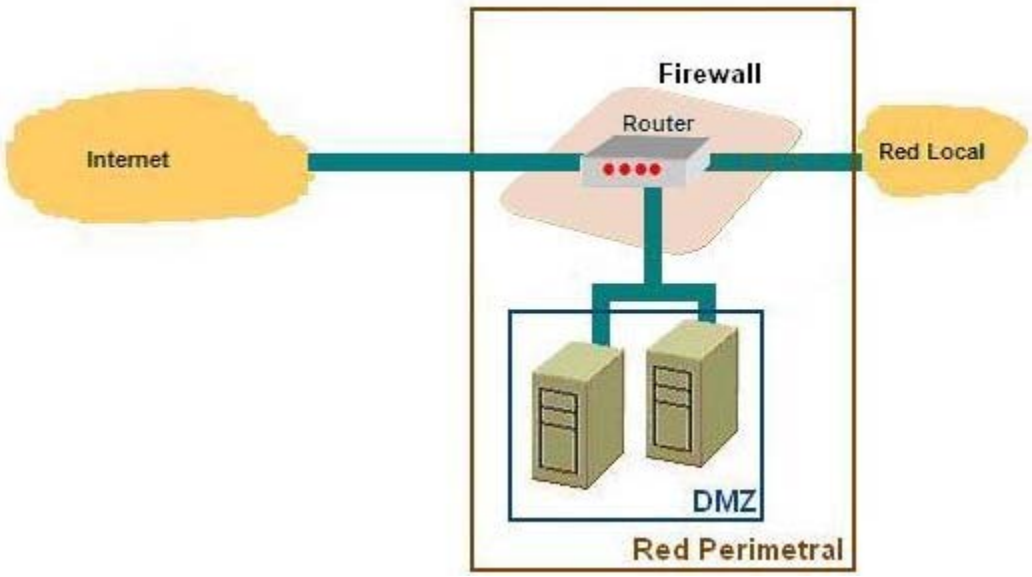


Figura 6.5 Protección envolvente del firewall

6.3.3 PROTOCOLOS DE ADMINISTRACIÓN DE RED

Existen además de los protocolos de comunicación y aplicaciones en red, protocolos encargados de la administración de las actividades que suceden en este entorno, que permiten a los administradores el control y depuración de errores con mayor uniformidad. Para ello existe un programa cliente de administración de red al cual accede el administrador, y un programa servidor de administración de red alojado generalmente en dispositivos de red (routers) administrados, estableciendo las relaciones administrativas entre estos dispositivos también.

6.3.3.1 ADMINISTRACIÓN CON SNMP

El protocolo estándar de administración de red en TCP/IP es SNMP (Simple Network Management Protocol – Protocolo Simple de Administración en Red), de esta forma el administrador puede consultar estadísticas registradas por un router

acerca del tráfico entrante y saliente, número de paquetes eliminados, etc., pero no puede determinar de manera específica los detalles. Para ello utiliza un estándar conocido como MIB (Management Information Base – Información Base de Administración). Básicamente el protocolo SNMP se compone de tres elementos:

1. **Administrador SNMP.** Es el sistema encargo de la administración de los dispositivos en la red utilizando el protocolo SNMP para el intercambio de información.

2. **Agente SNMP**. Es el software residente en el dispositivo administrado encargado de ejecutar el protocolo SNMP, e interactuar con el administrador SNMP a través de variables MIB.

3. **Objetos MIB.** Los objetos contenidos en la MIB se alojan en el dispositivo administrado, y contienen la información necesaria para la administración de los mismos.

Así como MIB define las variables administrativas de red a utilizar y su interpretación, existe otro estándar que define e identifica el tipo de variables: SMI (Structure Managemente Information – Estructura de Información Administrativa), se encarga además, de nombrar variables y reglas para distintos tipos de éstas, las cuales adoptan la forma ASN.1 (Abstract Syntax Notation 1 – Notación de Sintaxis Abstracta) de ISO, la cual permite que el uso y contenido de las variables no sea ambiguo, dada la diversidad de equipos en la red que pueden o no utilizar la misma representación de datos.

La siguiente figura 6.6 muestra el árbol jerárquico para la identificación de objetos en el espacio de nombres, donde cada sub-árbol MIB corresponde a cada una de las ocho categorías en que se divide la información de administración.

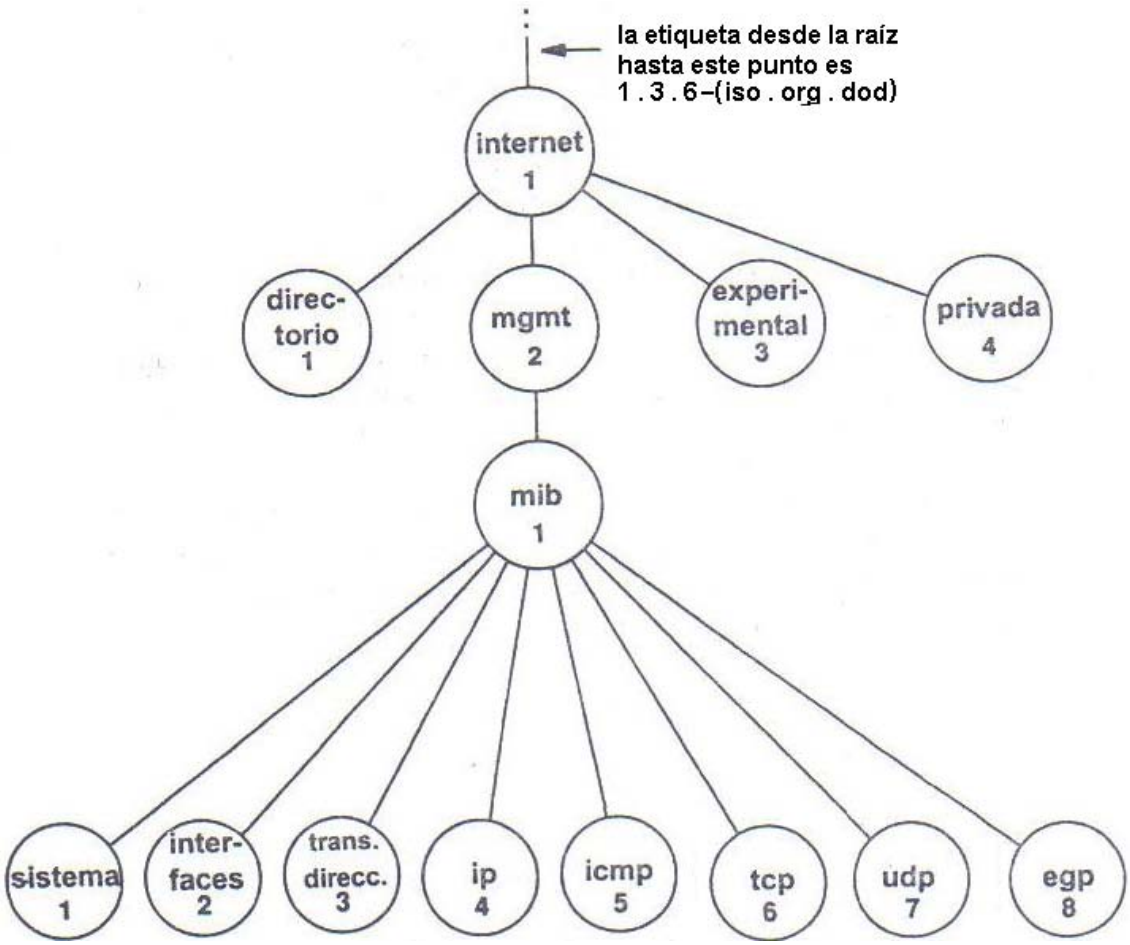


Figura 6.6 Árbol jerárquico para la identificación de objetos en SNMP

De este modo el nombre de un objeto utiliza la secuencia numérica a través de los nodos desde la raíz hasta llegar al objeto. Por ejemplo, la trayectoria o nombre numérico de la etiqueta ip en MIB es 1.3.6.1.2.1.4, si ahora existiera una variable llamada ipInReceives con identificador numérico 3 por debajo del nodo ip, su referencia numérica y nombre serían los siguientes:

1 . 3 . 6 . 1 . 2 . 1 . 4 . 3

iso.org.dod.internet.mgmt.mib.ip.ipInReceives

Cada una de las ocho categorías MIB se refieren a funciones específicas, que ayudan a obtener estadísticas e información necesaria para la administración. Las categorías se describen a continuación:

1 **Sistema.** Contiene información del sistema administrado: tipo de hardware, versión de software, tiempo a partir de la última inspección, etc.

2 **Interfaces.** Proporciona información del estado de la interfaz, dirección física, número de paquetes entrantes y salientes, así como errores en los mismos, entre otras.

3 **Translación** de direcciones AT (Adress Translation).Relaciona las direcciones IP relativas con direcciones IP específicas.

4 **IP.** Contiene información propia de la capa IP: número de datagramas entrantes y salientes, errores, etc.

5 **ICMP.** Proporciona información acerca de los distintos tipos de paquetes ICMP generados por algún tipo de falla.

6 **TCP.** Mantiene información propia de esta capa de red, tal como: número de segmentos enviados y recibidos, conexiones activas, puertos, etc.

7 **UDP.** Parecido a TCP.

8 **EGP.** (Exterior Gateway Protocol – Protocolo de Conexión Exterior). Indica el número de mensajes recibidos, enviados y con error, así como el estado de la entrada local EGP relativa a la conexión EGP vecina, con base en el sondeo periódico (hello/i hear you).

6.3.3.2 CONFIGURACIÓN DE SNMP CON MIKROTIK

Estos parámetros pueden verse claramente si se tiene habilitado un servidor SNMP. Para este ejemplo utilizamos el servidor SNMP incluido en el RouterOS de Mikrotik que se ha venido trabajando. Los OID del sistema (interfaces de red administradas por el servidor SNMP con Mikrotik), se obtienen desde la línea de

comandos. Para ello nos dirigimos al winbox para acceder al Mikrotik, y elegimos la opción New Terminal de las opciones mostradas en la parte izquierda, figura 6.7.

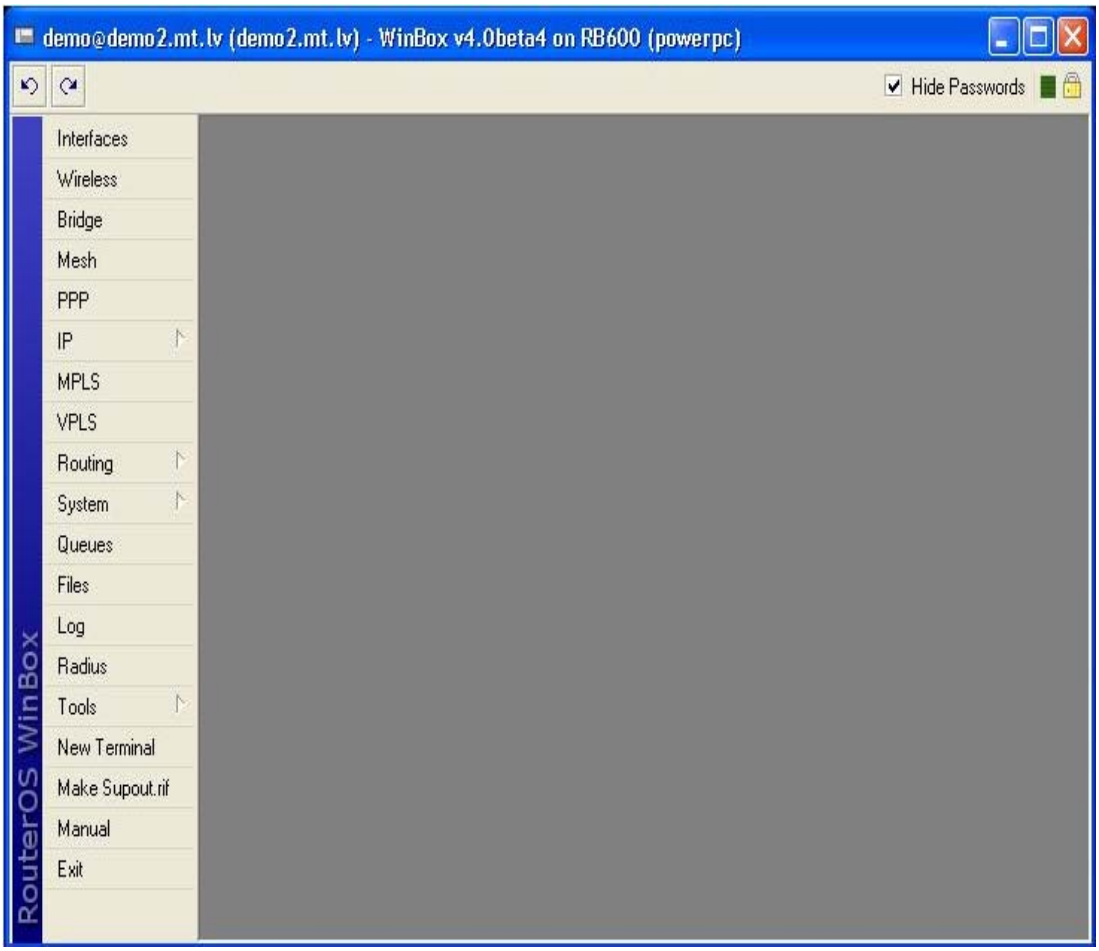


Figura 6.7 Ventana de inicio de winbox

Una vez que se abra la terminal solicitada escribimos el siguiente comando:

interfa print oid

El resultado de esta operación se muestra en la siguiente figura 6.8:

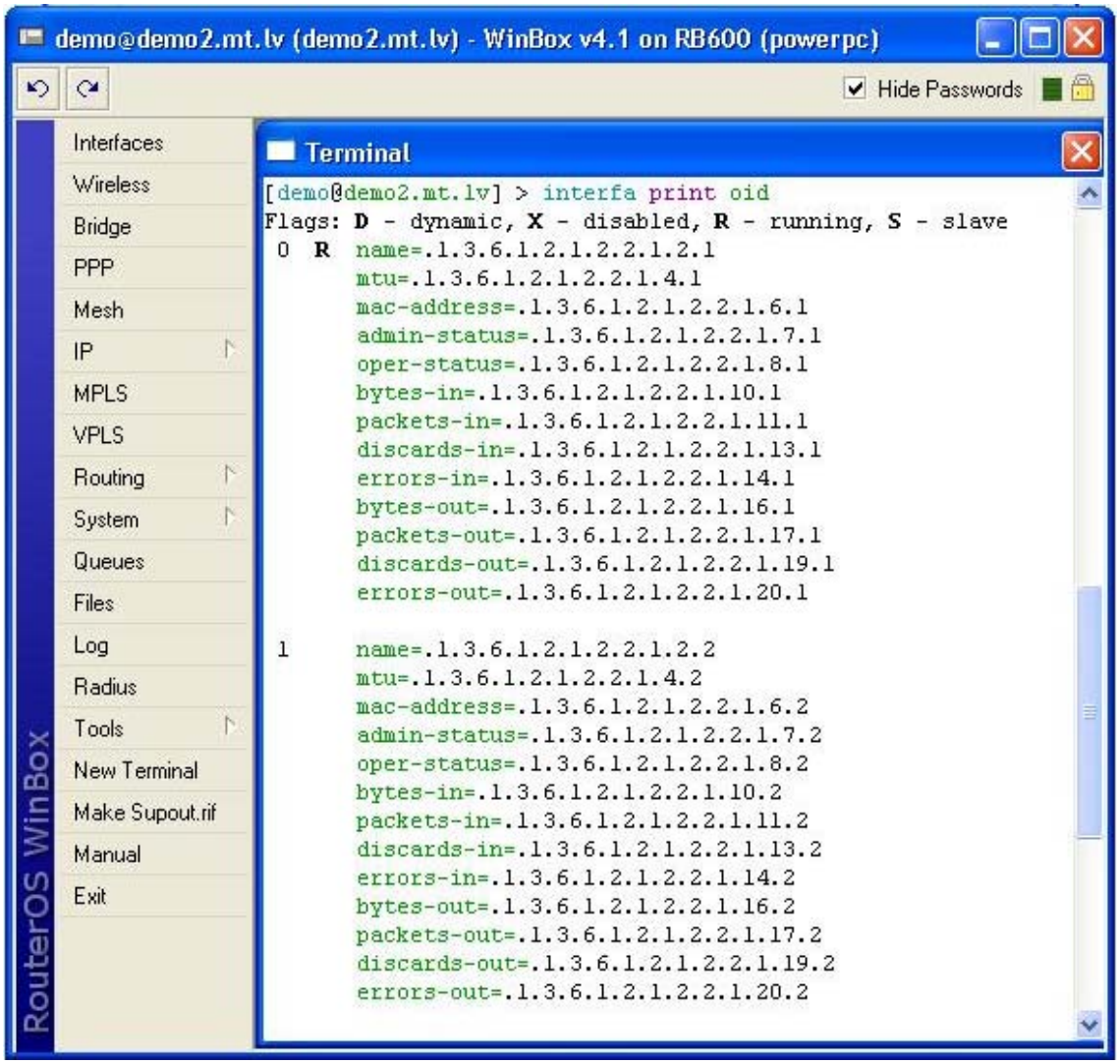


Figura 6.8 OID's de las interfaces Mikrotik

La configuración del servidor SNMP en Mikrotik es muy sencilla. Hay que ir a la opción IP y en el submenú escoger SNMP. En la pantalla que se abre hay que hacer click en la casilla "SNMP Settings" y llenar los datos que se piden con lo cual se habilita el servidor. Tal como se muestra en la figura 6.9.

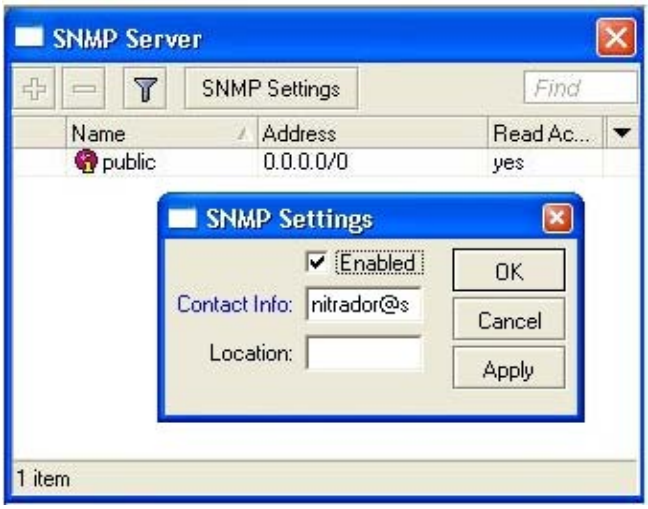


Figura 6.9 Ventana de configuración del servidor SNMP de Mikrotik

Location se refiere al mikrotik instalado, por ejemplo, si se trata de una empresa u organización distribuida, tal vez esta configuración sea la de la matriz, o alguna sucursal.

Después hacemos click en el icono con signo más “+” que está en la parte superior y configuramos los parámetros que se observa en la figura 6.10.

Figura 6.10 Habilitación del servidor SNMP de Mikrotik

La casilla de la figura anterior tiene dos valores: Name (nombre) y Address (dirección), los cuales tendrán que ser elegidos. El nombre puede ser cualquiera y la dirección, es la dirección IP de la subred desde la cual se desea administrar (generalmente es el área de cómputo o administración). Una vez hecho esto, el servidor SNMP (agente SMNP), quedará habilitado en dicha red.

Para acceder al servidor SNMP se utiliza alguna aplicación de administración como MRTG (Multi Router Traffic Grapher – Gráficador de Tráfico Multi Router), que acompaña a Linux. Esta herramienta permite monitorear el tráfico de red a través de las interfaces, las gráficas mostradas son generadas como páginas web (html), que pueden verse desde un servidor de aplicación externo donde se instale MRTG.

Del mismo modo una tabla de direcciones IP, llamada IPAdTable puede ser construida de forma unidimensional, en la que cada registro consta de cinco elementos que se mencionan a continuación:

1 Dirección IP (IP)
2 Identificador para Interfaz de Red (Entrada de Datos - IPAdEntry).
3 Máscara de Red (IPAdNetMask)
4 Dirección de difusión
5 Identificador para tamaño máximo de datagramas.

Bajo esta perspectiva es posible asignar un espacio (nodo) en el árbol jerárquico y un valor a cada elemento, para que de esta forma puedan ser referenciados en el espacio de nombres. Obviamente los nuevos nodos serían sub-árboles del nodo ip.

De este modo asignando valores a la tabla IPAdTable, y a los elementos de ésta, por ejemplo: IPAdTable = 20, IPAdEntry = 1, IPAdNetMask = 3, podemos hacer referencia a la máscara de red correspondiente con cierta dirección IP en la tabla

de ruteo. Para seleccionar un elemento específico de una tabla, (como la máscara de red solicitada) se utilizan sufijos en el estándar ASN.1 (dirección IP asociada a la máscara de red) y no subíndices como en la mayoría de los arreglos para formar referencias con los objetos. Para referirnos a la máscara de red de la dirección 192.168.1.64 se utiliza el siguiente nombre y referencia numérica:

iso.org.dod.internet.mgmt.mib.ip.IPAdTable.IPAdEntry.IPAdNetMask.192.168.1.64

1 . 3 . 6 . 1 . 2 . 1 . 4 . 20 . 1 . 3 . 192.168.1.64

Esta secuencia de números tienen un significado particular que sirven para identificar objetos en la red. En este caso particular mostrado anteriormente, se hace referencia al objeto “máscara de red” a través de la dirección IP asociada. A esta referencia se le conoce como OID (Objet Identifier – Identificador de Objetos), que técnicamente es el nombre del nodo, compuesto por la secuencia de números enteros que acompañan a cada una de las etiquetas en cada nodo, desde la raíz hasta el nodo en cuestión, los cuales son almacenados en la MIB.

6.4 E-MAIL

El correo electrónico es la aplicación más difundida ya que antecede a Internet mismo, siendo éste un paso crucial en el surgimiento de ésta gran red. Su origen se encuentra en el Instituto Tecnológico de Massachussets (MIT), en una demostración hecha en 1961, que permitió a varios usuarios acceder a una máquina remota para guardar y compartir información, suceso que cambio la forma de intercambiar y almacenar información. Ya para 1965 el correo electrónico se utilizó en una súper computadora dedicada de uso compartido, y para el año siguiente se difundió rápidamente.

La utilización del signo “@” se introdujo años después en 1971 por Ray Tomlinson, cuando ingresó a la empresa BBN, y que a su vez fue contratada para trabajar en la red ARPANET por parte del Departamento de Defensa de USA (DARPA). Con

la utilización del @ se dio la posibilidad de unir el nombre de usuario con el servidor (dominio) al que pertenece.

El correo electrónico es una de las aplicaciones TCP/IP más utilizadas, que permite, en su concepción más sencilla, enviar mensajes (cartas electrónicas) entre distintos equipos a través de un servidor.

El correo electrónico en Internet surgió de la investigación realizada en 1980 por Suzanne Sluizer y Jon Postel en la que desarrollaron un protocolo: MTP (Mail Transfer Protocolo – Protocolo de Transferencia de Correo) especificado en el RFC 780, que posteriormente se llamaría SMTP (Simple MTP – Protocolo Simple de Transferencia de Correo) bajo el RFC 821, y que hoy en día se utiliza con las respectivas actualizaciones.

El protocolo SMTP es el estándar en Internet, está a nivel de aplicación dentro del modelo TCP/IP y utiliza el puerto 25, pero sólo sirve para el envío de mensajes, es decir, para que el cliente pueda recibir sus mensajes es necesario otro protocolo: POP (Post Office Protocol – Protocolo de Oficina de Correo) a través del puerto 110, o IMAP (Internet Message Access Protocol – Protocolo de Acceso a Mensajes en Internet) puerto 143, que son los más utilizados, aunque prevalece aún más la utilización de POP, ya sea que se utilice uno u otro protocolo para recibir mensajes, ambos utilizan SMTP para el envío de correo.

6.4.1 AGENTES DE CORREO

De tal modo que podemos identificar dos tipos de “agentes” en la transferencia de correo: MUA (Mail User Agent – Agente de Usuario de Correo), y MTA (Mail Transfer Agent – Agente de Transferencia de Correo).

Un agente MUA se le denomina “cliente de correo”, éste tipo de programas ofrecen las funciones necesarias para recuperar mensajes de correo a través de

los protocolos POP o IMAP, administrar el buzón, y preparar los mensajes para ser enviados por uno o varios agentes MTA a su destino final utilizando el protocolo SMTP. La siguiente figura 6.11 muestra la estructura general que utiliza el correo electrónico.

Figura 6.11 Agentes de correo y protocolos

6.4.2 PROTOCOLO SMTP

La comunicación entre servidores MTA de SMTP es unidireccional, de modo que, en todo momento siempre existe un emisor y un receptor, y para que el receptor pueda volverse emisor tiene que esperar a que termine la conexión establecida antes, y posteriormente iniciar una nueva.

La comunicación entre el receptor y el emisor SMTP, consta de un código numérico de tres dígitos que son interpretados por el emisor, para indicarle cuál es el estado actual del receptor para cada solicitud echa por el emisor. El código es acompañado con texto descriptivo de cada estado. El mensaje es transferido como caracteres ASCII de siete bits.

De este modo cuando un cliente SMTP desea enviar un mensaje a un servidor SMTP, primero establece la comunicación por el puerto 25 del servidor, y posteriormente espera la respuesta de éste, ya sea que envíe “220 Service Ready” figura 6.12, o 421 “Service non available”.

CLIENTE	SERVIDOR
telnet servidor.smtp.xx 25	
	220 servidor.smtp.xx (versión y fecha)

Figura 6.12 Conexión cliente - servidor SMTP

Si el servidor responde aceptando la conexión, el cliente envía el comando HELO para que el servidor se identifique, figura 6.13.

CLIENTE	SERVIDOR
HELO smtp.xx	
	250 servidor.smtp.xx Hello
	(dirección IP), pleased to meet you

Figura 6.13 Respuesta del servidor al comando HELO

Después el cliente indica cuál es su dirección de correo y la, o las direcciones de los destinatarios, figura 6.14.

CLIENTE	SERVIDOR
MAIL FROM: usuario1@smtp.xx	
	250 usuario1@smtp.xx... Sender ok
RCPT TO: usuario2@dominio.yy	
	250 usuario2@dominio.yy... Sender ok

Figura 6.14 Dirección del remitente y destinatario de correo

Una vez que se conocen las direcciones de correo a las que se enviará el mensaje se procede a redactarlo, figura 6.15.

CLIENTE	SERVIDOR
DATA	
	354 Enter mail, end with "." on a line by itself
Esta es una prueba	
.	

Figura 6.15 Cuerpo del mensaje dentro de la carta

Si todo sale bien, el servidor responderá acertadamente y se podrá cerrar la conexión, figura 6.16

CLIENTE	SERVIDOR
	250 Message accepted for delivery
QUIT	
	221servidor.smtp.xx closing connection
	Connection closed by foreign host.

Figura 6.16 Fin de la conexión

También se puede utilizar la instrucción “TURN” para invertir los papeles, que el cliente sea el servidor y viceversa.

El dígito más significativo de los tres que se compone cada código descriptivo del protocolo SMTP, indica la categoría de la respuesta dentro un grupo de cuatro:

1 **2XX**. Operación concluida con éxito.
2 **3XX**. Orden aceptada y en espera de datos.
3 **4XX**. Respuesta de error, pero en espera de repetir la operación.
4 **5XX**. Respuesta de error, sin posibilidad de repetir la operación.

De esta forma se consigue la transferencia de correo entre servidores SMTP (buzones). Cuando el mensaje se envía es colocado en una cola de espera (en caso de que haya más solicitudes de envío esperando), y SMTP enviará el mensaje siempre y cuando se conecte con el siguiente servidor SMTP destinatario o intermediario, de lo contrario después de un tiempo límite el mensaje es regresado o se avisa al cliente que lo envió.

6.4.3 PROTOCOLO POP

Ahora para descargar los mensajes que se encuentran en el buzón, es necesario la utilización de protocolos como POP descrito en el RFC 1725, ya que en los inicios del correo electrónico no existían computadoras personales, sino grandes equipos de tiempo compartido multiusuario conectados permanentemente a la red, y no una conexión eventual como la que se da en la actualidad con los equipos de escritorio y portátiles. De modo que en 1984 surge el protocolo POP para resolver estas necesidades, ya que fue diseñado para trabajar aunque no exista una comunicación constante entre el cliente y el servidor de correo POP.

La comunicación entre el cliente y el servidor de correo POP es similar al usado por el protocolo SMTP. Primero hay que establecer la conexión a través del puerto 110, posteriormente se le pide al cliente que se identifique mediante su nombre de usuario y contraseña, si éstas son válidas el servidor permite entrar al buzón del usuario. La siguiente figura 6.17 muestra esta comunicación.

CLIENTE	SERVIDOR
telnet servidor.smtp.xx 110	
	OK POP3 servidor (versión) server ready
USER usuario1	
	OK User name accepted, password please
PASSWORD ******	
	OK Mailbox open, (No. de mensajes)
LIST	// lista los mensajes y el tamaño
mensaje1 1163	
mensaje2 2025	
mensaje3 1750	
RETR mensaje3	// recupera el mensaje 3
	E imprime en pantalla su contenido
DELE mensaje3	// borra el mensaje 3
QUIT	/ termina la sesión
	OK usuario1

Figura 6.17 Comunicación cliente – servidor POP

Los pasos a seguir en las comunicaciones mostradas (SMTP y POP), están basadas en el servicio “sendmail” de linux.

En la actualidad acceder a un servidor de correo en Internet es mucho más sencillo de lo que se muestra en el ejemplo anterior, ya que se accede a través de

la página web (dirección ip donde se aloja el servidor) de manera gráfica, y a través de ésta sólo hay que hacer click en los iconos respectivos para leer, escribir, enviar, borrar, etc. mensajes alojados en el buzón. A este tipo de servicio de correo se le denomina comúnmente correo web.

Al igual que otros protocolos SMTP y POP utilizan formatos para la transmisión de datos: cabecera y cuerpo del mensaje. Las cabeceras contienen los datos necesarios para la interpretación de órdenes por otros protocolos o el mismo, y el cuerpo del mensaje los datos propios del usuario.

6.4.4 SISTEMAS DE SEGURIDAD PARA e_mail

Los sistemas de seguridad para correo electrónico se basan generalmente en modelos híbridos, combinando algoritmos de clave simétrica y asimétrica. De modo que para que un mensaje sea confidencial ha de cifrarse; para el texto del mensaje se utiliza un algoritmo simétrico (clave de sesión), donde la clave de sesión utilizada se cifra mediante algoritmo asimétrico con la clave pública del receptor para que sólo éste pueda leer el mensaje creando un sobre digital.
El uso de sobres digitales brinda confidencialidad pero no autenticidad, es decir, el texto del mensaje queda oculto ya que está cifrado pero no puede asegurar que el remitente sea quién dice ser. Para resolver este problema ha de ser necesario que el sobre además contenga una firma digital utilizando claves asimétricas.

De este modo un mensaje de correo puede estar cifrado, firmado, o ambas cosas a la vez, los pasos a seguir en el último de los casos se muestran en la siguiente figura 6.18:

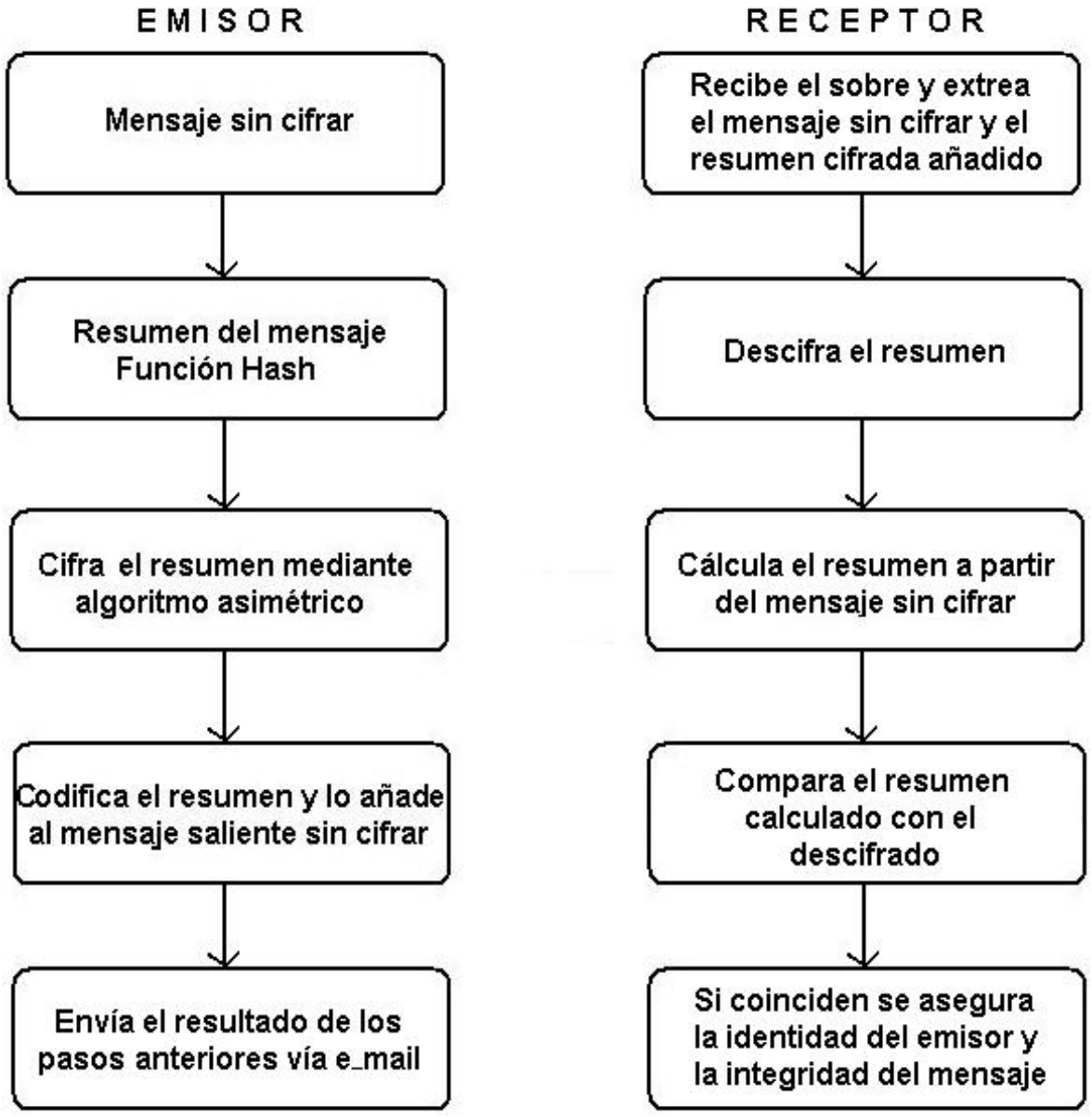


Figura 6.18 Diagrama de mensaje de correo cifrado y firmado.

Las técnicas y pasos mostrados en la figura anterior, son utilizados por protocolos y aplicaciones como PEM (Privacy Enhanced Mail – Correo de Completa Privacidad), PGP (Pretty Good Privacy – Muy Buena Privacidad) y S/MIME (Secure Multipurpose Internet Mail Extensions – Extensiones de Correo de Internet Multipropósito). Los algoritmos criptográficos utilizados por estos sistemas se muestran en la siguiente figura 6.19.

PROTOCOLO DE SEGURIDAD	INTEGRIDAD		IDENTIDAD
	Algoritmo Simétrico	Algoritmo Asimétrico	Función Hash
PEM	DES-EBC con MD2 o MD5	RSA con MD2 o MD5	DES-CBC
PGP	IDEA, CAST o 3DES	RSA con MD5, o SHA-1	MD5
S/MIME	RC2,RC5, DES-CBC o 3DES	RSA	SHA1 o MD5

Figura 6.19 Algoritmos de cifrado para correo seguro

Algunos de estos algoritmos ya fueron explicados en los capítulos tres y cuatro, y el resto se basan en el mismo concepto (simétricos – asimétricos), por eso sólo hago mención de ellos.

6.5 FTP

El servicio FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos), como su nombre lo indica, es un protocolo utilizado para la transferencia de archivos en red utilizando la capa de transporte TCP a través de los puertos: 20 para datos y 21 para comandos, de modo que la confianza y administración de la conexión queda a cargo de esta capa de red.

En 1969 en el MIT fue presentada la primera propuesta para este protocolo definido en el RFC 114. Del mismo modo que con el correo electrónico, el surgimiento de Internet hizo que éste protocolo fuera actualizado y difundido sobre esta gran red.

FTP se ejecuta desde un servidor, el cual almacena los archivos que están disponibles para los equipos remotos (clientes) con derecho a este servicio, siendo ésta la mejor aplicación para transferencia de archivos.

Este protocolo está orientado a efectuar distintos tipos de transacciones (operaciones), las cuales están representadas como entidades de información que sirven para comunicarse y ser interpretadas por los procesos correspondientes a este servicio. Los formatos de los paquetes que representan cada una de las transacciones son de 72 bits (no incluyen datos ni campos de relleno), tal como se muestra en la siguiente figura 6.20.

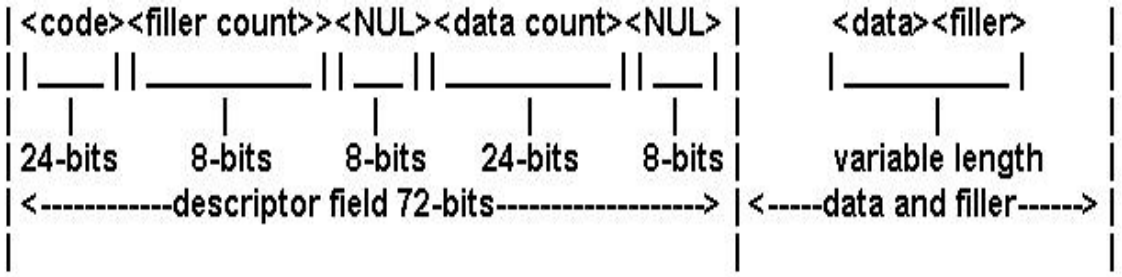


Figura 6.20 Campos de datos en FTP

El campo code (código) de 24 bits está separado en tres bytes e indica el tipo de transacción y tipo de datos, “filler count” (contador de relleno) es un contador de 8 bits que indica el número de bits de relleno utilizados; los cuales no exceden los 255 bits dado el tamaño del contador, “data count” (contador de datos) es un contador de 24 bits que sirve para saber la cantidad de datos en bits que contiene el paquete la cual no excede los 2^24-1 bits.

Los códigos de transacción se clasifican en cuatro categorías:

1 **REQUEST.** Son las peticiones solicitadas por el cliente a efectuarse sobre algún archivo, por ejemplo: store (almacenar), append (añair), open (abrir), close(cerrar), etc.

2 **RESPONSE.** Indican el estado en que se encuentra la comunicación, sólo hay dos posibilidades: ready to receive (listo para recibir), y ready to send (listo para enviar).

3 **TRANSFER.** Cuando se envía un archivo por partes este modo indica el avance de la transferencia mediante cuatro estados: complete_file indica que se ha completado la transferencia, heading para la cabecera, part_of_file sólo una parte del archivo, y last_part cuando se envía la última parte de éste.

4 **TERMINATE.** Sirve para terminar la conexión, la cual puede lograrse con éxito “successful”, o de lo contrario sería “unsuccessful”.

Este servicio difiere de la mayoría de las aplicaciones TCP/IP por dos razones fundamentales:

1 La transmisión se hace a través de dos canales distintos; el puerto 20 TCP para enviar datos y el puerto 21 TCP para comandos, ambos de forma simultánea. Estos canales se llaman DTP (Data Transfer Process – Proceso de Transferencia de Datos) y PI (Protocol Interpreter - Intérprete del Protocolo) respectivamente, tal como se muestra en la siguiente figura 6.21.

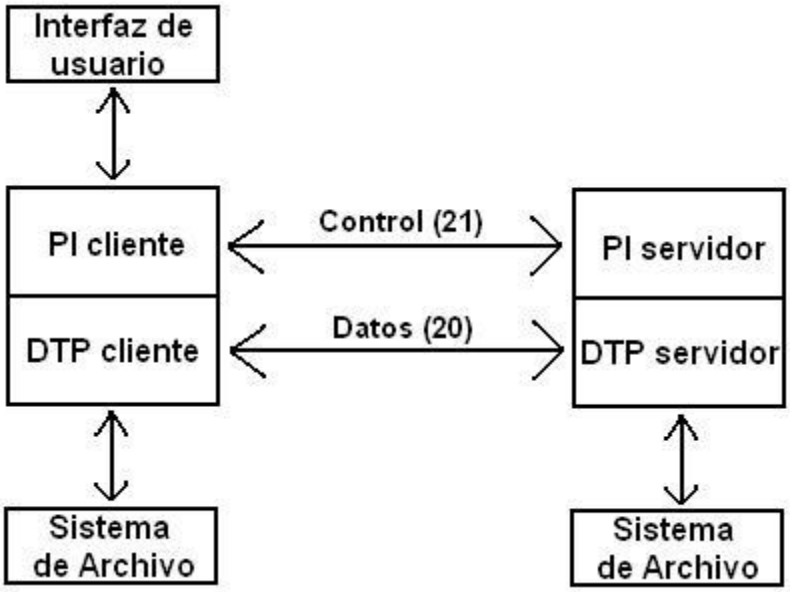


Figura 6.21 Canales DTP y PI de FTP

2 La transferencia de archivos se hace en primer plano, de modo que la ejecución es en tiempo real.

6.6 TELNET

TELNET (Telecommunication Network – Red de Telecomunicación) es un servicio para comunicar equipos en red con arquitectura cliente - servidor, de modo que el cliente puede acceder a los recursos y ejecutar programas de forma remota en el servidor, como si estuviera físicamente frente a él, ya que implementa una terminal virtual entre el cliente y el servidor a través del puerto 23 TCP.

Este programa surgió a finales de los años 60 (RFC 854), por la necesidad de conectar equipos con distintas características técnicas, que generaban incompatibilidad en los modos de operación e interpretación de órdenes, en los tiempos que sólo se utilizaban puertos serie para enlazar máquinas, y así compartir recursos. Además las computadoras personales no existían, y los

“servidores” de aquellas épocas eran grandes máquinas de tiempo compartido, que podían accederse desde una terminal.

El protocolo TELNET se basa en el concepto NTV (Network Virtual Terminal – Terminal Virtual de Red), que se aplica en ambos extremos de una conexón, donde cada equipo conectado se convierte en una NTV con terminales virtuales (teclado y monitor), llevados hacia los dispositivos físicos reales mediante un mapa de códigos que traduce las instrucciones. La siguiente figura 6.22 muestra una conexión TELNET.

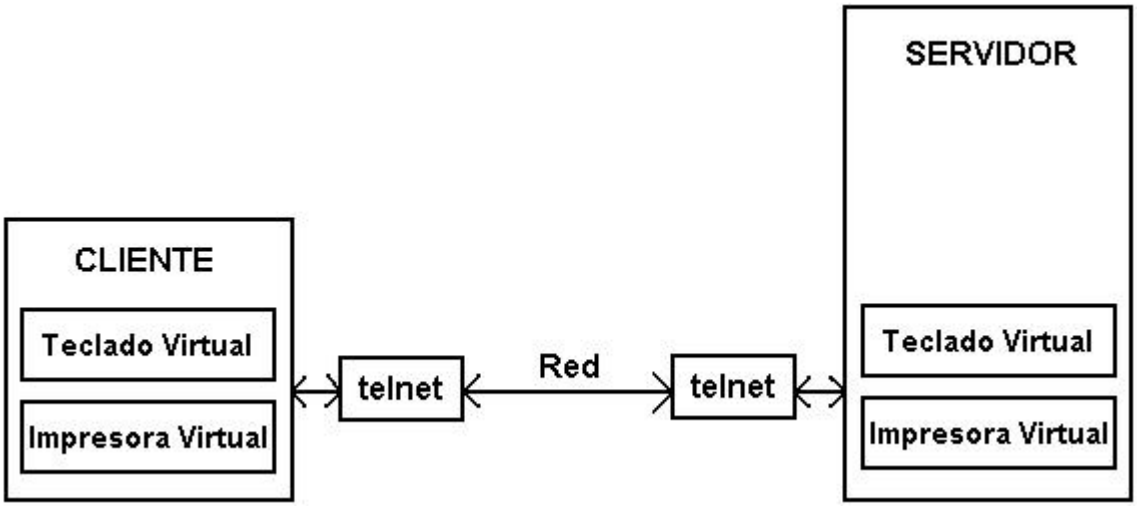


Figura 6.22 Terminales virutales NTV en Telenet

Los comandos TELNET son enviados en paquetes llamados “command”, que generalmente constan de dos o tres bytes. Un byte para la instrucción “IAC” (Interpret as Command – Interpretación de Comando), otro byte para el código asociado del comando, y el tercer byte de forma opcional, para algún parámetro asociado que necesite el comando. La figura 6.23 muestra el formato.

Figura 6.23 Formato de comandos en TELNET

Los aspectos de seguridad para ftp encajan con la descripción echa en el capítulo tres, en el que se propone la utilización de SSH, para la encriptación en los canales de comunicación. Lo que hay que tener en cuenta es que la versión SSH a utilizar ha de permitir asegurar los dos canales utilizados (datos y control), para de esta forma reforzar la comunicación.

Utilizar SSH en TELNET o FTP, permite un canal de comunicación seguro ya que hay que recordar que los datos van encriptados, evitando ataques del tipo ***"eavesdropping"*** y **"*session hijaking"***

El eavesdropping es una variante del *"sniffing",* caracterizada por interceptar el tráfico en la red de forma pasiva y, session hijaking, este tipo de ataque consiste en apoderarse de una sesión ya establecida, de modo que, el atacante se sitúa entre ambos equipos. Para poder tomar el control es necesario conocer información asociada al protocolo TCP a lo largo de la comunicación (número de secuencia en curso, número de bytes transmitidos, etc.), una vez tomado el control se utiliza la técnica "source-routing" para que los paquetes en vez de llegar a su destino real lleguen al atacante.

La seguridad de este tipo de aplicaciones esta ligada, como en muchos casos, a la configuración y administración correcta de los servidores, hay que tener especial cuidado con los permisos, archivos y aplicaciones que serán expuestos en la red.

Conclusiones

CONCLUSIONES

En este trabajo se han cubierto los puntos más importantes en cuanto a seguridad desde una perspectiva general, ya que la extensión y complejidad de algunos de estos temas necesitarían de una investigación completa, pero se han sentado las bases para que cualquier persona interesada en el ámbito de la seguridad en redes, como las que aquí se presentan basadas en tecnología ethernet, puedan contar con este material de apoyo y les permita empezar a explorar, y poco a poco adentrarse en este campo de la seguridad informática.

Para la implementación de los sistemas de seguridad se han tomado las herramientas de software y hardware más difundidas actualmente, pero que al mismo tiempo han demostrado ser las más efectivas dentro de su género, con las implicaciones y limitantes que cada una pueda presentar, y que en conjunto forman un sistema global de protección acorde con las necesidades más comunes de defensa para una Intranet.

También se analiza y explica el estrato de protocolos TCP/IP desde un enfoque práctico, con el cual se trata de entender el funcionamiento e interacción de éstos en el campo de las comunicaciones, y que a su vez sirven de soporte a las aplicaciones y sistemas de seguridad basados en estos protocolos, dejando en claro que el uso de protocolos es un estándar que permite regular la utilización de estos y otros protocolos, sin necesidad de replantear nuevamente su diseño cada vez que surge una nueva tecnología o aplicación, facilitando la creación de nuevas herramientas.

Aún así, los sistemas (aplicación de software, protocolo, o tecnología), mantienen inherente a su diseño, fallas o errores que los hacen vulnerables, las cuales se van descubriendo conforme se usan, y otras probablemente existan pero aún no se han descubierto. Es aquí donde tenemos que preocuparnos y tratar de

entender la necesidad de cubrir estos agujeros de seguridad, con modelos que permitan reforzar dichas vulnerabilidades.

Los motivos y ataques obedecen a distintas causas, pero existe una razón común desde el punto de vista táctico, ya que desde que la ciencia y la tecnología han evolucionado y avanzado a pasos agigantados, estas nuevas aportaciones o descubrimientos son usados de forma ambigua. Es decir, generalmente los mismos conocimientos aplicados a un nuevo proyecto o producto tecnológico con el fin de mejorar alguna situación, pueden ser utilizados para circunstancias totalmente opuestas. Y desde el punto de vista computacional, existen programas de aplicaciones específicas que se utilizan para mejorar procesos o situaciones laborales particulares, así como también existen programas dañinos (malware), cuya labor es opuesta y con resultados negativos.

En la cuestión de las redes de computadores, a cuatro décadas ya, de que un proyecto llamado Internet surgiera en los Estados Unidos, no se tenía contemplada ni la magnitud ni trascendencia que alcanzaría en el futuro. La idea no era crear un sistema de comunicación global, sino una aplicación que ayudará a los investigadores e instituciones gubernamentales, a enlazar sus equipos a través de una red, y pudieran de esta forma intercambiar información.

Con el paso de los años fue imposible detener su crecimiento y expansión, pero con esta situación pronto se dieron cuenta, que en su diseño no se habían contemplado varios factores, entre uno de ellos y de manera muy particular: “la seguridad”. En ese entonces se pensó que Internet estaría formado por redes particulares, fuera del alcance del público en general, los protocolos diseñados para soportar esta nueva tecnología no contemplaron varios aspectos técnicos, que hoy nos damos cuenta; dada la expansión que ha alcanzado Internet, hicieron falta desde un principio en su diseño.

Por eso es que han surgido, cada que se han descubierto fallas o vulnerabilidades en este aspecto, las herramientas necesarias para ir cubriendo o reforzando este sistema de comunicaciones. Como hemos visto existen aplicaciones de software y hardware que se utilizan para subsanar las carencias que pueda haber, dichas herramientas van desde criptografía aplicada hasta dispositivos de filtrado de paquetes.

Pero no sólo los protocolos de red han pasado por esta prueba a través del tiempo, también los sistemas operativos creados para ambientes de red, han tenido que mejorar los aspectos de seguridad, ya que no han quedado exentos de estas fallas, y en general con ellos las aplicaciones que van surgiendo y se van desarrollando día con día.

Pero todas estas experiencias no han sido en vano, la evolución y tendencias tecnológicas actuales contemplan este tipo de aspectos con mayor conciencia, tratando de respaldar lo más posible los servicios y aplicaciones ofrecidas. Tal es el caso de la segunda versión de Internet en fase experimental, donde los protocolos utilizados han sido reforzados y se han cubierto varios aspectos, entre otros, asegurar la disponibilidad de direcciones IP en el futuro. Estas nuevas tecnologías incluyen ya, algunos mecanismos de defensa utilizados en Internet de manera opcional, lo que permite deslindar al administrador de ciertas ocupaciones proporcionadas ahora por el protocolo. Por ejemplo, la versión IP (IPv6) de Internet 2, cuenta con encapsulación de datos de forma general, y no es opcional como en el caso de Internet si se desea mejorar la seguridad.

Pero aún la moneda está en el aire y falta mucho por decir, las comunicaciones inalámbricas son otro aspecto que hay que tener en cuenta, y que en la última década han cobrado suma importancia, ya que ofrecen portabilidad y acceso desde cualquier parte, asegurando de esta forma valor agregado a los servicios que se prestan en Internet.

Hay que recordar que Internet sólo ha sido la pauta y el comienzo hacia una nueva era en las comunicaciones, comprender y entender las tecnologías actuales, nos ayuda a adoptar las nuevas tecnologías, haciendo que la transición entre una y otra, sea mucho más sencillo, pudiendo vislumbrar con mayor claridad los retos y oportunidades que éstas presenten en la camino de la evolución informática y las comunicaciones.

Glosario

ACK (acknowledge), señal de control para todas las secuencias de entrada de comunicación que significa que la información recibida ha sido aceptada con éxito.

AH (Autentication Header – Autenticación de Encabezado), protocolo utilizado en IPsec.

Amenaza. Es una condición del entorno donde se encuentran los sistemas de información, que dada una condición especial u oportunidad puede producir alguna violación a la seguridad; estas pueden provenir de algún usuario, software o equipo, etc.

ARPANET (Advanced Research Projects Agency Network - Agencia de Investigación Avanzada en Redes), creada por el Departamento de Defensa de los Estados Unidos.

ASN.1 (Abstract Syntax Notation 1 – Notación de Sintaxis Abstracta), se trata de un estándar utilizado en protocolos de administración de red para representar entidades evitando posibles ambigüedades.

Ataque. Es la acción misma que produce una amenaza realizada.

Autenticación. Es el proceso a través del cual se verifica la identidad proporcionada por algún usuario, equipo o alguna otra entidad con el fin de asegurar que dicha identidad es verdadera.

Back Up. Copia de seguridad de una memoria auxiliar (disco, casete u otro), a fin de evitar la pérdida o destrucción de información que puede ser importante.

BDC (Backup Domain Controller - Respaldo del Controlador de Dominio).

Broadcast. Es un modo de trasmitir información en red, de modo que el emisor envía la información a todos los equipos o nodos receptores de manera simultánea.

Bug. Error de software como resultado del proceso de desarrollo que puede presentarse en n cualquiera de las etapas del ciclo de vida del programa.

CD-RW (Compact Disc-Read & Writte - Disco Compacto Regrabable).

CERT (Computer Emergency Response Team), organización sin fines de lucro involucrada en dar a conocer información relevante relacionada con aspectos de seguridad, sobre todo en materia de software.

CIFS (Common Internet File System – Sistema de Archivos Comunes para Internet). Protocolo de red que pertenece a la capa de aplicación del modelo OSI.

Métodos de Control de Acceso. Conjuntos de reglas que garantizan que todo acceso a los recursos de una red se haga de forma autorizada como parte de las medidas de seguridad implantadas.

Crackeo. Actividad ilícita para desbloquear programas ("candados de seguridad"), o hacer daño en algún sistema informático.

Criptografía. Es la ciencia de cifrar y descifrar información mediante técnicas sofisticadas que utilizan algoritmos matemáticos para proteger el contenido de la información.

Criptoanálisis. Es la utilización de técnicas para descifrar información para obtener el mensaje original sin conocimiento de las claves para hacerlo.

DAS (Direct Attached Storage – Conexión de Almacenamiento Directo). Arquitectura para almacenamiento de información, con conexión directa entre el servidor y el sistema de almacenamiento.

DMZ (Demilitarized Zone - Zona Desmilitarizada), es una zona de seguridad para una red donde se impide el tráfico desde el exterior al interior de la misma, y sólo es posible acceder a los servicios que se encuentran disponibles en ésta zona.

DOI (Domain Of Interpretation – Dominio de Interpretación), parámetros para establecer comunicaciones seguras con IPsec mediante Asociaciones de Seguridad.

Eavesdropping, es una variante del *"sniffing",* caracterizada por interceptar el tráfico en la red de forma pasiva.

Encriptación. La encriptación o cifrado, forma parte de la criptografía y permite el intercambio de información de forma segura ya que el contenido se vuelve ilegible una vez que es procesado por las técnicas propiamente utilizadas.

ESP (Encapsulating Security Payload – Seguridad de Encapsulado de Carga Útil), protocolo de encriptación y autenticación en IPsec.

Explit. Es un programa que permite de manera automatizada aprovechar algún error, falla o vulnerabilidad dentro de un sistema una vez que inicia su ejecución.

FDD Floppy Disc Device - Dispositivo de Disco de 3½).

Firewall. Dispositivo de seguridad para redes encargado de filtrar paquetes de datos en base a un conjunto de reglas y criterios previamente definidos por el administrador.

Firma Digital. Utilización de técnicas criptográficas para asegurar y garantizar la identidad del remitente en mensajes y documentos a través de un “sello digital” originado por el emisor o por alguna otra entidad confiable y autorizada para hacerlo.

Gateway. (Puerta de Acceso), es un equipo que permite la conexión entre distintos tipos de redes o aplicaciones.

IAC (Interpret as Command – Interpretación de Comando), es una instrucción de 1 byte utilizada en TELNET.

IDS (Intrusion Detection System - Sistema de Detección de Intrusos), es un dispositivo de seguridad para red que se encarga de detectar patrones comunes que indiquen una posible intrusión a los sistemas, en base al monitoreo constante de paquetes y cargas de trabajo.

IETF (Internet Engeenering Task Force – Grupo de Trabajo de Ingeniería en Internet); cuya labor es la revisión y normalización de protocolos en Internet.

IMAP (Internet Message Access Protocol – Protocolo de Acceso a Mensajes en Internet), es un programa "cliente de correo" que permite al usuario recibir y administrar sus correos.

ICANN (Internet Corporation for Asiggned Names and Numbers), organismo sin fines de lucro que a nivel internacional regula los nombres de dominios en Internet y las direcciones numéricas IP.

IPS (Intrusion Prevention System - Sistema de Prevención de Intrusos), al igual que un IDS, se trata de un dispositivo de seguridad para red cuya mayor virtud radica en que pude actuar e impedir los ataques detectados en tiempo real.

ISP (Internet Service Provider - Proveedor de Servicios de Internet), nombre con que se catalogan las empresas dedicadas a ofrecer servicios de conexión a redes para Internet.

Keylogger. Software que sirve para registrar de forma remota las actividades de unusuario através de su teclado, generalmente con el fin de obtener información confidencial.

Loopback. Se trata de una dirección IP "virtual" reservada, que indica al propio equipo o dispositivo utilizada para diagnósticos de conexión (en IPv4 es 127.0.0.1).

Malware. Término que engloba todo tipo de software malicioso (virus, troyanos, spyware,etc.) que se infiltra en un sistema con fines dañinos.

MTA (Mail Transfer Agent – Agente de Transferencia de Correo), como su nombre lo indica, se trata de un protocolo de aplicación para la transferencia de correo entre servidores.

NAS (Network Attached Storage - Conexión de Almacenamiento en Red), es un modelo de almacenamiento para grandes volúmenes de información de manera remota, es decir, los dispositivos de almacenamiento no están físicamente en el mismo lugar que las aplicaciones o usuarios que desean hacer uso de éstos dispositivos de resguardo de datos.

NIFS (Network File System – Sistema de Archivos en Red), es un protocolo a nivel de aplicación que permite compartir archivos en sistemas en red.

OSI (Open System Interconnection - Sistema de Interconexión Abierto), es un mód0elo de red desarrollado por la Organización Internacional de Estandarización (ISO), que sirve como referencia para la interconexión de redes que define siete

capas, permitiendo a los fabricantes, desarrolladores y demás, la compatibilidad de sus productos.

Payload. Se trata de la carga dañina que lleva consigo un virus informático, y que genera los efectos dañinos y muchas veces irreparables en el sistema infectado.

PDC (Primary Domain Controller - Controlador Primario de Dominio), es un servidor dedicado a las tareas de administración y autenticación de las cuentas de usuario principalmente, gracias la base de datos que guarda llamada directorio maestro.

POP (Post Office Protocol – Protocolo de Oficina de Correo), es un programa "cliente de correo" con mayor difusión que IMAP.

RAID (Redundant Arrays of Inexpensive Disk – Arreglo Redundante de Discos Económicos), es un arreglo de discos duros de almacenamiento pero que funcionan y son vistos como si se tratase de uno solo.

RFC (Request For Comments – Petición de Comentarios), descripción técnica de protocolos utilizados en Internet y aprobados por el IETF.

Riesgo. Es la proximidad de un daño ocasionado por algún tipo de amenaza.

Rootkit. Especie de troyanos para ocultar puertas traseras que faciliten el acceso y control del sistema infectado con los máximos privilegios de root.

Router. Dispositivo de interconexión de redes a nivel de capa tres (red), encargado del enrutamiento de paquetes a través de los distintos nodos y redes.

RPC (Remote Procedure Call, Llamadas a Procedimientos Remotos), es un mecánismo como parte fundamental de los sitemas distribuidos y utilizado en la arquitectura cliente - servidor para ejecutar procesos y aplicaciones en forma remota.

RST "Reset", se utiliza en comunicaciones para indicar la condición de reinicio.

SA (Security Asociations - Asociaciones de Seguridad), se trata de un esquema de seguridad entre entidades que se comunican utilizando el protocolo IPsec.

SAMBA Es un protocolo para compartir archivos entre sistemas con plataformas diferentes, de tal forma que sistemas Linux, Unix o Mac OS puedan compartir recursos bajo redes Windows.

SAN (Storage Area Network – Red de Área para Almacenamiento), se trata de una infraestructura planeada para la administración de un gran cantidad de unidades de almacenamiento (en el rango de los terabytes), permitiendo que varios servidores accedan a estas unidades de modo compartido. La mayor diferencia entre NAS y SAN radica en que en la arquitectura SAN las aplicaciones que se encuentran dentro de los servidores acceden a los datos de manera directa.

Seguridad (informática). Es el resultado de la utilización de diversas técnicas que tienen como finalidad la autenticación, confidencialidad, disponibilidad e integridad de los servicios que presta algún equipo, sistema o red, para que se utilicen y aprovechen de la mejor manera dentro de los límites establecidos por las políticas de seguridad para mantenerlos fuera de peligro.

SGID (Set Group ID - Indicador de Identificación de Grupo), es un término utilizado en sistemas tipo unix que establece permisos de acceso a archivos y directorios con alto privilegio de forma temporal para que los usuarios con pocos privilegios puedan ejecutarlos.

Shell. Es un programa por el cual se accede a una terminal para que el usuario pueda interactuar y dar órdenes a una computadora bajo ambiente linux, ya que la terminal funciona como un intérprete de comandos. El éxito de TELNET radica precisamente en el acceso remoto a un shell para ejecutar aplicaciones que se encuentren disponibles en el equipo remoto.

SNMP (Simple Network Management Protocol – Protocolo Simple de Administración en Red), es un protocolo que facilita la administración de redes en base a estadísticas de paquetes y revisión de tráfico.

Session hijaking, este tipo de ataque consiste en apoderarse de una sesión ya establecida, de modo que, el atacante se sitúa entre ambos equipos.

Spayware. Es un programa espía de tipo malware que sirve para recopilar información valiosa del equipo donde se encuentra.

SUID (Set User ID - Idicador de Identificación de Usuario), es parecido a SGID, sólo que aplica a nivel de usuario y no de grupo.

Switche. Dispositivo de interconexión de redes a nivel de capa dos (enlace de datos), su función es la de conectar segmentos de red.

SYN Señal de control para la sincronización entre equipos de comunicación.

TCP/IP Conjunto de protocolos de comunicación utilizados en Internet.

URG (Urgent - Urgente), se trata de un tipo de señal utilizada en comunicaciones para indicar un estado de "urgente" y dar mayor prioridad a las señales con éste apelativo.

UTM (Unified Threat Management – Administración Unificada de Amenazas), dispositivo que facilita de forma centralizada la gestión unificada de amenazas.

Vulnerabilidad. Aspectos ya sea de software, hardware o de organización aprovechados por los atacantes con el fin de violar la seguridad de algún sistema.

Bibliografía

* Administración de Red Hat Linux Al descubierto
Thomas Schenk, et al.
Prentice Hall

* Alta Velocidad y Calidad de Servicio en Redes IP
Jesús García Tomás
José Luis Raya Cabrera
Victor Rodrigo Raya
Alfaomega RA-Ma

* Aprendiendo TCP/IP en 14 días
Segunda Edición
Tim Parker
Prentice Hall

* Aprendiendo TCP/IP en 24 horas
Joe Casad
Bob Willsey
Prentice Hall

* Arquitecturas MPLS y VPN
Ivan Pepelnjak
Jim Guichard
Cisco Press

* Firewalls Linux
Robert L. Ziegler
Prentice Hall

* FIREWALLS Manual de Referencia
Keith E. Strassberg
Richard J. Gondek
Garry Rollie
McGraw-Hill

* Intranets paso a paso
Hacia la autopista de la información
Gonzalo Ferreyra C.
Alfaomega Ra-Ma

* LINUX Recursos para el usuario
James Mohr
Prentice Hall

* PC/MS DOS
Referencia Instántanea
Grey Harvey
Kay Yarborough Nelson
Macrobit

* Protocolos de Interntet
Diseño e Implementación en sistemas UNIX
Angel López
Alejandro Novo
Alfaomega Ra-MA

* Redes de Área Local
La Siguiente Generación
Thomas W. Madron
Noriega Editores

* Redes de Computadoras
Protocolos, Normas e Interfaces
Uyless Black
Macrobit

* Seguridad en Microsoft Windows XP y Windows 2000 Running +
Ed Bott
Carl Siechert
McGraw-Hill

* Seguridad Informática
Juan José Nombela
Paraninfo

* Sistemas Distribuidos Conceptos y Diseño
Tercera Edición
George Coulouris
Jean Dollimore
Tim Kindberg
Addison Wesley

* Sistemas Operativos
Cuarta Edición
William Stallings
Prentice Hall

* Sistemas Operativos
Quinta Edición
Abraham Silberschatz
Addison Wesley

* Técnicas Criptográficas de protección de datos
Segunda Edición
Amparo Fúster Sabater
Dolores de la Guia Martínez
Luis Hernández Encinas
Fausto Montoya Vitini
Jaime Muñoz Masqué
Alfaomega Ra-Ma

* Telecomunicaciones Redes de Datos
“GS Comunicaciones”
McGraw-Hill

* Todo Acerca de las Redes de Computadoras
Kevin Stoltz
Prentice Hall

* Elliptic Curve Public Key Cryptosystems
Alfred J. Menezes
Kluwer Academic Publishers Group

* Ethernet The Definitive Guide
Charles E. Spurgeon
O'Reilly

* Microsoft Windows NT Network Administration
Microsoft Press

* Planning for PKI
Best Practices Guide for Deploxing Public Key Infrastructure
Russ Housley
Tim Polk
Wiley Computer Publishing

Referencias de Internet

www.acronis.com
www.cert.org
www.icann.org
www.ietf.org
www.iso.org
www.mikrotik.com
www.vmware.com