6

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"A C A T L A N"

"MECANISMO DE PROTECCION DE UN SITE DE ACCESOS REMOTOS NO AUTORIZADOS".

T E S I N A

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN MATEMATICAS APLICADAS Y COMPUTACION
P R E S E N T A :
JOSE ANTONIO CORIA FERNANDEZ

ASESOR: ING. RUBEN ROMERO RUIZ

SANTA CRUZ ACATLAN, EDO. DE MEX., OCTUBRE DE 2000.

AGRADECIMIENTOS

A DIOS :

Por permitirme estar con vida y tener salud, amor, sueños y esperanza.

A MIS PADRES:

Por brindarme su cariño, paciencia, comprensión y darme siempre aliento para salir adelante de todas las situaciones que se me han presentado.

A MIS HERMANAS:

Agradecerles su apoyo, consejos, confianza y preocupación en mis momentos difíciles.

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO:

Por que gracias a ella tengo el conocimiento , para enfrentarme a los retos de la vida..

A MIS SINODALES:

Ing. Ruben Romero Ruiz
Ing. Silvia Larraza Hernández
Lic. Beatríz Trueba Ríos
Fís. Carlos Pedro Curiel García
Lic. Oscar Gabriel Caballero Martínez

Por su tiempo, disposición y apoyo en la realización de este trabajo.

A MIS AMIGOS:

Martha Arriaga Sánchez
Patricia Chávez González
Claudia Claudio Vázquez
Felisa Córtez Ruiz
Carlota Enriquez Reyes
Fernando García Minquini
Rubén Jiménez Cruz
Nancy Martínez Hernández
Carolina Martínez Rojas
Claudia Morales Ríos
Verónica Ruiz Rosales
Omar Villanueva Villanueva

Por brindarme su amistad, que hace agradable y hermosa la existencia sobre el camino del tiempo.

CONTENIDO

INTRODUCCIÓN

Internet es una amplia colección de redes a escala mundial en constante crecimiento, la cual ha cambiado la manera de comunicarnos y de hacer negocios entre las organizaciones y los individuos, estimulando a que muchas organizaciones busquen el disponer de las ventajas de los servicios y recursos que esta ofrece. Sin embargo, existen riesgos significativos de seguridad asociados a internet, que frecuentemente son ignorados o desconocidos por los usuarios, dando como resultado un enorme riesgo de ser atacado.

Particularmente, la actividad de intrusión es difícil de predecir y en ocasiones de descubrir y corregir, encontrando en ocasiones un camino para curiosear, destruir, cambiar o robar datos y hacer diversos tipos de daños; dependiendo de la vulnerabilidad que tenga un sistema, extendiéndose si el sistema en cuestión es demasiado débil.

En la mayoría de los casos en los que una organización se ha enfrentado a la intrusión, ha tenido que desconectarse temporalmente de internet e invertir una gran cantidad de recursos, tanto productivos como monetarios y poner en juego su reputación, para poder corregir el problema con el sistema.

Quizá el problema fundamental radicaría en que internet no se diseñó para ser seguro, pues desde su creación hasta el momento en que se implementó, el acceso abierto fue una de las propuestas primordiales; combinándose a esto la incorporación

de nuevas clases de usuarios (incluyéndose los usuarios sin ética), quienes agravan las deficiencias de seguridad existentes.

Otros factores que se pueden incluir a lo anterior, son los siguientes:

- La falta de políticas de seguridad en los sitios
- La vulnerabilidad de los servicios de internet
- La facilidad de monitorear el tráfico de internet y de burlar dispositivos de seguridad mediante el uso de direcciones IP falsificadas
- Lo complejo que resulta configurar anfitriones de control de acceso

El problema de la seguridad se incrementa, por el apogeo que se tiene en las organizaciones para conectarse internet, convirtiendo los riesgos en inevitables y catastróficos.

Aunque en la actualidad se cuenta con distintos sistemas de seguridad para mejorar la protección de una organización; su selección dependerá del tipo de acceso que se planee dar.

Al buscar las soluciones a los riesgos, hay que tener presente que es imposible obtener una seguridad absoluta, sin embargo, se pueden crear barreras para hacer más difícil la entrada de "extraños" a las redes corporativas.

Es posible comenzar a fortalecer el acceso a una red poniendo sistemas de protección de perímetro (aclarando que inicialmente se utilizó el término barreras de protección, adoptado en España, para referirnos a estos sistemas. Modificándose este término de acuerdo a nuestro léxico), comúnmente conocidos por su nombre en inglés

como: "firewalls", los cuales permiten limitar los accesos y filtrar las conexiones para salvaguardar la red.

En el presente trabajo se hace mención particularmente a esta clase de sistemas, con el objetivo de explicar de manera breve y sencilla las consideraciones y la manera en que efectúan su tarea, refiriéndonos al tema de la siguiente manera:

En el capítulo uno se definen los conceptos básicos requeridos en la comprensión del tema de seguridad como son: la definición misma de la seguridad de cómputo, las características en las que se basa, los factores implicados, los servicios de internet considerados como básicos y los problemas de seguridad asociados a cada uno de ellos, los riesgos implicados a la conexión con internet, tipos de ataque y atacantes y finalmente se definen varias estrategias de seguridad que permiten hacer un análisis antes de adoptar alguna herramienta.

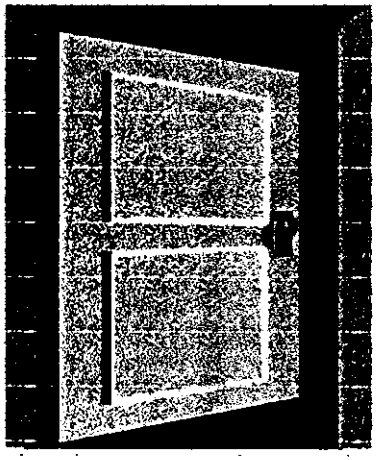
En el capítulo dos inicialmente se especifican los términos más frecuentes a los que se hace referencia durante el análisis de los sistemas de protección de perímetro, su historia, sus arquitecturas y las técnicas de las que se valen los sistemas de protección de perímetro como son las políticas de red, los anfitriones de protección, el filtrado de paquetes, los sistemas representantes, y la autentificación.

Dentro del capítulo tres basados en lo anterior se llevará a cabo la construcción de un sistema de protección de perímetro de manera conceptual, desde la implementación de las políticas de red hasta la creación de restricciones del servicio.

Y finalmente en el capítulo cuatro se explicará la instalación del sistema de protección de perímetro haciendo uso de un programa gratuito, basado en filtrado de paquetes, del cual se darán sus requerimientos, y se demostrará la manera en que podrán crearse las reglas de restricción.

CAPÍTULO 1

FUNDAMENTOS DE SEGURIDAD



"¿ qué quiere decir comentar, amigo, y entrar?", pregunto Merry
"es suficientemente claro", dijo Gimli
"si tu eres amistoso, comenta la contraseña, y las puertas se abrirán, y podrán entrar".

El señor de los anillos
- J. R. R. Tolkien

CAPÍTULO 1. FUNDAMENTOS DE SEGURIDAD

Es importante, conocer la definición de lo que es la seguridad de cómputo, para posteriormente introducirnos a los conceptos seguridad.

La seguridad de cómputo es: "el conjunto de procedimientos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo".[21]

1.1 CARACTERISTICAS DE SEGURIDAD

La estructura de la seguridad en cómputo se fundamenta en lo siguiente:

a) Confidencialidad – La información debe ser conocida, vista y manipulada únicamente por quienes tienen el derecho de hacerlo. Un ejemplo es la divulgación de información.

b) Integridad - La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la integridad, es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

c) Disponibilidad – Consiste en acceder a la información en el momento en que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio ("Denial of Service") o tirar el servidor

d) Control: Son las normas de acceso al sistema

e) Autentificación .- Se entiende como verificar que la persona que trata de acceder a los servicios de una red, es realmente una persona con permisos para ello.

f) Autorización .- Es el restringir a la persona que ha sido autentificada a accesar únicamente las áreas de trabajo sobre las cuales se tiene los permisos correspondientes.

g) Auditoría .- Es la continua vigilancia de los servicios en producción. Así como a los usuarios no autorizados, los que si lo están pueden causar daño (intencional o accidental), para esto es necesario determinar quién y qué esta haciendo en el sistema

h) Consistencia: Asegurarse de que el sistema se comporte como se espera por los usuarios autorizados.

1.2 NIVELES DE SEGURIDAD

El Centro Nacional de Seguridad en Computación (NCSC) en el año de 1985, creó un conjunto de estándares de seguridad en computación para el Departamento de Defensa de los Estados Unidos y los llamó *Criterios de evaluación confiable para sistemas de computación*, también conocidos como el *Libro Naranja*.

En este libro hay cuatro clases amplias de niveles de seguridad para computadoras:

- D: Seguridad mínima. Dentro de esta categoría se pueden clasificar los sistemas operativos tradicionales como DOS y Windows. La protección es únicamente para cambiar los atributos de archivo y con ello prevenir un borrado accidental.
- C: Seguridad discrecional. En ella se incluyen características y funciones que quedan a discreción del administrador de la red, como la decisión de que servicios se van a restringir a los usuarios y cuales no. Contiene 2 subniveles, el C1 que permite que los usuarios mantengan sus datos en privado con respecto a otros usuarios, e impiden que sean leídos o destruidos accidentalmente. Y el C2 que demanda procedimientos de registro más estrictos, la auditoría de los eventos relacionados con la seguridad y el aislamiento de los recursos del sistema.
- B: Protección obligatoria. Esto es que, el administrador de sistemas no puede desactivarlos aunque quiera. Y proporciona tres subniveles, el B1 tiene protección etiquetada, lo cual significa que los procedimientos de seguridad y etiquetas de sensibilidad (que son básicamente clasificaciones de seguridad) son requeridos para cada archivo. El B2 presenta además el requisito de que el sistema debe de ser capaz de llevar cuenta de todo el código que hay en el mismo, ayudando a prevenir fisuras de seguridad como los *caballos de troya*[1]. La clase B3 se refiere a la seguridad del acceso desde el punto de vista de prevención de falsificaciones y notificación de los eventos relevantes de la seguridad.

[1] Ver glosario.

- A: Protección Verificada. La clase más alta de seguridad la A1 requiere de diseños verificados. Aunque funcionalmente son iguales a los sistemas B3, estos también han sido definidos y probados de manera formal.

Durante muchos años sirvió como base para la seguridad en computación, pero recientemente se han reunido grupos en países como Canadá, Francia, Gran Bretaña, Holanda, Alemania y Estados Unidos, para actualizar los lineamientos definidos en el libro naranja, desarrollando los "Criterios Comunes", que son un estándar para los criterios de seguridad. Estos países han aceptado criterios comunes, y se han convertido en el estándar de factor para la seguridad de la tecnología de la información a nivel mundial.

Los dos documentos básicos para el Criterio Común (*CC*) son el Libro Naranja y Los Criterios de Evaluación para la Seguridad de la Tecnología Informativa en la Comunidad Europea (*ITSEC*). Sin embargo, el CC no es solamente una sinopsis de otros documentos; está planeado para que reemplace a esos otros documentos.

Dos de los conceptos primordiales en el CC son:

- El *perfil de protección*, no es específico a un producto, sino que, después de ser revisado, se convierte en parte del CC. En él se documenta un problema de seguridad particular y la solución adecuada. Considerando los requerimientos para los tipos de productos específicos para este problema y su solución.

- *El destino de la seguridad*, permite que los perfiles de protección se ajusten a un producto específico, es decir, el producto como una meta particular en relación a la seguridad. Con esto el destino de seguridad forma la base de la evaluación.

Una evaluación de producto determina si con un producto particular se ha identificado y resuelto de manera adecuada un problema de seguridad.

El proceso de evaluación tiene varias etapas. En la primera, un fabricante de productos identifica un problema de seguridad, y decide desarrollar una solución y quiere que la evalúen. Si existe un perfil de protección para este problema el fabricante puede ajustar el perfil del producto al perfil de seguridad.

Si no existe un perfil de seguridad, se puede desarrollar uno y establecer un estándar para medir productos similares. Sin embargo, es posible definir un destino de seguridad sin hacer referencia a un perfil de protección.

Después el producto mismo se evalúa de acuerdo con el destino de seguridad. Si el producto pasa la evaluación, se le da un nivel de seguridad de evaluación (EAL). La evaluación, realizada por una organización independiente al fabricante, confirma que no existan errores de seguridad obvios. En el caso de un EAL de alto grado, la evaluación confirma que no hay errores ocultos, y que se formule documentación para el usuario.

La ventaja que proporciona el CC es que es flexible y representa claramente un concepto de seguridad.

1.3 FACTORES DE SEGURIDAD

A grandes rasgos se puede decir que la seguridad en un sitio[2] está determinada por:

- EL FACTOR ORGANIZACIONAL:

a) Usuarios

- Tipo de usuarios que se tienen
- Reglamentos y políticas que rigen su comportamiento
- Vigilar que esos reglamentos y políticas se cumplan, y no queden sólo en papel

b) La alta dirección

- Inversión en capacitación de los administradores
- Apoyo económico orientado a la adquisición de tecnología de seguridad
- Negociar acuerdos de soporte técnico con los proveedores de equipo.

- EL FACTOR SOFTWARE:

a) La aplicación

- Vigilar que tenga mecanismos para control de acceso integrados
- Observar las facilidades de respaldo de información que se tienen
- Establecer qué tan flexible es la aplicación y desprender su disponibilidad de ahí.

[2] Ver glosario.

b) El sistema operativo

- Mostrar preferencias por los sistemas abiertos (UNIX)
- Vigilar que soporte estándares de seguridad como C2
- Observar las recomendaciones del fabricante y aplicar los parches que libere.
- Vigilar siempre las bitácoras
- Mantenerse informado sobre las alertas de seguridad

c) Software de red

- Vigilar de cerca las estadísticas de acceso y tráficos de la red
- Procurar implementar sistemas de protección perimetral, pero no confiar demasiado en ellos.
- En la medida de lo posible, apoyar las conexiones cifradas.

- EL FACTOR HARDWARE:

a) Hardware de red

- Elegir adecuadamente el tipo de tecnología de transporte (Ethernet[5], Token Ring[4], etc)
- Proteger muy bien el cableado, las antenas y cualquier dispositivo de red
- Proporcionar periódicamente mantenimiento a las instalaciones

b) Servidores

- Mantenerlos en condiciones de humedad y temperatura adecuados.

[5] Ver glosario.

- Establecer políticas de acceso físico al servidor.
- El mantenimiento también es importante aquí.

1.4 SERVICIOS DE INTERNET

Existe un sinnúmero de servicios estándar de Internet que los usuarios utilizan y que la mayoría de los sitios intentan soportar. También se tienen razones importantes para contar con tales servicios, ya que de hecho, sin ellos hay pocas razones para conectarse a Internet.

Ninguno de estos servicios es, en su totalidad seguro, cada uno tiene sus debilidades, por lo que antes de decidirse a soportar un servicio, se debe evaluar que tan importante es para los usuarios y si podrá protegerlos de posibles daños e intromisiones.

Cada administrador de una red debe decidir que servicios se deben soportar en el sitio y hasta que grado, pero pueden considerarse como básicos seis servicios:

- *Correo electrónico (SMTP)*: Es de riesgo bajo, pues es sencillo falsificar correo electrónico, facilitando dos tipos de ataque: de reputación y de *manipulación social* (ej. Cuando usuarios envían correos que se supone vienen del administrador, aconsejándoles que cambien de contraseña de forma específica). El aceptar correo electrónico ocupa tiempo y espacio en disco, exponiéndolo a ataques de negación de servicio, y en los servicios modernos de correo, a que les sean enviados programas que resulten caballos de troya. Aunque en la práctica los problemas más comunes

* Ver glosario.

son las inundaciones inadvertidas (incluyendo cadenas de cartas) y personas que confían plenamente en la confidencialidad del sistema de correo y envían datos por medio del correo de Internet.

- *Transferencia de archivos* (FTP): En ocasiones resulta necesario contar con una herramienta que nos permita transferir archivos al solicitarlos. El ftp es el protocolo estándar para este propósito. Al permitir que un usuario obtenga archivos, es probable que se adquieran programas y datos indeseables como son: juegos de computadoras, software pirata e imágenes pornográficas, que tiende a ocupar espacio en el disco. Si se hace lo siguiente puede ser un servicio razonablemente seguro: primero; educar a los usuarios para que desconfíen de cualquier software que obtengan por medio de ftp, y segundo comunique a los usuarios las políticas del sitio sobre material con contenido sexual y el uso de los recursos de la organización.

Ahora desde el punto de vista, de permitir a otras personas utilizar ftp para transmitir desde sus computadoras archivos, resulta ser más peligroso. Hay que ser cuidadosos en dar acceso solamente a un área pública separada del sistema donde se encuentren disponibles los archivos considerados confidenciales y así evitar potencialmente el que se pueda accesar a todo el sistema. También se debe de cuidar que los usuarios no depositen información delicada en el servidor de ftp, para que lo utilicen personas específicas, sin considerar que cualquiera en Internet puede leerlos, o que crean en la seguridad por ser desconocidos.

- *Noticias de Usenet* (NNTP): Los grupos de noticias están diseñados para la comunicación de muchos a muchos. Son como la televisión, suceden una variedad cosas; la mayor parte tiene poco valor social; una parte es divertida o informativa, y todos la quieren. Sus riesgos son similares a los del correo electrónico: los usuarios pueden confiar en la información recibida; pueden divulgar información confidencial; e inundarse de mensajes. Las noticias asemejan una inundación cuando funcionan normalmente, duplicando su volumen continuamente, así que deben de configurarse de manera que no afecten otros servicios. Debido a que este servicio no es esencial, los ataques de negación del mismo en un sitio generalmente se ignoran. Los riesgos de seguridad de las noticias son bajos, quizá se desee evitar las noticias porque no tienen el ancho de banda o el espacio en disco necesario para ello, pero no representa un riesgo de seguridad importante.
- *Acceso de terminal remota* (TELNET): Este servicio permite que se utilice un sistema remoto como si fuera un terminal (no una estación gráfica) conectada directamente. En algún momento se consideraba un servicio más o menos seguro porque requiere que los usuarios se autentifiquen por ellos mismos. Por desgracia envía toda su información sin codificar, lo que lo hace muy vulnerable a ataques de espionaje (valiéndose de *analizadores de protocolo*[5]) y robo, razón por la cual actualmente se considera como uno de los servicios más peligrosos cuando se utiliza para entrar a un sitio desde un sistema remoto. Debido a su utilidad como

[5] Ver glosario.

un mecanismo de acceso remoto de usuarios que viajan a sitios conectados a Internet y en extremo efectivo en cuanto a costo, se debe proporcionar este servicio, pero con sus debidas precauciones.

- *Acceso al World Wide Web* (HTTP): El World Wide Web es un concepto relativamente nuevo, basado totalmente en Internet y, en parte en servicios existentes y en un protocolo nuevo: el Protocolo de Transferencia de Hipertexto (HTTP). El Web utiliza tecnología de hipertexto para enlazar una gran cantidad de documentos que pueden incluir texto, imágenes, sonido, video y otros formatos. Se puede "navegar" por los documentos de cualquier manera (no sólo jerárquica) para buscar información. El hipertexto proporciona la posibilidad de ir de un documento a otro en Internet. Los usuarios pueden moverse libremente de uno a otro, sin importar en donde estén guardados, con solo hacer clic en una palabra o imagen para la cual se ha definido un enlace (o liga) HTTP. Por desgracia, los navegadores Web y los servidores son difíciles de asegurar. La utilidad del Web se basa, en gran medida, en su flexibilidad, pero ésta dificulta su control. Así como se facilita el transferir y ejecutar el programa correcto utilizando un navegador Web, es más fácil transferir y ejecutar uno peligroso. Se debe de advertir a los usuarios de no agregar visualizadores, o cambiar las configuraciones de los mismos, basándose en el consejo de otros usuarios.
- *Búsqueda de nombre anfitrión/dirección* (DNS): El servicio de nombres se encarga de traducir los nombres de anfitrión que utilizan las persona a direcciones

IP numéricas que utilizan las máquinas. En los inicios del Internet era posible mantener una tabla de anfitriones con el nombre y número de cada máquina. Actualmente no resulta práctico para ningún sitio el mantener una lista semejante, mucho menos que la tenga cada sitio. En lugar de esto, el Servicio de Nombres de Dominio, permite que cada sitio tenga información sobre sus propios anfitriones y pueda encontrar la información para otros sitios. DNS no es un servicio a nivel usuario en sí mismo, pero soporta SMTP, FTP y TELNET y casi cualquier otro servicio que los usuarios requieran. Se debe de utilizar y proporcionar el servicio de nombres para poder participar en Internet. Su riesgo principal es que proporcione más información de la que se tiene pensada. Por ejemplo, DNS permite incluir información sobre que hardware y software se está ejecutando, lo cual no conviene que lo conozca un atacante. El uso de DNS interno y luego la dependencia de los nombres de anfitrión para dar autenticación lo hace vulnerable a un intruso que pueda instalar un DNS mentiroso. Esto se puede manejar combinando algunos métodos, que incluyen: primero, usar direcciones IP (en lugar de nombres de anfitrión) para dar autentificación a los servicios que deben ser más seguros y segundo, dar autentificación a usuarios en lugar de anfitriones en los servicios más seguros, porque las direcciones IP también pueden falsificarse.

1.5 RIESGOS

Al momento de conectar un equipo a Internet se pueden tener los siguientes riesgos:

1) Los datos: la información que se guarda en las computadoras. Los datos tienen tres características que necesitan protegerse y son: confidencialidad, integridad, y disponibilidad, las cuales fueron explicadas anteriormente en el punto 1.2
2) Los recursos: (las computadoras en sí). Aún cuando no sea tan importante la información, es posible que si otras personas utilizan nuestra computadora, les agradaría sacar provecho de la situación. Bajo este contexto no es agradable que alguien no autorizado utilice el equipo de cómputo.
3) Reputación: Si alguien se hiciera pasar por el responsable, cualquier acto vandálico tendría repercusión directamente sobre su vida personal, pues asumida la responsabilidad de lo realizado perdería la confianza de las personas que se encuentran en la organización.

1.6 TIPOS DE ATAQUE

Existen muchos tipos de ataque a un sistema y varias formas de clasificar estos ataques:

- Intrusión: Es el más común de todos los ataques, en donde las personas pueden utilizar las computadoras, como si fueran usuarios verdaderos. Existen docenas de maneras de tener un acceso de este tipo, que va desde la manipulación social, hasta el simple trabajo de estar adivinando las contraseñas.
- Negación del Servicio: Esta dirigido principalmente al bloqueo de la computadora, para así evitar que puedan utilizarse. En este tipo de ataques es más frecuente que se utilice la inundación de la información (*Caso Quinte Stalla o el gusano de*

Internet[6]). Un intruso inunda un sistema o Red con procesos, mensajes o solicitudes a la red al grado que el sistema intentara responder las solicitudes sin poder cumplir ninguna de ellas.

- Robo de Información: Ciertos tipos de ataques dan facilidades al atacante de acceder a la información sin tener que utilizar de forma directa la computadora; normalmente este tipo de ataque aprovecha los servicios de Internet, cuya función es proporcionar información, provocando que de más información de la que se debe. Este tipo de robo no necesita ser activo o particularmente técnico.

Por ejemplo, las intervenciones de Red llamada Analizadores ("*Sniffers*"), son muy efectivos para encontrar las contraseñas, de una forma pasiva. Este tipo de Robo de información rara vez se utiliza para conseguir otro tipo de datos.

1.7 TIPOS DE ATACANTES

En esta parte solo se describen los tipos de atacantes más comunes que existen en el Internet, que son los siguientes:

- Pascadores ilegales ("Joyriders"): Solo buscan diversión. Suele ser gente curiosa, que piensa encontrar información interesante o conocer el tipo de equipo que se tiene. Con frecuencia dañan los sistemas por ignorancia o por tratar de borrar su rastro.
- Vándalos: Suelen causar estragos porque les agrada hacerlo o porque las personas no les agradan. Son un gran problema si a consideración del

[6] ver glosario.

"*underground*" del Internet lo consideran como enemigo (ej. Gobierno y compañías telefónicas). Se concentran en eliminar información o en arruinar el equipo.

- Busca Récords ("Score Keepers"): Son personas que se mueven por ganar fama basándose en la cantidad y tipo de sistemas infiltrados. Al igual que los dos casos anteriores, tienen predilección por sitios de interés, como lugares bien conocidos, defendidos u ordenados. No forzosamente desean la información que se encuentra en el sitio, y tampoco les interesa las características de equipo que sé este utilizando.
- Espías: Aunque no están muy interesados en el robo de información, cuando lo hacen suelen robar cosas que puedan convertir en dinero o a un acceso mayor (por ejemplo, tarjetas de crédito o información para acceder a redes). El espionaje basado en computadoras es poco común, sin embargo, cuando se da el caso es mucho más difícil de detectar que las intrusiones sin permiso. Alguien que entra, copia información y sale sin alterar nada es probable que lo logre en la mayoría de los sitios, y es rara la vez que se detecta de inmediato.
- Accidentes y Tonterías: Más del 50 % de los incidentes, son ocasionados por equivocaciones o accidentes. Por ejemplo los incidentes de negación de información con frecuencia ni siquiera son ataques. El correo electrónico puede bloquearse si un solo mensaje es enviado desde un servidor de correo con problemas a una lista de distribución de correo grande. Este correo da origen a una cascada de cientos de miles de mensajes de error (como le sucedió al corporativo de Apple).

1.8 MEDIDAS DE PROTECCIÓN

Existen distintos modelos que pueden utilizarse para resguardarse contra los ataques, antes mencionados.

- Nada de seguridad: Es la más sencilla de las medidas, no se hace uso más que la que el proveedor proporcione en forma preestablecida.
- Seguridad por Obscuridad: Aquí se presume que el sistema es seguro por el solo hecho del desconocimiento del mismo (existencia, contenido y medidas de seguridad). Se podría pensar que el ser una compañía pequeña o por tener una computadora en casa no será de interés para los intrusos, provocando que sean blancos fáciles y que se pueda hacer un daño considerable.
- Seguridad del anfitrión: Este es probablemente el modelo más común de seguridad. Con este modelo se refuerza la seguridad de cada anfitrión de forma individual y se hace el mayor esfuerzo para evitar o mejorar todos los incidentes de seguridad que puedan afectar al anfitrión en particular.
- Seguridad de Red: A medida que los ambientes crecen y se diversifican, es más difícil de mantener un esquema de seguridad de anfitrión. Muchos sitios de cómputo cambian su esquema de seguridad a la red. Con este modelo se puede controlar el acceso a los servidores y a los servicios que se ofrecen, en vez de estar asegurándolos de uno en uno. Este modelo incluye la construcción de sistemas de protección perimetral para proteger la red y los servidores internos,

b) Respaldar siempre.- No basta con efectuar respaldos. Una buena política de respaldos contempla, entre otras cosas: tiempos óptimos de respaldo y recuperación, periodicidad del mismo y verificación de integridad (de nada sirve un respaldo no íntegro), necesidad de duplicidad y expiración de los respaldos. Como usuario se debe hacer, además un respaldo propio adicional al que hace el administrador de la red, siempre que sea posible y dependiendo también de la importancia de la información.

c) Realizar verificaciones no predecibles.- Si un ladrón conoce las horas a las que la guardia de un banco hace su rondín, seguramente decidirá no robarlo a esas horas. Lo mismo sucede con los sistemas si se hacen verificaciones periódicas, y alguien más conoce qué y cuándo se realizan. Por lo que será necesario hacer verificaciones periódicas no predecibles, a fin de obtener una estadística más real del comportamiento del sistema.

d) Leer las bitácoras.- Las bitácoras del sistema reflejan lo que ocurre en el mismo. De nada sirve tenerlas si no son leídas. Es ahí donde pueden descubrirse ataques no exitosos perpetrados contra el sistema.

e) Aplicar "parches" o tener las últimas versiones del software.- Las vulnerabilidades[7] sobre algún producto o plataforma, pueden dar la vuelta al mundo rápidamente gracias a Internet. Es recomendable por ello contar siempre con la versión más actualizada del software, o bien aplicar los "parches" respectivos cuando son

[7] Ver glosario.

liberados. En este rubro, el software libre (como linux) cuenta con una ventaja sobre software comercial, pues el tiempo de respuesta es más rápido para el software gratuito.

f) Leer noticias sobre seguridad.- Si un proveedor mantiene una lista de seguridad, es importante incorporarse a ella. Así como suscribirse a listas que informen sobre seguridad en general de modo que se obtenga un panorama amplio pero conciso sobre el tema.

g) Cancelación de cuentas.- Todo lo anterior no sirve si personas que han trabajado para la organización poseen sus cuentas de acceso después de haber dejado de colaborar con ella. Las estadísticas demuestran que un 85% de los ataques de seguridad son realizados desde dentro de la organización, o bien a través de cuentas de personal que estuvo dentro de ella.

1.10 TÁCTICAS DE SEGURIDAD

Las siguientes estrategias nos servirán para realizar un mejor análisis antes de adoptar algún tipo de herramienta de seguridad.

- Permisos básicos: Probablemente es la base principal en cualquier tipo de seguridad (no siendo de manera exclusiva para el ámbito informático). Su significado se basa en la primicia de que solo se deben tener los permisos necesarios para cumplir con el trabajo que se haya asignado. De esta manera se contribuye a la reducción de ataques y se limita los estragos que puedan ocasionar estos. Por

ejemplo: No es necesario dar una contraseña de administrador si lo que requiere un usuario es simplemente mandar imprimir.

- Protección Completa: No se debe depender de un solo mecanismo de protección, aún cuando este mecanismo parezca lo suficientemente sólido. Deben de preverse los posibles fallos; y en la vulnerabilidad en que se deja al sistema al ocurrir un evento de esta clase. Se debe hacer uso de un conjunto de herramientas para salvaguardar el equipo de cómputo.
- Punto de monitoreo(o de choque): Se forza al uso de un canal estrecho, el cual se puede revisar y controlar. Por ejemplo las casetas de cobro de las autopistas serían un punto de monitoreo. Por otra parte se debe tener cuidado de no tener otro punto de enlace sin supervisión, es decir, no contar con otro punto de entrada al sistema, el cual se ignore y pueda ocasionar problemas.
- Componentes débiles: Deben conocerse los puntos más débiles de seguridad, ya sea para eliminarlos o bien para monitorearlos con más precaución, si es que no se pueden eliminar. Con el fin de no dar oportunidad a los atacantes de tener un punto donde puedan centrar sus ataques. Ahora todos los aspectos concernientes con la seguridad del sitio deben tener la misma atención para no tener desigualdades entre unos y otros. Hay que tratar de mantener los puntos débiles lo más fuerte que se pueda con respecto al riesgo que este represente.
- Fallas - Seguras: Si un sistema llega a fallar, debe de hacerlo de manera tal que se le niegue el servicio a un atacante en lugar de permitirle introducirse. Esta

negación también debe de extenderse a usuarios auténticos hasta que se repare la falla, pero por lo general es algo admisible. (Un ejemplo de falla-segura en la vida cotidiana es cuando: Los seguros de las puertas eléctricas se abren cuando la fuente de energía llega a fallar).

Existen dos situaciones en este sentido que se pueden adoptar:

1. *Lo que no este expresamente permitido está prohibido*: La negación preestablecida, tiene sentido desde el punto de vista de seguridad. Refiriéndose a que lo que es desconocido puede resultar dañino. Para determinar que se permite, partiendo del punto de vista de negación, se deben examinar los siguientes puntos:

    a) Los servicios que requieren los usuarios

    b) Las implicaciones de seguridad de estos servicios y como proveerlos de forma segura.

    c) Autorizar solo los servicios que se conocen y se necesitan

2. *Lo que no este expresamente prohibido esta permitido*: Muchos usuarios y administradores prefieren la postura de permisos preestablecidos. Se asume que todo esta permitido y que se irán prohibiendo los servicios que causen problemas de acuerdo a las necesidades que se susciten. Este punto de vista supone, que se conoce de antemano y de manera precisa los problemas que puedan ocurrir, teniéndose el dilema de como explicarlo a los usuarios para que se encuentren enterados y aprendan a protegerse de ellos. El adivinar que riesgos se pueden tener en el sistema o en Internet es un trabajo imposible, pues existen muchos posibles y

demasiada información como para poder mantenerse actualizado en todo lo que involucra a la seguridad. En ocasiones puede llegar a generarse una competencia entre los usuarios y la persona encargada de la seguridad del sistema, pues mientras el encargado de la seguridad prepara la defensa contra la acción o inacción del usuario, el usuario puede estar ideando nuevas formas de hacer las cosas de manera insegura.

- Participación Conjunta: Para que los sistemas de seguridad sean efectivos, es necesaria la participación de todo el personal de la organización. Si alguien se sale de los lineamientos de seguridad, podría ser un blanco fácil para algún atacante y provocar que a partir de ese punto se introdujera en el sistema completo. La participación de los usuarios debe ser de manera voluntaria (preferentemente) o involuntaria, ya que de no ser así se daría pie a un conflicto interno, en el que las personas en desacuerdo trataran por todos los medios de hacer caso omiso a las recomendaciones del encargado de la seguridad del sistema.
- Diversidad y Sencillez: El hacer uso de sistemas de seguridad de distintos proveedores puede reducir las probabilidades de un problema ("bug"), o de un error de configuración común que comprometa a todos los demás sistemas. Al pensar en esta posibilidad, hay que tomar en cuenta lo siguiente:

  a) Mantener e instalar sistemas diferentes (o bien varios sistemas idénticos) es más difícil.

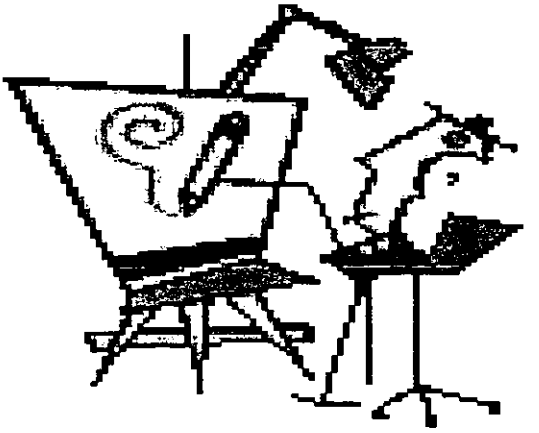
  b) Su mantenimiento e instalación toma más tiempo.

c) Es más costoso y se lleva también más tiempo y esfuerzo en la capacitación del personal.

Se considera que mantener las cosas de manera sencilla nos ayuda en la seguridad, ya que son más fáciles de entender (sino se conoce algo se convierte en algo complejo el saber sí es seguro o no). En caso contrario, entre mayor dificultad se tenga en algo, podríamos tener complicaciones al tener partes ocultas y tendríamos mayores probabilidades de tener problemas de cualquier tipo.

CAPÍTULO 2

ELEMENTOS Y DISEÑO DE LAS BARRERAS DE PROTECCIÓN



"El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy bien armados y muy bien pagados. Aún así, no apostaría mi vida por él"

Eugene Spafford

CAPÍTULO 2. ELEMENTOS Y DISEÑO DE LOS SISTEMAS DE PROTECCIÓN PERIMETRAL

2.1 CONCEPTOS DE SISTEMAS DE PROTECCIÓN DE PERÍMETRO

Algunos términos que se manejarán durante el desarrollo del presente capítulo son:

- Anfitrión("Host"): Cualquier computadora generalmente conectada a una red
- Anfitrión de Protección("Host Bastión"): Sistema identificado por el administrador como el punto más crítico en la seguridad de red y el cual debe estar altamente protegido.
- Anfitrión Doble: Computadora de propósito general que tiene al menos dos tarjetas de interfaz de red
- Filtrado de Paquetes: La acción que ejecuta un dispositivo para controlar de forma selectiva el flujo de datos hacia y desde una red.
- Red de perímetro: Red adjunta entre una red de protección y una red externa a fin de proporcionar un servicio de protección adicional. Esta red también se conoce como DMZ ("De-Militarized Zone").
- Servidor representante("proxy"): Programa que actúa como servidor interno, el cual responde a las solicitudes de los servidores externos. Los programas clientes se comunican con los servidores intermediarios, los que pueden redireccionar las solicitudes aprobadas del cliente al verdadero servidor y redireccionar las respuestas al cliente.

- Sistemas de protección perimetral: Sistema o grupo de sistemas que imponen políticas de control y restricción de acceso entre dos redes, una externa y la otra interna. En principio, estos sistemas pueden dar idea a un par de mecanismos, uno de los cuales existe para bloquear el tráfico y el otro para permitirlo. Probablemente la parte más importante de reconocer en un sistema de esta clase es la implementación de políticas de control de acceso; teniendo que ser lo bastante claros en lo que se quiere permitir o denegar.

El objetivo de los sistemas de protección de perímetro es el protegerse de otras redes para prevenir que usuarios no autorizados, tengan acceso a datos de vital importancia y a la vez permitir que los usuarios legítimos tengan libre acceso a los recursos de la red.

En general, un sistema de protección de perímetro se coloca entre la red interna confiable y la red externa no confiable. Este actúa como un punto estrecho que monitorea y rechaza el tráfico de la red local.

Conceptualmente hay dos tipos de sistemas de protección de perímetro:

- Nivel de red
- Nivel de Aplicación

1) Nivel de Red.- Generalmente hace sus decisiones basadas en las direcciones fuente, destino y puertos en paquetes IP individuales. Un simple ruteador es el tradicional sistema de protección de perímetro a nivel de red; aunque inicialmente no era posible hacer decisiones particularmente sofisticadas acerca de que

paquete estaba en ese momento comunicándose o de donde se estaba recibiendo, los modernos sistemas de protección de perímetro a nivel de red, se han convertido paulatinamente en sofisticados, y actualmente mantienen información acerca del estado de las conexiones que pasan a través de ellos, del contenido del flujo de datos, etc.

Una de las cosas que distingue a un sistema de protección de perímetro de nivel de red, es que rutean el tráfico directamente a través de ello, por lo que se requiere de una dirección IP válida para poder hacerlo.

Estos sistemas de protección de perímetro tienden a ser muy rápidos y transparentes al usuario.

2) *Nivel de Aplicación*.- Generalmente son anfitriones ejecutando servidores representante, los cuales no permiten el tráfico directo entre las redes y efectúan elaboradas bitácoras y auditorías del tráfico que pasa a través de ellos.

Como las aplicaciones representantes son componentes de software ejecutándose en el sistema de protección de perímetro, es un buen lugar para realizar la creación de bitácoras y controlar el acceso.

Los sistemas de protección de perímetro a nivel de aplicación, pueden ser usados como traductores de direcciones de red, a partir de que fluye el tráfico en un sentido y sale del otro, después de haber pasado a través de una aplicación que oculta el origen de la conexión de inicio.

Esta clase de sistema de protección de perímetro, tiende a proveer más detalle de los reportes de auditoría, forzando a conservar los modelos de seguridad.

2.2 HISTORIA DE LOS SISTEMAS DE PROTECCIÓN DE PERÍMETRO

- **Primera Generación**

La primera generación de sistema de protección perimetral – filtrado de paquetes – rastreaba la dirección fuente y destino de los paquetes IP en la red; los datos simplemente se verificaban cuando se recibían de Internet.

Aunque el filtrado de paquetes es implementado en la mayoría de los ruteadores y es transparente para los usuarios, puede ser desviado fácilmente mediante imitaciones al IP, lo que permite a los *hackers*[1] burlar a los ruteadores, permitiendo la introducción de datos ajenos a la red.

Los ruteadores que trabajan sin ningún otro complemento de seguridad no cuentan con herramientas para la detección de paquetes imitados, permitiéndose así el acceso no autorizado.

Las diferencia entre el filtrado de paquetes y la subsecuente generación de los sistemas de protección de perímetro, se destacan en el modelo OSI, ya que el filtrado de paquetes al enfocarse solamente a la información de las direcciones, trabaja exclusivamente en las capas más bajas del modelo.

[1] Ver glosario.

▫ Segunda Generación

La segunda generación – puertas de enlace[2] por hardware y software ("aplication and circuit gatewaye") – conecta una red local a una externa por medio de una estación de trabajo segura, ejecutando aplicaciones especializadas para el análisis de datos.

Estas puertas de enlace permiten a los usuarios comunicarse con sistemas seguros por medio de sistemas representantes, los cuales ocultan la información valiosa y los servidores, de los vándalos computacionales.

Las puertas de enlace por hardware se enfocan a la capa de transporte de TCP/IP del modelo OSI y usan la conexión de red TCP/IP como un sistema representante. Una aplicación representante es instalada entre el ruteador de la red y el Internet, reprimiendo el tráfico con Internet a favor de la red.

Las direcciones reales de la red se pueden ocultar, ya que la dirección del sistema representante es la que se transmite con el exterior, previniéndose la intromisión de los vándalos informáticos. Las puertas de enlace por hardware también bloquean paquetes de direcciones extrañas a la red local, haciéndolo de manera similar al filtrado de paquetes.

Las puertas de enlace por software (las cuales examinan la comunicación entre las aplicaciones IP), analizan los datos que están siendo transmitidos actualmente,

[2] Ver glosario.

esto frustra a los vándalos informáticos quienes tratan de imitar a los paquetes IP, para beneficiarse del acceso no autorizado a la red.

Estas puertas también pueden ser validadas con otras llaves de seguridad, como las contraseñas de usuarios y servicios de solicitud, que solamente aparecen dentro de la capa de aplicación del modelo OSI.

Aunque las puertas de enlace por software ofrecen un alto nivel de seguridad, hay varias desventajas:

1. Un atraso entre el anuncio de un nuevo servicio IP y la disponibilidad del correspondiente agente representante, traduciéndose en espera para los usuarios para disponer de la aplicación. También la instalación, mantenimiento y actualización de los agentes representantes, obliga a una carga en la administración adicional y mantenimiento.
2. Los sistemas representantes introducen un retraso en la ejecución, pues la entrada de los datos, debe ser procesada en dos ocasiones (una por la puerta de enlace y la otra por el agente del sistema representante).
3. Las puertas de enlace pueden requerir de una contraseña adicional o de otros procedimientos de validación, que producen nuevamente un retraso al trabajar y provocan frustración en el usuario.
4. Las puertas de enlace resultan costosas, pues requieren tanto de hardware como de software de costo elevado.

- **Tercera Generación**

A partir de las generaciones anteriores de los sistemas de protección de perímetro, la tecnología fue encaminándose a la examinación cada vez más directa del paquete, lo cual deja con menos oportunidades a los vándalos informáticos de robar o esconder información.

Tomando en cuenta el razonamiento que dice: " Si la seguridad pudiera hacerse cada vez más hermética, mientras que a la par se hiciera más fácil su acceso y su costo fuera menos alto, y sin sufrir por ello retraso en la ejecución" [8], fue que se inventó la Inspección de Estado Multi-Capas ("Stateful-Multi Layer Inspection") o bien sus siglas SMLI.

La inspección de estado multi-capas es la fundación de una nueva clase de sistemas de protección de perímetro, el cual puede ser aplicado internamente y externamente, a través de diferentes clases de protocolos y con una nueva característica de uso fácil.

La Inspección de Estado Multi-Capas es similar a las puertas de acceso en el sentido de que todos los niveles del modelo OSI son examinados, desde la capa física hasta la de aplicación.

En lugar de usar un sistema representante, el cual lee y procesa cada paquete a través de algunas manipulaciones lógicas de los datos, la Inspección de Estado Multi-Capas usa algoritmos de protección de tráfico optimizados, por un rendimiento efectivo en el análisis de datos.

Con la Inspección de Estado Multi-Capas cada paquete es examinado y comparado contra los estados conocidos (es decir, patrones de bits) de paquetes confiables.

Las soluciones basadas en esta clase de sistemas de protección de perímetro ofrecen dos tipos de beneficios:

1. El paquete completo es inspeccionado - por lo que el modelo OSI es totalmente cubierto – desde las direcciones hasta las aplicaciones.
2. El paquete es inspeccionado, no procesado - por lo que la redundancia y el tiempo de retraso resultante de los sistemas representantes se evita -.

El resultado es un sistema de protección perimetral transparente a los usuarios.

La comunicación toma lugar más rápidamente que antes, y el usuario no se percata de que otro programa se esta ejecutando por atrás, a través de contraseñas extras u otros procedimientos de validación.

2.3 ARQUITECTURA DE LOS SISTEMAS DE PROTECCIÓN PERIMETRAL

Algunas de las formas en que se pueden unir varios componentes de los sistemas de protección de perímetro son:

- Anfitrión de doble acceso
- Anfitrión de defensa
- Subred de protección

2.3.1 ANFITRIÓN DE DOBLE ACCESO O DE DOS BASES

La arquitectura más simple de un sistema de protección perimetral se basa en un anfitrión que tiene al menos dos tarjetas de red. Este anfitrión puede actuar como ruteador entre las redes que estén conectadas a dichas tarjetas de red.

Sin embargo, la función de ruteamiento es inhabilitada, en este tipo de arquitectura, ya que al deshabilitar esta función el anfitrión aisla a las dos redes, una de la otra, pero conservando la capacidad de reconocer el tráfico entre ambas redes.

Los sistemas dentro de la red interna pueden comunicarse con el anfitrión de doble acceso por medio de una de las interfaces de red, y los sistemas en Internet por la otra, de manera que estos sistemas no se pueden comunicar directamente

Por lo que los paquetes IP no se pueden rutear de forma directa entre una red y otra. Esta arquitectura se puede representar de la siguiente manera:

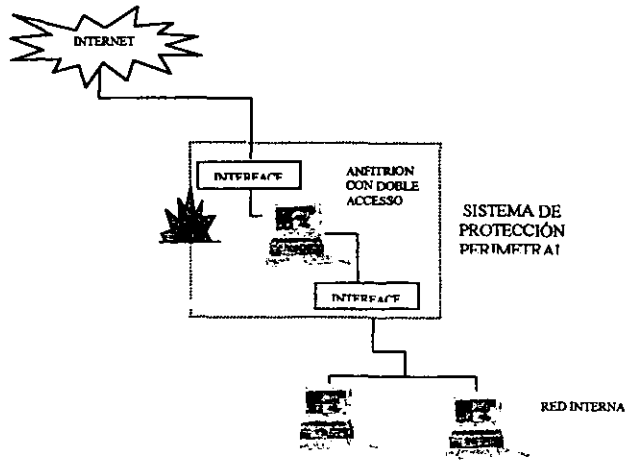


Fig. 2.3.1.1 Anfitrión de doble acceso

Como se aprecia en la figura anterior, la arquitectura es sencilla se coloca entre la red externa (en este caso Internet) y la red interna.

Una sistema de protección perimetral de este tipo puede proporcionar un alto grado de seguridad, permitiendo en ocasiones rechazar conexiones que intentan ser para un servicio en partícular, pero que contienen el tipo de datos incorrectos.

Un anfitrión de doble acceso sólo puede proporcionar servicios del tipo de sistemas representante, o hacer que los usuarios inicien una sesión directa con él.

El mayor problema con esta arquitectura es cuando un intruso puede obtener el acceso directo de conexión con el anfitrión de doble acceso. Estas invasiones pueden tener cualquiera de estos orígenes:

- Autorizaciones débiles en el sistema de archivo
- Programas de red que puedan restituir autorizaciones excesivas
- Comprensión del sistema a partir de antiguos niveles de revisión del software y notas que no se hayan asegurado de manera adecuada
- Instalación de antiguos kernels[3] de sistema operativo que activen el envío IP o la instalación de antiguos kernels de sistema operativo con problemas de seguridad conocidos.

En la práctica esta arquitectura esta propensa a fallos permitiendo que pasen paquetes de la red externa a la interna. Debido a lo imprevisto de estos sucesos es poco probable la existencia de protección a este tipo de ataques.

2.3.2 ANFITRIÓN DE DEFENSA

El anfitrión de defensa ("Screening Host") proporciona servicios en un anfitrión conectado únicamente a la red interna, y utilizando un ruteador[4] independiente para conectarse a la red externa(en este caso Internet). En esta arquitectura, ilustrada en la figura 2.3.2.1; la seguridad primaria es suministrada por el filtrado de paquetes y el anfitrión de protección, ubicado en la red interna, proporciona las aplicaciones que se requieran.

Las reglas de filtrado de paquetes de los ruteadores de defensa son configuradas de tal forma que el ruteador envíe primero todo el tráfico de la red externa a la interna hacia el anfitrión de protección, convirtiéndose así en el único medio accesible desde el Internet. Las conexiones a Internet pueden ser ruteadas a través de un programa representante en el anfitrión de protección, o en algunos casos permitirse directamente a través del ruteador de defensa, dependiendo de las políticas de seguridad de la red.

La configuración del filtrado de paquetes en el ruteador puede realizar una de las tareas siguientes:

- No permite todas las conexiones de los anfitriones internos
- Permite que anfitriones internos abran conexiones con anfitriones de Internet para ciertos servicios.

[3] Ver glosario.
[4] Ver glosario.

Asimismo, es más fácil la protección de un ruteador, que proporciona un conjunto muy limitado de servicios, que la protección de un anfitrión.

Algunas desventajas que se presentan en esta arquitectura:

- Si un atacante logra introducirse al anfitrión de protección, no queda nada en la ruta de seguridad de la red entre ese anfitrión y el resto de los anfitriones internos.
- Si el ruteador esta en peligro, toda la red estará al alcance del atacante.

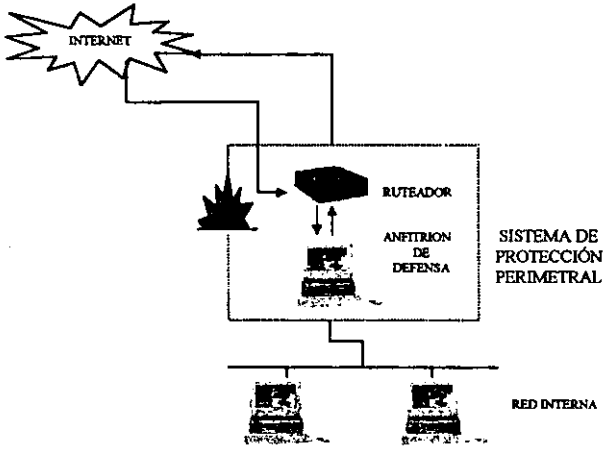


Fig. 2.3.2.1 Anfitrión de defensa

2.3.3 SUBRED DE PROTECCIÓN

En las arquitecturas anteriores (la de anfitrión de doble acceso y la de anfitrión de seguridad), la red de confianza es vulnerable si el anfitrión de protección es

comprometido. El impacto de comprometer al anfitrión de protección puede reducirse por el aislamiento de este, en una red de perímetro[5].

En la arquitectura de subred de protección ("Screened Subnet"), fig. 2.3.3.1, se agrega está capa de seguridad al adicionar una red de perímetro, proporcionando una mayor seguridad al aislar a la red interna del Internet.

En su forma más simple, se tienen dos ruteadores de protección, cada uno conectado a la red de perímetro. Uno ubicado entre la red interna y la red de perímetro, y el otro entre la red externa y el perímetro. Situando al anfitrión de protección en la red de perímetro entre los dos ruteadores

Para poder violar esta arquitectura se tendría que pasar por ambos ruteadores.

En algunos casos se establece una serie de capas de red de perímetro, colocando los servicios menos confiables y más vulnerables en estas redes exteriores, con el fin de alejar a los atacantes y evitar que incursionen en la red interna.

Dentro de la red de perímetro todo el tráfico debe ser:

1. De o para el anfitrión de protección
2. Hacia o desde Internet.

En consecuencia a que el tráfico rigurosamente interno, no pasa por la red de perímetro, se está seguro de los atacantes, en el caso de que el anfitrión de protección se encuentre en peligro.

[5] Ver inciso 2.1

En forma breve revisaremos los componentes de esta arquitectura, describiendo su función:

Anfitrión de Defensa

Sirve como punto de contacto para las conexiones que entran de redes exteriores. Ejemplo: Sesiones e-mail, conexiones ftp, etc.

Los servicios que salen (cliente interno - servidor externo) se manejan de la siguiente forma:

- Configuración del filtrado de paquetes en los ruteadores externo e interno, para permitir que los clientes tengan acceso de forma directa a los servidores externos
- Instalación de los servidores representantes para que sean ejecutados dentro del anfitrión protección, para permitir el acceso a servidores externos en forma directa.

Ruteadores

a) *Interno*: también conocido como ruteador de choque. Proporciona protección tanto de la red externa como de la red de perímetro. Ejecuta la mayor parte del filtrado de paquetes para el sistema de protección perimetral, permitiendo que sólo los servicios seleccionados salgan de la red interna hacia la externa.

El objetivo de esta limitación de servicios entre el anfitrión de protección y la red interna es el reducir el número de máquinas y servicios que pueden ser atacados desde el anfitrión de protección.

b) *Externo*: también conocido como ruteador de acceso. Da protección tanto a la red de perímetro como a la red interna.

Realiza muy poco de filtrado de paquetes permitiendo que salga casi cualquier cosa de la red de perímetro. Las reglas de filtrado establecidas en el ruteador externo son duplicadas en el interno.

Las únicas reglas especiales para el filtrado de paquetes en este ruteador, son los que protegen las máquinas de la red de perímetro.

Una de las tareas de seguridad que se pueden realizar con éxito y que no se realizan en ningún otro lugar, es el bloqueo de paquetes que entran de la red externa y que tienen direcciones fuentes falsas, las cuales dicen venir de la red interna, pero en realidad son de la red externa.

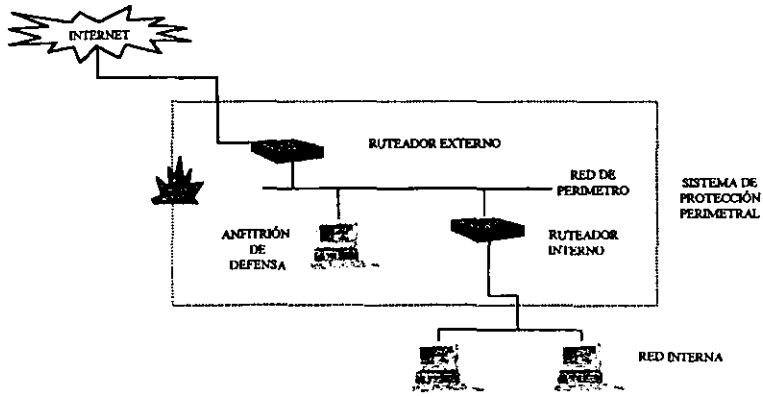


Fig. 2.3.3.1 Subred de Protección

2.4 TÉCNICAS QUE ULTILIZAN LOS SISTEMAS DE PROTECCIÓN DE PERIMETRO

Los componentes primarios son los siguientes:

- Políticas de seguridad
- Anfitriones de protección
- Filtrado de paquetes
- Sistemas representantes
- Autentificación

2.4.1 POLÍTICAS DE SEGURIDAD

Con antelación a considerar cualquier tipo de sistema de seguridad es necesario identificar qué recursos y qué servicios de la red son los que se quieren proteger y equilibrarlo contra la probabilidad de una violación de seguridad y costo de implantación de los medios de seguridad.

El primer paso debe ser planificar o revisar una política de seguridad.

Las *políticas de seguridad* son: códigos de conducta para el uso apropiado de los recursos disponibles en una organización y que definen de forma clara las actividades no permitidas, los pasos a seguir para obtener una protección adecuada, así como los lineamientos en el caso de presentarse un incidente de seguridad estableciéndose, además, responsabilidades y derechos [19].

2.4.1.1 PLANTEAMIENTO DE LA POLÍTICA DE SEGURIDAD

La política de seguridad justifica el uso y la protección de los recursos e información de la organización.

Es necesario tener presente que la política a usar debe estar planteada de tal forma de que no disminuya la capacidad de la organización.

La política que evita que los usuarios cumplan con sus tareas en forma efectiva disminuye la capacidad de la organización pudiendo tener consecuencias indeseables, pues los usuarios buscarían una forma de ignorar la política convirtiéndola en algo inservible.

Existen varios tipos de seguridad, mencionados en inciso 1.1 del capítulo uno, que tanto administradores como usuarios deben conocer para comprender las necesidades de operación, el medio y de acuerdo con esto definir los procedimientos y políticas que se adecuen a la organización.

Para plantear la política de seguridad, hay que tomar en cuenta los siguientes cuestionamientos:

- ¿Qué recursos se están tratando de proteger?
- ¿Qué probabilidades tienen de ocurrir la amenaza?
- ¿Qué importancia tiene el recurso?
- ¿De quienes se necesita proteger el recurso?
- ¿Qué medidas se pueden adoptar para proteger los recursos de una manera oportuna y económica?

- ¿Cuánto tiempo, esfuerzo y dinero se esta dispuesto a dedicar para obtener un nivel adecuado de protección?

Una vez considerados estos puntos se pueden formular de forma variada las políticas, desde una manera muy simple y particular, o específica (como ejemplo podemos citar: política de correo electrónico, de contraseñas, etc.), hasta una general que comprenda varias páginas.

El planteamiento de la política de seguridad significa desarrollar planes (que es lo que se espera o que se hará en el futuro) y procedimientos (la manera en que la política es instrumentada, es decir, la herramienta que ejecutara la política), que necesitarán de revisión continua para verificar si los objetivos y circunstancias de la red no han cambiado.

Lo que no se debe hacer en el planteamiento de la política, es mencionar amenazas específicas, máquinas e individuos con nombre.

En esencia la política de seguridad juega 3 tipos de roles:

1) ¿Qué es lo que se quiere proteger? y ¿por qué?. Haciendo uso de un lenguaje con descripciones informales, sin tecnicismos para hacer que la gente comprenda el documento y quiera cumplirlo.
2) Establecer de manera clara la responsabilidad para lograr esa protección. Debiendo establecer las expectativas y responsabilidades entre todos los miembros de la organización, estando consciente de que espera uno de otro,

puesto que no se puede hacer recaer toda la responsabilidad a alguna de las partes de la organización.

3) Provee la base sobre la que se interpreta y/o resuelve cualquier conflicto posterior. Requiriéndose el ir cambiando conforme a las necesidades a través del tiempo.

Para finalizar, es importante involucrar a todas las personas relacionadas con la seguridad; como podrían ser las implicadas en el control de la auditoría, sistemas de información y las relacionadas con la seguridad física, para contar con su cooperación y aceptación, y tener así un apoyo total en la seguridad de la red.

2.4.1.1.1 ANÁLISIS DE RIESGO

En ocasiones los sistemas de cómputo no se clasifican como seguros o inseguros, sino como confiables o no confiables. Para decir que un sistema es confiable es necesario desarrollar una serie de acciones que deben estar basadas en las políticas generales de la organización y el análisis de riesgos.

Es importante entender, que en la creación de una política, se debe estar seguro de que los esfuerzos invertidos en la seguridad son costeables.

Esto requiere conocer cuales son los recursos de la red que valen la pena protegerse y cuales son los más importantes, además de identificar la fuente de amenaza de los mismos.

El análisis de riesgo permite determinar en que recursos se debe invertir mayor esfuerzo en su protección, de acuerdo a la importancia que este tenga para la organización.

La clasificación de un riesgo[6] se da de acuerdo al nivel de su importancia y la severidad de la pérdida.

Existen tres pasos básicos en el análisis de riesgos:

i. *Identificación de recursos*: Para realizar esta actividad es necesario listar todos los recursos con los que cuenta la organización. Es posible que se requiera conocer más detalladamente los procedimientos, leyes, políticas de la organización, recursos disponibles e inclusive si se cuenta con un seguro sobre los bienes inmueble.

Para identificar los recursos hay que tomar en cuenta que existen dos clases: tangibles (monitores, impresoras, etc.) e intangibles (imagen pública, contraseña de usuarios, etc).

i. *Identificación de los desastres*: El siguiente paso es hacer una lista de desastres que puedan afectar los recursos, estos pueden ser ambientales (incendios, terremotos, etc), inesperados (fallas estructurales del edificio, pérdida del servicio telefónico, etc), o la introducción de virus informáticos y problemas en el software. Después de determinar lo anterior es necesario estimar qué tan

[6] ver glosario.

factible es que suceda cada una de ellas, siendo esta una tarea difícil por la cantidad de información que se recaba.

ii. *Revisión de riesgos*: Una vez realizado el análisis de riesgos, no debe de ser olvidado, sino por el contrario debe de actualizarse periódicamente. Además, el análisis de desastres debe de efectuarse cada vez que se observe un cambio importante en la operación o la estructura del inmueble por ejemplo: cambio de oficinas, remodelaciones, etc.

Después de completar el análisis de riesgo, se requiere de hacer un análisis de costo beneficio, es decir, asignar un costo a cada riesgo, por si llegará a presentarse algún suceso, conocer cuánto ascenderá el monto de la pérdida, y determinando también el costo de los métodos de prevención, y los costo de recuperación, etc.

2.4.1.1.2 USO DE LOS RECURSOS Y RESPONSABILIDADES

Otros puntos a que requieren analizarse en la política de seguridad son los siguientes:

- ¿A quién se le permite utilizar los recursos?

Puede realizarse una lista de usuarios que requieran ingresar a la red y dividirlos en grupos de trabajo para tener mayor control en los permisos que se les otorgaran.

- ¿Cuál es el uso correcto de los recursos?

Se deben de proveer reglas para el uso admisible de los recursos. Estas reglas dependerán del tipo de usuario del que se trate y establecerán lo que es aceptable o inaceptable y las restricciones de acceso a un recurso de la red.

- ¿Quién esta autorizado para garantizar el acceso y aprobar el uso?

Es de vital importancia identificar a quien autoriza el acceso a los recursos, pues si no se tiene control de la persona encargada del acceso a la red, será difícil controlar a las personas que la estén utilizando. Al identificar a las personas responsables del acceso a la red, se podrá averiguar el tipo de acceso o control otorgado.

Esto tiene como utilidad identificar las fallas de seguridad que se puedan generar al dar excesos de privilegios a los usuarios, por lo que deben ser los privilegios necesarios y suficientes para desempeñar las tareas cotidianas.

- ¿Quién debe tener privilegios de administración del sistema?

Las personas que cuenten con privilegios especiales deberán ser responsables y tener personalidad legal dentro de la autoridad política. Previéndose que los sistemas cuenten con mecanismos de auditoría que puedan utilizarse para monitorear que los usuarios con privilegios no abusen de estos. Los errores cometidos por un administrador suelen dar puntos vulnerables de seguridad, por lo que si se cuenta con procedimientos bien documentados, ayudara a disminuir el riesgo de errores.

- ¿Cuáles son los derechos y responsabilidades del usuario?

Algunos aspectos relacionados a la definición de los derechos y responsabilidades del usuario son: que conozca las reglas respecto al uso de los recursos de la red y sus restricciones para no llegar al abuso y afectar el desempeño del sistema, además de que conozca en que momento se debe o no compartir cuentas o permitir usar sus cuentas (como lo es en el caso de trabajar de manera temporal en un proyecto), y hasta que punto el propio usuario es responsable de respaldar su información. Dentro de los derechos de los usuarios se contempla el de su privacidad.

- ¿Cuáles son los derechos y responsabilidades del administrador del sistema frente a los del usuario?

Debe especificarse cual será el límite de los administradores, es decir, hasta donde podrán examinar los directorios y archivos privados del usuario, para diagnosticar problemas del sistema e identificar problemas de seguridad, y si podrán o no examinar el tráfico de la red o del anfitrión.

- ¿Qué es lo que se hace con la información delicada?

La información en extremo delicada (como sería el caso de una nómina), deberá restringirse a algunos servidores y administradores. Antes de otorgar el acceso a los usuarios, será necesario considerar que servicios e información existen y a cuales son a los que podrán ingresar; solo si es estrictamente necesario.

2.4.1.3 PLAN DE ACCIÓN EN CASO DE INCIDENTE DE VIOLACIÓN DE LA POLÍTICA

Cuando se detecte una violación de la política de seguridad, se debe clasificar si ocurrió por: una negligencia personal, un accidente o error o bien por ignorancia de la política actual.

Las acciones correctivas, deben ser de manera razonable al tipo y severidad de la violación que se cometió.

2.4.1.3.1 RESPUESTA A LA VIOLACIÓN DE LA POLÍTICA

La respuesta dependerá del tipo de usuario que causó la violación (ya que podría ser cometida por usuarios internos o externos), siendo necesario definir acciones basadas en el tipo de usuario y de violación.

Hay dos formas en las que un el usuario interno puede infringir la política, la primera de ellas la puede realizar en el sitio local, en este caso se puede tener mayor control en el tipo de respuesta que se le dará. En la segunda, puede realizarla en un sitio remoto, complicándose la situación al estar implicada otra organización, y cualquier respuesta que se contemple tiene que ser discutida con la organización a la que se violó su política.

Las acciones a tomar pueden ir desde una amonestación verbal o advertencia, una carta formal o bien un cargo legal; prefiriéndose en ocasiones arreglar solamente la falla de seguridad, ante una publicidad adversa.

2.4.1.3.2 ESTRATEGIAS DE RESPUESTA

Existen dos tipos de estrategias para responder a los incidentes:

1) *Proteger y proceder*, la meta de esta estrategia es proteger a la red de manera inmediata y restauraría a su estado normal para que los usuarios puedan continuar utilizándola. Teniéndose en ocasiones que interferir en forma activa con los daños causados por el intruso y evitar así, un mayor desastre. La desventaja que se presenta es que, el intruso al saber que ha sido descubierto, tomara acciones evasivas para no ser rastreado, además de cambiar de estrategia de ataque pudiendo continuar con su destrucción en cualquier otro sitio.

Esta estrategia puede usarse con las condiciones siguientes:

- Si los recursos de la red no están bien protegidos
- Si la continua actividad de los intrusos puede resultar en un gran daño y riesgo financiero
- Si el costo de la demanda es demasiado alta o si la posibilidad o los deseos de demandar no existen.
- Si hay un riesgo considerable para los usuarios existentes en la red
- Si los tipos de usuarios de una red interna grande no se conocen en el momento del ataque.
- Si el sitio está sujeto a demandas judiciales por los usuarios. (esto se presenta en compañías de seguros, bancos, etc.)

2) *Perseguir y procesar*, la meta de esta estrategia es permitir que los intrusos sigan con sus acciones mientras son observadas sus actividades. Debiendo hacerlo de la manera más disimulada que sea posible para que no se den cuenta de que son observados y de esta manera registrar estas actividades para tener pruebas disponibles y poderlas presentar a las instancias legales. La desventaja de este método es que el intruso podrá seguir robando información o haciendo otra clase de daños, dejando al sitio vulnerable a sus demandas.

Esta recurso puede emplearse de la siguiente manera:

- Si los recursos de la red y sistemas están bien protegidos.
- Si es un ataque concentrado y ha ocurrido antes.
- Si el sitio esta dispuesto a poner en riesgo los recursos de la red, al permitirle al intruso continuar.
- Si el acceso al intruso puede controlarse.
- Si los administradores de la red saben que tipo de evidencia presentar en un juicio y pueden crear los registros adecuados, de las actividades del intruso.
- Si las herramientas de monitoreo están bien desarrolladas para crear registros aptos y recabar evidencia para el proceso legal.
- Si el sitio está preparado para una posible acción legal de sus usuarios, si sus datos o sistemas se encontraran comprometidos durante la persecución.

- ❖ Si se cuenta con respaldos adecuados.

2.4.1.3.3 IDENTIFICACIÓN Y PREVENCIÓN DE PROBLEMAS

En una sección adicional a la política se deben abordar los procedimientos generales, que deben implementarse para evitar problemas de seguridad.

La siguiente lista puede orientarnos en algunas de las áreas problemáticas, pero de ningún modo es completa, ya que es probable que cada sitio tenga sus propios puntos vulnerables.

a) *Puntos de acceso*: son puntos de entrada (también conocidos como ingresos) para los usuarios no autorizados. Tener varios puntos de esta clase aumentan los riesgos de seguridad de la red.

b) *Sistemas configurados de manera incorrecta*: si la configuración de un anfitrión es de manera deficiente, el sistema puede ser fácilmente corrompido. Los sistemas mal configurados son responsable de un gran número de problemas de seguridad de red. También los proveedores pueden ser responsables de estos sistemas mal configurados, pues sus sistemas cuentan en ocasiones con seguridad abierta. Las contraseñas para cuentas críticas quizá no estén establecidas, o utilizan nombres de registro y combinaciones de contraseña fáciles de adivinar.

c) *Problemas de software*: acorde al crecimiento de complejidad del software, también crece el número y complejidad de problemas en cualquier sistema (tal vez el software nunca este libre de errores, a menos que surjan métodos nuevos de creación de software). Los problemas de seguridad conocidos por el público son

métodos comunes de entrada no autorizadas. Si la implantación de un sistema es abierto y conocido con amplitud, un intruso puede utilizar las debilidades en el código de software que trabajan en un modo privilegiado para ganar acceso al sistema; por lo que los administradores de sistemas deben permanecer atentos a las severidades en la seguridad en sus sistemas operativos y ser responsables de obtener actualizaciones e implantar soluciones al descubrir estos problemas.

d) Amenazas de usuarios internos: los usuarios internos tienen un acceso más directo al software de la computadora y de la red que al del hardware real. Si alguno de estos usuarios decide trastornar la red, puede representar una amenaza considerable a la seguridad de la misma.

e) Seguridad Física: si las computadoras por si mismas no cuentan con seguridad física, los mecanismos de seguridad de software pueden ser ignorados con facilidad. Como por ejemplo en estaciones de trabajo con dos, o Win 95 que no cuentan siquiera con un nivel de contraseña de protección.

2.4.2 ANFITRIÓN DE PROTECCIÓN

Usualmente entre la comunidad en Internet se le aplica él termino de anfitrión bastión, en este caso en particular le denominaremos anfitrión de protección. Para comprender el cambio de término, es necesario revisar el significado de la palabra bastión.

De acuerdo con el Diccionario de la lengua española, se define un bastión como:

1. Una parte saliente de una muralla u otra fortaleza.

2. Una posición o área – muy bien defendida.

3. Algo considerado como una fortaleza de protección.

Marcus Ranem nos dice que: los bastiones son las partes de un castillo medieval altamente fortalecidos; puntos donde se tiene a la vista las áreas críticas de defensa, usualmente teniendo paredes fuertes, cuartos para tropas extras, y útiles bañeras con aceite hirviendo para desalentar a los atacantes. Un anfitrión bastión es un sistema identificado por los administradores de los sistemas de protección de perímetro como el punto fuerte crítico en la seguridad de la red.

Al ser el anfitrión de protección la presencia pública de la red en Internet, podemos compararlo con el vestíbulo de un edificio, pues aunque no se pueda ingresar a interior del mismo, podemos entrar en forma libre al vestíbulo y preguntar por lo que queramos, si obtenemos o no la petición, dependerá de la política del edificio.

De manera semejante el anfitrión es el sistema(vestíbulo) al que los extraños deben conectarse por lo regular para tener acceso al sistema o servicio que se encuentra custodiado por el sistema de protección perimetral.

Por diseño, el anfitrión esta totalmente expuesto en Internet, pues su existencia es pública. Motivo por el cual los administradores de red deben centrar su atención y esfuerzos en la seguridad del mismo durante su construcción y su posterior operación.

Aunque se este hablando en singular, puede existir en una sola red varios anfitriones de protección.

El proceso de configuración o construcción del anfitrión de protección es frecuentemente referido como difícil. La efectividad de la configuración del mismo puede ser evaluado por las respuestas a las preguntas siguientes:

1. ¿Cómo se protege el anfitrión de protección a sí mismo de un ataque?

2. ¿Cómo protege el anfitrión de protección a la red de un ataque?

2.4.2.1 PRINCIPIOS BÁSICOS DE ANFITRIONES DE PROTECCIÓN

Existen dos principios en la construcción y diseño del anfitrión:

(a) *Mantenerlo Simple*: entre más simple sea el anfitrión de protección es más fácil asegurarlo. Cualquier servicio que el anfitrión ofrezca, podría tener problemas de software o errores de configuración, y cualquiera de ellos causaría daños en la seguridad, por lo que será preferible que el anfitrión proporcione el menor número de servicios posibles (siempre y cuando cumpla con todas sus tareas).

(b) *Prepararse para cuando se esté en dificultades*: Aún cuando se trate de asegurar al máximo al anfitrión de protección, este puede encontrarse en algún momento comprometido. Solamente previendo lo peor y elaborando planes para ello, se tendrán mayores posibilidades de evitar. Se debe poner énfasis en el siguiente cuestionamiento: ¿qué sucederá si el anfitrión se encuentra en problemas?, la razón es simple, ya que está máquina es la más accesible desde el mundo exterior y por lo tanto tiene mayores posibilidades de ser atacada. Para evitarlo, es necesario que los servicios que proporcione el anfitrión a las computadoras internas, sean los absolutamente necesarios para que este funcione. Una vez tomadas las decisiones

se pueden instalar mecanismos estándar para el control de acceso (contraseñas, dispositivos de autentificación, etc.) en las computadoras internas, o bien instalar un filtrado de paquetes entre el anfitrión de protección y las computadoras internas.

2.4.2.2 CLASES ESPECIALES DE ANFITRIONES DE PROTECCIÓN

Existen diversas clases de anfitriones, que tienen requisitos especiales pero se configuran de forma similar.

- *Anfitriones con doble acceso sin ruteamiento:* Esta clase de anfitrión tiene varias conexiones de red, pero no pasa el tráfico entre ellas. Este tipo de anfitrión podría ser por si solo un sistema de protección perimetral o bien parte de uno más complejo. En términos generales la configuración de estos anfitriones necesita de extremo cuidado, para asegurarse de que no ofrezcan ruteamiento.
- *Máquina víctima:* Si se requiere ejecutar servicios difíciles de proporcionar de forma segura o de servicios nuevos, de los que se desconocen las repercusiones de seguridad que puedan traer, puede considerarse de utilidad una máquina de esta clase. Se trata de una máquina que no tiene nada importante y que no tiene acceso a las máquinas de las cuales un intruso podría obtener provecho. Proporciona solamente lo indispensable para ser utilizado por los servicios que se necesitan (de preferencia se proporciona sólo un servicio que no es seguro, o que no ha sido probado, para evitarse situaciones inesperadas). El factor clave para este tipo de máquinas es que son desechables, si se ve comprometida, no tiene mayor importancia.

- Anfitriones de protección internos: En la mayoría de las configuraciones de los anfitriones de esta clase, se tiene interacciones entre el anfitrión principal y los anfitriones internos. Estas máquinas son realmente anfitriones de protección secundarios y deben de configurarse y protegerse más como anfitrión de protección que como anfitriones internos normales. Quizá se deba de dejar más servicios en ellos, pero se debe de seguir el mismo proceso de configuración.

2.4.2.3 SELECCIÓN DEL ANFITRIÓN DE PROTECCIÓN

Lo primero que se debe hacer en la construcción de un anfitrión de protección, es decidir que tipo de máquina utilizar. Se necesita confiabilidad, soporte y ser fácil de configurar.

- Sistema operativo: el sistema operativo con el que cuente el anfitrión nos debe de ser familiar, pues no es conveniente empezar a conocer uno nuevo.
- Rapidez: no debe de ser una máquina muy rápida, de hecho en ocasiones es mejor que no sea computacionalmente atractiva, pues además del costo, normalmente los servicios que provee no necesitan de mucho poder de cómputo. Lo que debe de hacerse generalmente esta limitado por la velocidad de la conexión con el mundo exterior.

Las razones por las cuales no es conveniente contar con una máquina poderosa son las siguientes:

a) Una máquina menos rápida es un blanco menos tentador, no hay tanto prestigio para quien trata de atacarla

b) Si se compromete, es menos útil para atacar otros sistemas internos o sitios

c) El hacer uso de una máquina más lenta, hace que sea menos atractiva para los usuarios internos y esto los desanime para utilizarla en otros propósitos. Ayudándonos a mantener la seguridad del anfitrión.

♦ Configuración del hardware: es importante no usar hardware y periféricos no conocidos o probados, es mejor hacer uso de lo que ya esta conocido y probado y que, además, se encuentra documentado. También es importante que se tengan unidades de respaldo propias, para que sea, en la medida, lo más independiente posible del resto del sistema.

♦ Seleccionando el sitio físico: se requiere de contar con lugar físicamente seguro, por dos razones:

a) Es imposible asegurar una máquina contra un atacante que tiene acceso físico a ella.

b) El anfitrión de protección provee de la conectividad y funcionalidad de la conexión a Internet, si se pierde, daña o roba se presenta el problema de disponibilidad de servicios.

♦ Ubicación en la red: Debe de ubicarse en una red que no lleve tráfico confidencial, de preferencia en una red especial para este fin. Pues en algunas interfaces como Ethernet y Token Ring, se puede operar en "modo promiscuo", en el cual se pueden capturar todos los paquetes que circulan en la red a la que se encuentren

conectadas, en lugar de capturar solamente a los paquetes dirigidos o máquinas específicas. Una forma de enfocar el problema es no colocar el anfitrión en una red interna, sino, ponerlo en una red de perímetro. La red de perímetro debe estar separada de la red interna por un ruteador o una puerta de enlace, manteniendo el tráfico interno en la red interna, sin estar visible en la red de perímetro. Si no es posible ponerlo en una red de perímetro, puede evaluarse ponerlo en una red que no sea susceptible de ser vigilada

2.4.2.4 SELECCIÓN DE LOS SERVICIOS A PROPORCIONAR POR EL ANFITRIÓN DE PROTECCIÓN

Se puede proporcionar cualquier servicio que requiera el sitio para tener acceso a Internet, o que se quiera ofrecer a Internet.

Los servicios se pueden dividir en cuatro clases:

1. *Servicios que son seguros*. Esta clase de servicio se puede proporcionar a través del filtrado de paquetes.

2. *Servicios inseguros por cómo se proporcionan comúnmente pero que pueden asegurarse*. Estos servicios pueden proporcionarse directamente por el anfitrión.

3. *Servicios inseguros por cómo se proporcionan comúnmente y que no pueden asegurarse*. Estos tendrán que desactivarse y proporcionarse en un "anfitrión víctima", si realmente se necesitan.

4. *Servicios que no utiliza o que no utiliza junto con Internet*. Debe desactivar todos los servicios de esta categoría.

Los servicios que más comúnmente se proporcionan o se niegan en los anfitriones de protección son: Correo electrónico, Ftp, Telnet, Http y Nntp.

Para soportar cualquiera de estos servicios, tiene que dar acceso y proporcionar el servicio de nombres de dominio[7].

2.4.2.4.1 NO PERMITIR CUENTAS DE USUARIO

De ser posible no se deben permitir cuentas de este tipo en un anfitrión de protección, ya que existen varias razones, entre las que podemos mencionar:

- Vulnerabilidad de las mismas cuentas.
- Vulnerabilidad de los servicios requeridos para soportar las cuentas.
- Reducida estabilidad y confiabilidad de la máquina.
- Alteración inadvertida de la seguridad del anfitrión por los usuarios.
- Incremento en la dificultad para detectar ataques

Las cuentas de usuario ofrecen caminos de ataque relativamente sencillos para alguien que desea forzar la entrada al anfitrión de protección, puesto que el soportar las cuentas de usuario de un modo útil requiere que el anfitrión habilite servicios (por ejemplo, impresión y correo local) que de otra manera estarían inactivos.

Cada servicio disponible en el anfitrión puede hacer que los usuarios contribuyan a problemas de seguridad en el mismo, aún cuando no lo hagan a propósito, estos pueden alterar el sistema de varias formas: desde lo trivial (eligiendo

[7] Ver glosario.

contraseñas erróneas) a lo complejo(estableciendo un servidor de información no autorizado).

O bien, se ofrece otra ruta de ataque a través de problemas en el software o errores en la configuración.

2.4.2.5 CONSTRUCCIÓN Y OPERACIÓN DEL ANFITRIÓN

Para hacerlo hay que seguir los siguientes pasos:

1. Asegurar la máquina. Se debe construir el anfitrión iniciando con un sistema operativo estándar y virgen, que habrá de configurarse instalando lo menos posible (será más sencillo agregar elementos que borrarlos completamente). También será necesario sacar una lista de parches y recomendaciones de seguridad ya conocidos para el sistema operativo, trabajar sobre ellos y determinar cuáles son más relevantes para el propio sistema y corregir todos los problemas mencionados en los parches y recomendaciones.

2. Deshabilitar servicios no requeridos. Cualquiera de los servicios proporcionados por el anfitrión podría tener problemas de seguridad. Se proporcionarán los servicios que los usuarios necesiten siempre que la política lo permita. Hay dos reglas simples que se deben de aplicar:

   a) Si no se necesita o si se desconoce, se desactiva.

   b) Si el desactivarlo causa problemas, se sabrá lo que hace y puede activarse nuevamente (si realmente se necesita), o bien analizar que hacer con este servicio.

3. *Instalar o modificar servicios que se requieren.* Algunos de los servicios que se desea proporcionar pueden no estar provistos en el sistema operativo, otros pueden estarlo pero son inapropiados para usarse en un ambiente seguro u omiten características que quizá se requieran.

4. *Reconfigurar la máquina de modo apropiado para desarrollarla hasta su estado final.* Se debe cambiar la configuración inicial de la máquina; con el fin de mejorar y actualizar su operación. A través de los siguientes pasos:

a) *Reconfigurar y reconstruir el kernel*

b) *Quitar todos los programas innecesarios.*

c) *Activar tantos sistemas de archivo como sea posible en modo de solo lectura.*

5. *Hacer revisiones de seguridad para establecer su "normal de operación".* Una vez configurado el anfitrión es necesario ejecutar una auditoría de seguridad. Teniéndose dos razones para hacerlo, primero es una forma de asegurarse que no se ha omitido nada durante la instalación del sistema. Segundo, establece una "línea base", o una base de comparación, contra la que puede comparar auditorías futuras. Así se podrá detectar cualquier descompostura en la máquina.

6. *Conectar la máquina a la red en la que se usará.* Una vez asegurada la máquina completamente, se puede dar paso a su conexión a la red.

Asegurándose de no tener la máquina accesible a Internet hasta que no se ejecute el último paso.

7. *Operación del anfitrión*. Una vez puesto a funcionar el anfitrión de protección, se debe comenzar a vigilar muy de cerca sus operaciones. Si se va a tener monitoreo del anfitrión buscando anormalidades que indicarán alguna intrusión, se debe desarrollar un conocimiento del perfil de uso normal de anfitrión, haciéndose los siguientes cuestionamientos:

- ¿ Cuantos trabajos tienden a ejecutarse a la vez ?
- ¿ Cuál es la carga típica en diferentes horas del día ?
- ¿ Cuanto tiempo de CPU consume cada uno de los trabajos ?

Aunque es difícil hacer un trabajo de monitoreo del sistema a fondo, el objetivo es tener el mayor conocimiento en cuanto a la ejecución normal del sistema, para que de una manera rápida se pueda reconocer e investigar una actividad anormal.

2.4.3 FILTRADO DE PAQUETES

Es un mecanismo de seguridad que funciona controlando de forma selectiva el flujo de datos de y hacia una red.

En el filtrado de paquetes se permiten o se bloquean los paquetes mientras se realiza el ruteamiento de los paquetes de una red a otra; basando la verificación de los paquetes en un conjunto de reglas que especifican cuales paquetes pueden accesar nuestra red y cuáles no. Este proceso puede ocurrir en un ruteador, puente o servidor.

El negar o permitir la transferencia de información en el filtrado de paquetes, se basa en lo siguiente:

- La dirección IP de donde proviene la información.

- La dirección IP a donde se dirige la información.
- Los protocolos de nivel de sesión y aplicación que se emplean para transferir información.

El filtrado de paquetes puede emplearse de diversas formas: desde el bloqueo de un anfitrión específico, o una red, o bien el bloqueo de conexiones a puertos específicos.

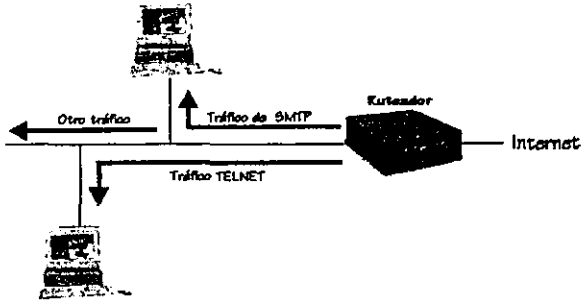


Fig. 2.4.3 Representación del Filtrado de paquetes de SMNTP y Telnet

2.4.3.1 FUNCIONAMIENTO DEL FILTRADO DE PAQUETES

Para comprender el funcionamiento del filtrado de paquetes es necesario tener presente los siguientes conceptos:

Paquete: Se construye de modo que los protocolos de cada nivel lo envuelven, como las capas de una cebolla (encapsulamiento). Y en cada nivel se tienen dos partes: encabezado y cuerpo.

El encabezado contiene información relevante a ese nivel, y el cuerpo la información, que con frecuencia consiste en un paquete completo para el siguiente nivel en el conjunto.

Niveles de TCP/IP: que se analizaran en forma descendente, y particularmente el contenido de los encabezados en cada nivel para una red ethernet.

- Acceso a la red: la información contenida en el encabezado del paquete a este nivel es la siguiente:

  a) El tipo de paquete que es (ethernet, token ring, etc)

  b) La dirección de hardware de la máquina fuente

  c) La dirección de hardware de la máquina destino.

  Teóricamente es posible filtrar la información a este nivel, pero no es de mucha utilidad, ya que generalmente los paquetes externos vienen de una misma dirección de hardware, como podría ser la dirección del ruteador que controla la conexión con internet, o se tendría la situación de contar con múltiples conexiones con diferentes protocolos, dando como resultado la configuración de interfaces distintas con diferentes clases de reglas para los diversos protocolos, como en el caso de contar con conexiones ethernet y FDDI[6].

- Internet: la información contenida en el encabezado es la siguiente:

  a) La dirección IP fuente

  b) La dirección IP destino

  d) El tipo de protocolo IP (tcp, udp, icmp)

  e) El campo de opciones IP

[6] Ver glosario.

Dentro del campo de opciones, que generalmente se encuentra vacío, se buscó desde su diseño que fuera un lugar que incluyera información especial o instrucciones para el manejo del paquete en el caso que no tuvieran un campo especifico en el encabezado. La opción más común a la que se podrían enfrentar los sistemas de protección de perímetro es la de "ruteamiento IP fuente", la cual especifica la ruta que seguirá el paquete hasta su destino, en lugar de permitir al ruteador usar sus tablas de ruteamiento para decidir a donde enviarlo, en los casos de que estas se encuentren dañadas. En la práctica rara vez se utilizan las opciones, salvo en los intentos de los atacantes por esquivar la seguridad.

Otra consideración a este nivel en el filtrado de paquetes es la fragmentación, en la que sólo el primer fragmento contendrá en el encabezado la información para los protocolos de niveles superiores. La reacción a esto, es permitir el paso de fragmentos no iniciales, y filtrar solamente al primer fragmento del paquete. Esto es seguro, pues al eliminarse fragmento inicial, el sistema destino será incapaz de reconstruir el paquete a su estado original, y no aceptara un paquete formado parcialmente. El anfitrión destino guardara los fragmentos en la memoria durante un lapso de tiempo, en espera de la pieza faltante;

esto hace posible que los atacantes usen los paquetes fragmentados en un ataque de negación de servicio.

- Transporte: en este nivel se analizarán los protocolos tcp y udp.

  1) Tcp: Este protocolo proporciona una conexión bidireccional confiable entre dos extremos, y se le da el calificativo de confiable porque cumple con tres garantías al nivel aplicación:

     a) El destino recibe la información de nivel de aplicación en el orden en que se envío

     b) El destino recibe toda la información de nivel de aplicación

     c) El destino no recibe duplicados de ninguna información a nivel de aplicación

  Estas garantías ocasionan cierto costo tanto en tiempo de espera como en desempeño, pues en ambos lados se intercambian datos antes de comenzar la transferencia de información y se lleva un control de estado de la conexión para determinar que información debe enviarse al otro extremo para cubrir lo faltante.

  Y se dice bidireccional porque sobre la misma conexión, un servidor puede contestar las peticiones del cliente, sin necesitar de otra conexión para que el servidor de las respuestas al cliente.

  El encabezado del paquete tcp contiene tres piezas de información

     a) El puerto fuente

b) El puerto destino

c) El campo de banderas tcp

El campo de banderas contiene un bit de interés para el filtrado, el ACK[9]. Al examinarse con una herramienta de filtrado este bit, se puede determinar si un paquete es el que inicia una conexión (si el bit esta apagado) o si es subsecuente (si el bit esta encendido). Este bit se activa siempre que un extremo de la conexión ha recibido información del otro extremo.

El proceso de filtrado se inicia cuando el anfitrión A envía un segmento al anfitrión B con el bit SYN[10] encendido y el bit ACK apagado, al reconocerse el bit de inicio de conexión el paquete es bloqueado. En caso de aceptación el segmento enviado por A indica al anfitrión B que número de secuencia se usará como número inicial de los segmentos, para mantener la información en el orden apropiado. El anfitrión B responde al A con un segmento que tiene encendido el bit SYN y encendido el bit ACK. El segmento enviado por B reconoce la recepción del segmento de A e informa con cuál número de secuencia comenzara el anfitrión B.

La figura 2.4.3.1 ilustra lo anterior.

[9] (Acknowledgment Segment) bit de confirmación de recepción

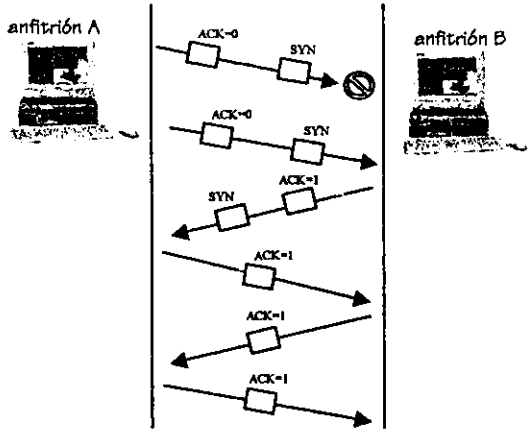


Fig. 2.4.3.1 filtrado de bit Ack en paquetes tcp

2) Udp: el cuerpo de un paquete tcp también puede contener un paquete udp, el cual se dice es no confiable, puesto que no brinda ninguna de las garantías con las que cuenta tcp. El envío de paquetes de esta clase se puede comparar con el envío de tarjetas postales, aunque se tenga la misma dirección en varias tarjetas no se tiene la convicción de que todas llegan a su destino, y las que lleguen no están en el mismo orden en que fueron enviadas, y como no se confirma su recepción, se pueden duplicar.

El encabezado UDP contiene número de puerto fuente y destino como tcp, pero no contiene nada semejante al bit Ack. Para solucionar la falta de este campo lo que se realiza es lo siguiente:

El mecanismo de filtrado debe "recordar" los paquetes udp salientes que ha visto, así puede permitirse que regresen únicamente los paquetes de respuesta correspondientes. Para que se tome como respuesta un

[10] Sincronizar números de secuencia

paquete entrante, debe de ser del anfitrión y puerto a los que se envío el paquete saliente y debe estar dirigido al anfitrión y puerto desde donde se envío el paquete de salida. A esta capacidad de recordar se lo conoce como: "filtrado dinámico de paquetes", pues la regla de filtrado creada para permitir la respuesta son de tiempo limitado y vence después de cierto tiempo. La fig. 2.4.3.2 ilustra lo anterior.

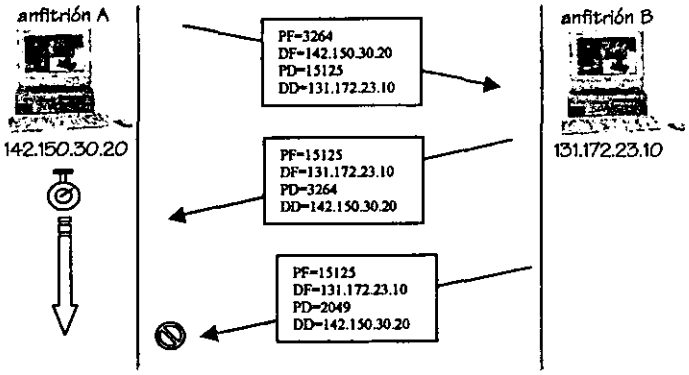


Fig. 2.4.3.2 filtrado dinámico de paquetes udp

- Aplicación: en algunas aplicaciones actuales se puede proporcionar la capacidad de filtrar en protocolos de este nivel, como ejemplo se puede citar una operación ftp, en la que se puede ser capaz de reconocer información específica para instalar filtros dinámicos, o bien se puede comparar la información de un paquete con la aplicación a la que se supone va dirigido.

2.4.3.2 VENTAJAS DEL FILTRADO DE PAQUETES

- La principal ventaja del filtrado de paquetes es el concentrar, ya que permite desde un solo lugar proteger toda la red.
- No se requiere del conocimiento o cooperación del usuario, es traneparente para ellos.
- La capacidad de filtrado de paquetes está disponible en muchos productos para ruteamiento, tanto en hardware como software, comerciales y/o gratuitos.

2.4.3.3 DESVENTAJAS DEL FILTRADO DE PAQUETES

- A pesar de la amplitud y disponibilidad del filtrado de paquetes, aún no se perfeccionan las herramientas actuales que cuentan con esta capacidad, ya que suelen ser difíciles de configurar, y en otras ocasiones una vez configuradas no es fácil de probar.
- Ciertos protocolos, por alguna razón no están diseñados correctamente para el filtrado de paquetes como es el caso de RPC, NFS y NIS/YP.
- Algunas políticas no pueden aplicarse por medio de filtrado de paquetes, un ejemplo de esto, es que se pueden filtrar los paquetes que se dirigen a un puerto definido pero no así la aplicación a la que se dirigen.

2.4.3.4 CONVENCIONES PARA LAS REGLAS DE FILTRADO DE PAQUETES

Para comenzar a crear las reglas, se deben tener en cuenta los siguientes conceptos para convertir las decisiones sobre servicios a reglas sobre paquetes:

1) Editar las reglas de filtrado fuera del sistema: es más conveniente guardar las reglas en un archivo de texto para editarlas ahí, y una vez que se tiene la seguridad de que están correctas, cargar el archivo al sistema de filtrado. Teniendo como ventaja adicional el agregar comentarios en este archivo.

2) Recargar los grupos de reglas desde el inicio cada vez que se modifiquen: para reconstruir el conjunto de reglas existentes, es necesario quitar las reglas usadas anteriormente, para no preocuparse por como interactúan con las nuevas reglas, y así cargar todas nuevamente desde el inicio.

3) Siempre hay que hacer uso de direcciones IP, y nunca los nombres de anfitrión: si se especifica el nombre del anfitrión en las reglas para filtrado, este podría ser alterado si alguien corrompe accidental o intencionalmente la traducción del nombre a la dirección.

4) Es buena idea establecer una regla explícita como valor predeterminado al final de las reglas para el filtrado de paquetes, a fin de no preocuparse que valor predeterminado usará el sistema.

2.4.3.5 TIPOS DE FILTRADO

El filtrado de paquetes trabaja bloqueando paquetes basados en su dirección fuente o destino, o en el puerto fuente. El filtrado puede realizarse en el momento de entrada, salida, o en ambos casos a la vez.

2.4.3.5.1 FILTRADO POR DIRECCIÓN

Es la forma más sencilla pero no la más común de filtrado de paquetes, la cual permite restringir el flujo de paquetes basándose en la dirección fuente y/o destino de los paquetes, sin considerar los protocolos involucrados.

Se emplea para permitir que alguno anfitriones externos se comuniquen con anfitriones internos, y evitar que atacantes introduzcan paquetes falsificados dentro de la red.

Hay dos clases de ataques basados en falsificación de dirección fuente o destino:

(a) Dirección fuente: un atacante envía sus paquetes que dicen venir de alguna dirección fuente confiable, y espera la acción que se tome basada en esa confianza, sin esperar obtener paquetes de regreso, pues las respuestas se enviarán a la dirección que el atacante finge ser y no al atacante. Para que esta actividad se efectúe es necesario que:

- Se realice el ataque cuando la máquina verdadera este fuera de servicio
- Inutilizar la máquina verdadera mientras se realiza el ataque

(b) Hombre en el camino: consiste en establecer una conversación completa afirmando ser un anfitrión confiable. Para hacerlo, la máquina atacante debe ser capaz no sólo de enviarle paquetes sino, también de interceptar los paquetes de respuesta. Para lograrlo se toman las siguientes acciones:

- Interponer a la máquina atacante dentro de la ruta de acceso entre la máquina atacada y la verdadera.
- Alterar la ruta de acceso entre las máquinas para que se dirija a la máquina atacante.

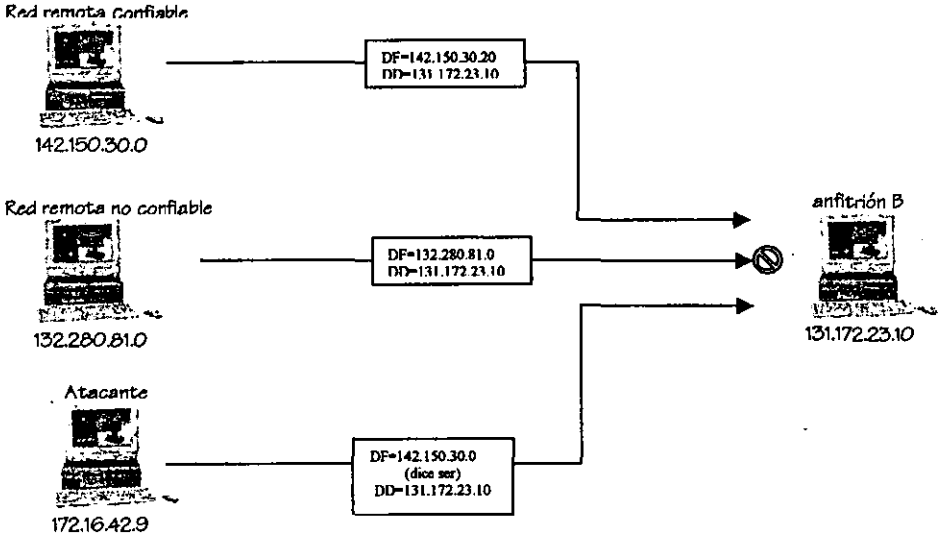


Fig. 2.4.3.3 Filtrado por dirección

2.4.3.5.2 FILTRADO POR PUERTO FUENTE

También llamado filtrado por servicio, pues involucra un tipo de servicio de internet asociado a un número de puerto específico.

Para comprender este caso, se tomara un breve ejemplo basado en el servicio Telnet.

Dirección del servicio	Dirección del Paquete	Dirección Fuente	Dirección Destino	Tipo de Paquete	Puerto Fuente	Puerto Destino	ACK (encendido)
Salida	Salida	Interna	Externa	TCP	>1023	23	X
Salida	Entrada	Externa	Interna	"	23	>1023	Sí
Entrada	Entrada	Externa	Interna	"	>1023	23	X
Entrada	Salida	Interna	Externa	"	23	>1023	Sí

En esta tabla se muestran dos punto de vista, una conexión de un cliente local a un servidor remoto(dirección del servicio de salida) y una conexión de un cliente remoto a un servidor telnet local(dirección del servicio de entrada).

Gráficamente quedaría representada la tabla anterior de la siguiente forma:

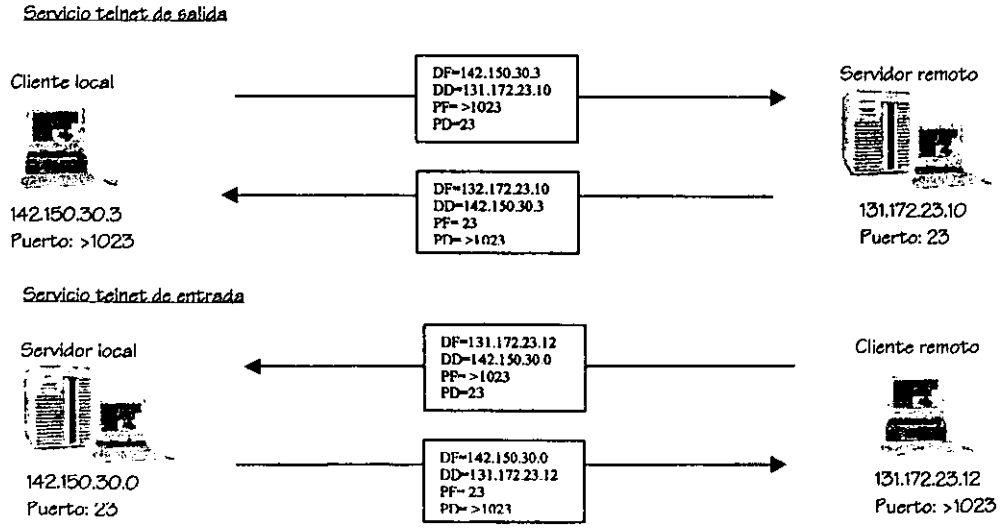


Fig. 2.4.3.4 Funcionamiento del servicio telnet

Si lo que se quiere restringir mediante el filtrado, son las conexiones de clientes remotos al servidor local y bloquear cualquier otra acción, la regla podría quedar de la siguiente forma:

Regla	Dirección del Paquete	Dirección Fuente	Dirección Destino	Tipo de Paquete	Puerto Fuente	Puerto Destino	ACK (encendido)	Acción
A	Entrada	Externa	Interna	TCP	>1023	23	X	Prohibir
B	Entrada	Interna	Externa	TCP	23	>1023	Sí	Prohibir
C	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Prohibir

Gráficamente se mostraría la prohibición de paquetes al servidor local de la siguiente manera:

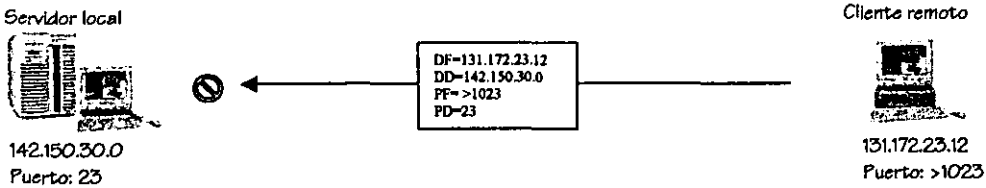


Fig. 2.4.3.5 Filtrado por puerto fuente

Hay un problema en esta clase de filtros: sólo se puede confiar en el puerto fuente tanto como se confía en la máquina fuente.

Una solución posible sería restringir los números de puertos locales lo más posible, sin importar a que tan pocos puertos remotos se les permite el acceso. Si se permiten conexiones entrantes a un puerto "X", que se encuentra en un servidor confiable, no importará si el programa con el que se conversa es en realidad un cliente genuino o no.

2.4.4 SISTEMAS REPRESENTANTES

El uso primario de un servidor representante es permitir el acceso de clientes internos ubicados dentro de un sistema de protección perimetral a internet. Cualquiera dentro del sistema de protección perimetral puede tener acceso total al internet. (con un mínimo esfuerzo y sin comprometer la seguridad) Fig. 2.4.4.1

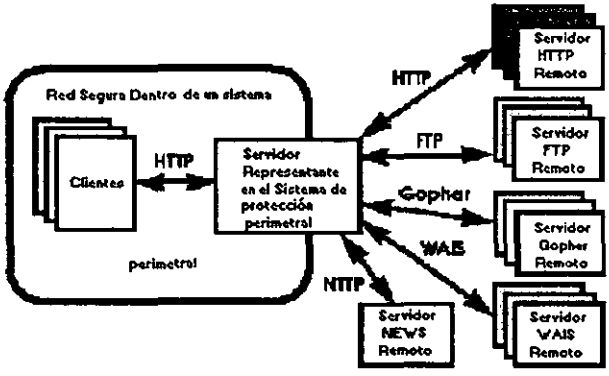


Fig. 2.4.4.1 Estructura total de un sistema representante

Un servidor de este tipo es un servidor HTTP especializado; el servidor representante se sitúa entre una aplicación cliente, como un navegador web y un servidor real de servicio, interceptando las solicitudes de los clientes dentro del sistema de protección perimetral y es el encargado de evaluar las solicitudes del cliente y decidir cuáles deja pasar y cuáles no. Si una petición es aceptada, verifica si puede llevar a cabo la solicitud por sí mismo y si no lo puede realizar envía la petición a él servidor remoto en nombre del cliente, transmitiendo las respuestas del servidor remoto al cliente interno.

En el caso normal, todos los clientes dentro de una subred determinada usan el mismo servidor representante. Esto hace posible que el sistema representante se desempeñe más eficientemente almacenando temporalmente los documentos que son requeridos por un número de clientes. Los usuarios que usan un servidor representante piensan que tratan directamente con el servidor remoto que esta en internet. Fig. 2.4.4.2

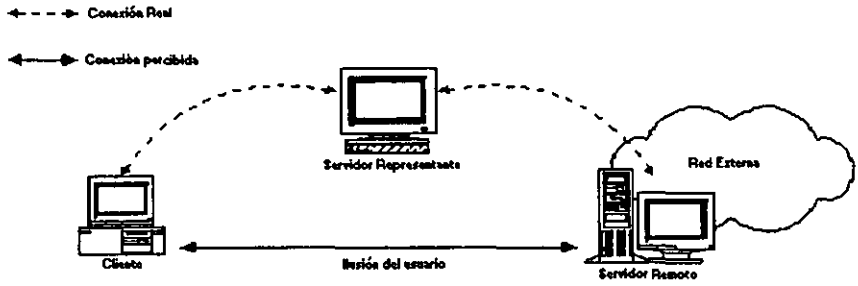


Fig. 2.4.4.2 Sistema representante, realidad e ilusión

Es importante realizar las conexiones a través de un sistema representante junto con algún método de restricción de tráfico IP entre los clientes y los servidores en la red insegura, como un ruteador con filtrado de paquetes o un anfitrión con doble acceso que no proporcione ruteo de paquetes. Ya que si existe conectividad a nivel IP entre clientes y servidores de la red insegura, los clientes pueden saltarse el servidor representante y también producirse ataques desde el exterior.

2.4.4.1 FUNCIONALIDAD

Se puede hacer uso de un servidor representante para:

- Permitir y restringir el acceso de clientes al Internet basándose en la dirección IP del cliente
- Almacenar documentos para solicitudes internas
- El controlar selectivamente el acceso al Internet y a las subredes basándose en el URL presentado
    a) Especificando URLS o máscaras de URL, que no se quiere que el servidor accese.
    b) Decidir que solicitudes aceptar y cuales rechazar
    c) Especificando a ciertos clientes los protocolos que pueden usar. Por ejemplo, se podría permitir a ciertos clientes (con base en sus direcciones IP) hacer peticiones HTTP pero no permitirles usar FTP.
- Conversión de la información a formato HTML que es legible para los navegadores.
- Proveer acceso a Internet a compañías que usan redes privadas.

2.4.4.1.1 OPERACIONES WEB MEDIANTE UN SERVIDOR REPRESENTANTE

Para ejemplificar esta actividad, es necesario explicar primero una operación web normal sin la intervención de un servidor representante.

Cuando una petición HTTP normal es hecha por un cliente, el servidor HTTP obtiene únicamente la ruta y el nombre del servicio solicitado en el URL; otras partes como el nombre del protocolo, específicamente "http:" y el nombre del anfitrión son borrados por el servidor HTTP remoto --- ya que sabe que es un servidor HTTP, y sabe que el anfitrión esta en ejecución ("corriendo"). La ruta solicitada, especifica el documento o un script CGI[11] en el sistema de archivos local del servidor, o algún otro recurso disponible en ese servidor (fig. 2.4.4.3). Ejemplo:

Petición HTTP normal hecha por el cliente:

http://micompania.com/información/servidorproxy_Detalles.html

El servidor obtiene solamente la ruta y el nombre del recurso solicitado:

GET /información/ servidorproxy_Detalles.html

(El cliente se conecta al servidor ejecutándose en: micompania.com se emite la solicitud y espera una respuesta que puede ser un documento o un mensaje de error).

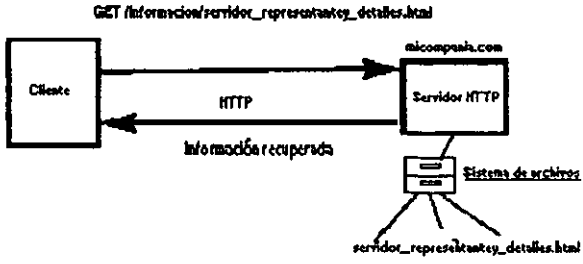


Fig. 2.4.4.3 Operación HTTP

[11] ver glosario.

Ahora cuando un cliente envía una solicitud al servidor representante la situación es ligeramente diferente, pues tiene la capacidad de actuar como ambas partes, como sistema servidor y como un sistema cliente.

Es un servidor cuando acepta las solicitudes HTTP de los clientes conectados a él, y actúa como sistema cliente al conectarse a servidores remotos para recuperar los documentos para sus clientes.

El servidor representante usa los campos del encabezado enviados por el cliente sin modificación cuando se conecta al servidor remoto, por lo que el cliente no pierde ninguna funcionalidad cuando pasa a través del servidor representante.

En vez de especificar solamente el nombre de la ruta y buscar el nombre del recurso en el servidor representante, el URL es especificado completamente.

De esta manera el servidor representante tiene toda la información necesaria para hacer la solicitud al servidor remoto, especificado en la solicitud URL, usando el protocolo especificado en el mismo. Ejemplo:

Cuando un usuario introduce un URL completo:

http://micompania.com/información/servidorproxy_Detalles.html

El cliente convierte el URL a:

GET http://micompania.com/información/servidorproxy_Detalles.html

El cliente se conecta al servidor representante que provee la conexión al Internet.

El servidor representante convierte este solicitud a:

GET /información/servidorproxy_Detalles.html

El servidor representante se conecta al servidor remoto ejecutándose en micompania.com, emite el comando y espera una respuesta, devuelta la respuesta el servidor representante, reenvía la respuesta al cliente. (fig. 2.4.4.4)

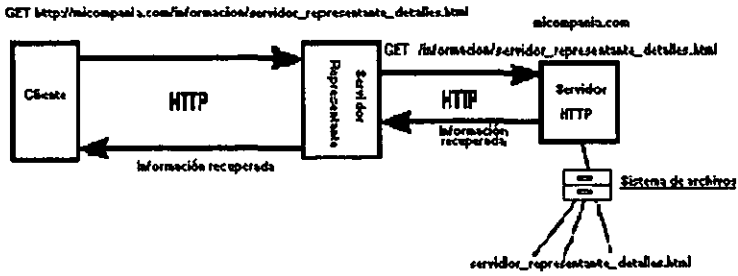


Fig. 2.4.4.4 Operación HTTP mediante un servidor representante

Un servidor representante completo debe ser capaz de comunicarse con todos los protocolos web, ya que los clientes siempre usan HTTP para las operaciones con el servidor, incluso cuando accesan a recursos que usan otros protocolo como ftp. Ejemplo:

Un cliente usando HTTP solicita por medio de un servidor representante un documento en un servidor FTP en la Internet. El servidor representante ve desde el URL completo que debe hacer una conexión FTP. El servidor representante hace la conexión y recupera el archivo del servidor FTP remoto y lo envía al cliente usando HTTP. En este caso, el servidor representante devuelve un directorio FTP listado como un documento HTML. (fig. 2.4.4.5)

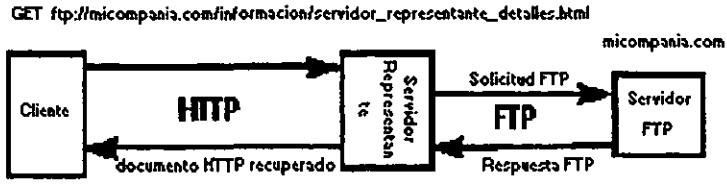


Fig. 2.4.4.5 Una operación ftp mediante un servidor representante

La única diferencia entre una operación HTTP normal y una a través de un servidor representante es que la operación HTTP ruteada a través de un servidor representante requiere un URL completo.

2.4.4.1.2 ALMACENAMIENTO TEMPORAL DE DOCUMENTOS

La idea básica en el almacenamiento es simple: guardar los documentos recuperados en un archivo local para su uso posterior, por lo que no será necesario conectarse al servidor remoto la próxima vez que se solicite el documento (Fig. 2.4.4.6)

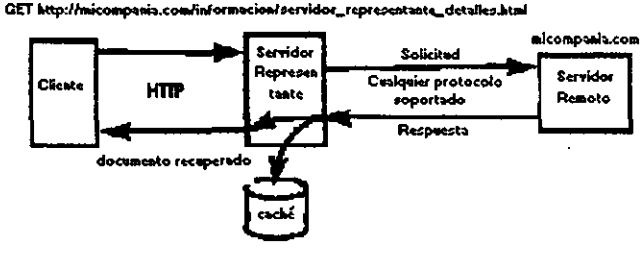


Fig. 2.4.4.6 El documento solicitado es recuperado del servidor remoto y almecenado localmente en el servidor representante, para su uso posterior

Cuando un cliente local pide un archivo, el servidor verifica su cache para ver si tiene el documento, si el archivo existe en el cache, el servidor envía la copia local al cliente (fig. 2.4.4.7).

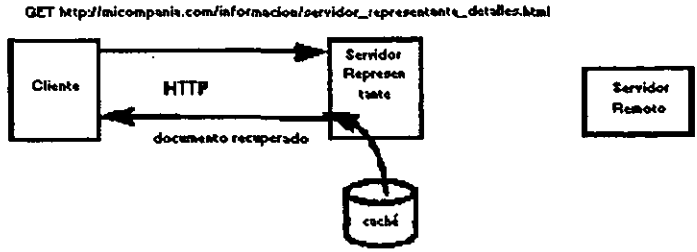


Fig. 2.4.4.7 El documento almecenado localmente en el servidor representante, es enviado a solicitud de un cliente

El almacenamiento de documentos en el caché puede ahorrar considerable tiempo a los usuarios cuando solicitan documentos normalmente ubicados en la Internet. Un servidor representante puede enviar estos documentos mucho más rápido que los servidores remotos. En adición, guardar un documento que muchos usuarios necesitan puede ahorrar considerablemente el costo de red y tiempo de conexión. El almacenamiento puede ahorrar la cantidad de espacio en disco utilizado, porque únicamente existe una copia almacenada en el servidor representante y no en cada uno de los clientes locales y a la que varios de ellos pueden accesar simultáneamente.

Sin embargo, hay muchos problemas que necesitan ser arreglados una vez que el almacenamiento es agregado, como:

1.- ¿Decidir que documentos valen la pena almacenar?

2.- ¿Cuánto tiempo es posible guardar esos documentos en él caché y todavía estar seguro de que son actualizados?

Actualmente muchos de los documentos disponibles en la Internet son documentos "vivientes", determinar cuando deben ser actualizados o borrados es generalmente una tarea difícil.

Algunos de estos documentos pueden permanecer estables por un largo tiempo y repentinamente cambiar, o bien cambiar diariamente o cada semana; estos cambios pueden haber sido de manera imprevista por el autor del documento sin reflejarse en la información de vencimiento. Lo que implica tomar decisiones cuidadosas de con que frecuencia se actualizan o borran los documentos almacenados en él caché.

2.4.4.2 VENTAJAS Y DESVENTAJAS DE LOS SISTEMAS REPRESENTANTES

Ventajas:

a) Permiten el acceso "directo" a Internet

Al utilizar un servidor representante, los usuarios pueden conectarse de una forma transparente a un servidor en internet de forma directa, sin que se den cuenta que están pasando por una máquina intermedia; el servidor representante.

b) Registros del sistema

Gracias a que los servidores representantes trabajan a nivel aplicación resulta fácil generar registros o monitorear las conexiones de los usuarios a cada tipo de servicio de forma efectiva.

Desventajas:

a) Disponibilidad de sistemas representantes para nuevos servicios

Debido a que es necesita un programa representante específico para cada tipo de servicio; resulta problemático utilizar servicios de reciente aparición, porque existe un rezago entre la introducción de un nuevo servicio y la disponibilidad de un sistema representante para él. Obstaculizando que se pueda brindar ese servicio inmediatamente después de estar disponible.

b) Dependencia del servicio

Puede ser necesario utilizar un servidor representante exclusivo para cada protocolo, para que pueda desempeñarse de manera eficiente como servidor ante el cliente y como cliente ante el servidor remoto del servicio especifico, determinando así lo que esta permitido y lo que no lo esta. La instalación, configuración y administración de varios servidores puede requerir mucho trabajo. Por otra parte existen servicios para los cuales difícilmente existirá alguna vez un servidor representante, como es el caso de talk que tiene interacciones complicadas y desordenadas entre cliente y servidor.

c) Modificaciones en los clientes

El uso de un servidor representante requiere la modificación o configuración de los clientes, requiriéndose tiempo y trabajo. Esta clase de modificaciones no siempre pueden utilizar las herramientas disponibles con sus instrucciones normales. Por ejemplo: al iniciar una sesión ftp con un cliente TIS, primero se hace la conexión con el servidor representante, en lugar del sitio ftp al que se quiere accesar (en este caso ftp.greatcircle.com), después en el indicador de sistema además de especificar el nombre de usuario, también se debe indicar el nombre del verdadero servidor ftp, por lo

que en lugar de escribir anonymous únicamente en el indicador de sistema, se tecleará anonymous@ftp.greatcircle.com

En la actualidad los clientes HTTP (como el caso de los navegadores) de última generación incluyen la opción de centralizar las configuraciones en los sistemas representantes.

Desde un puesto de trabajo, el administrador puede cambiar la configuración del servidor representante afectando estás modificaciones a todos los clientes de forma automatizada.

2.4.4.3 TIPOS DE SERVIDORES REPRESENTANTES

1) Servidores representantes a nivel aplicación

Un sistema representante a nivel aplicación hace a un sistema de protección perimetral sin riesgo y transparente para los usuarios de una organización, sin crear agujeros de seguridad potenciales a través de los cuales los intrusos lograrían penetrar en la red de la organización.

Permite el registro de las operaciones de los clientes, incluyendo la dirección IP, fecha y hora, y el URL. Puede controlar el acceso a servicios para métodos individuales, anfitriones y dominios, etc.

Facilita el almacenamiento temporal de información, que hace posible el uso del web cuando algunos servidores externos, están desconectados, y agiliza la recuperación de información en el caso en que la conexión a un sitio exista mucho tráfico.

En general, los sistemas representantes a nivel aplicación emplean procedimientos modificados, obteniendo la información necesaria para conectarse al servidor exterior del protocolo de aplicación.

Este tipo de servidor se tomo como referencia para los puntos 2.4.4.2 y 2.4.4.3.

2) Servidores representantes a nivel circuito

Un sistema representante a nivel circuito crea un circuito entre el cliente y el servidor sin interpretar el protocolo de aplicación. La vereión más avanzada de un sistema representante a nivel circuito actúan como servidor representante para el exterior pero como ruteador con filtrado para el interior.

Los servidores representantes a nivel circuito emplean clientes modificados ya que no pueden interpretar el protocolo de aplicación directamente y necesita que le proporcionen información como la de la dirección destino.

La ventaja de un sistema representante a nivel circuito es que proporciona servicios para una amplia gama de protocolos, adaptándose para servir casi a cualquier protocolo.

La desventaja de un servidor representante a nivel circuito es que proporciona muy poco control sobre lo que circula a través del mismo. Al igual que el filtrado de paquetes, controla las conexiones con base a la dirección fuente y destino y no puede determinar fácilmente si los comandos que están pasando a través de él son seguros o están en el protocolo esperado.

3) *Servidores representantes genéricos y dedicados*

Un servidor representante dedicado funciona para un único protocolo, mientras que uno genérico sirve para varios protocolos. En la práctica los servidores representante dedicados son a nivel aplicación y los genéricos son a nivel circuito.

4) *Servidores representantes inteligentes*

Se denomina servidor representantes inteligente a aquellos que son capaces de hacer algo más que transmitir solicitudes. Como por ejemplo funciones de caché de datos (páginas web, archivos de ftp, etc). Generalmente los servidores representantes inteligentes son servidores dedicados a nivel aplicación.

5) *Servidores representantes vinculados a Servidores representantes*

Vincular servidores representantes permite ejecutar un servidor representante como un "cache" local en nombre de un departamento dentro de una organización. Los departamentos individuales tienen control sobre el servidor y el "cache".

Estos servidores representantes departamentales pueden conectarse a un servidor representante en un sistema de protección perimetral entre el Internet y la organización. Este servidor representante se conecta a al Internet como se muestra en la Fig. 2.4.4.8

Cualquier restricción para el acceso determinada por el servidor representante de la organización tiene precedencia sobre las restricciones de acceso determinadas por los servidores representantes departamentales.

Por ejemplo, el servidor representante departamental 1 podría establecerse para permitir todas las solicitudes URL, y el servidor representante organizacional, de acuerdo con las políticas corporativas podría negar todas las solicitudes URL para ciertas publicaciones en línea. Una solicitud para una de estas publicaciones que viene de los clientes del servidor representante 1, se remitiría a él servidor representante de la organización, el cual negaría la solicitud.

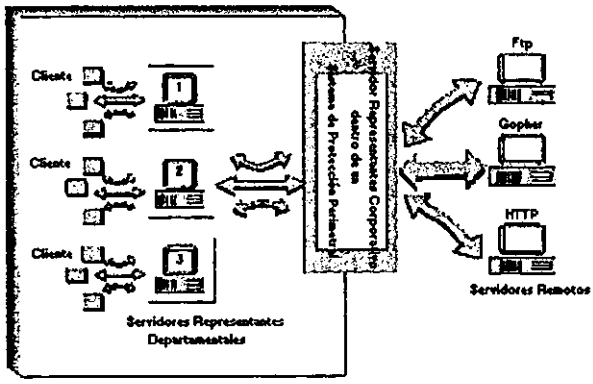


Fig. 2.4.4.8 Servidores representantes vinculados

Y viceversa, el servidor representante 1 podría configurarse para negar URLS dirigidos a un sitio FTP designado, mientras los servidores 2 y 3 y el servidor organizacional, tienen permitido el acceso al sitio.

2.4.4.4 USO DE SOCKS PARA SISTEMAS REPRESENTANTES

Un sock es una librería de software adicionada a aplicaciones individuales para la comunicación segura a través de los sistemas de protección perimetral; puede ser usada con cualquier aplicación tcp virtual, incluyendo los navegadores web y los

clientes ftp. Suministra un sistema de protección perimetral simple porque verifica los paquetes de entrada y salida y oculta la dirección ip de las aplicaciones cliente.

Socks requiere de clientes modificados. Para facilitar el soporte de nuevos clientes, es excesivamente genérico, razón por la cual se ha popularizado, pero tiene la desventaja de que no puede proporcionar acceso inteligente o control de acceso.

Cuando brinda el acceso al sistema, la mayor parte se efectúa en el cliente, haciendo difícil la reunión de la información en una sola parte para examinarla.

Lo que si puede registrar socks ,son las solicitudes de conexión en el servidor, proporcionando control de acceso por dirección fuente del anfitrión y protocolo destino; permitiendo respuestas configurables para las negaciones de acceso. Por ejemplo, se puede configurar para notificar a un administrador los intentos para tener acceso de entrada y para indicar a los usuarios por qué fueron negados sus intentos para tener acceso de salida.

Una de las desventajas que presenta es que funciona sólo para clientes basados en TCP y no funciona para clientes basados en UDP.

El apoyarse en socks, por estar disponible en forma gratuita, además de encontrar ayuda fácilmente para el uso de servidores y clientes de esta aplicación, puede resultar un arma de dos filos, pues se han reportado casos en donde los intrusos han instalado sus propios clientes, en sitios con sistemas de protección perimetral..

Socks está formado por los siguientes componentes:

a) El servidor de socks

b) La librería para clientes Socks (Unix, Windows, etc)

c) Las versiones tipo Socks de clientes FTP, Telnet, etc.

Para convertir un programa cliente que soporte socks, es necesario modificarlo para que se comunique con el servidor de socks, en lugar de hacerlo con el servidor externo, reemplazando todas las llamadas a funciones estándar de red con llamadas a las versiones de socks de esas funciones.

Los socks también sufren de una ejecución incómoda, por el proceso redundante, similar a la de los sistemas representantes de aplicación.

2.4.5 SISTEMAS DE AUTENTIFICACIÓN

Los sistemas de protección de perímetro realizan su autentificación mediante el uso de direcciones IP, que son asignadas a cada servidor, cliente y dispositivo de red y que pueden ser burladas.

Por lo que si se requiere dar acceso remoto a los usuarios a través de Internet, hacia archivos y datos internos sensibles, se debe de asegurar de autentificar al usuario real.

La autentificación es el proceso que comprueba una identidad. Esto es distinto a la declaración de identidad (conocido, suficientemente razonable, como identificación) y de la decisión de cuáles son los permisos a otorgar a la identidad (autorización).

Mientras que estos conceptos son importantes, autentificación es el más engañoso desde el punto de vista de seguridad de redes. Dentro de este tema hay dos

formas de autentificación, la de un usuario a una máquina durante la secuencia inicial de conexión y la autentificación máquina a máquina durante la operación.

La autentificación simplemente describe los diversos métodos que identifican positivamente a un usuario.

El nivel de autentificación dependerá de la importancia del bien y del costo del método.

2.4.5.1 AUTENTIFICACIÓN DE USUARIOS

a) Contraseñas: son el método más común como medio de autentificación personal que se utiliza actualmente y están clasificadas como "*algo que se conoce*". Esto es una ventaja porque no se requiere el uso de equipo especial, y representan una desventaja porque los usuarios se distinguen por hacer selecciones de contraseñas deficientes, y por eso pueden ser adivinadas por intrusos con experiencia, además, de que pueden ser divulgadas a alguien más o bien pueden ser robadas.

b) Contraseñas de una sola vez: se puede conseguir un incremento significativo en seguridad valiéndose de contraseñas de un solo uso. Se comportan como su nombre lo indica: se usa exactamente una vez, después de lo cual ya no es válida. Esto provee una defensa muy fuerte contra espionaje.

Hay dos formas en que puede funcionar un sistema de esta clase: en la primera la lista se puede generar al azar y guardarse una copia para el usuario y otra para el sistema, y en la segunda la lista puede generarse a petición del usuario y ser validada por el sistema.

El problema de contar con una lista en el sistema es que si éste se compromete, también se compromete la lista, y esta puede ser usada entonces para tener acceso futuro. Esto es tan peligroso, como que alguien monitoree mientras se hace uso de una contraseña reutilizable.

Para solucionar este problema se desarrollo el sistema s/key[12] que autentifica de modo confiable a un usuario, sin que haya nada en el sistema que comprometa la contraseña del mismo, aún cuando el propio sistema este comprometido. Ya que tiene la habilidad de validar la respuesta actual del usuario, pero no la tiene para predecir cuál será la siguiente respuesta del usuario.

S/key usa un algoritmo conocido como md4[13]. Funciona comenzando con una semilla (que se puede generar al azar o la puede proporcionar el usuario). Y aplicando el algoritmo md4 iterativamente para obtener una secuencia de claves. Se aplica md4 a la semilla para obtener la primera clave, se vuelve a aplicar md4 a la primera clave para obtener la segunda, y así sucesivamente. Para autentificar al usuario el sistema debe saber alguna clave en la secuencia (n). El sistema pide al usuario la clave previa (n-1), aplica md4 a la respuesta del usuario y verifica que el resultado sea la clave (n) que conoce, como se muestra en la siguiente figura 2.4.5.1.

[12] es un esquema basado en contraseñas de una sola vez, diseñado por Leslie Lamport y desarrollada por Bellcore.

[13] MD4, quiere decir la función núm. 4 de Message Digest y fue desarrollado por Ron Rivest, inventor del algoritmo RSA.

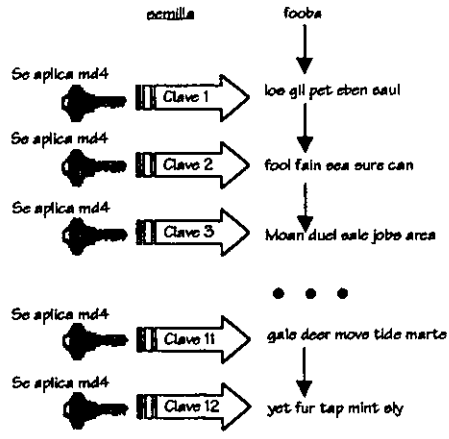


Fig. 2.4.5.1 Funcionamiento de s/key

2.4.5.1.1 TARJETAS INTELIGENTES

Además de las contraseñas, muchas organizaciones están cambiando a soluciones que también requieren *"algo que se tiene"*, como son las estafetas[14] y las tarjetas inteligentes ("smart card").

Una tarjeta inteligente es un dispositivo portátil similar a una estafeta, excepto que requieren de un lector de tarjeta inteligente para procesar el reto, además de que contiene una unidad de procesamiento central -- CPU-- que actualmente tiene la capacidad de almacenar y asegurar información, y "tomar decisiones," como es requerido por la aplicación específica de la tarjeta emisora y algunos puertos de entrada/salida.

Como las tarjetas inteligentes ofrecen la capacidad de "leer/escribir" nueva información puede agregarse y procesarse. Si el lector es sincronizado adecuadamente

[14] ver glosario

Lo atractivo de usar esta clase de identificación, es que se puede usar sin ser robada o divulgada.

En la práctica hay algunas limitaciones, ya que la experiencia en la seguridad convencional nos dice que los datos de la autenticación deberían cambiarse regularmente. Esto es imposible de hacer con la mayoría de las clases de autentificación por biometría.

Algunos otros métodos han encontrado resistencia por parte de los usuarios, como ha sido el caso de la huella de labios. También, por su misma naturaleza, la biometría no da respuestas exactas. Dos firmas de un mismo individuo no son absolutamente idénticas, descartándose para este caso en particular, efectos tales como: el cansancio, el mal humor, o enfermedad.

Ciertos sistemas usan tarjetas inteligentes para almacenar los datos biométricos sobre cada usuario. Esto evita la necesidad de contar con una base de datos en un anfitrión, en vez de esto se confía en la seguridad de la tarjeta para impedir alteraciones. Es también posible incorporar un reto aleatorio desde el anfitrión remoto entre la tarjeta inteligente y el usuario, para evita la repetición de ataques.

Hasta el momento se desconoce alguna clase de sistema biométrico en aplicaciones comunes en internet.

La tecnología más tentadora es el de la voz, pues es usual que hoy en día las máquinas tengan micrófono. Pero tampoco es universal y no se puede tener la garantía que cada máquina a la que se quiere accesar cuenta con micrófono, y mucho menos la aplicación para digitalizar y transmitir su propia voz.

Fig. 2.4.5.4 Técnica biométrica de reconocimiento

2.4.5.2 AUTENTIFICACIÓN DE ANFITRIÓN A ANFITRIÓN

La forma dominante de autenticación de anfitrión a anfitrión en internet hoy día, es confiar en la red. Esto es, la red por si misma no transmite la identidad del usuario remoto, pero se presume que puede ser lo suficientemente exacta como para usarla como un autentificador de identidad, lo cual suele ser peligroso.

La autenticación de red por sí misma entra en dos conceptos, la basada en la dirección y la basada en el nombre.

Para lo primero, las direcciones ip numéricas fuentes se aceptan. Los ataques que se usan en este punto, consisten en el envío de algo desde una dirección

fraudulenta. La exactitud de la autenticación de este modo se limita en la dificultad de detectar imitaciones y detectarlas suele ser muy difícil.

La autentificación basada en el nombre es todavía más débil. Requiere que no solamente la dirección sea correcta, sino también el nombre asociado con la dirección.

Esto abre una forma diferente de ataque para los intrusos: corrompiendo cualquiera de los mecanismos que se usan para relacionar las direcciones ip a los nombres de los anfitriones. Los ataques sobre el dns intentan explotar este camino.

2.4.5.2.1 ENCRIPTACIÓN

La encriptación permite tener conexiones seguras sobre canales inseguros, ya que al encriptar el tráfico de la red se crean dos garantías, la privacidad y la autentificación. La privacidad se da cuando el extremo emisor encripta la información que se transmitirá por la red y el receptor la desencripta, permaneciendo confidencial para quienes huemean en la red. La autentificación aunque menos clara, sucede básicamente al desencriptar la información, pues al realizar esta acción se sabe si proviene del emisor confiable.

Hay varios niveles en donde se puede dar la encriptación a lo largo de internet:

a) A nivel aplicación.- requiere de soporte en todas las aplicaciones (tanto clientes como servidores), en las que se desee emplear y puede ser un método efectivo si se tiene una o dos aplicaciones en uso constante (y que son de partícular atención) a través de internet, entre un número pequeño

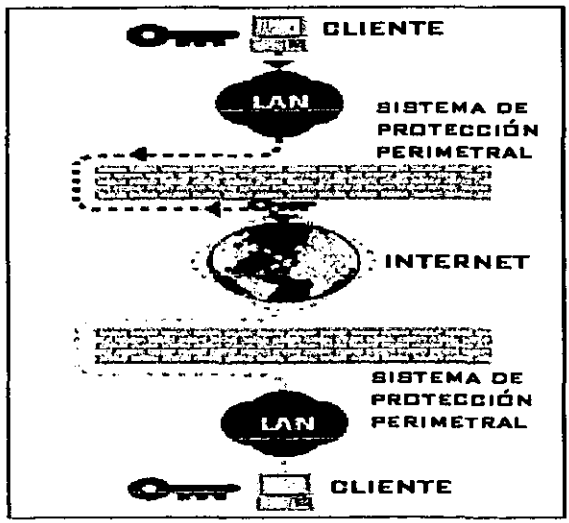
de máquinas, ya que se puede instalar la versión a la medida de la aplicación y de encriptación entre los clientes y servidores de las máquinas.

b) A nivel de enlace.- como su nombre lo indica, esta forma de encriptación protege un enlace individual. Esto es una combinación de fortaleza y debilidad. Es fuerte, porque (para ciertos tipos de hardware) el paquete completo es encriptado, incluyendo la dirección fuente y destino. Protegiéndolo contra el análisis de tráfico, una forma inteligente que opera registrando quien habla a quien. Bajo ciertas circunstancias - por ejemplo, la encriptación de un enlace punto a punto- incluso la existencia del tráfico puede ser disfrazado. Sin embargo, la encriptación de un enlace sufre de una debilidad seria: protege exactamente una conexión a la vez y mientras atraviesa esa línea. Los mensajes están expuestos al pasar por otras líneas, ruteadores u otros anfitriones intermedios. Aún cuando están demasiado protegidos por los encriptadores, los mensajes permanecen vulnerables mientras se encuentren en el nodo conmutador. La encriptación de enlace es el método de elección para la protección estrictamente de tránsito local(un cable coaxial compartido) o para la protección de un número pequeño de líneas altamente vulnerables. Los circuitos satelitales son un ejemplo típico, ya que son circuitos transmisores transoceánicos que pueden ser conmutados al satélite base para hacer respaldos en cualquier momento.

c) A nivel de red.- todo el tráfico de red entre dos sitios en los que se confía se encripta en un extremo, se envía a través de una red intermedia en la que no se confía y luego se desencripta en el otro extremo. La desencriptación se realiza por medio de ruteadores u otros aparatos de red en el perímetro de cada sitio de confianza. Un sistema de protección perimetral es el lugar natural para hacer encriptación a este nivel. Para el intercambio de información entre sitios confiables, no se encripta, en caso contrario se requiere que se encripten, para que por lo tanto sean privados (no legibles para quienes no tengan las claves) y autentificados (solamente pueden ser enviados por quien conoce la clave).

CAPÍTULO 3

EJEMPLO DE UNA BARRERA DE PROTECCIÓN



El tonto dice: " No pongas todos los huevos en una canasta", pero el hombre sabio dice:"Coloca todos los huevos en una sola canasta y vigila la canasta"

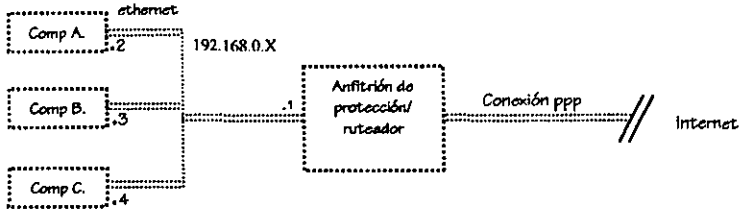
- Puddin'head Wilsons's Calendar

CAPÍTULO 3. EJEMPLO DE UNA BARRERA DE PROTECCIÓN

Se explicará el diseño de un sistema de protección perimetral basado en filtrado de paquetes para propósitos ilustrativos del presente trabajo. Aunque proporcionará protección a una red interna para algunos puntos, se hace hincapié en no considerarlo como una solución completa y robusta de un sistema de protección perimetral.

3.1 MARCO REFERENCIAL

Para este ejemplo se considera el siguiente escenario:



Donde se cuenta con una conexión PPP, que además de suministrar la información de internet, nos permite conectarnos con el sistema remoto con el cual se está interesado intercambiar información.

El sistema de protección es la puerta de enlace para todas las computadoras de la red interna (computadoras A, B y C), para alcanzar internet. La red interna usa un de las direcciones de red privada (RFC-1918[1]); para este caso se hace uso de una dirección de red de clase C, 192.168.0.0.

El sistema de protección perimetral, tiene como sistema operativo, Linux, y las computadoras que componen la red interna pueden ejecutar cualquier sistema

[1] Solicitud para comentarios 1918, asignación de direcciones ip para redes privadas

operativo que pueda comunicarse vía TCP/IP, como win 95,win 98,win NT, macintosh o bien el mismo linux.

Como sistema de protección se utiliza una sola máquina con doble acceso, como anfitrión de protección y ruteador exterior (puesto que se cuenta con una conexión PPP conmutada con internet, es posible ejecutar un sistema de protección de paquetes y permitirle actuar como anfitrión de protección y como ruteador). Esta arquitectura es equivalente en función a la configuración de dos máquinas: el anfitrión de protección y el ruteador exterior, descrita para la arquitectura de anfitrión de defensa.

Aunque el uso del anfitrión para rutear el tráfico no dará el rendimiento o la flexibilidad de un ruteador dedicado, no se requiere mucho de ambas cosas, teniendo una conexión de bajo ancho de banda.

El fusionar el anfitrión de protección con el ruteador exterior, no crea nuevas vulnerabilidades, pero si expone aún más al anfitrión de protección, el cual esta protegiéndose únicamente por filtrado de paquetes, por lo que se requiere de atenciones adicionales para su protección.

3.2 ARQUITECTURA

La arquitectura que se maneja es la de defensa, por los siguientes motivos:

- Se usa frecuentemente en sitios muy pequeños con limitantes de costo importantes.
- Es una alternativa de menor costo, que la de subred de protección, pues no requiere de una red de perímetro, ni de un ruteador interno, lo cual provoca una disminución de seguridad.
- En la arquitectura de defensa con frecuencia, el anfitrión de protección no se dedica exclusivamente a esta tarea, en nuestro caso se hará uso del anfitrión para proporcionar los servicios de correo y DNS del sitio.

3.3 POLÍTICAS

El sistema se construye basándose en las siguientes políticas y suposiciones:

- No se confía en nadie en la Internet
- No se confía plenamente en los sistemas de seguridad del proveedor de internet para mantener la red local segura
- Se confía que los usuarios de la red no intentaran burlar el sistema de protección y que no se requiere monitorear o acceder a sus actividades en internet.
- Se permitirán los servicios que se consideran como básicos (telnet, ftp, smtp, http y dns), y los restantes permanecerán sin estar disponibles.
- No se confía en ninguno de los sitios, que no sean exclusivamente con los que se desea intercambia información.
- Se confía que se respetara la privacidad de cada uno de los integrantes de la organización.
- Se hará uso del equipo solamente para fines relacionados, con el desarrollo personal de los individuos de la organización, y no para el detrimento de intereses de terceros.

3.4 REGLAS DE FILTRADO DE PAQUETES

De forma previa a la organización de las reglas, se explicará que es lo que se desea proporcionar de cada servicio.

1. Telnet. Solo se proporcionara este servicio de salida a servidores confiables y no de entrada, pues si se permitiera el servicio de entrada se estaría comprometiendo a toda la red, pues afectaría directamente al anfitrión. El servidor usa el puerto 23 y el cliente puertos mayores al 1023.

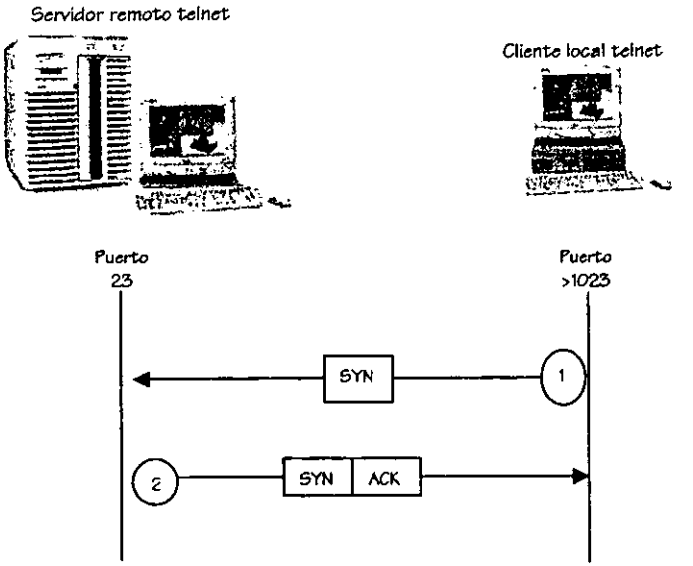


Fig. 3.1 Servicio telnet

2. Ftp. Como se trata de un sitio pequeño, se trabajara el ftp en modo "pasivo", y al igual que en el telnet, se prohibe el servicio de entrada. Como comentario adicional este servicio usa dos conexiones, una de ellas transporta comandos y resultados entre el cliente y el servidor (canal de comandos); otra transporta cualquier archivo real y lista de directorios transferido (canal de datos). El servidor usa los puertos 20 y 21, para datos y comando respectivamente, y el cliente usa puertos mayores a 1023 para comandos y datos. El navegador netscape, utiliza un cliente ftp integrado que utiliza el modo pasivo.

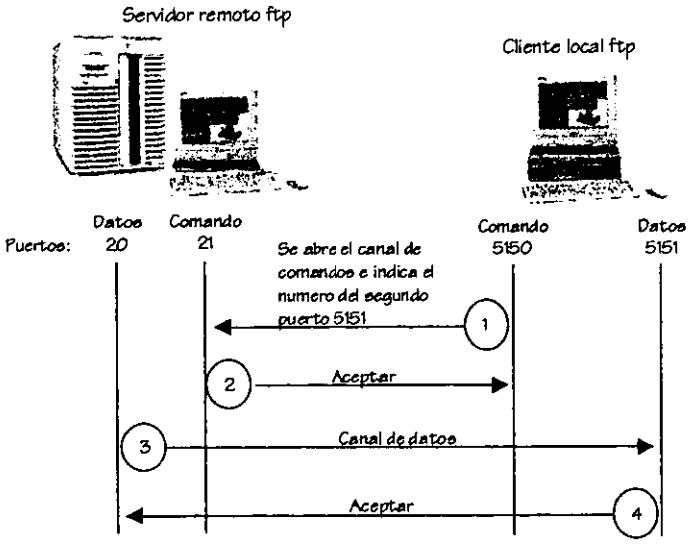


Fig. 3.2 Ftp en modo "normal"

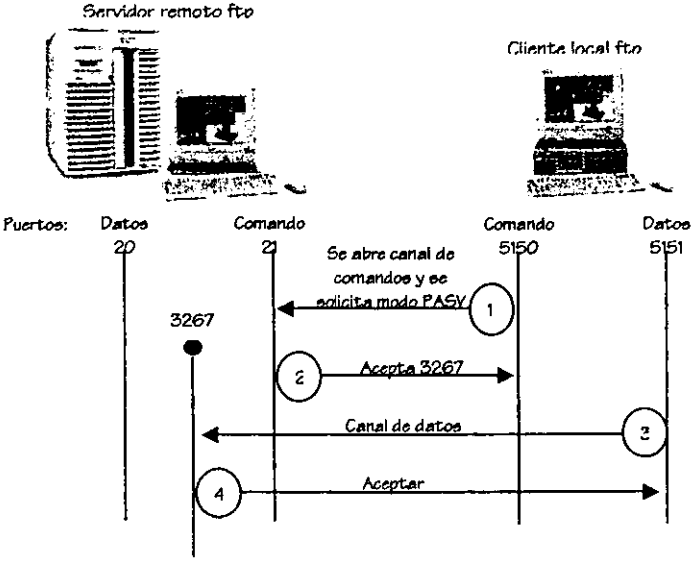


Fig. 3.3 Ftp en modo "pasivo"

3. Smtp. En esta arquitectura, probablemente exista solo un modo de configurar SMTP, el correo de entrada debe dirigirse al anfitrión y el correo de salida debe salir a través del mismo. Realmente no existiría otra alternativa, pues no es recomendable permitir que el correo entrante vaya directamente a todas las máquinas internas, además de que una vez dirigido el correo de entrada a través de un solo punto, se facilita rutear el correo de salida por ahí.

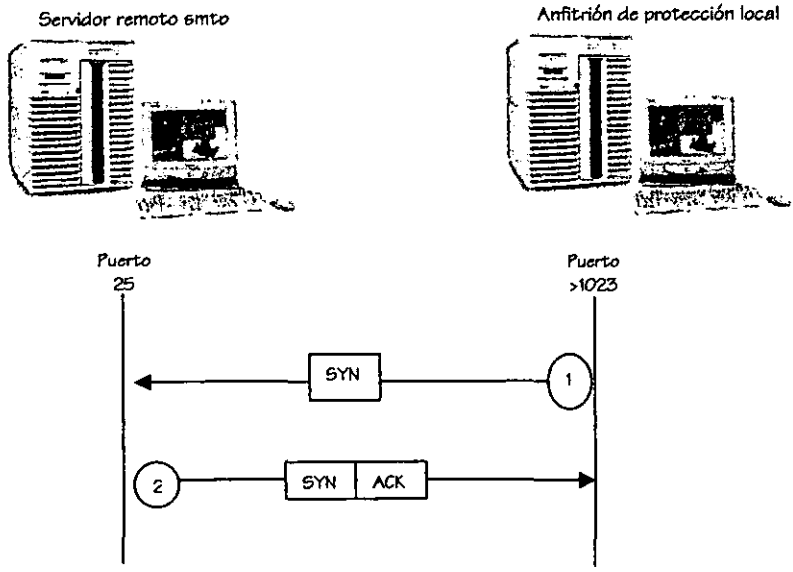


Fig. 3.4 Servicio smtp de salida

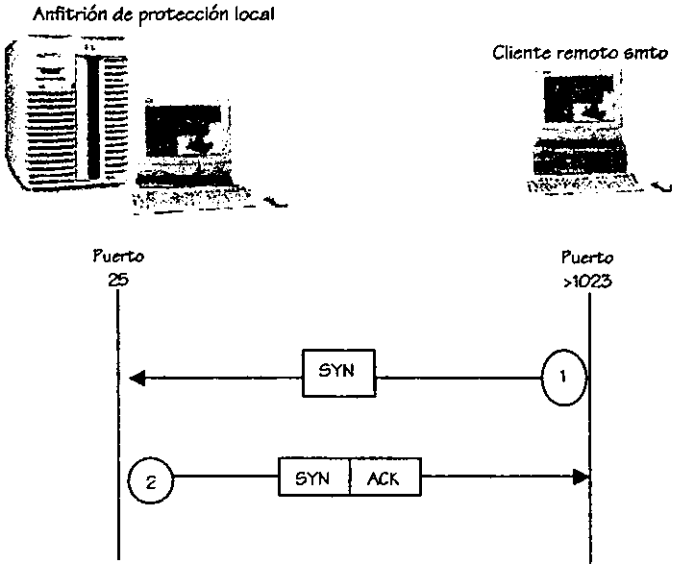


Fig. 3.5 Servicio smtp de entrada

4. Http. Se puede proporcionar este servicio en forma directa a través del filtrado de paquetes. Para proporcionar este servicio por filtrado de paquetes, hay que considerar el siguiente punto: que este tipo de servicios por lo general no hace uso de un puerto estándar, pero se considerará que la mayoría emplea el puerto 80, y se agregaran los siguientes puertos que se han identificado en el uso del servicio http en los servidores como son: 81, 800, 8000, 8080.

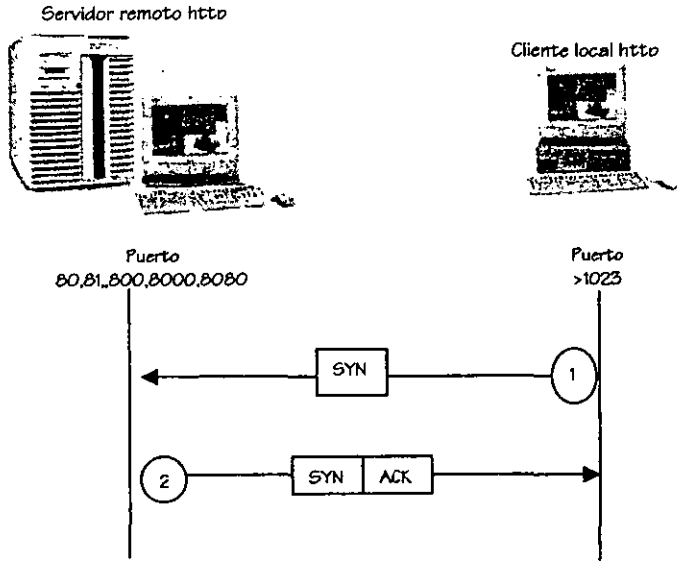


Fig. 3.6 Servicio http

5. Dns. Para proporcionar este servicio se supondrá que:
   a) El anfitrión de protección es el servidor Dns primario.
   b) Se cuenta con un servidor Dns secundario externo, que puede ser una máquina del proveedor de servicios.
   c) No se va a ocultar ninguna información Dns, por ser el anfitrión de protección, el mismo servidor para el interior como para el exterior.

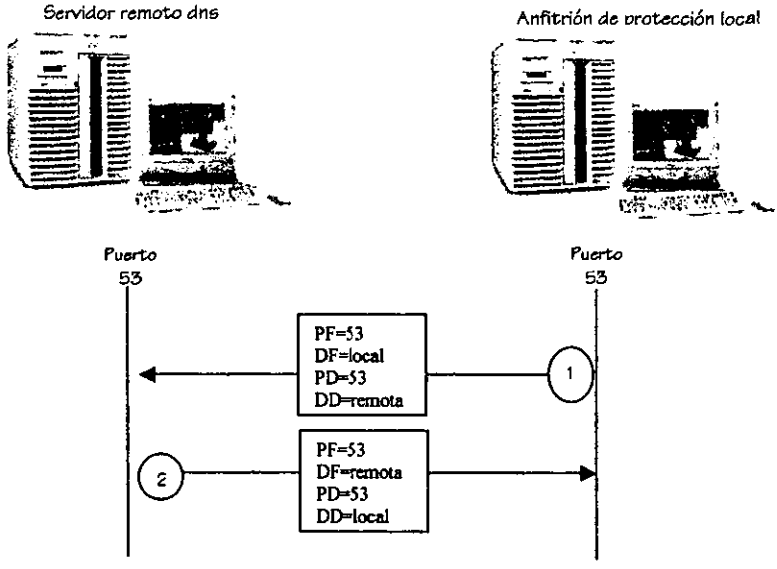


Fig. 3.7 Servicio dns (paquetes udp)

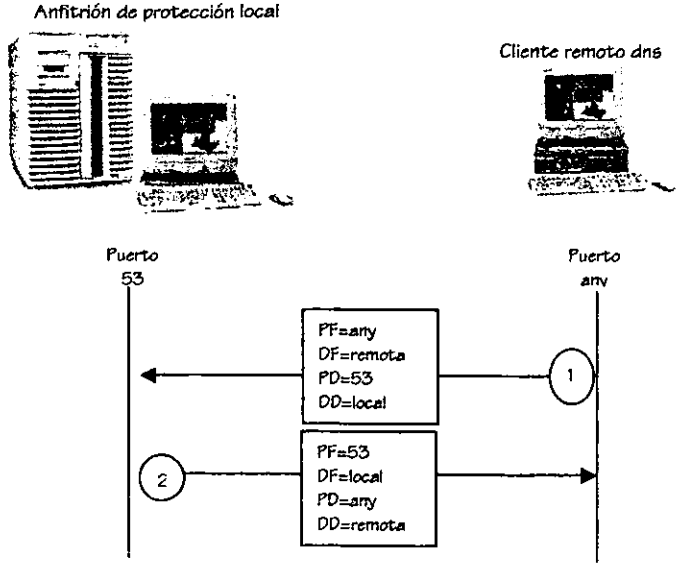


Fig. 3.8 Servicio dns (paquetes udp)

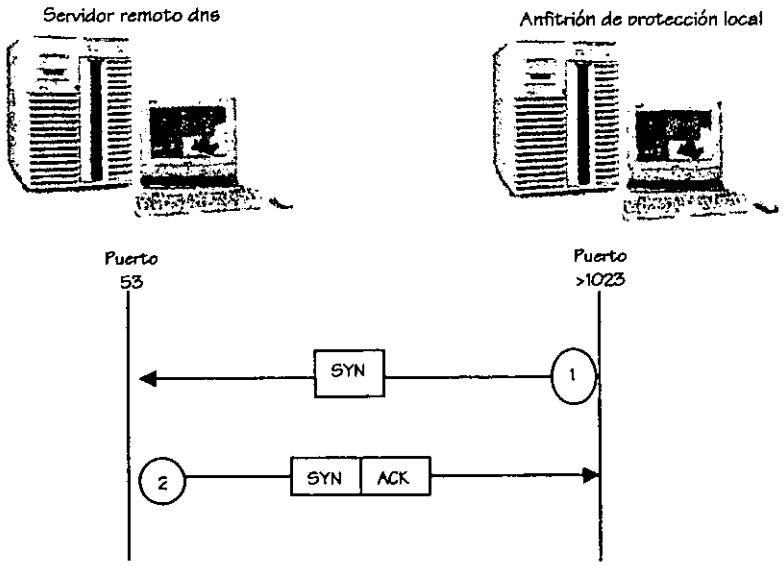


Fig. 3.9 Servicio Dns (paquetes tcp)

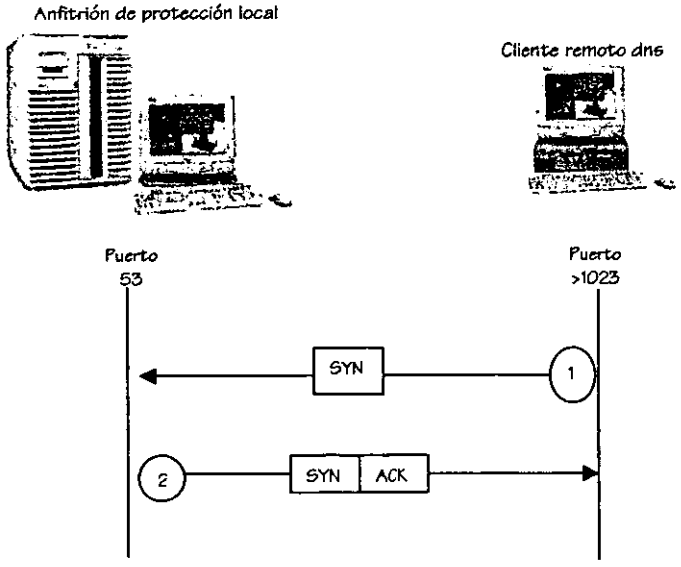


Fig. 3.10 Servicio dns (paquetes tcp)

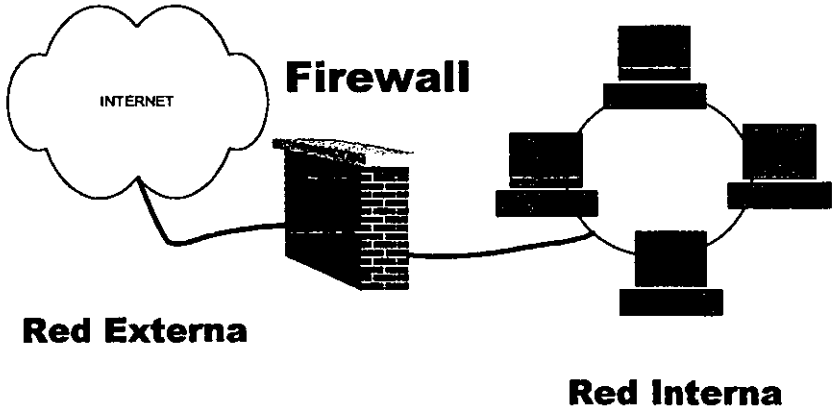
A continuación se organizaran las reglas de filtrado que deberá soportar nuestro sistema:

REGLA	DIRECCION	DIRECCION FUENTE	DIRECCION DESTINO	PROTOCOLO	PUERTO FUENTE	PUERTO DESTINO	ACK	ACCIÓN
Spoof	entrada	cualquiera	interna	cualquiera	cualquiera	cualquiera	cualquiera	prohibir
telnet-1e	salida	interna	cualquiera	tcp	>1023	23	------	permitir
telnet-2e	entrada	cualquiera	interna	tcp	23	>1023	si	permitir
ftp-1c	salida	interna	cualquiera	tcp	>1023	21	-----	permitir
ftp-2c	entrada	cualquiera	interna	tcp	21	>1023	si	permitir
ftp-3d	salida	interna	cualquiera	tcp	>1023	>1023	-----	permitir
ftp-4d	entrada	cualquiera	interna	tcp	>1023	>1023	si	permitir
Smtp-1e	salida	servidor	cualquiera	tcp	>1023	25	-----	permitir
Smtp-2e	entrada	cualquiera	servidor	tcp	25	>1023	si	permitir
Smtp-3e	entrada	cualquiera	servidor	tcp	>1023	25	-----	permitir
Smtp-4e	salida	servidor	cualquiera	tcp	25	>1023	si	permitir
Http-1	salida	interna	cualquiera	tcp	>1023	80	-----	permitir
Http-2	entrada	cualquiera	interna	tcp	80	>1023	si	permitir
Htp-3	salida	interna	cualquiera	tcp	>1023	81	-----	permitir
Http-4	entrada	cualquiera	interna	tcp	81	>1023	si	permitir
Http-5	salida	interna	cualquiera	tcp	>1023	800	-----	permitir
Http-6	entrada	cualquiera	interna	tcp	800	>1023	si	permitir
Http-7	salida	interna	cualquiera	tcp	>1023	8000	-----	permitir
Http-8	entrada	cualquiera	interno	tcp	8000	>1023	si	permitir
Http-9	salida	interna	cualquiera	tcp	>1023	8080	-----	permitir
Http-10	entrada	cualquiera	interna	tcp	8080	>1023	si	permitir
Dns-1	salida	servidor	cualquiera	udp	53	53	-----	permitir

REGLA	DIRECCION	DIRECCION FUENTE	DIRECCION DESTINO	PROTOCOLO	PUERTO FUENTE	PUERTO DESTINO	ACK	ACCIÓN
Dns-2	entrada	cualquiera	servidor	udp	53	53	-----	permitir
Dns-3	entrada	cualquiera	servidor	udp	cualquiera	53	-----	permitir
Dns-4	salida	servidor	cualquiera	udp	53	cualquiera	-----	permitir
Dns-5	salida	servidor	cualquiera	tcp	>1023	53	-----	permitir
Dns-6	entrada	cualquiera	servidor	tcp	53	>1023	sí	permitir
Dns-7	entrada	cualquiera	servidor	tcp	>1023	53	-----	permitir
Dns-8	salida	servidor	cualquiera	tcp	53	>1023	sí	permitir
Default-1	salida	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera	prohibir
Default-2	entrada	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera	prohibir

CAPÍTULO 4

APLICACIÓN



"La moraleja de esta historia es: cualquier cosa que no conozcas es peligrosa, hasta que la llegas a conocer"

Beowulf Schaefer in Flatlander
- Larry Niven

CAPÍTULO 4. APLICACIÓN

Basados en el análisis del capítulo anterior, en el presente capítulo se explicará cómo funciona el filtrado de paquetes que brinda de forma nativa, en el kernel del sistema operativo.

4.1 ESQUEMA DEL FILTRADO DE PAQUETES

El kernel de linux provee de soporte para filtrado de paquetes IP, en diferentes acciones:

1. Cuando un paquete es recibido
2. Cuando un paquete es enviado
3. O cuando un paquete es reenviado

Cada uno de los tres filtros consiste de una política predeterminada y una lista de reglas de filtrado. Cada regla de filtrado define algunas características del paquete como dirección IP, un dispositivo de red opcional, y muchas otras opciones.

Además, cada regla tiene una política asociada con esta, que define que hacer cuando un paquete coincide con la regla.

El algoritmo empleado en el filtrado de paquetes puede describirse de la siguiente forma:

- La información recibida o transmitida pasa a través de la lista de reglas de filtrado asociadas y verifica si el paquete coincide o no con la regla.

- La primera regla de filtrado que coincida (en caso de que suceda) determina las siguientes acciones:
  a) La política de la regla se aplica al paquete
  b) Cada regla contiene contadores de paquete y bytes, los cuales incrementan cuando un paquete coincide
  c) Opcionalmente, alguna información acerca del paquete se escribe en el archivo de registro del kernel de linux.
  d) Finalmente una regla puede contener parámetros que definen como cambiar el campo TOS[1] en el encabezado IP, de acuerdo a la prioridad del paquete.
- Si ninguna de las reglas coincide con el paquete, se usa la política predeterminada asociada con el filtro.

Hay actualmente tres políticas soportadas en linux:

1. Aceptar: permite al paquete pasar por el filtro.
2. Denegar: niega el acceso sin mostrar ninguna notificación.
3. Rehusar: niega el acceso y envía un mensaje IMCP, de destino inalcanzable, de regreso al remitente como una notificación.

Las reglas de filtrado en linux contienen los siguientes componentes:

[1] Type Of Service

1. Dirección IP fuente y destino, ambas con su propia máscara, lo que nos permite cubrir una (sub)red completa.
2. El protocolo que puede ser TCP,UDP, ICMP o cualquiera.
3. Nombre del puerto fuente y destino (servicios), usados en combinación con paquetes TCP o UDP. Se puede incluir rangos de puertos (ejemplo. 1024:65535, que representan todos los puertos sin privilegios).
4. Tipos de mensajes, usados con los paquetes ICMP. Bits que coinciden con las banderas TCP, ACK y SYN, usados para rechazar el establecimiento de nuevas conexiones TCP en una cierta dirección.
5. El nombre o dirección IP de un dispositivo de red. Las reglas contienen la especificación de un dispositivo que coincidirá solamente con los paquetes que entran (o salen) por medio de ese dispositivo en partícular.
6. Una especificación de cambio del campo TOS en el encabezado IP, que es usado cuando un paquete es aceptado por la regla.
7. Una bandera indicando si alguna información básica del paquete debería ser escrita al archivo de registro del kernel de linux, en el caso de que la regla coincida.

4.2 MANEJO DE LOS FILTROS

La forma para manejar las reglas de filtrado a nivel kernel; principalmente a nivel usuario, consiste en usar una interface a nivel-comando denominado ipfwadm, que permite cambiar o inspeccionar todos los aspectos de los filtros del kernel.

Existen algunos comentarios para el manejo de los comandos para el filtrado de paquetes, que deben tomarse en cuenta:

1. El orden de las reglas es importante; solamente la primer regla coincidente es tomada dentro del contador, por lo que los comandos se deben poner en el orden correcto.
2. Combinar las reglas (especificando múltiples puertos o nombres de servicios) tanto como sea posible, porque cada verificación de la regla de filtrado, para cada paquete consume tiempo del cpu.
3. Asegurarse de definir los filtros en el momento apropiado de inicio del sistema. El mejor lugar para hacer esto es antes de que los dispositivos de red sean configurados.
4. Aunque ipfwadm permite especificar el nombre de la red o del anfitrión cuando se define la regla de filtrado, esta no trabajará en la mayoría de los casos, porque el sistema probablemente no pueda resolver los nombres antes de que la red este operacional. Por lo misma razón, es necesario usar

la opción -n[2] cuando se listan los filtros en los momentos en que la red no sea (todavía) operacional.

5. Cuando sea necesario cambiar un filtro en un sistema operacional, la cuestión es poner los comandos necesarios en el orden correcto:
   - Colocar como política predeterminada del filtro, la negación.
   - Borrar todas las reglas pertenecientes al filtro.
   - Colocar las nuevas reglas del filtro.
   - Colocar la política predeterminada en el valor deseado.

Esto asegura que no se tendrán intervalos de tiempo durante las cuales el tráfico de la red no deje de ser controlado por el sistema de protección perimetral.

4.3 ENMASCARAMIENTO

Además de la utilidad de filtrado de paquetes, linux emplea un mecanismo adicional en el uso de soluciones de sistemas de protección perimetral: el enmascaramiento de paquetes ip.

Esto significa que algunos o todos los paquetes reenviados por el sistema linux pueden ser cambiados como si fueran enviados por el propio sistema. Por lo que la dirección ip del anfitrión local es reemplazada por la dirección ip del sistema linux y el puerto fuente es reemplazado por un puerto generado localmente (ej. 60005).

[2] ver inciso 4.4 de este capítulo

Como se mantiene una administración en una sesión de enmascaramiento; los paquetes entrantes por ese puerto serán automáticamente desenmascarados y reenviados al sistema que originalmente inicio la sesión.

La siguiente tabla muestra la función de enmascaramiento, aplicándose a una sesión telnet, desde un anfitrión interno (192.168.37.15), a un anfitrión externo (10.42.7.8), pasando por un sistema linux (192.168.37.1) el cual ejecuta el enmascaramiento.

	Fuente		Destino	
	Dirección IP	Puerto	Dirección IP	Puerto
Paquete original	192.168.37.15	1027	10.42.17.8	23
Enmascaramiento	192.168.37.1	60005	10.42.17.8	23
Contestacióndel paquete	10.42.17.8	23	192.168.37.1	60005
Desenmascaramiento	10.42.17.8	23	192.168.37.15	1027

El enmascaramiento toma lugar despuée de pasar por el filtro de reenvío del sistema de protección perimetral.

El desenmascaramiento es realizado después de recibir un paquete, y el paquete desenmascarado es pasado al filtro de reenvío.

El enmascaramiento no es tan fácil como parece, algunos protocolos necesitan un especial cuidado (como el protocolo ftp, al usar una segunda sesión iniciada normalmente por el sistema remoto, el IRC y el Real Audio que presentan problemas similares). La implementación del enmascaramiento entonces, tiene un tratamiento para esos protocolos específicos, al tener por separado módulos cargados para esas características.

Esto nos será de gran ayuda al permitirnos compartir la conexión a internet por medio del módem, con las computadoras restantes.

4.4 COMANDOS UTILIZADOS EN LA INTERFAZ DE USUARIO IPFWADM

(a) Parámetros principales:

Bandera	Significado
- I	Especifica las reglas para paquetes de entrada
- O	Especifica las reglas para paquetes de salida
- F	Especifica las reglas para reenvío de paquetes
- M	Admón de el enmascaramiento ip
- P	Especifica el protocolo al cual se aplicarán las reglas. Los protocolos pueden ser TCP, UDP, ICMP o any (indica cualquier protocolo)
- S	Especifica la dirección fuente, el formato es: Dirección[/máscara][puerto]
- D	Especifica la dirección destino, y el formato es el mismo que el anterior
- W o - V	Especifica la interface por la que entra o sale el paquete

(b) Opciones:

Bandera	Significado
- a	Agrega una o más reglas al final de la lista
- i	Agrega una o más reglas al inicio de la lista
- d	Borra una o más reglas de la lista
- l	Muestra las reglas en la lista
- f	Borra todas las reglas de la lista
- p	Indica si el paquete debe ser aceptado, denegado o rehusado
- h	Ayuda
- c	Verifica que una regla asignada sea seguida por un paquete (debug)

Bandera	Significado
- k	Hace que la regla de entrada coincida solamente con los paquetes que tienen la bandera ack, en protocolos tcp asignado
- o	Registro del archivo coincidente (archivo log)
- m	Indica que el paquete obtendrá el enmascaramiento antes de ser enviado.
- n	Salida numérica de las direcciones ip
- v	Muestra todos los detalles de la regla como contadores de bytes y de paquetes
- s	Muestra los parámetros de enmascaramiento

Ejemplos:

ipfwadm -I -a -p deny -S 192.168.22.0/24 -D any/0

Niega el acceso a todos los paquetes de entrada que procedan de toda la red 192.168.22.0.

ipfwadm -O -a -p accept -P tcp -S 192.168.37.1 1024:65535 –D any/0 telnet

ipfwadm -I -a -p accept -k -P tcp -S any/0 telnet –D 192.168.37.1 1024:65535

Estas dos reglas aceptan los paquetes pertenecientes a la conexión de salida telnet. El nombre del servicio en este caso telnet, hace referencia al puerto 23.

ipfwadm -M -l

lista las reglas que están siento enmascaradas, en tiempo real en una sesión, y la salida producida es la siguiente:

IP masquerading entries

prot	expire	source	destination	ports
tcp	13:00.15	int1.foo.com	ext2.bar.com	1017 (60001) -> login
tcp	14:15.60	int2.foo.com	ext1.bar.com	1346 (60010) -> telnet
tcp	14:52.82	int1.foo.com	ext1.bar.com	1348 (60015) -> ftp

ipfwadm -I -a -p reject -P tcp -W eth0 -S 12.75.41.3 1633 –D 10.20.12.2 telnet -o

Se rehusa la entrada del paquete de conexión telnet (asumiendo que el servidor telnet local tiene la dirección 10.20.12.2), que entra por la interface eth0 (haciendo referencia a la tarjeta de red) y además es almacenada en el archivo de registro cualquier evento relacionado con esta regla. El registro se leería de la siguiente manera:

Mar 03 07:37:01 anfi_prote kernel: IP fw-in rej eth0 TCP 12.75.147.174:1633 \
100.200.0.212:23 L=44 S=0x00 I=54054 F=0x0040 T=254

Hora y fecha: Mar 03 07:37:01

Computadora donde se ejecuta: anfi_prote

Protocolo: IP

Sentido del paquete (entrada, salida, reenvío): fw-in

Indicador si el paquete es aceptado,rehusado o negado: rej

Interfaz ligada a internet: eth0

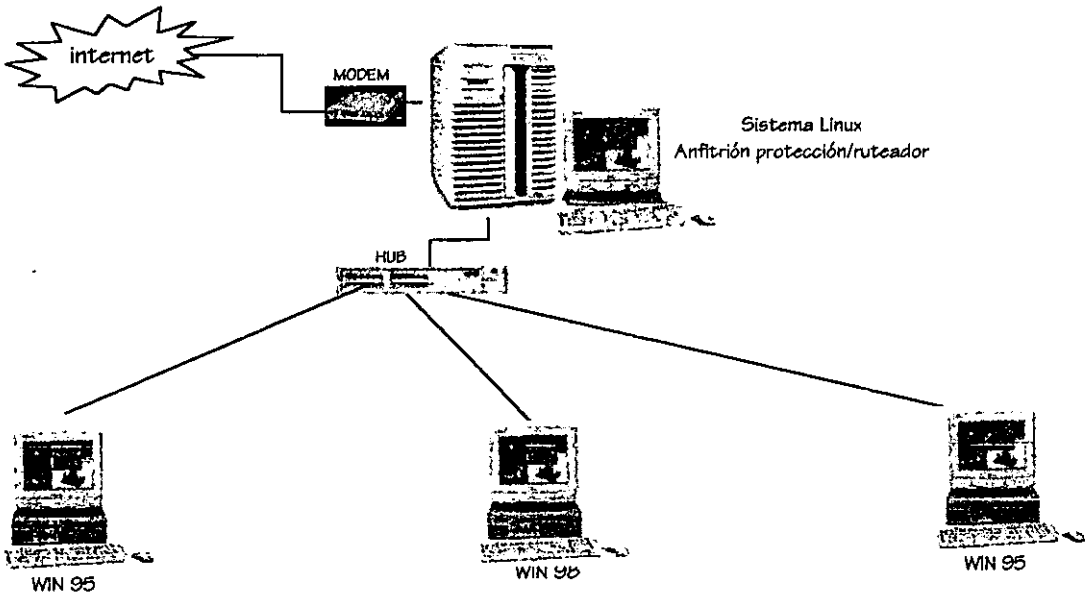
Tipo de paquete: TCP

Dirección ip y puerto fuente: 12.75.147.174:1633

Dirección ip y puerto destino: 100.200.0.212:23

4.5 INSTALACIÓN

a) Esquema de la red



b) Especificación del hardware

- Tarjetas de red ethernet base 10
- Mini hub ethernet 8 port base 10
- Cableado y conectores
- Módem interno a 56 kbps
- Para el sistema linux, una computadoras intel pentium a 166 mhz con 32 en ram.

- Para los tres sistemas restantes, el primero de ellos cuenta con procesador amd k5 a 166 mhz con 32 megas en ram y sistema operativo win 95, el segundo cuenta con un procesador k6-II a 450 mhz con 32 megas en ram y sistema operativo win 98 y el otro con win 95, el tercer y último sistema cuenta con un procesador intel pentium a 166 mhz y 32 en ram e sistema operativo win 95.

c) Compilación del kernel

- Lo primero que se necesita es tener el código fuente del kernel (preferentemente el más actualizado). Para este ejemplo se hace uso de la versión 2.0.36.
- Antes de realizar la compilación es importante sacer un respaldo del directorio fuente. Cambiandose al directorio /usrc/src/ y ejecutando el siguiente comando cp -R linux.fecha_de_la_copia y cambiando este archivo a otro directorio
- Después se desempaca el código fuente del kernel en el directorio /usr/src/ con el comando tar xvzf linux-2.0.36.tar.gz –C /usr/src, lo que nos permite descomprimir y estraer el directorio al mismo tiempo. Una vez realizado esto asegurarse que exista un directorio o liga simbólica al directorio /usr/src/linux/
- A continuación nos colocamos en el directorio /usr/src/linux/ y se ejecuta el siguiente comando: make config, el cual hará una serie de preguntas acerca

de los manejadores que habrán de incluirse en el kernel. Estas son preguntas si/no directas, siempre y cuando se tenga conocimiento del sistema. Lo que realmente se ejecuta es un script localizado en el subdirectorio /usr/src/linux/arch/i386/config.in (si se ejecuta una máquina intel).

- Aplicar cualquier parche opcional o necesario al código fuente del kernel. Para la versión 2.0.36 de kernel, no se requiere ningún parche específico para que funcione bien.
- Las opciones mínimas que se requieren en la compilación del kernel, para el funcionamiento del enmascaramiento y filtrado de paquetes son las siguientes:

* Opción para el desarrollo y/o drivers/código incompletos
(CONFIG_EXPERIMENTAL) [Y/n/?] YES
Esta opción permite más tarde la selección del código de características de enmascaramiento de IP.
* Habilita la carga de soporte de módulos
(CONFIG_MODULES) [Y/n/?] -YES
Permite el cargar los módulos del kernel del enmascaramiento ip.
* Soporte de red
(CONFIG_NET) [Y/n/?] - YES
Habilita el subsistema de red
* Sistemas de protección perimetral de red
(CONFIG_FIREWALL) [Y/n/?] - YES
Habilita la herramienta de sistema de protección perimetral IPFWADM

* Red tcp/ip

(CONFIG_INET) [Y/n/?] - YES

Habilita el protocolo tcp/ip

* IP: reenvío/puerta de enlace

(CONFIG_IP_FORWARD) [Y/n/?] - YES

Habilita el reenvío y ruteo de paquetes en la red. Controlado por IPFWADM

* IP: SYN cookies

(CONFIG_SYN_COOKIES) [Y/n/?] – YES

Recomendado ampliamente para la seguridad básica de la red. Ataques SYN suelen repercutir en la negación de servicios.

* IP: firewalling

(CONFIG_IP_FIREWALL) [Y/n/?] - YES

Habilita las características de sistema de protección perimetral.

* IP: Registro de paquetes de sistema de protección perimetral.

(CONFIG_IP_FIREWALL_VERBOSE) [Y/n/?] – YES

(Opcional pero altamente recomendado). Permite el registro de daños al sistema perimetral.

* Enmascaramiento IP

(CONFIG_IP_MASQUERADE [Y/n/?] – YES

Habilita el enmascaramiento

*IP: Soporte de enmascaramiento ipautofw (experimental)

(CONFIG_IP_MASQUERADE_IPAUTOFW) [Y/n/?] – NO

IPautofw es un método heredado de el reenvío de puertos tcp/ip. No es recomendado

* IP: Soporte de enmascaramiento ipportfw (experimental)

(CONFIG_IP_MASQUERADE_IPPORTFW) [Y/n/?] – YES

Opción disponible solamente por medio de parches para el kernel 2.0.x.

Con esta opción la computadoras externas en la internet pueden directamente comunicarse a una máquina interna enmascarada. Esta característica es usada genralmente para accesar servidores internos.(SMTP, TELNET, y servidores WWW).

* IP: Enmascaramiento ICMP

(CONFIG_IP_MASQUERADE_ICMP) [Y/n/?] – YES

Habilitar esta opción soporta el enmascaramiento de paquetes ICMP. Aunque se considero opcional, muchos programas no funcionara apropiadamente sin soporte ICMP.

* IP: Manejo de puertos extraviados Udp (experimental)

(CONFIG_IP_MASQ_LOOSE_UDP) [Y/n/?] - YES

Opción disponible solamente por medio de parches para el kernel 2.0.x.

Con esta opción, las máquinas internas enmascaradas puede jugar, juegos amigable en la internet.

* IP: Siempre defragmentar

(CONFIG_IP_ALWAYS_DEFRAG) [Y/n/?] - YES

Esta característica optimiza las conexiones IP masq. Recomendado ampliamente.

* IP: Optimizado como ruteado y no como anfitrión.

(CONFIG_IP_ROUTER) [Y/n/?] – YES

Se optimiza el kernel para el subsistema de red.

* IP: Drop source routed frames

(CONFIG_IP_NOSR) [Y/n/?] - YES

Recomendado ampliamente para la seguridad básica de la red.

* Soporte de manejadore de red para principiantes

(CONFIG_DUMMY) [M/n/y/?] - YES

Puede ser opcional, esta opción puede ayudarnos cuando se depuran problemas.

* Soporte archivos de sistema /proc

(CONFIG_PROC_FS) [Y/n/?] - YES

Requerido para habilitar el sistema de red linux de reenvío

Hay que hacer hincapié de que las opciones anteriores solo nos describen los componentes necesarios para que el enmascaramiento y filtrado de paquetes funcione. Se necesita también el especificar las opciones sobre el montaje de los componentes de red y hardware.

- Al terminar la elección de las opciones de compilación del kernel se ejecuta el comando make boot que inicia la reconstrucción del kernel.
- Después de la compilación del kernel, también se necesitan compilar e instalar los módulos que se hubieran definido en la configuración del kernel

para ellos se usa el comando make modules que construye los módulos correspondientes al sistema, después se ejecuta el comando make modules_install, que instala los módulos construidos. Aun cuando no se haya construido algún módulo, para dar por concluida una compilación de kernel es necesario instalarlos.

- Como se obtiene una dirección ip dinámica mediante una conexión PPP, y para poder ejecutar el script /etc/rc.d/rc.filtrado de manera eficiente, es necesario, que al concluir los puntos anteriores se agreguen un par de líneas al final del script /etc/ppp/ip-up (el cual es un script que se encuentra en ejecución cuando se inicia una conexión PPP, y en donde se localiza la dirección ip asignada en forma dinámica).

```
# rc.filtrado script que comienza el enmascaramiento y filtrado
/etc/rc.d/rc.filtrado
```

d) Creación del script

Crear el archivo rc.filtrado dentro del directorio /etc/rc.d, y escribir las siguientes líneas:

```
##########################################################
# rc.filtrado – Inicia el enmascaramiento y las reglas de filtrado
# Llamar los módulos requeridos, se necesita iniciar el llamado de los módulos
/sbin/depmod -a
##########################################################
# Habilita IP forwarding, pues de manera predeterminada se encuentra
# deshabilitado. (habilitación en forma dinámica)
echo "1" > /proc/sys/net/ipv4/ip_forward
##########################################################
```

```
#########################################################
# Si se obtiene la dirección ip de manera dinámica desde una conexión SLIP,
# PPP o DHCP, se debe habilitar la siguiente opción. La siguiente línea hace
# más fácil el uso de diald y programas similares.
echo "1" > /proc/sys/net/ipv4/ip_dynaddr
#########################################################
# Especificación de la dirección ip dinámica. Si la conexión a internet es
#mediante una conexión PPP la siguiente línea nos servirá para obtener
# la dirección ip, asignada en forma dinámica al realizar la conexión.
 ppp_ip = "`/sbin/ifconfig ppp0 | grep 'inet addr' | awk '{print $2}' | sed -e s/.*://`"
#########################################################
# Tiempos de terminación en IP MASQ
# 1 hr para sesiones TCP
# 10 seg para tráfico después de recibir el paquete "Fin" en tcp/ip
# 60 seg para sesiones UDP
/sbin/ipfwadm -M -s 3600 10 60
#########################################################
#                  Creación de las reglas de filtrado
#########################################################
#  Políticas predeterminadas
/sbin/ipfwadm -I -a -p deny
/sbin/ipfwadm -O -a -p deny
/sbin/ipfwadm -I -a -p deny
#########################################################
# Evitar paquetes de engaño
/sbin/ipfwadm -I -a -p deny  -V$ppp_ip -S 0.0.0.0/0 -D 192.168.0.0/24
/sbin/ipfwadm -I -a -p deny  -V$ppp_ip -S 192.168.0.0/24 -D 192.168.0.0/24
#########################################################
# Reglas para el servicio telnet
/sbin/ipfwadm -O -a -p accept -m -P tcp  -S 192.168.0.0/24 1024:65535  \
        -D 0.0.0.0/0 telnet
/sbin/ipfwadm -I -a -p accept.-k -P tcp  -S 0.0.0.0/0 telnet \
         -D 192.168.0.0/24 1024:65535
#########################################################
# Reglas para el servicio ftp
/sbin/ipfwadm -O -a -p accept -m -P tcp  -S 192.168.0.0/24 1024:65535  \
        -D 0.0.0.0/0 ftp
/sbin/ipfwadm -I -a -p accept -k -P tcp  -S 0.0.0.0/0 ftp \
         -D 192.168.0.0/24 1024:65535
/sbin/ipfwadm -O -a -p accept -m -P tcp  -S 192.168.0.0/24 1024:65535  \
        -D 0.0.0.0/0 1024:65535
```

```
/sbin/ipfwadm -I -a -p accept -k -P tcp  -S 0.0.0.0/0 1024:65535 \
        -D 192.168.0.0/24 1024:65535
#########################################################
# Reglas para el servicio smtp
/sbin/ipfwadm -O -a -p accept -m -P tcp  -V$ppp_ip \
    -S 192.168.0.0/24 1024:65535 -D 0.0.0.0/0 smtp
/sbin/ipfwadm -I -a -p accept -k -P tcp  -V$ppp_ip \
    -S 0.0.0.0/0 smtp -D 192.168.0.1 1024:65535
/sbin/ipfwadm -I -a -p accept  -P tcp  -V$ppp_ip \
    -S 0.0.0.0/0 1024:65535 -D 192.168.0.1 smtp
/sbin/ipfwadm -O -a -p accept -m -k -P tcp  -V$ppp_ip \
    -S 192.168.0.1 smtp -D 0.0.0.0/0 1024:65535
#########################################################
# Reglas para el servicio http
/sbin/ipfwadm -O -a -p accept -m -P tcp -S 192.168.0.0/24 1024:65535 \
      -D 0.0.0.0/0 http
/sbin/ipfwadm -I -a -p accept -k -P tcp -S 0.0.0.0/0 http
      -D 192.168.0.1 1024:65535
/sbin/ipfwadm -O -a -p accept -m -P tcp -S 192.168.0.0/24 1024:65535 \
      -D 0.0.0.0/0 81
/sbin/ipfwadm -I -a -p accept -k -P tcp -S 0.0.0.0/0 81
      -D 192.168.0.1 1024:65535
/sbin/ipfwadm -O -a -p accept -m -P tcp -S 192.168.0.0/24 1024:65535 \
      -D 0.0.0.0/0 800
/sbin/ipfwadm -I -a -p accept -k -P tcp -S 0.0.0.0/0 800
      -D 192.168.0.1 1024:65535
/sbin/ipfwadm -O -a -p accept -m -P tcp -S 192.168.0.0/24 1024:65535 \
      -D 0.0.0.0/0 8000
/sbin/ipfwadm -I -a -p accept -k -P tcp -S 0.0.0.0/0 8000
      -D 192.168.0.1 1024:65535
/sbin/ipfwadm -O -a -p accept -m -P tcp -S 192.168.0.0/24 1024:65535 \
      -D 0.0.0.0/0 8080
/sbin/ipfwadm -I -a -p accept -k -P tcp -S 0.0.0.0/0 8080
      -D 192.168.0.1 1024:65535
#########################################################
# Reglas para el servicio Dns
/sbin/ipfwadm -O -a -p accept -m -P udp  -V$ppp_ip \
    -S 192.168.0.1 53 -D 0.0.0.0/0 53
/sbin/ipfwadm -I -a -p accept  -P udp  -V$ppp_ip \
    -S 0.0.0.0/0 53 -D 192.168.0.1 53
```

```
/sbin/ipfwadm –I –a –p accept –P udp  -V$ppp_ip \
    –S 0.0.0.0/0 0:65535 -D 192.168.0.1  53
/sbin/ipfwadm –O –a –p accept –m  –P udp  -V$ppp_ip \
    –S 192.168.0.1  53 -D 0.0.0.0/0 0:65535
/sbin/ipfwadm –O –a –p accept –m –P tcp  -V$ppp_ip \
    –S 192.168.0.1 1024:65535 -D 0.0.0.0/0 53
/sbin/ipfwadm –I –a –p accept –k –P tcp  -V$ppp_ip \
    –S 0.0.0.0/0 53 -D 192.168.0.1 1024:65535
/sbin/ipfwadm –I –a –p accept  –P tcp  -V$ppp_ip \
    –S 0.0.0.0/0 1024:65535 -D 192.168.0.1 53
/sbin/ipfwadm –O –a –p accept  –m –k –P tcp  -V$ppp_ip \
    –S 192.168.0.1  53 -D 0.0.0.0 1024:65535
##########################################################
```

CONCLUSIONES

A través del desarrollo de trabajo, se observó lo siguiente:

- La implementación de un sistema de protección perimetral basado en filtrado de paquetes requiere de tener comprendidos los conceptos de TCP/IP.
- Se debe conocer los directorios y comandos de UNIX que nos sirven para la configuración del sistema de protección expuesto.
- Al contar con una conexión a internet, es indispensable el tener presente que se deben de proteger los recursos, aún cuando no se considere una organización grande.
- No es fácil contar e implementar herramientas de sistemas de protección perimetral debido a sus altos costos y requerimientos de hardware.
- Es benéfico contar con programas gratuitos como linux, que nos permiten crear un ambiente de protección de red mediante una herramienta de filtrado de paquetes que el propio kernel proporciona.
- Se necesita tener definidos los servicios que se quieren permitir y los que no, para establecer las políticas de seguridad, y así crear las reglas de filtrado de paquetes.
- No es sencillo crear reglas de filtrado de paquetes, hay que tener conocimiento de los puertos que utilizan los servicios de red, y cómo se

realiza el intercambio de paquetes en una conexión, para poder interpretarlo a los comandos que ejecuten los filtros.

- No existe una estandarización para crear un sistema de protección perimetral, cada organización debe de valorar los riesgos que supone una conexión en la internet, elaborar la política de seguridad adecuada a sus necesidades y tomar en consideración el producto que se ajuste a sus requerimientos.
- Se debe tener presente que el no tomar en cuenta las normas básicas de toda política de seguridad (como parte fundamental en la seguridad), podría dar como resultado un gasto innecesario el pensar en un sistema de protección perimetral.
- La seguridad de la red debe ser una responsabilidad conjunta del administrador de la misma, y de los usuarios que la emplean, por eso es indispensable enseñar a los usuarios para que sigan las políticas de seguridad establecidas.
- No existe un sistema de protección perimetral lo suficientemente flexible y seguro que pueda adaptarse a cualquier situación, la mejor seguridad proviene de la combinación de varias técnicas.
- Hay que mantenerse informado constantemente de las mejoras a la seguridad del sistema operativo involucrado, implementar los parches

necesarios en caso de ser necesario, e informarse de las nuevas tecnologías que día a día surgen.

GLOSARIO

Administrador de redes o sistemas.	La persona que organiza, mantiene, resuelve problemas y generalmente vigila la red.
Analizador de protocolos.	("Sniffer"). Es un programa y/o dispositivo que monitorea el viaje de los datos a través de la red. Los analizadores pueden ser usado para funciones de administración de red legitima y para robar información de la red. Los analizadores si autorización pueden ser extremadamente peligrosos a la seguridad de la red porque son virtualmente imposibles de detectar y pueden ser conectados casi en cualquier lugar. Esto los convierte en una de las herramientas favoritas en el arsenal de un hacker.
Ancho de banda.	La cantidad de datos que pueden ser enviados a través de canales de comunicación como una red o un módem.
Anfitrión.	Cualquier computadora. Normalmente se usa cuando la computadora está en red.
Caballo de Troya.	Un tipo de virus de computadora el cual viene disfrazado como un programa útil o interesante (como un juego), usualmente es bajado de la internet. Mientras este programa se encuentra en ejecución, quizá borre archivos del disco duro o solamente los dañe.
CGI.	("Common Gateway Interface"). Una interfaz escrita en un lenguaje de programación (perl, c, c++,visual basic, etc) y posteriormente ejecutada o interpretada por una computadora servidor para contestar a pedidos del usuario desde una computadora con una aplicación cliente; casi siempre desde el World Wide Web. Esta interfaz permite obtener los resultados pedidos, como los que resultan al consultar una base de datos.
Cliente.	a) Una aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red. b) Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio.

Cracker.	Individuo que irrumpe en los sistemas para causar algún daño, o para obtener algún beneficio (económico o información confidencial).
Dns.	Sistema de nomenclatura de dominios ("Domain Name System") Es un sistema que se establece en un servidor (que se encarga de un dominio) que traduce nombres de computadoras (como servidor.dgeca.unam.mx) a domicilios numéricos de Internet (direcciones IP, como 132.248.10.1).
Estación de trabajo o de datos.	Computadora que se usa para accesar a la red y sus recursos. Dispositivo que puede ser conectado a una red de área local. Computadora que se usa para accesar a la red y sus recursos. Dispositivo que puede ser conectado a una red de área local.
Estafeta.	Dispositivo pequeño del tamaño de una tarjeta de crédito que los usuarios remotos traen consigo y que despliega un código de identificación que cambia constantemente. Un usuario introduce primero una contraseña y entonces la tarjeta despliega un identificador que puede usarse para conectarse a una red. Típicamente el identificador cambia cada 5 minutos aproximadamente
Ethernet.	Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus. Y que tiene un ancho de banda de 10 Mbps.
FDDI.	("Fiber Distributed Data Interface"). Abreviación de Interface de fibra de distribución de datos, un conjunto de protocolos ANSI para el envío de datos digitales sobre cable de fibra óptica. Las redes FDDI son redes de pase de señal ("token-passing"), y soportan la transmisión de datos a velocidades de 100 Mbps (100 millones de bits) por segundo. Las redes FDDI son usadas típicamente como centrales ("backbones") para redes de área extensas. Una extensión de FDDI, llamada FDDI-2, soporta la transmisión de información de audio y video, como de datos. Otra variación de FDDI llamada, tecnología en ambos sentidos ("Full Duplex Technology", FFDT) usa la misma infraestructura

	de red pero puede soportar potencialmente velocidades de 200 Mps.
Gusano de internet.	Programa que se duplica y propaga a través de una red. El primer gusano ("worm") fue definido en 1982 por Shoch & Hupp de Xerox en ACM Communications. Una característica de estos programas es que solo pueden afectar computadoras que utilicen el mismo sistema operativo.
Hacker.	Normalmente son personas con grandes deseos de obtener conocimiento sobre las computadoras, se dan a la tarea de irrumpir los sistemas para demostrar su capacidad.
INTERNIC.	Es un proyecto elaborado entre AT&T y Soluciones de red sociedad anónima ("network solutions inc.", NSI), apoyado por la Fundación Nacional de Ciencia. El proyecto ofrece los siguientes 4 servicios a los usuarios de la internet: Directorio y servicio de base de datos.- directorio de páginas blancas en línea y directorio de base de datos públicas accesibles administradas por AT&T. Registro de servicios.- nombre de dominios y direcciones IP asignadas administradas por NSI. Soporte de servicios.- servicio especial de asistencia pública, educación e servicios de información para la comunidad de la internet administrada por NSI. Servicios de exploración de la red.- publicaciones en línea que resumen los acontecimientos recientes, de interés para los usuarios de internet, administrado por NSI.
Kernel.	Es el módulo central de un sistema operativo. Es la parte del sistema operativo que carga primero, y permanece en la memoria principal. Como permanece en la memoria, es importante que el núcleo sea lo más pequeño posible, mientras provea todos los servicios esenciales requeridos por otras partes de las aplicaciones y sistema operativo. Típicamente, el núcleo responsabiliza con gestión de memoria, proceso y gestión de tareas, y gestión de disco.
Internet.	Una red global de redes interconectadas y de computadoras sencillas que actúan como si fueran redes.

Paquete.	Un bloque de datos mandados en una comunicación en una red que: identifica las estaciones fuente y destino, controla errores, lleva datos.
PCMCIA.	("Personal Computer Memory Card International Asociation"). Asociación internacional de tarjetas de memoria para computadoras personales, es una asociación que ha desarrollado un estándar para dispositivos pequeños del tamaño de una tarjeta de crédito, y que originalmente fueron diseñados para adicionar memoria a las computadoras portátiles. Existen tres tipos de tarjetas PCMCIA, todas tiene el mismo tamaño rectangular: El tipo 1 es usado esencialmente para adicionar RAM o ROM a una computadora. El tipo 2 es usado para tarjetas módem y fax-módem. El tipo 3 se utiliza para unidades de disco portátiles.
Protocolo.	Secuencia ordenada y común que se debe seguir para realizar una tarea. Reglas de comunicación entre procesos similares, dando una forma de controlar ordenadamente la transferencia de información entre estaciones conectadas en línea.
Puente.	("Bridge"). Es una computadora o dispositivo de red que se usa para conectar dos redes. Se suele considerar que los puentes conectan sistemas similares, como dos redes ethernet.
Puerta de enlace.	("Gateway"). Es una computadora u otro dispositivo de red que se usa para conectar un sistema con otro. Frecuentemente se considera que las compuertas conectan sistemas disímiles, como una red que ejecuta TCP/IP y otra que ejecuta Netware.
Puerto.	Uno de los conectores de entrada/salida de una computadora. Un número que identifica a un servidor Internet en partícular.
Red.	Conjunto de computadoras enlazadas entre sí y/o con otros conjuntos de computadoras, cuya configuración permite compartir, transferir y manejar información. Su objetivo principal es compartir recursos.
Sitio.	Lugar de acceso en una computadora destinado a una tarea específica. Generalmente de acceso público.

Solicitud de Comentarios (RFC).	("Request For Comments"). Serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet y experimentos similares. No todos los rfcs (en realidad muy pocos de ellos) describen estándares de Internet pero todos los estándares Internet están escritos en forma de rfcs. La serie de documentos RFC es inusual en cuanto los protocolos que describen son emitidos por la comunidad Internet que desarrolla e investiga, en contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como CCITT y ANSI.
Riesgo.	Es la posibilidad de que un intruso pueda tener éxito al tratar de accesar de manera ilegal un red de área local (LAN) a través de la conectividad que se mantenga con una red de área amplia (WAN).
Ruteador.	("Router"). Máquina procesadora colocada en una red que lee las cabeceras de mensajes para determinar la dirección destino y calcular la mejor ruta para su envío.
Servidor.	Computadora que tiene la mayoría de los recursos de una red y en algunos casos todos y se dedica a dar los servicios a las demás entidades de la red. En el servidor se instala el programa que permite el manejo de la red.
Token Ring.	1) Un tipo de red de computadoras en la cual todas las computadoras son adaptadas (esquemáticamente) en un círculo. Una señal, la cual es un patrón de bit especial, viaja alrededor del círculo. Para enviar un mensaje, una computadora captura la señal, adjunta un mensaje a esta, y entonces le permite continuar el viaje alrededor de la red 2) Cuando se capitaliza, Token Ring se refiere al protocolo de red para pc desarrollado por IBM. Las especificaciones de Token Ring han sido estandarizados por el IEEE como el estándar IEE 802.5.
Usenet.	Áreas de mensajes de grupos de interés, cada una de las cuales está enfocado a un tema en partícular

Vulnerabilidad. Esencialmente significa la forma cuan protegida está la red de cualquier ataque externo para ganar acceso ilegal a ella, y de la forma cuan protegida se encuentra de alguien dentro de la misma red que intencional o accidentalmente da la oportunidad de obtener acceso ilegal o cualquier otro daño.

REFERENCIAS BIBLIOGRÁFICAS

[1] MOHR, James, *Linux (Recursos para el usuario)*, Ed. Prentice Hall, México, 1999.

[2] SIYAN Karanjit y Chris HARE, *Firewalls y la Seguridad en Internet*, 2ª edición , Ed. Prentice Hall, México, 1997.

[3] CHAPMAN D. Brent y Elizabeth D. ZWICKY, *Building Internet Firewalls*, Ed. Mc Graw Hill, Estados Unidos, 1997.

[4] CHESWICK R. William y Steven M. BELLOVIN, *Firewalls and Internet Security repelling the wily hacker*, Ed. Addison Wesley, Estados Unidos, 1994.

[5] WACK John P. Y Lisa J. CARNAHAN, *Keeping Your Site Comfortably Secure: An introduction to Internet Firewalls, NIST (National Institute of Standard Technology) Special Publication 800-10*, U.S. Department of commerce, 1995, http://csrc.ncsl.nist.gov/nistpubs/800-10/main.html

[6] THE PARTNER'S INFORMATION CORNER OF SIEMENS NIXDORF, *Internet Security and Firewalls*, Estados Unidos, 1996, http://www.sin.be/en/new/online/pchip/pchip3/firewall.html

[7] GILBERT H., *Introduction to TCP/IP*, Estados Unidos, 1995, http://pclt.cis.yale.edu/pclt/comm/tcpip.html

[8] KESSLER Gary C., *An Overview of TCP/IP Protocols and the Internet*, Estados Unidos, 1994, http://pclt.cis.yale.edu/pclt/comm/tcpip.html

[9] ON TECHNOLOGY, *Firewalls Explained*, Estados Unidos, 1996, http://www.on.com/onguard/ogexpl.html

[10] GONCALVES Marcus, *Firewalls Complete*, Edit. Mc Graw Hill, Estados Unidos, 1998

[11] MONTOYA Eduardo, *Fundamentos Tecnológicos y de uso del Internet*, Colombia, 1997, http://sigma.eafit.edu.co/~emontoya/fundtec/seg_int1.html

[12] GERMAN Daniel M., *Seguridad en Internet*, Estados Unidos, 1996, http://csg.uwaterloo.ca/~dmg

[13] ZARCO, Roberto, "Crackers, Piratas y Chaneques.....", *Personal Computing*, México, Edición N° 126, Noviembre 1998, pp. 26-29

[14] MERINO, Marco A., "Seguridad un asunto fundamental", *Personal Computing* , México, Edición N° 126, Noviembre 1998, pp. 80-82

[15] WAYNER, Peter, "¿Quién vigila su red?", *Revista Byte México*, México, Año 9, Edición N° 113, Junio 1997, pp. 8-17

[16] SEACHRIST, David, "Software para Unix y NT", Revista Byte México, Año 9, N° 113, Junio 1997 pp. 18-23

[17] ERLANGER, León, "El desarme de la red", Revista PC Magazine en Español, México, Vol. 8, N° 7, Julio 1997 pp. NE1-NE10

[18] FINNIE, Scott, "Protección en el escritorio", Revista PC Magazine en Español, México, Vol. 8, N° 9, Septiembre 1997 pp. 100-117

[19] ACEVEDO Juárez Héctor, "Paredes de fuego: para conectar su red a Internet sin riesgo", Revista Red , México, Año V, N° 62, Noviembre 1995, pp. 38-43

[20] ÁREA DE SEGURIDAD DE CÓMPUTO, *Políticas de Seguridad*, México, 1997, http://www.super.unam.mx/seguridad/Informacion/politicas.html

[21] TANENBAUM, Andrew, *Redes de Ordenadores*, Ed. Prentice Hall, España, 1991

[22] LISTA SEG-I, *Lista de Seguridad en Castellano*, México, 1999, http://master.cic.uanl.mx/~mhoz/seguridad/

[23] GUEL López Juan Carlos, *¿Firewalls una solución?*, México, 1998, ftp://www.super.unam.mx/pub/asc

[24] CASTILLO Ulises, *Nuevas Tecnologías de Seguridad en Internet*, México, 1998, ftp://www.super.unam.mx/pub/asc

[25] STEVES Kevin, *Building a Bastion Host Using HP-UX*,
Holanda , 1998, http://people.hp.se/stevesk/security/bastion.html

[26] RANUM Marcus J. , *Thinking About Firewalls*,
SANS 1993, http://www.clark.net/pub/mjr/pubs/think/index.htm

[27] MCGIBBON, *Firewalls and Internet Security*,
SANS 1993,
http://www.darmstadt.gmd.de/ice-tel/deliverables/download/firewall/

[28] LUCAS Néstor, "Seguridad: Conceptos Básicos",
Revista Linux Actual, España, Año 1, N° 3, Junio 1998, pp. 71-73

[29] CÁCERES Javier, "Servidores proxy",
Revista PC World España, N° 148, Noviembre 1998, pp. 268-285

[30] GARCÍA Ramón, "Conexión a internet por módem en linux",
Revista Linux Actual, España, Año 1, N° 3, Noviembre 1998, pp. 14-15

[31] SÁNCHEZ Javier, "Protocolo IP",
Revista Internet Online, España, Año 2, N° 12, Noviembre 1998, pp. 26-27

[32] ROMERO Santiago, "PPP- La conexión a internet",
Revista Internet Online, España, Año 2, N° 12, Noviembre 1998, pp. 58-60

[33] VOS Jos, *Linux firewall facilities for kernel-level packet screening*,
Holanda, Noviembre 1996, http://www.xos.nl/linux/ipfwadm/paper/

[34] RANCH David, *Linux IP MASQ How to*,
Estados Unidos, Agosto 1999,
http://www.redhat.com/mirrors/LDP/HOWTO/IP-Masquerade-HOWTO.html

[35] WARD Brian, *Linux Kernel How to*,
Estados Unidos, Junio 1999,
http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html