ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACION

"Seguridad de redes de computadoras frente a Internet: Estudio, diagnóstico e implementación de firewalls"

TESIS DE GRADO
Previa a la obtención del Titulo de:

INGENIERO EN COMPUTACION

Presentada por:
Giovanni Mazzari G.

Guayaquil-Ecuador
1998

AGRADECIMIENTO

Agradezco a todos los profesores que colaboraron en este trabajo: Dr. Entrique Pelaez, Director de CESERCOMP; y al Ing. Guido Caicedo, Jefe de Redes.

A CESERCOMP y la empresa TELCONET por haber hecho posible la realización de estos estudios y pruebas.

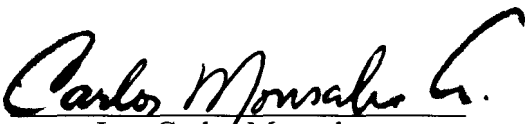
A mis padres por su apoyo y comprension en todo mornento.

A todos los arnigos que me brindaron ayuda en los momentos mas oportunos.

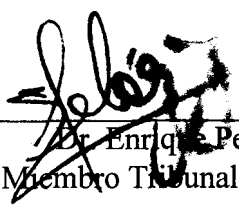
A *mis Padres.*

A mi Abuelo(+).

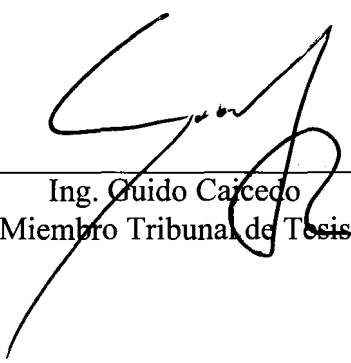
Ing. Armando Altamirano
Presidente Tribunal de Tesis



Ing. Carlos Monsalve
Director de Tesis



Dr. Enrique Peláez
Miembro Tribunal de Tesis



Ing. Guido Caicedo
Miembro Tribunal de Tesis

DECLARACION EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en esta tesis, me corresponden exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

Giovanni Mazzari G.

RESUMEN

La red Intenet, que nació como un proyecto militar de Estados Unidos, se ha convertido en un medio de abundante informacion y cornunicacion con el mundo entero. Por estas ventajas que ofrece, muchas organizaciones han enlazado sus redes a Internet. Sin embargo, si no lo hacen con las precauciones apropiadas, no representa mucha ventaja ya que como en toda sociedad, siernpre existen personas maliciosas e Internet no es la excepción. Estas personas maliciosas o "hackers" tratan de accesar ilegalmente a los sistemas de las organizaciones para robar o cambiar informacion, dañar recursos, etc. Las consecuencias de estos ataques pueden ser rnuy perjudiciales para una organización ya que la violación de sistemas representan pérdidas de dinero, tiempo y esfuerzo.

Ante esta necesidad de protección, muchas organizaciones optan por colocar ambientes restringidos en sus redes a traves de mecanismos de seguridad entre sus redes e Internet. A estos mecanisrnos de seguridad se les conoce con el nombre de firewalls.

La **ESPOL** como institución académica no puede restringir totalmente el ambiente de sus redes que se enlazan con Intenet. El ambiente que implemente la ESPOL debe ser abierto sin descuidar la seguridad en sus recursos. La presente tesis constituye una contribución en la implementación de medidas de seguridad para las redes de cornputadoras de la ESPOL a traves de un estudio de las tecnologias de firewalls y el diseño de un modelo de seguridad.

Esta tesis consta basicamente de seis secciones ordenadas cronologicamente:

1. Riesgos de las redes de la ESPOL. En el capítulo **1** se puede apreciar toda una gama de tipos de ataques conocidos a lo largo de la vida de Internet, desde los mas ingenuos hasta los

mas sofisticados. También se analizan los distintos tipos de atacantes, clasificados de acuerdo a su comportamiento.

2. Estrategias de seguridad, diseño de politicas, tecnologias y arquitecturas de sistemas de firewalls. En los capitulos 1, 2, 3 se pueden apreciar los criterios de como diseñar mediuas de seguridad que se pueden tomar y las tecnologias y arquitecturas de sistemas de firewall que un adrninistrador podría seleccionar.

3. Necesidades, distribución y funcionamiento de los recursos conectados al backbone de la ESPOL. Se recoge información acerca de la distribución y funcionamiento de los recursos conectados al backbone de la ESPOL. A traves de una análisis de riesgo de recursos implernentado en lógica difusa (capitulo 4), se puede observar el nivel de riesgo e importancia que posee cada recurso y las medidas a tomar para su proteccion.

4. Diseño de politicas de seguridad de redes para la ESPOL. En base a los requerimientos analizados en la seccion anterior se diseña las politicas de seguridad, en las cuales se establece un modelo de seguridad que cubra con todas las necesidades de protección establecidas en la seccion anterior.(Capítulo 4).

5. Evaluación de firewalls publicos y privados para la ESPOL. (Capitulo 5) Con todos los conocimientos adquiridos se procede a evaluar tanto firewalls publicos corno privados en base a sus caracteristicas asi como su evaluación de rendimiento. Este estudio concluye con la evaluacion de la mejor plataforma para el firewall seleccionado.

6. Implementación de un modelo de seguridad para la ESPOL. (Capitulo 6) A traves de un diagnóstico de las medidas de seguridad implementadas en la actualidad en la ESPOL, se

recomienda nuevas medidas que se implementarán de acuerdo con la autorizacion de la Jefatura de Redes de CESERCOMP.

De esta rnanera, este trabajo pretende otorgar una visión de la tecnologia de firewalls y todas las medidas de protección en redes de computadoras que en la actualidad existen para contribuir con la seguridad a las redes de la ESPOL.

INDICE GENERAL

CAPITULO 11

CAPITULO III

CAPITULO VI

APENDICE B

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Ante la creciente apertura de las organizaciones hacia Internet, surge el gran riesgo de ser víctimas de ataques electronicos por parte de personas inescrupulosas. Estos ataques electronicos varian desde los mas sencillos hasta los mas sofisticados. Las consecuencias de estos generalmente involucran pérdidas de informacion y recursos.

Toda organizacion que se enlaza con Internet debe tener conocimiento los servicios de Internet que desea disponer y de los riesgos que pueden correr los recursos conectados en sus redes para luego diseñar un modelo de seguridad que brinde protección a la red de la organizacion (tambien llamada red interna).

La ESPOL, como una institución académica que fomenta la investigación, posee una conexión a Internet en un esquema abierto. Por lo tanto las redes de computadoras de la ESPOL corren peligros de ser atacadas si no se toman las medidas de seguridad necesarias. Pero jcuales son los riesgos de las redes de la ESPOL?, jcuales son las medidas que se deben tomar?, jcual es el alcance de un firewall?, jque tipo de firewall necesita la ESPOL?, jcual es la mcjor plataforma para colocar un firewall?. Todas estas preguntas seran contestadas a lo largo de esta tesis con la esperanza de brindar una vision global a un aspecto importante en Internet: "seguridad".

La presente tesis abarca el diseño de politicas de seguridad, evaluación de firewalls para la ESPOL y la implementación de un modelo de seguridad. Los fuentes de informacion fueron diversas: Libros, revistas, listas de discusion, recomendaciones de expertos en el tema y el World Wide Web (WWW).

Los objetivos del presente trabajo son:

1. Establecer los requerimientos de seguridad tanto para la actualidad como para el futuro, de las redes de computadoras de la ESPOL que se enlazan con Internet para demostrar la necesidad de mecanismos de seguridad (firewalls).

2. Proveer un estudio de arquitecturas y tecnologias de firewalls disponibles en el mercado a fin de obtener una vision global del alcance de estos mecanisrnos de seguridad.

3. Evaluar firewalls publicos y privados de acuerdo a los requerimientos mínimos de un firewall para la ESPOL.

4. Implementar un modelo de seguridad para la ESPOL de acuerdo a las recomendaciones del autor de la tesis y a la autorizacion de la Jefatura de Redes de CESERCOMP.

El desarrollo de estos objetivos y todos los detalles hallados en la investigación en orden cronologico son presentados a lo largo de los seis capitulos siguientes.

Los capitulos I, II, III constituyen una base teorica de conocimientos para el desarrollo de la presente tesis. La base teorica de los capitulos I y III ha sido obtenida del texto: "Building Internet Firewalls" de Chapman & Zwicky, O'Reilly Associates, **1995;** y el capítulo II fue obtenido a partir del texto "Internet Firewalls and Network Security" de Siyan & Hare, New Riders Publishers, 1995. Ambas fuentes han sido complernentados con otros textos

referenciados en la bibliografía. El objetivo de incluir una base teorica en la tesis es que esta información este disponible y contribuya a la investigación de personas interesadas en el tema.

CAPÍTULO I

INTRODUCCIÓN A LA SEGURIDAD DE REDES DE COMPUTADORAS ANTE INTERNET

1.1. Introducción

Ante la necesidad imperiosa de tener acceso a fuentes de informacion globalmente distribuidas, muchas organizaciones se han integrado a la red de redes, Internet. Esta red mundial, que nacio como un proyecto militar de Estados Unidos, se ha convertido en un puente que une al mundo entero.

Actualmente, en todos los lugares del mundo se conoce de Internet pues las ventajas que ofrece esta super carretera de la informacion son cuantiosas. Pero todo progreso tiene su nivel de riesgo. Así como se puede obtener y publicar informacion rapidamente, tambien se puede corromper y destruir la informacion rápidamente. En toda sociedad existe gente con malicia que tiende a destruir en lugar de construir. Al conectar una organización a Internet, todos sus recursos: informacion, maquinas, programas, usuarios, etc., quedan expuestos a las

reprochables acciones de personas inescrupulosas que arbitrariamente se infiltran en la red. Quienes originan estos accesos no autorizados tratan de accesar a algun servidor para ganar los privilegios del administrador y eventualmente provocar daños tales como: robo de información, corrupción de sistemas, destrucción de recursos. Para muchas organizacicnes estas pérdidas pueden significar cuantiosos gastos e inclusive la bancarrota. El numero de incidentes de seguridad reportados a nivel mundial aumenta cada año [CHAP95].

Ante esta eminente necesidad de seguridad, han surgido mecanismos que dan proteccion y confiabilidad a los sistemas. Estos mecanismos, llamados firewalls (corta fuegos), perrniten la conectividad con Internet manteniendo un cierto grado de seguridad. Un firewall es una manera de restringir el acceso a una red interna desde Internet. Por esta razon se recomienda incluir un firewall en el plan de seguridad de toda organización.

Tambien es vital establecer políticas de seguridad, enforzar la seguridad propia en cada maquina disponible, considerar facilidades de autenticacion (verificar que un usuario es verdaderamente quien clama ser) y optar por la encriptacion de datos (codificar datos).

A medida que los mecanismos de seguridad son cada vez mas eficaces, los ataques cada vez son mas sofisticados. Los ataques perpetrados a sistemas conectados a Internet cada día son mas serios y tecnologicamente mas complejos que en el pasado. Los firewalls representan una tecnologia que cambia de acuerdo a las necesidades, para de esta manera cubrir las brechas descubiertas por los atacantes o “hackers” [CHES94].

Para elaborar un sistema de seguridad efectivo, que brinde proteccion a un sistema de redes de computadoras, es necesario conocer contra que o quienes se va a proteger. En este capítulo se

trataran topicos referentes a los tipos de ataques y de atacantes, así como a las estrategias de seguridad para enfrentarlos, pero sin dar detalles tecnicos ya que ese es el objetivo de los siguientes capitulos.

1.2. Tipos de ataques

En realidad existen muchos tipos de ataques a sistemas y los autores de textos sobre seguridad de redes de cornputadoras tienen diferentes concepciones al respecto [CHAP95]. Sin embargo, se los puede categorizar en tres grupos: acceso no autorizado, negación de servicio y hurto de información.

1.2.1. Acceso no autorizado

Este tipo de ataque consiste en el uso no autorizado de cornputadoras de la red de una organización. La intrusion o acceso no autorizado es el ataque mas comun que se da en las redes de cornputadoras.

Existen muchas maneras en que usuarios no autorizados ganan acceso a una red de computadoras. Varian desde ataques de ingenieria social (engañar al administrador de la red fingiendo ser alguien que no es y pedirle que cambie su cuenta o contraseña) y adivinanza de contrasetias hasta metodos mas sofisticados que capturan cuentas y contrasetias de usuarios.

Dentro de esta categoria existen:

1.2.1.1. Ingenieria social

Un atacante puede engañar al administrador haciendose pasar por un usuario autorizado, se comunica ya sea via correo electronico o por telefono indicandole al administrador que olvido su contraseña y que se la cambie por otra.

1.2.1.2. Personificación

Este tipo de ataque tambien se llama ***sniffing o packet sniffing.*** Un atacante interno o externo puede "olfatear" (capturar) todos los paquetes de la red (a traves de programas especiales llamados **sniffers)** y capturar los paquetes de inicio de una sesion de un usuario autorizado. Luego el atacante puede iniciar una sesion autorizada con la cuenta y contraseña del usuario autorizado cuya informacion fue "olfateada".

Otro ejemplo puede ser el de un atacante que tiene acceso a una sala de terminales (laboratorio), donde puede dejar ejecutando un programa especial que, cada vez que un usuario intente abrir una sesion Telnet o FTP, guarda toda la informacion de la cuenta y contraseña tipeados por un usuario autorizado. De esta manera un atacante que se encuentra en un laboratorio puede posteriormente ingresar con estas cuentas y contraseñas capturadas a los usuarios que abrieron sesiones desde una maquina determinada.

1.2.1.3. Explotacion e infraestructura

Estos ataques consisten en explotar todas las fallas en los programas o sistemas operativos que se encuentran disponibles en un computador servidor; y de los protocolos en Internet.

El atacante obtiene informacion de un servidor (a traves de la ejecucion de comandos tales como **finger** o **ping)** para saber con que sistema operativo trabaja y que programas son

usuales en este sistema operativo. Al obtener esta información el atacante puede aprovecharse de fallas de dominio publico que brinda algun programa. Muchos de los programas que ejecuta el sistema operativo son grandes y poderosos y utilizan privilegios del sistema. Por ejemplo, utilizando el programa Sendmail el atacante podría enviar un mensaje de correo electronico que contenga comandos y como este programa se ejecuta con privilegios de usuario administrador, los comandos se ejecutaran con estos mismos privilegios. De esta manera un atacante puede hacer y deshacer de un sistema enviando comandos que se ejecutaran como si fuera el mismo administrador.

Algunos protocolos en Internet tienen debilidades en cuanto a seguridad se refiere. Los ataques mas comunes basados en las debilidades de los protocolos mas populares son:

- **Ataque de numero de secuencia:** Consiste en engañar al recipiente (maquina cliente) cambiando la direccion fuente de un paquete por una direccion autorizada por la red interna.
- **Ruta fuente:** Todos los paquetes proveen de un campo llamado ruta fuente, el cual puede especificar una ruta especifica que debe seguir el paquete hasta su destino. De esta manera se puede introducir un paquete engañando al recipiente clamando ser de una direccion autorizada.
- **DNS (Domain Name Server) spoofing:** Un atacante puede comprometer una red interna cambiando el dominio de su maquina a un dominio que la red interna considera autorizada. De esta manera el atacante tendra un acceso a la red interna.
- **Ataque via UDP (User Datagram Protocol):** Debido a que UDP no tiene control sobre el orden de llegada de sus paquetes, es mas fácil engañar al recipiente (maquina clienrc) clamando venir de una direccion autorizada y confiable.
- **Ataque via ICMP (Internet Control Message Protocol):** ICMP es un protocolo que frecuentemente se utiliza para enviar mensajes cuando el destino de un paquete es

inalcanzable. Un atacante puede dejar a una maquina fuera de una conexion enviandole un paquete ICMP que le diga que su destino es inalcanzable.

- **Ataque via FTP (File Transfer Protocol) anonimo:** Un usuario puede ejecutar programas en un directorio no permitido, ejecutar comandos que ocasionen grandes perjucios. Por ejemplo: borrar directorios, colocar programas ejecutables con virus, transferir el archivo de contraseñas, etc.
- **Web spoofing:** Consiste en desviar la conexion de un cliente web a un servidor web falso en lugar del real, a fin de recoger los datos confidenciales que envía el usuario (nurneros de tarjetas de creditos, contraseñas, etc.)

Existen muchas mas falencias en protocolos y programas que se utilizan en Internet. Periodicamente se van descubriendo nuevos errores y tipos de ataques por las debilidades de protocolos y programas. Organizaciones como CERT (Computer Emergency Response Team) y CIAC (Computer Incident Advisory Capability) publican en sus páginas web todas las debilidades por protocolos y programas y las posibles soluciones para tapar estas falencias. En la seccion **4.4.** Modelo de seguridad para la ESPOL, se detallaran con exactitud las falencias de los protocolos mas comunes en Internet y las recomendaciones para brindar con seguridad los servicios basados en estos protocolos.

1.2.1.4. Confianza transitiva

En un sistema de redes de computadoras, la confianza entre redes y hosts significa que ambos pueden comunicarse sin necesidad de contraseñas. Esta confianza puede ser explotada por los atacantes.

Por ejemplo, en sistemas UNIX existe un archivo <<rhosts>>, en el cual se configura que hosts son confiables a una red. Si se manipula este archivo para que se habilite un host no confiable, un atacante en ese host no confiable puede ingresar al sistema sin la necesidad de contraseiias.

Otra fuente para este ataque puede suceder cuando existen dos estaciones de trabajo que compartes archivos via **NFS** (Network file System), un atacante puede comprometer una de las estaciones y manipular a la otra estacion con programas ejecutables exportados desde la maquina comprometida.

1.2.1.4. Orientado a datos

Estos ataques se dan a traves de los datos que fluyen en una red. Un atacante puede enviar datos de tal manera que al llegar a su destino ocasione grandes perdidas. Por ejemplo, el atacante envía un mensaje en formato Postscript (lenguaje de programacion) con una serie de operaciones (como colocar el nombre de un host en el archivo rhosts). Cuando el usuario recibe este mensaje ejecuta el interpretador de Postscript, y este ejecutara cualquier acción que lea del mensaje. (en este caso el nombre de un host sera añadido al archivo rhosts).

Por ejemplo, puede suceder que exista un programa que ejecute comandos para leer todo el archivo de contraseiias de un sistemas, y el atacante engañe al usuario enviandole mensajes de que el programa es un innovador juego o algo que llame la atencion del usuario. El usuario lo recogerá y ejecutara y ni siquiera se dara cuenta del daiio que causó.

7.2.2. *Negación de servicios*

Este tipo de ataque consiste en inundar al sistema con infinito numero de requerimientos de procesos para ocasionar un cuello de botella reduciendo el ancho de banda de la red, de tal manera que los usuarios no puedan utilizar sus propias maquinas.

Muchos de los casos de sabotaje electronico involucran la destrucción de datos, la desactivacion de equipos, la interrupción de servicios remotos, el envio de mensajes electronicos con lazos infinitos de requerimientos, etc. Así, el sistema pierde mucho tiempo atendiendo todas las llamadas de los procesos hasta colapsar.

La inundacion de procesos es la manera mas comun de generar un ataque de negacion de servicios, pero un atacante hábil puede desabilitar servicios, re-rutearlos, o reemplazarlos. Por ejemplo, un atacante podría desabilitar un servidor de acceso remoto re-ruteando los paquetes a algun otro lugar o simplemente cambiar la informacion interna de cada paquete.

El riesgo de sufrir este tipo de ataques es inevitable. Si se tiene una red abierta al mundo exterior que recibe correo electronico o que mantiene conexiones via modem, es muy probable que ocurra una sobrecarga de informacion alguna vez. La mejor recomendacion para evitar una inundacion es configurar los servicios de tal manera que si uno de los servicios se sobrecarga, el resto del sistema se mantenga funcionando mientras se encuentre y se repare el problema.

La negacion de servicios es considerado por los atacantes como 'antideportivo' debido a que es muy fácil causar este tipo de ataques, por lo tanto no es muy popular entre ellos. Hay que recordar que el mayor objetivo de un atacante es lograr el acceso a un sistema, usar los recursos de una red y no dejar huella o rastro que lo identifique.

1.2.3. Hurto de información

Este tipo de ataque consiste en obtener datos sin la necesidad de penetrar en un sistema. La mayoria de estos ataques tratan de explotar los servicios de Internet que proveen informacion tales como **GOPHER,** WWW, WAIS, etc., induciendo a estos servicios a que den mas informacion de lo que originalmente proporcionan.

Utilizando programas olfateadores (sniffers) en un punto de una red considerada promiscua (por ejemplo redes Ethernet, Token Ring), se puede examinar toda la informacion que por ella pasa. La mayoria de personas que roban informacion son aquellas que tratan de accesar indebidarnente a un sistema para lo cual olfatean las cuentas y contraseñas de los usuarios con acceso permitido. Afortunadamente para los atacantes, pero desafortunadamente para los demas, las cuentas y contraseñas es el tipo de informacion mas fácil de obtener debido a que esta inforrnacion fluye en la red por lo regular al inicio de cada sesion.

Obtener otro tipo de informacion requiere de mucha paciencia y dedicación a menos que los atacantes conozcan que la informacion pasara en un tiempo y por un lugar determinado. Por ejemplo, si un atacante conoce que todos los miercoles a las 12 p.m. un banco envía estados de cuenta a sus usuarios, el atacante podría conectar un olfateador y apropiarse de esta informacion confidencial y valiosa.

Un firewall correctamente configurado protegera a las redes de personas que traten de obtener mas inforrnacion de la que el sistema deba proporcionar.

1.3. Tipos de atacantes

Existe una gran variedad de atacantes en el mundo de Internet. Sin embargo, todos ellos comparten ciertas caracteristicas:

- No quieren ser atrapados, así que entre ellos mismos se encubren.
- Si ganan acceso a un sistema, intentaran conservar este acceso, y descubrir vías de acceso alternas.
- La mayoría de ellos tienen contactos con otras gentes que comparten los mismos intereses.
- Comparten la información que han obtenido de un sistema.

Los atacantes se pueden categorizar dentro de los siguientes grupos: "joyriders", vandalos, jugadores y espías.

1.3.1. Joyriders

Se trata de personas que buscan diversion irrumpiendo en sistemas. Ellos irrumpen en sistemas porque:

- Creen que el sistema maneja datos interesantes,
- Se divierten manejando las computadoras de otro sistema,
- No tienen nada mejor que hacer.

Se trata sencillamente de gente curiosa que no desea hacer daño; sin embargo, ocasionan daños por ignorancia o por tratar de cubrir sus huellas [CHAP95].

1.3.2. Vándalos

Son personas que ocasionan grandes problemas en los sistemas. Si una organizacion es blanco de un vandalo, rapidamente lo sabra. Por lo regular, los vandalos ocasionan problemas a una organizacion si alguna vez esta los molest6 haciendoles perder tiempo o recursos [CHAP95].

Afortunadamente los vandalos son algo escasos, a la mayoría de los atacantes no les agrada ser vandalos.

Los daños que ocasionan son facilmente hallados y reparados. Habitualmente borran datos y arruinan equipos de computación. Sin embargo no todo esta perdido por que los datos y los equipos son recuperables.

1.3.3. Jugadores

Muchos atacantes que irrumpen sistemas lo hacen por ganar prestigio y puntos ante sus colegas de oficio. Estos puntos o creditos se basan en el numero o tipos de sistemas que ellos han quebrado.

Estos atacantes prefieren irrumpir sistemas muy populares, tienen fama de ser bien defendidos o cualquier otra cualidad especial. Irrumpir en lugares como estos les otorga mas puntos y fama. Ellos van por cantidad y por calidad [CHAP95].

Los jugadores pueden o no hacer daño al sistema violado, ciertamente lo que les interesa es reunir información y mantenerla para posterior uso. Probablemente tratan de regresar al sistema

por las mismas vias de acceso por las que irrumpieron, hasta inclusive utilizar el sistema violado como plataforma para atacar a otros sistemas [CHAP95].

Los ataques de estas personas son muy dificiles de encontrar, se descubren lentamente ya sea por cosas extrañas en las maquinas, por noticias de sistemas violados, por copias de información privada de la organización, etc.

1.3.4. Espias

Este tipo de atacantes no es como los anteriores tipos descritos. Estas personas roban cosas que son directamente convertidas en dinero tales como tarjetas de creditos, telefonos, etc. Si ellos encuentran secretos que piensan que pueden vender, lo hacen.

Los espias son mucho mas dificiles de detectar que los anteriores atacantes. Ellos rompen las seguridades de un sistema, copian datos y abandonan el sistema sin ocasionar disturbios o cualquier situación extraña que haga sospechar.

Muchas organizaciones se protegen de los espias, especialmente cuando se trata de gobiernos y empresas grandes que no quieren que sus secretos sean copiados. Estas organizaciones utilizan soluciones muy complejas y costosas.

1.4. Tipos de protección en sistemas de redes de computadoras

Despues de analizar todos los tipos de ataques y los posibles tipos de atacantes, la gran pregunta es ¿qué hacer para protegerse de estos ataques? . Existen cuatro esquemas o

metodos de seguridad: protección basica, seguridad a traves de ocultamiento, seguridad de host y seguridad de red.

1.4.1. Protección básica

Este esquema consiste simplemente en no poner esfuerzo en cuanto a seguridad, operar el sistema con el minimo de seguridad que brindan los sistemas operativos existentes en una red de computadoras. No es aconsejable.

7.4.2. Seguridad a traves de ocultamiento

Este modelo establece que un sistema es seguro si nadie conoce de el, de su existencia, de su contenido y de las medidas de seguridad que posee.

El problema es que cualquier red que se desea conectar a Internet tiene que tener un registro autorizado (nombre del dominio reconocido por el ente que regula las conexiones con Internet), el cual puede ser obtenido por cualquier persona (por ejemplo al hacer un ping, finger y otros comandos que muestren informacion del dominio). Es decir, no hay un completo ocultamiento del sistema a proteger. Los intrusos estan atentos a nuevas conexiones con la esperanza de que estos nuevos sitios no tengan todavia medidas de seguridad y así infiltrarse.

Existen muchas maneras diferentes mediante las cuales alguien puede irrumpir y conocer los datos sensitivos de una organización. Por ejemplo, conociendo el hardware, software y la version del sistema operativo un intruso sabra los posibles agujeros en la seguridad y por donde iniciar un ataque. Los intrusos pueden obtener esta informacion del registro del host o

intentar conectarse al host. Es por esto que es recomendable ocultar el tipo de sistema operativo cuando alguien se conecta a un host.

La manera en que se oculta informacion puede ser a traves de la prohibición de uso de ciertos servicios tales como finger, ping, u otros que otorguen información a los usuarios. Se pueden corregir archivos de configuración del sistema para no presentar el nombre de la maquina, dominio, sistema operativo, etc. Además, resultaria recomendable colocar un ambiente restrictivo o controlado en la maquina a fin de que se permita a los usuarios ejecutar solo ciertos comandos.

Sin embargo, siempre habrá un factor ante el cual poco se puede hacer, y es el hecho de que los intrusos tienen bastante tiempo en sus manos para tratar de ingresar a un sistema. Simplemente, esos atacantes violarán el sistema tratando con todas las posibilidades de ingreso que tengan en base a la información disponible. Por lo tanto, a largo plazo este acercamiento no es un elección muy acertada.

1.4.3. Seguridad de Host

Este esquema consiste en darle seguridad por separado a cada host de la red de computadoras. Es decir aplicar todos los esfuerzos para evitar problemas de seguridad en cada host. Esto involucra desactivar servicios (rlogin, TFTP, X11, etc.), procesos del sistema operativo, accesos libres de cuentas sin contraseñas, etc.

Pero existe un problema en este esquema, actualmente el ambiente de computadoras es abierto a diversas plataformas lo que hace que este modelo sea impracticable por lo complejo

que se torna configurar las máquinas. La mayoría de ambientes incluyen maquinas de muchos distribuidores (MACHINTOSH, IBM, HP, etc.), cada una con sus propios sistemas operativos y cada una con sus propios problemas de seguridad. Aun si una red de computadoras tiene maquinas del mismo distribuidor, utilizar diferentes versiones del mismo sistema operativo conllevaría problemas de seguridad.

Este metodo de seguridad es rnuy apropiado para lugares pequeños o lugares que requieren de extrema seguridad. Sin embargo, muchas organizaciones incluyen seguridad de host en sus planes de seguridad para asegurar por separado a todos los hosts considerados importantes. Lo recomendable es utilizar este modelo en conjunción con el esquema de seguridad de red que se tratara a continuación, para de esta forma dar mayor seguridad a ciertos hosts considerados criticos en un sistema de red de computadoras.

1.4.4. Seguridad de red (firewalls)

A medida que los ambientes de computadoras han ido creciendo, el asegurar cada host se ha hecho muy dificil. Debido a esto surgio el modelo de seguridad de red. Este modelo consiste en controlar todos los puntos de accesos a la red, a los hosts y a los servicios que ellos ofrecen mas no asegurarlos uno por uno.

En este metodo intervienen los firewalls como mecanismos que protegen los hosts y redes internas utilizando tecnicas de autenticacion, listas de accesos y servicios autorizados, archivos de log, y encriptacion para proteger datos en tránsito dentro de las redes.

En el capítulo III se explicara con mas detalles las caracteristicas, alcances y diseños de sistemas de firewalls.

1.5. Estrategias de seguridad

Antes de detallar las caracteristicas, alcances y diseños de sistemas de firewalls es necesario entender las estrategias de seguridad empleadas para construir estos sistemas. Es importante mantener en mente estas estrategias cuando se fabrica un sistema de firewalls.

Las estrategias son las siguientes:

- Menor Privilegio
- Defensa en profundidad
- Punto de estrangulamiento
- Enlace mas débil
- Fallas seguras
- Participación universal
- Diversidad de defensa
- Simplicidad

1.5.1. Menor Privilegio

Se trata del principio de seguridad mas fundamental que existe. Basicamente este principio establece que cualquier objeto sea usuario, administrador, sistema, programa, etc., deben tener tan solo aquellos privilegios que necesita para ejecutar sus tareas correctamente.

La mayoría de problemas de seguridad en Internet pueden deberse a fallas por no seguir el principio del menor privilegio. Por ejemplo, el popular programa Sendmail (encargado de manejar el correo electronico) se ejecuta con privilegios del administrador de red debido a que accesa a ciertos archivos privados de cada usuario (buzon de mensajes electronicos). Esto constituye un verdadero blanco para los atacantes, ya que si un programa existente en un sistema es complejo y utiliza privilegios, hace el trabajo de los atacantes mas facil.

Existen dos problemas al utilizar esta estrategia:

El primer problema es que el proceso de otorgar el menor privilegio a los objetos puede resultar complicado si no se conocen las caracteristicas de diseño de los programas y protocolos a usar. Si no se conocen las caracteristicas de un programa, el administrador puede otorgarle a un usuario o programa mas privilegios de los que verdaderamente le corresponde y constituirse en una brecha de seguridad. Se corre un gran riesgo si se piensa que se aplica esta estrategia cuando en realidad no se lo hace.

El segundo problema sucede cuando a un objeto se le otorga menos privilegios de lo que le corresponde. Esto puede reducir su alcance e inclusive entorpecer sus tareas. Un ejemplo puede ser cuando se le reducen los privilegios a los usuarios. Se puede predecir facilmente como va a funcionar un programa con menos privilegios, pero un usuario puede actuar impredeciblemente y al sentirse frustrado por sus limitaciones puede constituirse en un potencial enemigo interno para el sistema.

1.5.2. Defensa en profundidad

Este principio se basa en que la seguridad de un sistema no debe depender de un solo mecanismo (ya sea que este mecanismo sea muy eficiente o bastante seguro) sino de multiples mecanismos que se respalden entre sí en caso de que alguno falle.

Un firewall no representa un solución completa para el ancho rango de problemas de seguridad en Internet. Cualquier esquema de seguridad por mas impenetrable que sea, puede ser violado por atacantes que estan dispuestos a gastar todos los recursos por lograr sus objetivos. El plan a seguir por el administrador es hacer que los intentos de violación de los atacantes sean costosos. Esto se puede lograr adoptando varios mecanismos de seguridad que proporcionen redundancia entre ellos. Por ejemplo, combinando seguridad de red (firewalls) con seguridad de host (asegurar las maquinas una por una) y con seguridad humana (buena administración, etc.).

La configuración de cada mecanismo de seguridad debe ser diferente, *es* decir que en caso de que un atacante encuentre la forma de violar el primer mecanismo, le sea dificil violar el segundo mecanismo, y así sucesivamente. De esta manera se retarda mas al atacante para llegar a un recurso de la red.

1.5.3. Punto de estrangulamiento

Esta estrategia consiste en colocar un solo punto de conexión entre una red e Internet para así forzar a los usuarios a pasar por un canal angosto que pueda monitorear y controlar los accesos.

En el esquema de seguridad de red, un firewall representa el punto de estrangulamiento entre una red e Internet, así cualquier persona que vaya a atacar al sistema desde Internet tendra que pasar por ese canal en donde se concentraran todas las medidas de seguridad.

Sin embargo, un punto de estrangulamiento deja de ser efectivo si el atacante encuentra una manera de penetrar una red por otro lugar como una "puerta trasera". Por ejemplo para que molestarse en construir un punto de estrangulamiento para controlar y monitorear la red si existen docenas ,de conexiones dial-up mal configuradas permitiendo la entrada de cualquier usuario.

Cuando una red tiene una segunda conexión aumenta el riesgo de sufrir un ataque, es por esto que al establecer las políticas de seguridad es necesario verificar cuantas conexiones a Internet va a tener una red de computadoras.

1.5.4. Enlace mas *debil*

Un principio fundamental en materia de seguridad es que una cadena es tan fuerte como su enlace mas debil y una pared es tan fuerte como su punto mas debil. Los atacantes hábiles siempre estan buscando puntos debiles en una red para concentrar todos sus esfuerzos para perpetrar un ataque.

Para diseñar un sistema de seguridad hay que estar atentos a todo lo que se puede considerar' como punto debil para luego eliminarlo. Sin embargo, es imposible eliminar todos los puntos debiles. Siempre existira un punto que se constituira el enlace mas debil. Lo mas aconsejable es

fortalecer los enlaces lo suficiente y mantener la fuerza del enlace proporcional al riesgo; por ejemplo, proteger por igual a todos los servicios que tienen los mismos riesgos [CHAP95].

1.5.5. Fallas Seguras

Esta estrategia se basa en el principio de seguridad que establece que si un sistema tiene fallas seguras, entonces el sistema debe fallar de tal manera que niegue el acceso a todas las sesiones posteriores hasta que el daño se solucione.

La mayor aplicacion de este principio se ve reflejado en la elección de la posición o punto de vista para tomar las decisiones con respecto a la seguridad de un sisterna. Estos puntos de vista son los siguientes:

- Negar por defecto: ***Todo lo que no es expresamente permitido es prohibido***
- Perrnitir por defecto: ***Todo lo que no es expresamente prohibido es permitido***

Arnbos puntos de vista pueden ser válidos, depende del criterio del administrador que lo elija. Para ciertos administradores "negar por defecto" es el mejor punto de vista mientras que para otros lo es el "permitir por defecto". Lo importante es entender que hay por detras de estos puntos de vista para no equivocarse al elegir uno de ellos.

1.5.5.1. Negar por defecto

Se trata de un criterio de extrema seguridad. Este punto de vista reconoce que lo desconocido puede causar daño. Se prohibe todo por defecto y para determinar que es lo se va a permitir *se* tiene que:

- Examinar los servicios que se van a brindar

- Considerar los riesgos que conllevan estos servicios elegidos y cuanto se pueden proteger
- Permitir solo los servicios que se entiendan, aquellos que se puedan proveer seguramente

Los servicios deben ser tratados por separado analizando la seguridad de cada uno y balanceando sus implicaciones de seguridad con las necesidades de los usuarios, basado en un análisis y disponibilidad de mecanismos que brinden protección estos servicios.

Por ejemplo, de acuerdo a las politicas de una organización solo se habilitan ciertos servidores tales como: correo electronico, web, DNS y FTP hacia fuera, porque la organización considera que son los unicos servicios con que debe contar para su normal funcionamiento. En base a esto se desabilitan todos los servicios restantes y se procede a estudiar: el funcionamiento de los servicios elegidos, posibles agujeros de seguridad que poseen y la forma de protegerlos.

1.5.5.2. Permitir por defecto

Este punto de vista asume que todo debe ser permitido por defecto y que se debe prohibir solo aquello que represente problemas de seguridad. La mayoría de usuarios y administradores prefieren este punto de vista, quienes piensan que todo debe habilitarse por defecto y solo algunos servicios que no se puedan habilitar.

A pesar de ser muy convincente, este punto de vista tiene dos inconvenientes basicos:

- Se asume que se conocen especificamente todos los peligros que involucra cada servicio y como explicarles a todos los usuarios el riesgo que corren al usarlo y la manera de prevenirse. Tratar de adivinar que peligros pueden involucrar todos los servicios de Internet es una tarea casi imposible debido a la cantidad de posibles problemas y a la excesiva información disponible sobre nuevos peligros, explotaciones de agujeros de seguridad antiguos, etc. Si algun

protocolo o servicio de Internet no se conoce todavia no se lo prohibe hasta que se tenga noticias de algun agujero de seguridad en este servicio o protocolo.

- El costo de mantener al sistema en buen estado. Este trabajo, que lo realiza el administrador, se constituye en toda una faena, tendra que estar atento a cada agujero o brecha de seguridad que se abre, reconfigurar o limitar el servicio o protocolo que provoco el problema, salvar los datos o recursos perdidos durante la violación del sistema y reconfigurar el firewall. Además de esto, el administrador tendra que educar a los usuarios internos para que no cometan errores. Evidentemente que mientras esto sucede el sistema puede ser víctima de un nuevo ataque y como el administrador esta realizando otras actividades pasara algun tiempo hasta que se percate del nuevo ataque y quizás ya sea muy tarde.

1.5.6. Participación Universal

Todos los sistemas de redes de computadoras requieren de la participación universal, es decir de la cooperación de todos los usuarios internos del sistema. Si algun usuario interno puede desactivar o desconfigurar la seguridad en un sistema, es posible que un atacante desde Internet ocasione un problema desde el interior del sistema. Aun el mejor firewall del mundo no podría proteger a un sistema si un usuario interno coloca líneas dial-up mal configuradas y ocasiona puntos de ingreso desde Internet.

Un usuario interno puede llegar a ser un potencial enemigo a la seguridad de un sistema. Es por esto que un sistema debe proveer seguridad a sus recursos protegiendose de sus propios usuarios internos.

Existen multiples formas en las que un usuario interno puede destruir o desactivar los mecanismos de seguridad voluntaria o involuntariamente. El administrador necesita que los usuarios de una red de cornputadoras le reporten situaciones extrañas y sospechosas que involucren fallas en la seguridad. Por ejemplo, los usuarios pueden contribuir a la seguridad del sistema utilizando contraseñas dificiles de adivinar, cambiando sus contraseñas regularmente, no prestar sus cuentas, etc.

La participación universal se logra voluntariamente e involuntariamente o a traves de las dos. Voluntariamente cuando los usuarios por sí solos ayudan al administrador y comprenden los riesgos que corre el sistema ante un eventual ataque. Involuntariamente cuando una autoridad les exige a los usuarios que actuen en base a reglas que contribuyan a fortalecer las politicas de seguridad.

7.5.7. *Diversidad de defensa*

Se considera como un complemento a la estrategia de "defensa en profundidad". Consiste en elegir multiples mecanismos de seguridad pero de diferentes tipos. Es decir, usar mecanismos de seguridad de diferentes distribuidores para reducir errores comunes o errores de configuración que los comprometan a todos.

La implementación de esta estrategia es compleja y costosa. Instalar varios mecanismos de seguridad llega a ser mas dificultoso, largo y caro que instalar solo un mecanismo .

Hay que tener cuidado de no caer en una falsa diversidad de defensa, instalando productos de seguridad que, a pesar de pertenecer a diferentes distribuidores, poseen las mismas

caracteristicas y no ofrecen una diversidad. Tambien se puede caer en falsa diversidad si los mecanismos de seguridad son configurados por la(s) misma(s) persona(s) ya que estos pueden compartir los mismos problemas si estos problemas se derivan de errores conceptuales por no comprender como funciona realmente un protocolo o servicio.

1.5.8. Simplicidad

La estrategia de simplicidad consiste en que el sistema de seguridad que se utilice debe ser simple. Este principio se basa en dos razones muy importantes:

- El mantener mecanismos simples los hace mas faciles de entender. Si no se entiende algo, es difícil saber si realmente es seguro o inseguro.
- Un sistema de seguridad complejo puede provocar fallas o agujeros. Los programas complejos tienden a fallar, y esas fallas pueden constituirse en problemas de seguridad. Aún si no provocan problemas de seguridad, los usuarios se acostumbraran a estas fallas y no lo notificaran a su administrador para prevenir futuros problemas.

CAPÍTULO II

DISENO DE LAS POLÍTICAS DE SEGURIDAD

2.1. Introducción

Antes de construir un sistema firewall para proteger a una red de Internet, es importante saber cuales son los recursos y servicios que ofrece la red. Por esta razon es importante elaborar un documento de "Politicas de seguridad de red" el cual describa todo lo concerniente a la seguridad en una red. En este capitulo se trataran ios siguientes puntos: definición y alcance de las politicas, método para establecer las politicas estableciendo el uso y responsabilidades en la red, el diseño de un modelo de seguridad y los planes de contingencia o planes de acción en caso de que la seguridad haya sido violada.

2.2. Politicas de Seguridad de red

Las politicas de seguridad son normas que marcan el comportamiento de una red con relación a su seguridad. Definir politicas de seguridad de una red significa desarrollar procedimientos y planes que protejan a los recursos de la red contra pérdidas y daños. Es importante tener

politicas de seguridad bien concebidas y efectivas, ya que de ellas depende que una organizacion pueda protegerse. Las politicas de seguridad son optimas cuando los recursos de la organizacion estan bien protegidos.

Lo primero y mas importante para que un administrador de red pueda elaborar las politicas de seguridad de su organizacion, es identificar que tipo de servicios y recursos se permitan a los usuarios accesar y cuales tendrán restricción debido a riesgos de seguridad.

Si los usuarios estan acostumbrados a gozar de un total acceso a la red, puede resultar difícil establecer politicas que restringan estos accesos. Hay que mantener en mente que las politicas de seguridad de la red que se implementen deben ser de tal manera que no impidan el buen funcionamiento de la organizacion. Si las politicas de seguridad no permiten que los usuarios ejecuten sus tareas efectivamente, los usuarios empezaran a buscar maneras de violar las seguridades.

Las politicas de seguridad estaran bien concebidas y seran efectivas, si tanto los usuarios como el administrador las aceptan y ayudan a mantenerlas.

2.2.1. Politicas de Seguridad Local

Una organizacion puede tener multiples lugares y en cada lugar sus propias redes. Si la organizacion es grande lo mas probable es que cada lugar tenga diferentes administraciones con diferentes objetivos. Si los lugares no estan interconectados entre sí a traves de una red interna, estos pueden tener sus propias politicas locales, pero si estos lugares estan interconectados entre sí, las politicas de seguridad deben tener metas comunes.

Las politicas de seguridad local deberan tomar en consideración la proteccion de sus recursos. Debido a que los lugares estan conectados a otras redes, las politicas deben considerar las necesidades de seguridad y requerimientos de las otras redes interconectadas.

2.3. Acercamiento a las politicas de seguridad

Para desarrollar las politicas de seguridad en una organizacion es necesario considerar los siguientes pasos:

- **Determinar la importancia y el riesgo de los recursos con que dispone la organizacion:** Para esto se realiza un análisis de riesgo de cada recurso en el cual se reconoce, la importancia en el normal funcionamiento de la organizacion y el riesgo o peligro al que esta expuesto. Con este paso se logra descubrir los puntos mas sensibles de la red.
- **Determinar la relación entre los usuarios y los recursos:** Para esto es necesario distinguir que tipos de usuarios van a tener acceso a los recursos, y cual es el comportamiento adecuado de los usuarios frente a los recursos.
- **Disenar un modelo de seguridad:** Con los dos pasos anteriores desarrollados, ya es posible diseñar una estrategia de seguridad para brindar proteccion a los puntos mas sensibles de la red. Para esto es necesario aplicar los conocimientos de arquitecturas y teconologías de firewalls. La información que se recopile en los pasos relatados anteriormente puede ser almacenada en la siguiente tabla:

Recursos de la Red			Probabilidades de rresgo	Tipo de usuario De quienes protegerse	Medidas de proteccion
codigo	nombre	importancia			

Las columnas de la tabla describen la siguiente información:

- **Codigo del recurso:** es una identificación interna del recurso asignada por el administrador (Información del 1er. paso).
- **Nombre:** es el nombre con que se reconoce al recurso (Información del ler. paso).
- **Importancia:** En este campo se anota el grado de importancia del recurso en el normal funcionalmiento de la organización. Puede ser evaluada en una escala numérica de 0 a 10, o usando expresiones difusas en lenguaje natural como: alta, moderada, baja, etc. [SIYA95].
- **Probabilidades de Riesgo:** Esta columna contiene la probabilidad de riesgo de que se den sobre cada recurso. Puede ser evaluada con valores numericos o con expresiones difusas en lenguaje natural como en el caso anterior de la columna de importancia (Información del ler. paso)
- **Tipos de usuarios de quienes protegerse:** Es una columna que describe que tipos de usuarios pueden ocasionar daños a los recursos de la red interna dependiendo de la accesibilidad tanto fisica como remota a dichos recursos (Información del 2do. paso).
- **Medidas de proteccion:** Contiene valores como: permisos del sistema operativo para archivos y directorios, alertar para servicios de red, firewalls para hosts y dispositivos de red, o cualquier otro tipo de descripción del tipo de control de seguridad (Información del 3er. paso).

En este acercamiento a las politicas de seguridad se desarrollara el primer paso (analisis de riesgo) y los dos siguientes, en las secciones **2.4.** Uso y responsabilidades de la red y *2.5.* Modelo de seguridad respectivamente, debido a la extension de estos temas.

2.3.1. Análisis de riesgo

Cuando se diseñan politicas de seguridad es importante entender que la razon para crearlas es asegurar que los mayores esfuerzos de proteccion se enfoquen a los puntos más importantes de la red. Esto significa que hay que entender que recursos de la red requieren ser protegidos y cuales son mas importantes que otros. Además, hay que identificar la fuente de peligro de la cual se estan protegiendo los recursos para brindar el tipo de proteccion que necesitan los recursos.

Para iniciar este analisis es necesario que el administrador tome en consideración las respuestas a las siguientes preguntas :

- ¿ **Clue** es lo que necesita proteger ?
- ¿ De que o quienes necesita proteger a los recursos ?

En las siguientes sub-secciones se despejaran estas incognitas y se detallara cómo se efectua el analisis de riesgo.

2.3.1.1. Identificación de los recursos

A continuación se provee una lista de los recursos que deberian ser considerados en la estimación de amenazas:

- **Hardware:** Procesadores, tarjetas, teclados, terminales, computadoras personales, impresoras, disqueteras, líneas de comunicacion, servidores de terminal, ruteadores, etc.
- **Software:** programas fuentes, programas objetos, utilitarios, programas de diagnostico, sistemas operativos, programas de comunicacion, etc.
- **Datos:** durante ejecucion, almacenados en línea, archivados, respaldos, archivos de auditoria, base de datos, etc.
- **Personas:** usuarios, operadores, etc.
- **Docurnentacion:** en programas, hardware, sistemas, procedimientos locales administrativos, etc.
- **Surninistros:** medios magneticos, formas, etc.

2.3.1.2. Identificación de amenazas

Para cada recurso es necesario establecer que tipos de peligro puede correr en su normal funcionamiento, para esto se hace una revision de todos los posibles riesgos que puede sufrir cada recurso de acuerdo a la clasificacion de tipos de ataques detallados en el capítulo I.

2.3.1.3. Cálculo del riesgo

El riesgo debe ser graduado en base a dos factores:

- Estirnacion de riesgo ante la perdida del recurso ***R***
- Estirnacion de la importancia del recurso en el normal funcionamiento de la red ***W***

Estas variables pueden tomar valores numericos o difusos mediante terminos linguisticos. Por ejemplo, al riesgo de perdida de un recurso (R) se le puede asignar un valor de 0 hasta 10; donde 0 representa **ninqun riesqo,** y 10 representa **alto riesqo.** Similarmente, a la importancia

de un recurso (W) se le puede asignar un valor entre 0 y 10; donde 0 representa **ninguna importancia** y 10 significa **alta importancia**. El peso total de riesgo de un recurso entonces es el producto del valor del riego y su importancia. Se podría expresar de la siguiente manera:

$$Wr_i = R_i \; O \; W_i \qquad \text{[SIYA95]}$$

Donde:

Wr_i = Peso total de riesgo del recurso i.

R_i = Riesgo del recurso i.

W_i = Importancia del recurso i.

En donde ***"O"*** es el producto aritmetico de los valores de Ri y Wi en el caso de utilizar valores numericos **[SIYA95]**. En el caso de utilizar valores difusos, Wri es el producto de la evaluación de reglas definidas por los expertos que proporcionaron los datos **[PELA95]**

A continuación se presenta una tabla donde se pueden distribuir los datos y guardar los

Recursos de la red		Riesgo del Recurso (R)	Importancia del Recurso (W)	Peso total de riesgo R O W
Numero	Nornbre			

Aun no se puede completar la Tabla I, ya que hasta ahora solo se ha podido listar la importancia y el riesgo de los recursos. Falta por determinar las columnas: tipos de usuarios de quienes

proteger y las medidas de protección. En las siguientes secciones se detallan los metodos para obtener la inforrnacion faltante.

2.4. Uso y responsabilidades en la red

Otro aspecto que debe considerarse en la definición de las politicas de seguridad es el uso y responsabilidades en la red. A continuación se da una serie de preguntas que ayudarian a determinar el uso y responsabilidades en una red:

- ¿ A quien es permitido el uso de recursos?
- ¿ Cual es el uso apropiado de los recursos ?
- ¿ Quien esta autorizado a otorgar accesos y aprobar usos ?
- ¿ Cuales son las responsabilidades de los usuarios ?
- ¿ Cuales son las responsabilidades del administrador ?
- ¿ Que hacer con la información susceptible ?

2.4.1. Identificando a quien es permitido el uso de recursos de la red.

Es necesario llevar un registro de todos los usuarios con sus alcances y caracteristicas por cada recurso para luego, identificar a quien es permitido el uso de los mismos. Por ejemplo:

- Usuarios internos: Son las cuentas asignadas a personas de la red interna. Estas personas pueden tener acceso físico y remoto a los recursos. Pueden constituirse en enemigos potenciales de la seguridad.
- Usuarios externos: Son usuarios de Internet. Estos usuarios pueden tener acceso remoto a la red y perpetrar un ataque.

- **Nombres** de grupos: Son un conjunto de usuarios clasificados de acuerdo al caracter de la organizacion. Por ejemplo: gerentes, asistentes, etc., para una organizacion comercial. **Estos** grupos pueden contar con usuarios internos o externos, por lo que pueden ganar acceso físico o remoto a la red interna.

2.4.2. Identificando el uso apropiado de un recurso.

Despues de determinar cuales son los usuarios que pueden accesar a los recursos de la red, se debe proveer de guias para el uso adecuado de estos recursos. Estas guias dependeran de la clase de usuario (interno, externo, grupos) y del recurso (servidores: Telnet, FTP, de impresion, etc.). Las guias de usuarios deben definir que se considera como uso aceptable, inaceptable y restringido por cada recurso. Estas guias se colocaran dentro de un documento llamado "Uso aceptable de politicas" (UAP).

El UAP debe indicar claramente a los usuarios que estos son responsables por sus acciones. No tiene sentido que se construyan mecanismos de seguridad si el usuario libera información haciendola disponible para posibles atacantes.

A continuación se presentan algunas preguntas que serviran de guia para que el administrador pueda un UAP:

- ¿ Esta permitido forzar contraseñas ? : Si a los usuarios les es permitido forzar las contraseñas pueden infiltrarse en cualquier sistema y provocar un ataque.
- ¿ Esta permitido el interrumpir servicios ? : No todos los usuarios deben tener privilegios (mayor acceso a recursos) sobre los sistemas, ya que por ignorancia o malicia, pueden provocar daños (interrupción de servicios, eliminación de datos, etc.).

- ¿ Esta permitido al usuario modificar archivos que no son de su propiedad ? : Se debe controlar el ambiente sobre el cual interaccionan los usuarios, caso contrario, estos pueden modificar archivos que no son de su propiedad y provocar daños.
- ¿ Podrian los usuarios compartir sus cuentas ? : Es aconsejable establecer que las cuentas de usuarios son personales y no se deben compartir. De esta manera si un usuario interno causa un daño se sabra de que persona se trata.

Otro aspecto a tomar en cuenta es lo concerniente a licencias y derechos de software. El UAP incluye un grado de penalización por el uso indebido de software. Un UAP que no establece claramente que es lo que esta prohibido, puede hacer difícil probar que un usuario ha violado un sistema.

Las excepciones a estas politicas podrian ser los miembros de un grupo especial de pruebas ("tiger team"), quienes poseen cuentas especiales y se encargan de probar las debilidades de las redes. Sin embargo, es necesario establecer con exactitud cuales son los privilegios de que gozan estos usuarios para realizar sus pruebas. A continuación se anotan algunas preguntas que ayudan a definir el alcance de estas cuentas :

- ¿ Que tipo de actividades de pruebas de seguridad son permitidos ?
- ¿ Qué controles deben colocarse para asegurase que las pruebas de seguridad no escapen del control ?
- ¿ Quien tendría el permiso para hacer pruebas de seguridad y cual es el proceso para obtener permiso para conducir estas pruebas ?

2.4.3. Determinando quien esta autorizado para otorgar acceso y aprobar el uso.

Las politicas de seguridad en una red deben establecer quien esta autorizado para otorgar acceso a los servicios de la red. Si el administrador no tiene control de quien esta otorgando acceso al sistema, es difícil controlar quien esta usando la red. Si el administrador puede identificar a las personas que estan encargadas de dar acceso a la red, se puede establecer que tipo de acceso o control ha sido otorgado. Esto ayuda a identificar la causa de posibles agujeros en la seguridad, como por ejemplo el otorgamiento de privilegios a usuarios que no lo anieritan.

Hay que considerar los siguientes factores para determinar quien o quienes daran acceso a los servicios en las redes:

- ¿ Se otorgara el acceso a servicios desde un punto central ?
- ¿ Que metodos se usaran para crear cuentas ?

Si la organización es grande y descentralizada, se pueden tener diversos puntos, por ejemplo uno para cada departamento, con propia responsabilidad sobre su red. En este caso, se debe tener una guía global de que tipos de servicios son perrnitidos para cada clase de usuario. Por otro lado, la administración centralizada puede crear problemas cuando los departarnentos quieran tener mas control sobre sus propios recursos.

El administrador necesitara acceso especial a la red, pero otros usuarios tambien pueden necesitar ciertos privilegios. Es cierto que al restringir el acceso y no otorgar privilegios a los usuarios, hacemos mas segura a la red, pero podriarnos hacer que los usuarios no cumplan

eficientemente con sus tareas. Por lo tanto, es necesario un balance entre denegar privilegios para hacer mas segura la red y otorgar privilegios a las personas que realmente los necesiten.

Si existe un gran numero de redes y administradores es difícil mantener un seguimiento de que permisos han sido otorgados. Despues que el usuario hace el requerimiento de privilegios y este es autorizado por el usuario supervisor, el administrador debe documentar los cambios producidos. A continuación se presenta una tabla cuyo formato sirve para este proposito:

Recursos de la red		Tipo de usuario	Tipo de Acceso
Codigo	Nombre		

Tabla 111. Cuadro para otorgar acceso a los recursos

- **Tipos de usuarios:** Los diversos tipos de usuarios que posee una organizacion. Por ejemplo, usuario externo, interno, etc.
- **Tipo** de **acceso:** puede ser usado para una descripción del acceso, por ejemplo “solo lectura“ o “solo ejecucion”, etc.

Tambien hay que examinar el procedimiento que se utilizara para crear cuentas de usuarios y asignacion de permisos. La persona que esta autorizada para dar acceso debe gozar de privilegios tales como “root” en Unix, y ser alguien muy confiable para esta tarea. Las vulnerabilidades en la seguridad pueden facilmente ocurrir como resultado de errores hechos por el administrador del sistema. Si se tienen bien documentados los procedimientos, se

reducira el riesgo. Se recomienda que el proceso de creación de cuentas sea simple y facil de entender, para de esta manera evitar errores.

Otro aspecto a considerar es la selección de una contraseiia inicial para cada cuenta. El hecho de dejar que la contraseña inicial sea el mismo nombre del usuario o que sean espacios en blanco, puede dejar cuentas ampliarnente abiertas a un ataque. La contrasefia inicial no debe ser obvia, es por esto que tampoco es valido que la contraseña sea una funcion del nombre del usuario, parte del nombre o algun algoritmo, que genere contrasefias, puesto que pueden ser adivinados.

Existen usuarios que casi no utilizan sus cuentas, e incluso algunos que nunca se han conectado. En estas circunstancias la contrasefia inicial no es segura, por lo que se aconseja al administrador desabilitar la cuenta para forzar a que el usuario se acerque a preguntar al administrador por su cuenta y cambie su contrasefia.

Otro grave error es mantener la contrasefia inicial ya que pudo haber sido robada, lo aconsejable es cambiarla. Existen sistemas operativos o programas especiales que forzan a los usuarios a cambiar sus contrasefias, por ejernplo, utilizando contraseñas que caducan o dejan de funcionar de acuerdo a un tiempo establecido por el administrador.

2.4.4. Determinando las responsabilidades de los usuarios.

Las politicas de seguridad deben definir los derechos y responsabilidades para usar los recursos y servicios de la red. A continuación se citan una serie de aspectos a considerar:

- ¿ Que se considera abuso en terrninos de uso de recursos en la red ?

- ¿ Esta permitido a los usuarios compartir cuentas o dejar que otros las usen ?
- ¿Deberían los usuarios revelar sus contraseñas en bases temporales para permitir que otros trabajen con sus cuentas ?
- En las politicas de contrasefias: ¿Cuán frecuente deben los usuarios cambiar sus contraseñas?
- ¿ Son los usuarios responsables de sacar respaldos de sus datos o es responsabilidad del administrador ?
- ¿ Que acciones legales se tomarian en caso de revelación de informacion ?
- Una política concerniente a correos controversiales, listas de correo o discusion. Establecer que tipos de foros seran permitidos, contenido de correo, etc.

2.4.5. Determinando las responsabilidades del administrador del sistema.

Cuando se corre riesgo en la seguridad de un sistema, el administrador puede tener la necesidad de recoger informacion de los archivos del sistema, incluyendo los del directorio "home" de cada usuario. Por otro lado el usuario tambien requiere de cierta privacidad. Entonces surge una controversia de la privacidad y derechos del usuario con la necesidad de los administradores.

Las politicas de seguridad deben especificar si el o los administradores pueden examinar los directorios privados para el diagnóstico de problemas e investigaciones de violaciones a la seguridad. Tambien se adjuntarían las respuestas a las siguientes preguntas:

- ¿ Puede el administrador monitorear o leer archivos de un usuario por cualquier razon?
- ¿ Pueden los administradores tener el derecho de examinar la red y su trafico ?

2.4.6. *Que hacer con la informacion sensible.*

Se debe determinar que tipo de datos importantes y sensibles por su confidencialidad estan almacenados en un sistema especifico. Antes de otorgar acceso a servicios en un host, hay que considerar a que otros servicios e informacion los usuarios pueden ganar acceso. Si el usuario no necesita trabajar con datos sensibles, entonces no debe tener una cuenta en el sistema que contiene estos datos.

Se tiene que considerar si existe una adecuada seguridad en el sistema para proteger los datos sensibles. Las politicas tambien les haría conocer a los usuarios que necesitan trabajar con informacion sensible, de que servicios ellos disponen (servicios de Internet, procedimientos de almacenamiento, actualización, etc. dependiendo del tipo de usuario).

En la culminación de esta seccion, ya es posible obtener la informacion de la columna de "tipos de usuarios de quienes proteger" de la Tabla I. Sin embargo aun es necesario deterrninar la columna de las medidas de protección para cada recurso. Esta informacion faltante se la obtiene a traves del diseño de un modelo de seguridad.

2.5. Modelo de seguridad

En esta seccion se discuten todos los aspectos generales para diseñar un modelo de seguridad y prevenir problemas futuros. Entre estos se encuentran:

- Identificación de posibles problemas
- Diseño de controles en las politicas
- Detectando y monitoreando actividades no autorizadas
- Reportes de procedimientos

2.5.1. Identificacion de posibles problemas

Ademas de diseñar un modelo de seguriodad es necesario revisar los siguientes aspectos:

- Puntos de acceso
- Sistemas mal configurados
- Errores en software
- Amenazas de usuarios internos
- Seguridad física

2.5.1.1. Puntos de acceso

Hay que identificar todos posibles accesos externos a la red, ya que estos se pueden convertir en puntos de entrada para usuarios no autorizados. Tener muchos puntos de acceso incrementaran los riesgos de seguridad en la red.

En las redes de la figura No. 2-1 se observan diversos puntos de ingreso a las redes. En el segmento A los puntos de acceso son el servidor de terminales y el ruteador 2. Ademas el computador 1 tiene un modem privado el cual es usado para conexiones dial-out. En el segmento B, el host 2 tambien es un punto de acceso a la red.

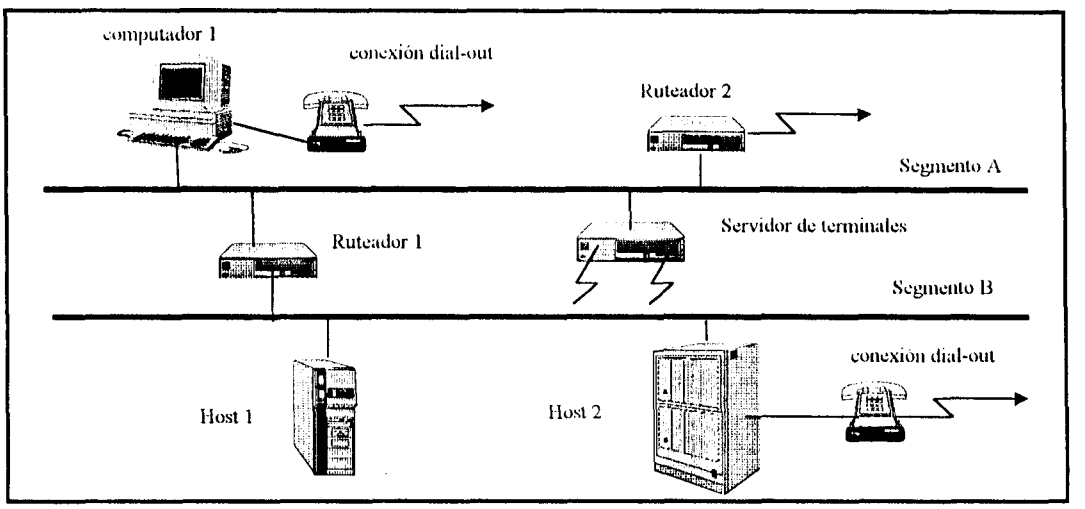


Figura No. 2-1. Identificando los puntos de acceso en una red

Considere la siguiente situación: El usuario del computador 1 en el segmento A, puede tener una cuenta con un proveedor de internet. Supongamos que este usuario utiliza una conexión SLIP o PPP. Si el software TCP/IP, que el usuario corre en el computador 1, está configurado con características de un ruteador, es decir que pueda enviar paquetes tanto adentro como afuera de su red, es muy posible que un intruso pueda invadir la red. Hay que anotar que el usuario pudo no deliberadamente habilitar el computador como un ruteador. El sistema operativo pudo haberlo hecho por defecto. Si la conexión dial-up del usuario fuese para mantener una emulación de terminal y no una sesión TCP/IP, quizás no habría daño.

Si las políticas de seguridad establecen la prohibición de conexiones privadas las situaciones de riesgo de este tipo pueden ser prevenidas. Esto también subraya la importancia de tener políticas de seguridad que claramente delínean el AUP para la red.

Los servidores de terminales pueden representar un riesgo de seguridad si no son adecuadamente protegidos, ya que muchos de estos servidores de terminales disponibles en el mercado no requieren algún tipo de autenticacion. Por lo tanto, los intrusos pueden usar los servidores de terminales para disfrazar sus acciones.

2.5.1.2. Sistemas mal configurados

Si los intrusos penetran la red, usualmente tratan de comprometer todos los hosts. Los hosts que actuan como servidores de telnet son blancos populares. Si el host esta mal configurado, el sistema puede ser facilmente comprometido.

2.5.1.3. Errores en software

Cuanto mas complejo sea un programa, mas probable es que existan errores en su codigo. Estos errores se constituyen en posibles agujeros o brechas de seguridad que pueden ser aprovechados por los intrusos. Es por esto que los administradores de sistemas deben tener en consideración las posibles fallas de los programas que utilicen, y si es posible instalar parches y versiones actualizadas a fin de controlar estos errores.

2.5.1.4. Amenazas de usuarios internos

Si un usuario interno decide atacar la red, puede representar una considerable amenaza a la seguridad de la red. Si se tiene acceso físico a los componentes de un sistema, este es aun mas fácil de comprometer. Por ejemplo, muchas estaciones de trabajo, facilmente, pueden ser manipuladas para otorgar acceso. Muchos servicios de aplicaciones TCP/IP tales como telnet, rlogin y ftp tienen mecanismos muy debiles de autenticacion donde las contraseñas son enviadas por teclado.

2.5.1.5. Seguridad física

Todos los recursos críticos tales como backbones, enlaces de comunicacion, hosts, servidores importantes y maquinas claves deben ser localizadas en areas fisicamente seguras. Fisicamente seguras significa que la maquina es colocada en una habitación o colocada en una manera que restringa el acceso físico los dispositivos de almacenamiento de datos.

Muchas veces no siempre es facil rnantener una seguridad fisica en las maquinas. Tambien hay que limitar el acceso de maquinas no muy seguras a las demas que sí son seguras. En particular no permitir ingresos a hosts usando mecanismos de acceso remotos (rsh, rlogin, rcp, etc.)

2.5.2. Diseno de controles en las politicas

Para diseñar los controles en las politicas es necesario tener en mente los tipos de proteccion y estrategias de seguridad analizadas en el capitulo I (1.4. Tipos de proteccion y **1.5.** Estrategias de seguridad). El objetivo principal de estos controles es solucionar los problemas de seguridad que posee la red interna.

Los mecanismos de control y proteccion deben ser adecuadamente seleccionados, ya que ellos brindaran seguridad y podrán registrar apropiadamente los daños encontrados durante un posible ataque. Estos controles deben ser implementados de acuerdo a sus costos reales, es decir no gastar esfuerzos para sobreproteger y restringir el uso de un recurso si el riesgo de exposicion de este es muy pequeño.

El sentido comun es frecuentemente una herramienta muy efectiva para diseñar un modelo de seguridad. Si se elaboran esquemas muy sofisticados e impresionantes, estos pueden ser muy caros. Tambien si la solución de seguridad es muy elaborada, puede resultar dificil de implementarla y administrarla (ver sección 1.5.8 estrategia de simplicidad).

Los controles que se seleccionen constituyen la primera línea de defensa en la protección de la red. Si la mayor amenaza al sistema son usuarios externos (de Internet), no deberia gastarse por ejemplo en tarjetas de identificación magneticas para cada usuario interno sino más bien en la implementacion de un firewall. Si la mayor amenaza son los accesos no autorizados, habria que establecer procedirnientos para carnbiar las contraseñas de los usuarios periodicarnente.

2.5.3. Detectando y Monitoreando actividades no autorizadas

Monitorear un sistema involucra observar diversas partes de un sistema y buscar cualquier situación inusual o sospechosa (actividades no autorizadas). La meta del monitoreo es detectar las posibles brechas de seguridad lo mas tempranamente posible a fin de poder responder inmediatamente.

El monitoreo debe realizarse periodicamente: por días o semanas. Lo recornendable es no dejar mas de una sernana entre los monitoreos, de esta manera si se perpetra un ataque, este pueda ser rapidarnente detectado.

Si se utilizan herrarnientas para monitoreo, se deben examinar las salidas de las misrnas. Si se tienen archivos de logs voluminosos, los cuales resultan complicados de leer y manipular, se

pueden utilizar pequeños programas que lean estos archivos y obtengan la informacibn deseada.

En las siguientes secciones se dan ideas de como se puede monitorear a un sistema.

2.5.3.1. Mecanismos de Monitoreo

Muchos sistemas operativos almacenan informacion de los logins en archivos especiales. Los siguientes consejos pueden resultar muy apropiados para realizar un monitoreo basado en estos archivos de logins:

- Se pueden comparar listas de los actuales usuarios conectados con historias de login pasados. La mayoría de los usuarios tienen horas regulares de trabajo y si una cuenta presenta actividad en una hora fuera de lo normal, debe ser monitoreada muy cercanamente ya que puede tratarse de un intruso.
- El sistema operativo puede tener facilidades de sistemas de login, tales como el **syslog** usado en Unix. Los logs producidos por tales herramientas pueden ser examinados buscando mensajes de error del software del sistema. Por ejemplo, un gran numero de fallas en el login intentado en un período de tiempo indica que alguien posiblemente esta tratando de adivinar las contraseñas.
- Muchos sistemas operativos tienen comandos, como el **ps** en Unix, para listar los procesos que se estan ejecutando. Estos pueden ser utilizados para detectar a usuarios corriendo programas a los que ellos no estan autorizados usar.
- Los firewalls pueden ser usados para producir un archivo de log para todos los accesos a la red.
- Si se tienen recursos especiales que se quieren monitorear, se puede construir una herramienta propia usando utilitarios estandares del sistema operativo. Por ejemplo se

puede combinar los comandos ***ls*** y ***find*** en un programa para exarninar los accesos a archivos privilegiados y cambios de permisos a los mismos. Las diferencias en los permisos a archivos claves indicarían modificaciones no autorizadas.

2.5.3.2. Esquemas de monitoreo

El administrador puede realizar monitoreos frecuentes a lo largo del día. Si el monitoreo es hecho permanentemente, puede llegar a ser muy tedioso, pero algunos cornandos de monitoreo pueden correrse en algun tiempo durante los momentos ociosos.

Si el administrador corre varios comandos para monitorear a diferentes tiempos a lo largo del dia, es muy difícil para un intruso predecir las acciones del administrador. Si el intruso no puede adivinar cuando el administrador hizo un monitoreo, corre un gran riesgo de ser detectado.

Por otro lado, si un intruso conoce que a las 6:00 p.m. diariamente el sistema es chequeado para ver quien esta conectado, los intrusos esperaran para conectarse despues del monitorec.

2.5.4. Reportando procedimientos

Si un evento de acceso no autorizado es detectado, se deben tener procedirnientos de cómo actuar ante este evento y a quien debe ser reportado. Las politicas de seguridad tambien deben cubrir los siguientes aspectos:

- Procedimientos de manejo de cuentas
- Procedirnientos para manejo de configuración
- Procedimientos de recuperación
- Procedimientos de reportes de problemas para administradores del sistema

Estos aspectos nombrados son establecidos de acuerdo al criterio del administrador de la red. Se trata de procedirnientos internos que deben ser definidos por el administrador ya que el es quien va a rnanejar la red.

2.5.4.1. Procedimientos de manejo de cuentas

Cuando se crean cuentas a los usuarios, se debe tener cuidado de no dejar cualquier agujero en la seguridad. Las cuentas sin contraseñas son peligrosas aun cuando estas no ejecuten un interpretador de comandos, tales como cuentas que existen solo para ver quien esta conectado en el sistema. Si estas no estan configuradas correctamente, la seguridad del sistema puede ser comprometida. Por ejemplo, si el usuario anonimo usado por FTP no es configurado correctarnente, podria permitir que cualquier usuario accese al sistema y baje archivos. Si existen errores en la configuración de esta cuenta y los permisos de escritura son otorgados, un intruso puede cambiar el archivo de contraseñas o destruir el sistema.

Las politicas deben incluir procedimientos para mantener rastros de quien tiene una cuenta con privilegios, tales como la cuenta del administrador en Unix (root). Si se conoce la contraseria de la cuenta root, se podria usar el comando ***su*** y asumir privilegios de root. Se deben irnplementar politicas que de enfasis al carnbio de contraseñas para usuarios privilegiados en tiernpos regulares.

2.5.4.2. Procedimientos para el manejo de la configuración

Se deberian mantener actualizadas las versiones del sistema operativo y utilitarios críticos. Las debilidades de seguridad en sisternas viejos son usualmente bien conocidas, y es muy probable que cualquier intruso conozca de estos problernas. Desafortunadarnente, algunas nuevas

versiones de programas, mientras por un lado arreglan viejos problemas de seguridad, por otro introducen nuevos problemas.

2.5.4.3. Procedimientos de recuperación

Cuando se instale una nueva version de un sistema operativo, no solo hay que sacar respaldo del kernel, sino tambien de los archivos que son usados para compilar y configurar el sistema operativo. Lo mismo se aplica para otras aplicaciones y programas de la red.

Los resplados de archivos de un sistema representan una seguridad dentro de las politicas. No solo protegen en el eventual caso en que un dispositivo de hardware falle, sino tambien contra eliminaciones accidentales o como medida de seguridad si el sistema ha sido violado. Si el administrador sospecha que el sistema ha sido comprometido, se puede restaurar todo desde un respaldo de protección. Si no se puede detectar cuando un cambio no autorizado toma lugar, se tiene que examinar los diversos respaldos a fin de encontrar la configuración original.

2.5.4.4. Procedimientos de reportes de problemas para administradores del sistema

Los administradores del sistema deberian tener un procedimiento definido para reportar problemas de seguridad al jefe de la organizacion. En instalaciones de una red grande, puede ser hecho creando “mailing lists” que contengan las direcciones de e-mail de todos los administradores en la organizacion.

2.6. Plan de accion cuando las politicas de seguridad son violadas

Un aspecto aparte del método para desarrollar politicas de seguridad anteriomente detallado es el establecimientos de acciones de contingencia. Si las politicas de seguridad son violadas, el sistema esta abierto a cualquier tipo de ataque. Algunas veces es facil detectar cuando una política ha sido violada, pero otras veces puede ser indetectable. Los procedimientos de seguridad que el administrador implemente minimizan la posibilidad de que la infracción no sea detectada. Cuando se encuentre una violacion a las politicas, se la debe clasificar si fue por negligencia, por accidente o error, ignorancia de las reglas, o deliberadamente. Para cada una de estas circunstancias, las politicas de seguridad deben proveer la guia necesaria de las acciones a tomar.

Cuando una violacion toma lugar, la respuesta puede depender del tipo de usuario responsable y el tipo de violacion.

Las violaciones pueden ser convertidas por una gran variedad de usuarios. Algunos de estos usuarios pueden ser internos y otros externos. Dependiendo de esto se determina que accion debe tomarse. Los usuarios internos y externos deben tener conocimiento de las normas de seguridad. Si la red tiene usuarios externos que la usan legalmente, es responsabilidad del administrador verificar que estos tengan conocimiento de las politicas que se tienen. Esto ultimo es muy importante si el administrador necesita tomar una accion legal contra la parte ofensiva.

La sancion que debe imponerse tanto al usuario interno como externo responsable tambien depende de las consecuencias que acarreen las faltas cometidas. Por esto la organización

debe definir cuales son las faltas graves o faltas leves. Por ejemplo, el robo de información financiera confidencial es una falta muy grave ya que puede atentar contra la estabilidad de una organizacion; la inhibición de un sistema es una falta leve ya que se puede reiniciar al sistema nuevamente.

2.6.1. Respuesta a violaciones por parte de usuarios internos

Ante violaciones por parte de los usuarios internos se pueden tener las siguientes situaciones:

- Un usuario local viola las politicas del sistema local.
- Un usuario local viola las politicas de un sistema externo.

Si se trata del primer caso, el adrninistrador puede tener mas control sobre que tipo de respuesta se debe tomar por la falta cometida. En el segundo caso, si un usuario local ha irrumpido en la seguridad de una sistema externo, la situación es muy complicada debido a que involucra a otra organizacion, y la respuesta que se tome sería discutida con la organizacion cuya política ha sido violada. Además, tendría que consultarse con organizaciones internacionales especializadas en leyes de seguridad de computadores.

2.6.2. Respuesta a violaciones por parte de usuarios externos

En el caso de que usuarios externos (usuarios de Internet, ajenos a la organizacion), al igual que en el segundo caso de violaciones de usuarios internos a un sistema externo, la situación es complicada. Dependiendo de la gravedad de la falta, lo recornendable es que la organizacion interna se ponga en contacto con la organizacion a la que pertenece el usuario externo a fin de discutir la acción a tomar. Como medida adicional se debe tomar en

consideración los criterios de agencias de leyes internacionales que definen protocolos para estos casos.

2.6.3. Estrategias de respuesta

Ante las posibilidades de respuesta anteriormente descritas, existen dos tipos de estrategias de respuestas opuestas:

- Proteger y Proceder
- Perseguir y Acusar

2.6.3.1. Proteger y Proceder

Si los administradores sienten que la organización es muy vulnerable, deben elegir esta estrategia. La meta de esta estrategia es proteger inmediatamente la red y restaurarla a su normal funcionamiento para que los usuarios continuen con su trabajo. Para hacer esto el administrador debe interferir con las acciones de los intrusos y prevenir futuros problemas. Al final, se requiere hacer un análisis de la cantidad del daño hecho.

A veces no es posible restaurar inmediatamente la red y ponerla en su normal funcionamiento resulta un proceso lento. Tambien puede ser necesario aislar segmentos de red y apagar los sistemas con el objetivo de prevenir accesos no autorizados. Una desventaja de este método es que los intrusos conocen si han sido detectados y evitan ser perseguidos. Además en un futuro ya conocen los puntos debiles del sistema de seguridad.

La estrategia "proteger y proceder" debe ser usado bajo las siguientes condiciones:

- Si los recursos de la red no estan bien protegidos: Si los recusos estan desprotegidos, es muy probable que se originen ataques que ocasionen daños potenciales y urgentes de restaurar.
- Si una actividad intrusa continuamente resulta un gran dano y riesgo financiero: Si los intrusos ocasionan graves daños financieros, es necesario restaurar antes de que se haga rnas grande.
- Si existe un considerable riesgo para los usuarios de la red: Los usuarios internos pueden ser objeto de robos de contraseñas, robo de informacion personal, numeros de cuentas de banco, tarjetas de credito, etc.), etc. Esto puede constituirse en una puerta abierta para los intrusos.
- Si el costo de una persecución a un intruso es muy alto: Para perseguir a un posible intruso es necesario tener mecanismos de monitoreo, programas especiales o trampas, los cuales pueden tener un costo muy elevado para una organización.

2.6.3.2. Perseguir y Acusar

Este metodo tiene como meta permitir intrusos para perseguir sus acciones mientras se monitorea sus actividades. Este metodo no establece restricciones a los potenciales intrusos, de tal manera que éstos no se dan cuenta que estan siendo monitoreados. Es recomendado por agencias de leyes, debido a que se llevan pruebas a estas agencias para que puedan iniciar una acusación legal contra los intrusos. La desventaja de este metodo es que el intruso continuara robando informacion o haciendo otros daiios mientras se esperan los resultados de la acusacion formulada anteriormente.

Una posible manera de monitorear a los intrusos sin que puedan causar daños al sistema es construir una carcel, la cual define un ambiente simulado con datos falsos en el que los intrusos puedan ser monitoreados y registrados sin sospechar que los estan vigilando.

Es recomendable instalar una carcel en una maquina de sacrificio que se encuentre en un segmento aislado de una red para minimizar el riesgo de las actividades del intruso. Se puede construir una carcel usando dos metodos: modificando el sistema operativo o utilizando un programa especial o trampa. El primer metodo depende del grado de manejo del sistema operativo. La persona que modifique el sistema operativo tiene que tener gran dominio sobre las variables de ambiente, procesos, y comandos del sistema operativo. El segundo metodo consiste en utilizar programas especiales (comerciales o publicos) sobre el sistema operativo, los cuales pueden ser complejos de instalar.

Por ejemplo en un sistema Unix, existe el mecanismo ***chroot*** para crear una carcel. El ***chroot*** confina un proceso a un directorio de los archivos del sistema. Este mecanismo puede restringir el acceso de un usuario (FTP, Telnet, etc.) a directorios del sistema operativo (/etc/passwd, etc.). Además crea un ambiente falso, en el cual el usuario es engañado pensando que tiene acceso a todos los directorios mientras todas sus actividades son registradas.

En su mayoría los programas comerciales tales como el firewall de IBM, utilizan agentes SNMP (Simple Network Management Protocol), para crear trampas. Estos agentes simulan un ambiente falso a fin de capturar infraganti al intruso. Para configurarlos se requiere tener conocimientos del protocolo SNMP.

El metodo “Perseguir y acusar” puede ser usado bajo las siguientes condiciones:

- Si los recursos y sistemas estan bien protegidos: Si los recursos son seguros, el administrador no se preocupa por restaurar y se dedica a perseguir a los autores del daño.
- Si la red ha sido centro de ataques de intrusos y estos no dejan de hacerlo: El administrador puede cansarse de restaurar los daños frecuentemente y dedicarse a perseguir a los causantes.
- Si la red es apropiada: Si la red de la organizacion es segura como para incurrir el riesgo de permitir intrusos, es decir que existan mecanismos de seguridad, monitoreo, registro de acciones se puede obtener pruebas para acusar sin sufrir un ataque.
- Si las herramientas de monitoreo y registro pueden archivar bastante información: Si la capacidad de registro es completa se pueden recoger evidencias y posteriormente acusar al intruso.
- Si existe disponibilidad para acusar: En el caso de que un usuario interno sea el causante de un daiio, la organizacion deberá sancionarlo; si se trata de un usuario externo, este tendría que ser denunciado a la organizacion a la que pertenece y establecer una demanda si ambas organizaciones estan afiliadas a agencias de leyes de seguridad de computadores.

2.6.4. Contactos y responsabilidades con organizaciones externas.

Las políticas de seguridad de red incluyen tambien la definición de procedimientos para interactuar con organizaciones externas que puedan tener contactos con agencias de leyes o expertos legales. En el Ecuador no existe aun ley o entidad alguna que delimite el comportamiento adecuado entre organizaciones nacionales que se conectan a Internet. Por lo tanto lo recomendable es afiliarse a las organizaciones extranjeras que ofrecen ayuda (soporte)

ante problemas de seguridad, como CERT (Computer Emergency Response Team), CIAC (Computer Incident Advisory Capability). .

CAPITULO III

DISENO DE SISTEMAS DE FIREWALL

3.1. Introducción

Este capítulo abarca conceptos fundamentales como: ¿qué es un firewall?, y ¿qué es lo que puede y no puede hacer un firewall?. Adicionalmente se estudian los diseiios de sistemas de firewall de acuerdo a la tecnologia usada (filtraje de paquetes, sistemas proxy, host bastion, autenticacion y encriptacion) y arquitecturas que manejan (host dual-homed, screened-host y screened subnet). Finalmente se estudia cada una de las tecnologías de firewalls, sus ventajas, desventajas y funcionamiento.

3.2. Firewall: Alcance y limitaciones

Un firewall es un mecanismo del modelo de seguridad de red que tiene como objetivo proteger un sistema de red de computadoras de ataques electronicos provenientes de Internet u otra red. El termino “firewall” (corta-fuego en español) se lo adquirio por la semejanza con el corta-fuego

en el campo de la construcción. Un corta-fuego es una pared que evita que el fuego pase de un extremo a otro. De igual manera, un firewall para Internet evita que los peligros que se encuentran en otras redes no penetren a un sistema de red de computadoras. Sin embargo, un firewall se asemeja mas al foso o estanque que los castillos medioevales colocaban a su alrededor para protegerse de ataques cumpliendo con los siguientes objetivos:

- Restringir el ingreso solo por un punto de control.
- Prevenir que intrusos tomen control de otros mecanismos de protección con el fin de arruinar todo el sistema defensivo.
- Restringir la salida por un unico punto de control.

Un firewall para Internet se coloca por lo regular en un punto entre Internet y la red de computadoras que se desea proteger, como se observa en la figura No. 3-1. Así, todo el trafico dirigido a la red interna y proveniente de Internet tiene que atravesar el firewall. Es por esto que un firewall tiene la oportunidad de dejar pasar solo el trafico aceptable y rechazar lo que las politicas de seguridad establecen.

Desde el punto de vista lógico, un firewall es un objeto separador, restringidor y analizador de trafico. Pero fisicamente puede constituirse de un conjunto de hardware: ruteadores, combinación de ruteadores, computadoras y redes, todos ellos con su respectivo software. Las maneras de configurar todos estos equipos depende de las politicas de seguridad y del presupuesto de la organización que se conecta a Internet.

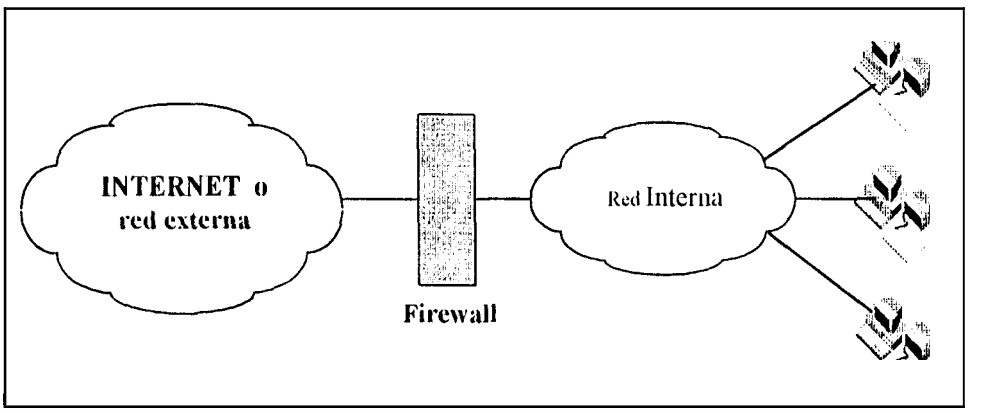


Figura No. 3-1. Representación de un firewall

Así como el foso de un castillo medioeval no es invulnerable, de igual manera no lo es un firewall para Internet. Un foso no protege contra personas que ya estan adentro, y aunque se coloquen mas defensas internas, los intrusos pueden hacer sus ataques mas efectivos y penetrar al castillo. Asi mismo, un firewall para Internet tiene sus desventajas, que hacen que ningun firewall sea invulnerable. Disponer de uno involucra mucho costo y esfuerzo, y muchas veces no se compensa si la seguridad de un sistema puede ser violada.

Pero pese a estas limitaciones y desventajas, los firewalls constituyen la mejor manera de proteger a una red que se conecta a Internet. Aqui se presenta el gran dilema de conectarse a Internet; abrirse al mundo, obtener mayor publicidad, obtener información y otros beneficios en contra de los costos que esto representa. Por lo tanto, antes de conectarse a Internet una organización debe hacer un balance entre los beneficios y costos (incluyendo un sistema de seguridad) que puede tomar.

Un firewall no solo es útil para proteger una red de computadoras de posibles ataques provenientes de Internet, tambien sirve para proteger lugares que poseen diferentes necesidades de seguridad. Es decir cuando en dos redes que se enlazan, una tiene que ser mas segura que la otra. Por ejemplo, en un ambiente universitario, una red administrativa que se enlaza con una red de laboratorios para estudiantes, la red administrativa debe protegerse de ataques provenientes de los laboratorios.

Los firewalls representan grandes beneficios al brindar la seguridad en un sistema, pero no resuelven todos los problemas de seguridad ya que tienen limitaciones.

3.2.1. Alcance de los firewalls

Las ventajas que ofrece un firewall son:

3.2.1.1. Concentra las medidas de seguridad en un sólo punto

Un firewall debe representar el punto de estrangulamiento entre una red interna y externa o Internet. Por este punto debe pasar todo el trafico que entra o sale de la red interna que se desea proteger. La gran ventaja de este esquema es que permite concentrar todas las medidas de seguridad en el punto de estrangulamiento.

Esta manera de enfocar la seguridad es mas eficiente que tomar decisiones de seguridad en varios puntos alrededor de una red. Si una red tiene varios puntos por los cuales deja una "puerta abierta" a Internet, las medidas de seguridad se convertirian complejas y difíciles do implementar. Además, desde el punto de vista economico es mas factible concentrar la seguridad en un solo punto que en varios.

3.2.1.2. Fortalece las políticas de seguridad

Toda organizacion antes de conectarse a una red externa o Internet debe elaborar sus politicas de seguridad para establecer claramente los servicios que esta organizacion va a permitir y cuales va a rechazar. Ante esto, un firewall como punto de estrangulamiento, se constituye en un regulador de trafico entre Internet y una red de cornputadoras; es el organo que decide aprobar o reprobar algun servicio obedeciendo a las politicas de seguridad de una organizacion. El firewall que se coloque en una red de computadoras debe ser configurado correctamente evitando cualquier ambiguedad conforme a lo que las politicas de seguridad establecen.

El nivel de control de un firewall varía, puede controlar servicios, usuarios, direcciones de un dominio, maquinas, etc. Por ejemplo: una organizacion decide permitir el servicio FTP anonimo entrante (protocolo de transmision de archivos) hacia una maquina interna con dirección **192.188.59.3** desde el dominio 200.10.0.0 y solo a los usuarios gmazzari, **slima, kchong** de ese dominio.

No todos los firewalls tienen todas estas habilidades, ni todas las organizaciones las requieren. Para una organizacion representara una gran ayuda y para otra sera demasiada tecnologia. Todo depende de las necesidades de seguridad y los recursos que una organizacion posea.

3.2.1.3. Archiva información activamente

Debido a que un firewall se encuentra ubicado entre una red de computadoras e Internet, por este pasa todo el trafico. Por lo tanto, el firewall se convierte en un buen lugar para registrar todos los eventos que ocurre entre la red de computadoras protegida y la red externa o Internet. Esta medida es beneficiosa porque si sucede algun ataque, revisando el registro de eventos se puede localizar la falla y el posible culpable.

3.2.1.4. Limita la exposición

A pesar de que un firewall no es la solución a todos los problemas de seguridad, sí limita el daño que un problema de seguridad de red puede hacer sobre toda una red.

3.2.2. Limitaciones de los firewalls

Existen amenazas que están fuera del alcance de un firewall. Es por esto que surge la necesidad de complementar la seguridad incorporando seguridad de host (ver sección 1.4.3.), seguridad fisica e informacion a los usuarios internos. Las liminitaciones de un firewall son:

3.2.2.1. No protege de usuarios internos

Un firewall puede proteger que un usuario interno transfiera informacion interna sensitiva desde una red de cornputadoras hacia Internet, pero no puede proteger de la transmision de esta informacion por otros medios. Por ejemplo, el firewall es incapaz de evitar que un usuario interno copie la informacion sensitiva por medio de un disquete o tape y la distribuya.

Los usuarios internos pueden robar datos y dañar el hardware y el software de la red. Ante esto un firewall no sirve de nada. Por esto es necesario adoptar medidas de seguridad interna como la seguridad de hosts y la seguridad fisica.

3.2.2.2. No protege de conexiones que no pasan a través de éste

Esta limitación esta relacionada con la anterior, un firewall puede controlar todo el trafico que por este pasa, pero no puede hacer absolutamente nada cuando esto no sucede. Esta es la situación cuando se tiene un acceso dial-up en una red y el firewall desconoce de este acceso.

Esto constituye un problema de manejo de recursos mas que un problema tecnico. Al adoptar un sistema de seguridad se tiene que analizar los puntos de acceso a una red de computadoras y si es posible reducirlos a uno solo en donde se colocara un firewall.

3.2.2.3. No protege completamente de las nuevas amenazas

Un firewall es disefiado para proteger de amenazas conocidas que existen en la actualidad. Un firewall bien disefiado tambien puede proteger de nuevas amenazas negando todos los servicios y tan solo habilitando algunos servicios confiables de tal forma que evita que personas configuren nuevos servicios inseguros (ver sección 1.5.5.1 Negar todo por defecto). Sin embargo, un firewall no puede defender automaticamente de una nueva amenaza que surja.

Periodicamente las personas descubren nuevas maneras de violar las seguridades usando servicios que son considerados confiables o usando servicios que nadie antes utilizó. Es preciso que una vez instalado un firewall se le de el debido mantenimiento.

3.3. Diseño de Sistemas de Firewalls

Desafortunadamente no existe una estandarizacion en la terminologia aplicada para tecnología y arquitecturas de firewalls. Muchos autores de libros y personas vinculadas con la tecnologías de firewalls usan los terminos de diferentes maneras. Sin embargo existen definiciones muy básicas y populares como las siguientes:

- **Firewall:** Un componente o conjunto de componentes que restringen el acceso entre una red protegida e Internet, o simplemente entre dos redes.
- **Host interno:** Computador servidor de la red interna que se desea proteger.
- **Host** externo: Cornputador de una red externa o Internet.

- Red Perimetro: Es una red añadida que esta entre una red interna (red protegida) y una red externa (Internet) para proveer una capa de seguridad. Tambien se le denomina zona desmilitarizada (ZDM).
- Host Bastion: Un computador que esta expuesto a Internet y es el punto de contacto para los usuarios de la red interna (redes seguras).
- Host Dual-Homed: Es un host bastion que tiene como minimo dos interfases de red.
- Filtraje de paquetes: Es la acción que un dispositivo (filtro de paquetes) toma para controlar selectivamente el flujo de datos desde y hacia afuera de una red. Los filtros de paquetes dejan pasar o bloquean paquetes mientras estos son ruteados de una red a otra. Para filtrar paquetes se debe configurar un conjunto de reglas que especifiquen que tipos de paquetes van a ser permitidos ingresar y que tipos de paquetes van a ser rechazados. El filtraje de paquetes puede realizarse en un ruteador, en un bridge o en un host. Muchas veces al filtraje de paquetes se lo llama *screening.*
- **Servidor** Proxy: Es un programa que comunica a los servidores externos con clientes internos. Los clientes proxy se comunican con los servidores proxy, los cuales se comunican a su vez con el servidor real para responder a los clientes.
- Autenticacion: Es el proceso por el cual se asegura que el usuario es verdaderamente quien clama ser.
- Encriptacion: Es la codificación de la inforrnacion en tránsito para que esta no pueda ser capturada y leída. El emisor codifica la información y tan solo el receptor puede decodificarla.

Despues de familiarizarnos con la terminología que se utilizara, brevemente se explicara en que consisten las tecnologias de firewalls: host bastion, filtraje de paquetes, sistemas proxy, autenticacion y encriptacion.

3.3.1. Host bastion

Un host bastion es un computador que representa la existencia de la organización ante una red externa o Internet. Por esta razon este computador debe ser el mas seguro de toda la red interna.

En el host bastion se deben aplicar los principios y procedimientos que implica la seguridad de host. Las siguientes son las caracteristicas de un host bastion:

- Por lo general posee dos interfases de red (dual-homed), una conectada a la red interna y otra a la red externa. Posee solo los servicios de Internet que la red interna desea disponer.
- Tiene desabilitado todos las capacidades de ruteo.
- Se puede instalar programas de filtradores de paquetes o sistemas proxy

En la sección 3.4. Host bastion, se detallara su funcionamiento y se daran recomendaciones para construir un host bastion.

3.3.2. *Filtraje de Paquetes*

Los sistemas de filtraje de paquetes rutean paquetes entre hosts internos y externos, pero selectivamente. Estos bloquean o permiten el paso de ciertos tipos de paquetes de acuerdo con

la política de seguridad de la organización. Cuando se utiliza un ruteador para filtrar paquetes en un firewall, este es conocido como “screening router”

El ruteador evalua la información proporcionada en cada paquete, tales como:

- Direccion IP fuente
- Direccion IP Destino
- Protocolo (TCP, UDP, ICMP)
- Puerto fuente TCP o UDP
- Puerto destino TCP o UDP
- Tipo de mensaje ICMP

Los servidores para servicios de Internet residen en ciertos puertos (por ejemplo: el puerto TCP 23 que corresponde a conexiones Telnet), permitiendole al filtrador bloquear o permitir las conexiones simplemente especificando el puerto apropiado del servicio en el conjunto de reglas para el filtraje de paquetes. La figura No.3-2 ilustra el filtraje de paquetes, permitiendo accesar o negar el paso de conexiones a traves del ruteador.

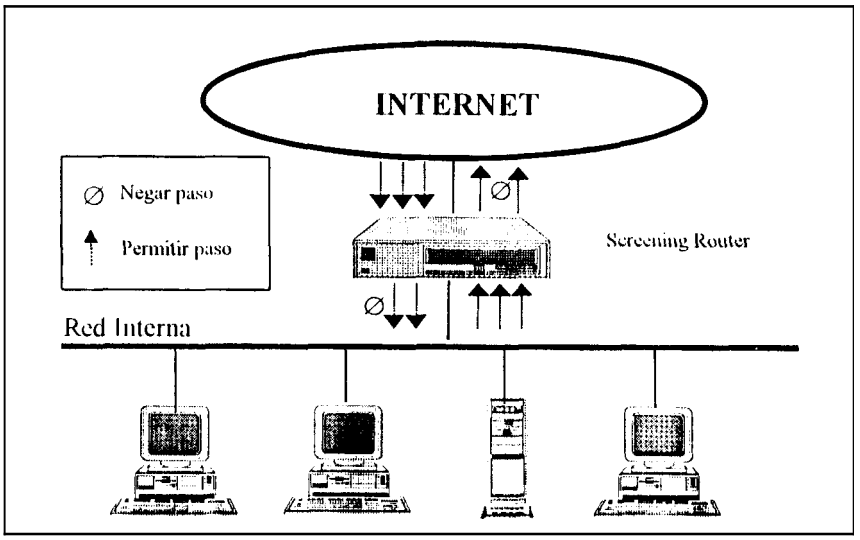


Figura No. 3-2. Representación de un filtrador de paquetes

Para entender como trabaja el filtraje de paquetes hay que conocer la diferencia entre un ruteador ordinario y un "Screening router".

Un ruteador ordinario simplemente examina la dirección destino de cada paquete y elige el mejor camino que conoce para enviarlo a su destino. La decision de cómo manejar al paquete es basado solamente en su destino. Existen dos posibilidades: que el ruteador conozca como enviar el paquete a su destino, o que el ruteador no conozca como enviarlo a su destino y lo retorna a su emisor via ICMP con un mesaje de "destino no alcanzado".

Un screening router en cambio, examina los paquetes minuciosamente. Además de determinar si puede o no rutear un paquete a su destino, un screening router determina si lo rutea o no dependiendo si el paquete cumple con el conjunto de reglas que reflejan las politicas de seguridad.

3.3.3. Servicios Proxy

Los servicios proxy son aplicaciones servidoras especializadas que se ejecutan en un host con el proposito de enlazar directamente a los clientes internos de una red con los hosts externos. El sewidor proxy puede ser un host tipo dual-homed con una interfase en la red interna y otra en la red externa, o algun host bastion que tenga acceso a Internet y sea accesible desde las maquinas de la red interna. Estos programas toman los requerimientos de los usuarios para los servicios de Internet (corno FTP o Telnet) y los envian de acuerdo con la política de seguridad establecida para esos servicios. Los sistemas proxy actuan como compuertas (gateways) para los servicios. Por esta razon se les conocen como ***compuertas a nivel de aplicación*** (application-level gateways).

Los servicios proxy se colocan lógicamente entre un cliente interno (en la red interna) y un servidor externo (en Internet). En vez de conectarse directamente uno al otro, cada uno se conecta a traves del proxy. Los sistemas proxy manejan "detras del escenario" toda la comunicacion entre los usuarios y los servicios de Internet.

El mayor beneficio de los servicios proxy es la transparencia. Para el usuario, un servidor proxy le presenta la ilusion de que esta tratando directamente con el verdadero servidor. Para el servidor real, el servidor proxy le presenta la ilusion de que esta tratando con un usuario en el host proxy y no en la rnaquina del usuario.

(capa de aplicacion). Por ejemplo, un proxy FTP puede negar o permitir a los usuarios exportar o importar archivos solo de cierto tipo.

3.3.4. Autenticacion y Encriptacion

La autenticacion es un proceso que se recomienda implernentar en todos los servicios entrantes a la red interna (por ejemplo: servidor Telnet, FTP) para evitar que usuarios no autorizados (atacantes) penetren libremente y perpetren un ataque.

Habitualmente los servidores proxy otorgan capacidades de autenticacion a traves de modulos o programas alternos que permiten autentificar a los usuarios que provienen de Internet debido a que examinan la intormacion de los paquetes hasta la capa de aplicacion donde tienen acceso a las contraseñas de los usuarios.

Existen diferentes esquemas estandares de autenticación, los cuales evitan que las contraseñas puedan ser capturadas y utilizadas posteriormente. Los detalles de la autenticacion se revisaran en la sección 3. 7 Autenticacion y encriptacion.

La encriptacion es un proceso recomendado cuando se envía inforrnacion confidencial a traves de una red insegura como Internet. La encriptacion provee un camino seguro por el que viajan los datos dando la sensacion de un canal privado virtual (VIP: Virtual Private Nets).

Actualmente los productos comerciales y publicos de firewalls ofrecen caracteristicas de encriptacion. Igual que en la autenticacion, existen esquemas estándares de encriptacion ya que

estos marcan la interoperabilidad entre firewalls de diferentes marcas. Los detalles de la encriptacion se revisaran en la sección 3. 7 Autenticacion y encriptacion.

La autenticacion y la encriptacion son dos tecnologias que van de la mano ya que el verdadero receptor es el que puede desencriptar la información. Además dentro de los esquemas de autenticacion se utilizan algoritmos para encriptar las contrasetias.

Ambas tecnologias estan disponibles en hardware y en software. Cuando se trata de hardware, estos se colocan entre la red interna y la externa. Cuando se trata de software, los programas se colocan preferiblemente en servidores bastiones.

3.3.5. Arquitecturas de Firewalls

Hasta ahora se han revisado las tecnologías que ofrecen los firewalls. La solución correcta para construir un firewall es el resultado de una combinación de estas tecnicas para resolver los diferentes problemas de seguridad. Los problemas que se necesitan resolver, dependen a su vez de los servicios que se desean proveer a los usuarios de la red y del nivel de riesgo que se corre al aceptarlos.

Existen diversas formas en la que se puede diseñar un sistema de firewall. A continuación se detallan las arquitecturas de firewalls.

3.3.5.1. Arquitectura de host Dual-homed

Una arquitectura Dual-Homed es construida con un computador host Dual-homed que se coloca entre la red interna y la externa, como se ve en la figura No. 3-3. Un host Dual-homed actua

como un ruteador entre las dos redes a la que sus interfaces estan conectadas, es decir que los paquetes de una red (Internet) no sean directamente direccionados a la otra red (red interna). Por lo tanto, los sistemas detras del firewall (sistemas de la red interna) y fuera de este (Internet) no se comunican directamente sino a traves del host dual-homed.

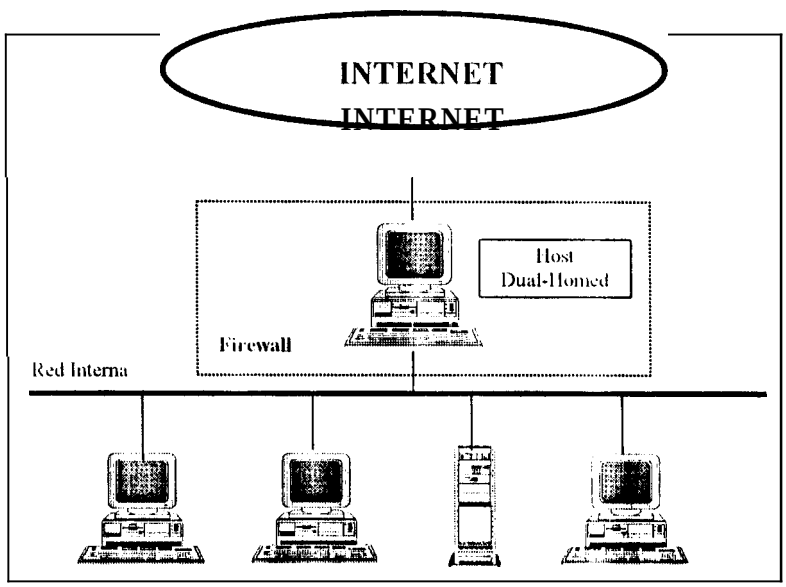


Figura No. 3-4. Arquitectura host Dual-homed

En esta arquitectura, el host dual-homed puede contener sistemas proxy, filtradores de paquetes (a traves de programas de software) o ambos. Habitualmente se colocan mas sistemas proxy que filtradores de paquetes.

La desventaja de esta arquitectura es que se cuenta con un solo objeto dedicado a la seguridad y no brinda redundancia (ver la sección **1.5.2** Defensa en profundidad). Por mas que este contenga varios rnecanismos (filtrador de paquetes, sisternas proxy, autenticacion y encriptacion) instalados en el host dual-homed, si un atacante llega a comprometerlo (mediante

cualquier tipo de ataque, ver sección 1.1 Tipos de ataques), tiene toda la red interna a su disposición.

3.3.5.2. Arquitectura Screened Host

La arquitectura de screened host provee servicios proxy desde un computador (host bastion) que esta conectado a la red interna y utiliza un ruteador como tiltrador, es decir combina las tecnicas de sistemas proxy y filtradores de paquetes. La seguridad primaria es provista por un filtraje de paquetes (screening router) y la secundaria a traves del sistema proxy instalado en el host bastion como se ve en la figura No. 3-5.

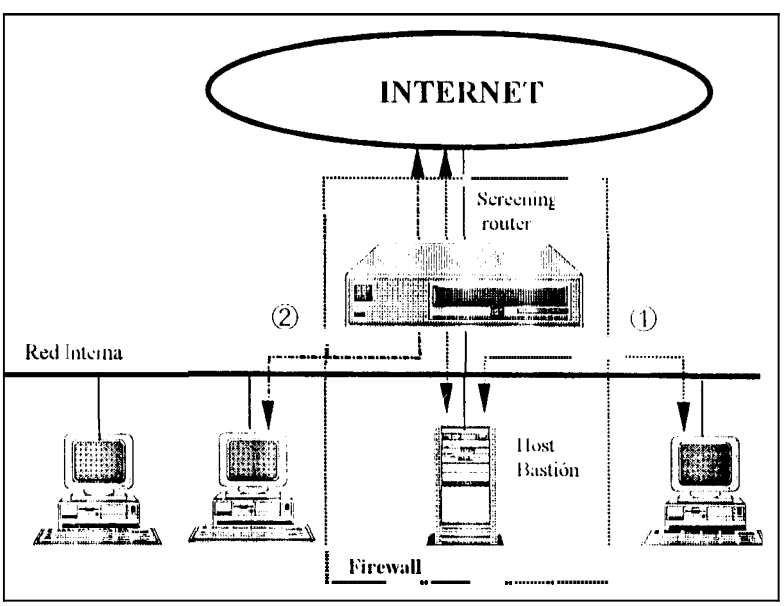


Figura No. 3-5. Arquitectura Screened host

El host bastion se coloca en la red interna. El filtraje de paquetes en el screening router es configurado de tal manera que las conexiones pasen o no por el host bastion antes de ingresar a la red interna.

La configuración del screening router puede ser una de las dos siguientes maneras:

- Permitir a algunos clientes internos abrir conexiones a Internet directamente para ciertos tipos de servicios confiables indicado en la figura No. 3-5 con el numero ②.
- Deshabilitar todas las conexiones de hosts internos a Internet, forzando a aquellos hosts a usar servicios proxy instalado en el host bastion indicado en la figura No. 3-5 con el numero ①.

Se pueden planear diferentes metodos para los diferentes servicios, algunos pueden ser habilitados por screening routers, mientras otros pueden ser permitidos a traves de servicios proxy ubicados en el host bastion o la combinación de ambas tecnologias. Todo depende de las politicas de seguridad de la organización.

Debido a que esta arquitectura deja que los paquetes penetren desde Internet a la red interna, parecería de mayor riesgo que una arquitectura dual-homed, la cual es diseñada para que ningun paquete externo pueda alcanzar a la red interna. Sin embargo en la practica, ante fallas no esperadas, una arquitectura de host dual-homed es muy propensa a dejar pasar paquetes a la red interna. En carnbio un ruteador es mas facil de defender debido a que es un mecanismo de defensa facil de configurar, y como seyuridad secundaria se encuentra el host bastion. Por esto la arquitectura screened host provee mayor seguridad y usabilidad que una arquitectura dual-homed.

Sin embargo, esta arquitectura tambien presenta limitaciones. Si un intruso rompe la seguridad del host bastion, no existe ningun otro mecanismo de seguridad entre el host bastion y los hosts

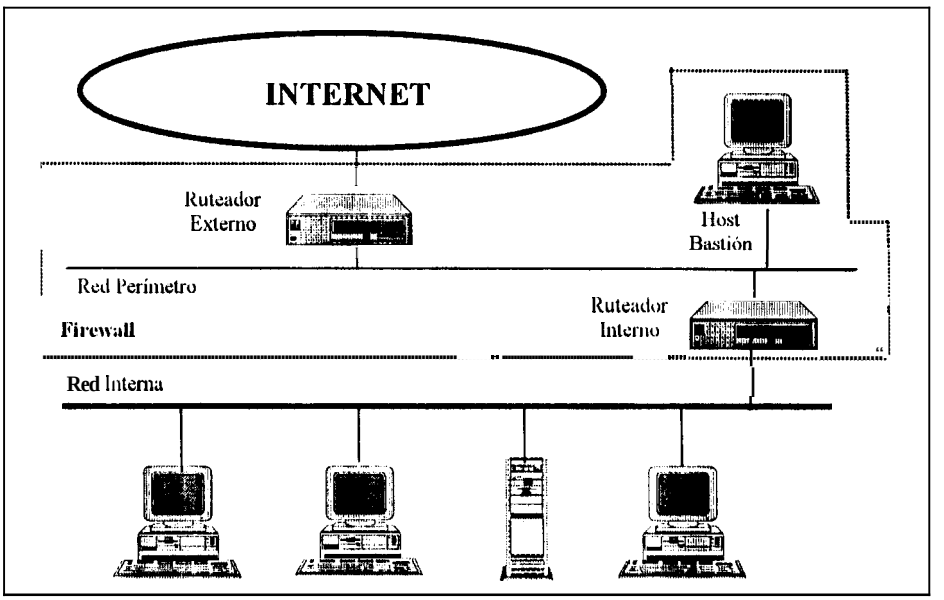
internos, por lo que la red interna queda expuesta ante cualquier ataque. El ruteador tambien representa un punto de falla, si el ruteador es comprometido, el intruso puede cambiar las tablas de ruteo y habilitar otros puntos de la red interna.

3.3.5.3. Arquitectura Screened Subnet

La arquitectura screened Subnet añade una capa extra de seguridad a la arquitectura screened host a traves de una red perimetro que aisla a la red interna de Internet. En esta arquitectura el host bastion se conecta a la red perimetro y no a la red interna; aislando el host bastion en una red perimetro se puede reducir el impacto de una violación dentro un host bastion.

Toda arquitectura screened subnet cuenta con dos screening routers, cada uno se conecta a la red perimetro. Uno se coloca entre la red interna y la red perimetro (ruteador interno), y el otro entre la red externa y la red perimetro (ruteador externo). Para ingresar a la red interna desde Internet es necesario pasar por ambos ruteadores. Si se ejecuta un ataque al host bastion, el intruso todavia tendra que romper las seguridades del ruteador interno para ingresar a la red interna. La figura No. 3-6 ilustra una posible configuración que usa esta arquitectura.

Algunas organizaciones utilizan varias capas de redes perimetro entre el mundo exterior y su red interna. Los servicios menos confiables y mas vulnerables son colocados en las redes perimetros más externas hasta así llegar a la red mas interna (red segura). La idea es que para un intruso que rompe las seguridades en una maquina dentro de la red mas externa, este tendra que hacerlo con cada capa hasta llegar a la red interna. Sin embargo, los sistemas de filtrajes entre capas tendrán que ser diferentes, ya que si cada ruteador tiene las mismas reglas de filtraje, las redes perimetro no daran seguridad adicional porque si un intruso penetra en una capa puede hacerlo en todas [CHAP95].



Fiyum NO. *3-6.* Arquitectura screened subnet

A continuación se describe mas detalladamente los componentes de este tipo de arquitectura.

Red Perimetro

La red perimetro es una red intermedia entre la red externa y la red privada o interna que ofrece una capa adicional de protección en caso de que un ataque se perpetre.

En la mayoría de redes (Ethernet, Token Ring, FDDI) es posible, para cualquier máquina conectada a la red, observar el trafico de esa red. Los curiosos o intrusos se pueden aprovechar de esta caracteristica para observar las contrasefias generadas por sesiones Telnet, FTP y rlogin. Aun si las contrasefias no son comprometidas, los curiosos pueden tambien observar el contenido de archivos, correo electronico, etc. En realidad ellos pueden "ver sobre los hombros" de cualquier usuario en la red.

En una red perimetro, si algún intruso rompe las seguridades en un host bastion, solo podra obsewar el trafico de la red perimetro que es el trafico que entra o sale al host bastion, o el que entra o sale de Internet. El trafico interno se mantiene a salvo del intruso aun si el host bastion es comprometido.

Host Bastion

En una arquitectura screened subnet, el host bastion se conecta a la red perimetro con el fin de colocar sistemas proxy.

Tanto los servicios entrantes como salientes pueden ser manejados de las siguientes maneras:

- Colocando mecanismos de filtración de paquetes en ambos ruteadores para permitir que los clientes accesen directamente a servidores externos .
- Colocando servidores Proxy en el host bastion para permitir que clientes internos accesen indirectamente a servidores externos. Además, configurar los ruteadores para que "hablen" solo con los servidores proxy en el host bastion y viceversa.

En cualquier caso, el filtraje de paquetes le permite al host bastion establecer una conexión con hosts en Internet; cuales hosts y para que servicios, lo dictamina la política de seguridad de la organización.

Ruteador Interno

El ruteador interno, muchas veces llamado ruteador de estrangulacion (choke router), protege a la red interna tanto de Internet como de la red perimetro. Este ruteador permite las conexiones de ciertos servicios desde la red interna a Internet. Estos servicios son aquellos que según la

organización no involucran peligro y que pueden ser provistos sin necesidad de servidores proxy.

Los servicios que debe permitir el ruteador interno entre el host bastion y la red interna no son necesariamente los mismos servicios que debe permitir entre Internet y la red interna. La razon para limitar los servicios entre el host bastion y la red interna es reducir el numero de máquinas (y servicios en esas maquinas) que puedan ser víctimas de un ataque desde el host bastion. Hay que limitar los servicios entre el host bastion y la red interna a solo aquellos que realmente lo necesitan. Además, se debe permitir la comunicacion del host bastion a ciertos hosts en la red interna, como por ejemplo SMTP del host bastion puede ser limitado solo a conexiones con un servidor de correo electrónico interno.

Ruteador externo

Tambien llamado ruteador de acceso, en teoría protege tanto a la red perimetro como a la red interna de posibles ataques desde Internet. En la practica, los ruteadores externos tienden a permitir casi cualquier conexión saliente desde la red perimetro, y generalmente hacen muy poca labor de filtraje de paquetes hacia el exterior.

Las reglas de filtraje especiales en el ruteador externo son aquellas que protegen a las maquinas en la red perimetro (el host bastion y el ruteador interno). Generalmente no es necesaria tanta protección, debido a que el host bastion por sí mismo tiene mecanismos de seguridad.

El resto de reglas que se colocan en este ruteador pueden ser las mismas colocadas en ruteador interno. Estas reglas se utilizan para prevenir trafico inseguro desde hosts internos e Internet.

Una de las tareas mas importantes que el ruteador externo realiza es bloquear todos los paquetes entrantes desde Internet que tienen direcciones cambiadas, prentendiendo ser direcciones internas para accesar a la red (spoofing). El ruteador interno tambien podría hacerlo, pero no sabria si los paquetes que claman ser de la red perimetro no son los autenticos. Mayores detalles se dan en la sección 3.4. Host bastion.

3.3.6. Variaciones en las Arquitecturas

A traves de las figuras anteriores se han mostrado las arquitecturas mas comunes de firewalls. Sin embargo existen variaciones de estas arquitecturas las cuales dependen mucho de los componentes que la organización este dispuesta a colocar, del presupuesto y de las politicas de seguridad.

Estas variaciones pueden ser seguras si ofrecen un esquema redundante, e inseguras si ofrecen un esquema con redudancia pobre. Todas estas variaciones clasificadas en variaciones seguras e inseguras, se detallaran a continuación con un análisis del por que se consideran seguras o inseguras.

3.3.6.1. Variaciones Seguras de Arquitecturas

a. Multiples hosts Bastiones

Aunque en las secciones anteriores se ha hablado de colocar un solo host bastion, la organizacion puede requerir de varios hosts bastiones en la configuración de su firewall, tal como se ve en la figura No. 3-7. Las razones para hacerlo podrian ser perfomance, redudancia o simplemente la necesidad de separar datos o servidores.

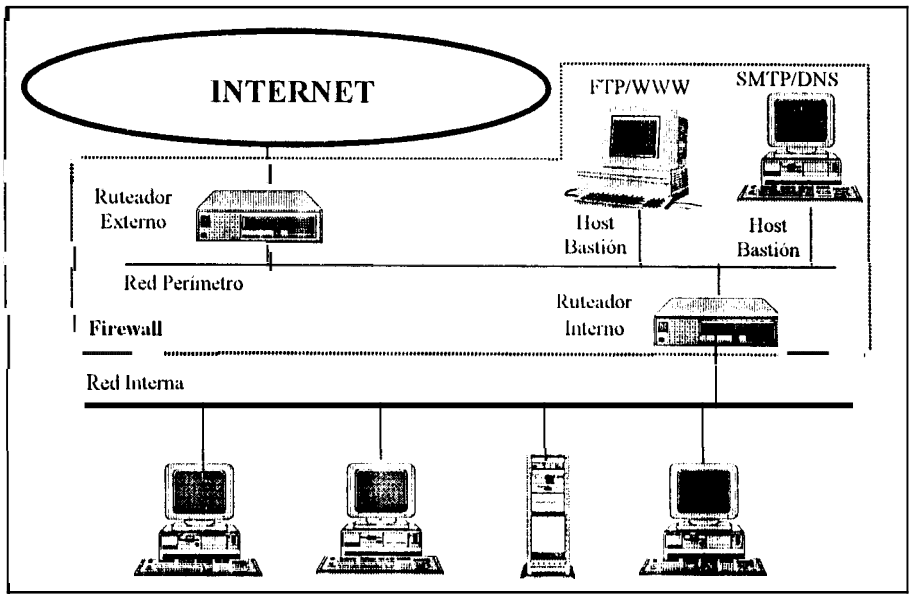


Figura No. 3-7. Arquitectura de firewall con múltiples hosts bastiones

La organizacion puede decidir tener un host bastion para manejar los servicios que son importantes a los usuarios, tales como servidores SMTP, proxy, DNS etc.; y otro para rnanejar servicios para Internet que para los usuarios no sean tan irnportantes, tales como servidores anonirnos FTP, WWW, etc. De esta forma, al dividir el trabajo, el perfomance se elevara y adicionalmente ganamos algo en seguridad, pues si el servidor FTP se ve comprometido esto no afectara al servidor SMTP.

Si se cuenta con varios hosts bastiones, estos pueden ser configurados para adquirir redundancia; es decir que si uno falla, los servicios de ese host pueden ser provistos por el otro.

Por ejemplo, se puede configurar varios hosts como servidores DNS, o SMTP, luego si uno de los hosts bastiones esta deshabilitado o sobrecargado, los servicios DNS y SMTP usaran los otros hosts de respaldo. Para implementar este esquema hay que definir un host bastión principal y otro secundario. Cuando los usuarios se percaten que falla el principal, inmediatamente se cambiaran al secundario.

Un consejo valido seria colocar varios hosts bastiones para separar información. Por ejemplo mantener un servidor HTTP con ciertos datos para los usuarios internos y otro servidor HTTP con otros datos para los usuarios de Internet.

b. Fusion del Ruteador interno y externo

Se pueden fusionar los ruteadores interno y externo en uno solo que cuente con tres interfases de red siempre y cuando se cuente con un ruteador lo suficientemente capaz, flexible y que permita especificar filtros internos y externos en cada interface.

Si se une el ruteador interno con el externo, como se ve en la figura No. 3-8, se sigue contando con una red perimetro (en una interface del ruteador). Algún trafico podría fluir directamente desde la red interna a Internet (dependiendo de las reglas del filtro), y otro trafico fluirá entre la red perimetro e Internet o entre la red perimetro y la red interna.

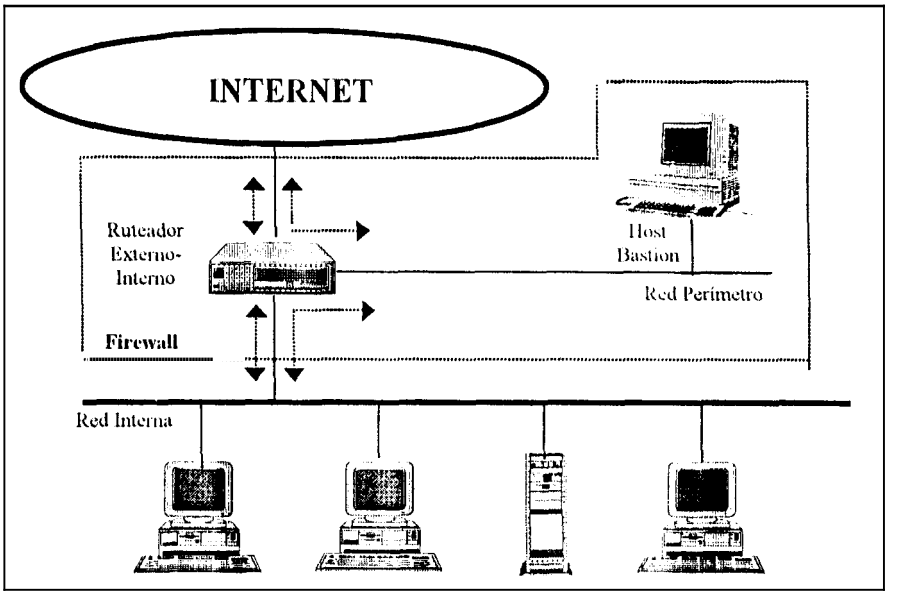


Figura No. 3-8. Arquitectura de firewall con fusión de ruteador externo e interno

Tal como la arquitectura screened host, esta tarnbien es vulnerable si se compromete el ruteador. En general los ruteadores son mas faciles de proteger que los hosts, pero no son impenetrables.

c. Fusion del Host Bastion y ruteador externo

Pueden existir casos en los cuales se utilice una máquina dual-horned como un host bastion y un ruteador externo como se aprecia en la figura No. 3-9.

Usar un dual-horned para rutear el trafico no proporciona el peifomance y la flexibilidad de un ruteador dedicado. Dependiendo del sisterna operativo y del software que se utilice en el host bastion, se puede o no habilitar la capacidad del filtraje de paquetes. Pero debido a que el ruteador externo no requiere de muchas reglas de filtraje, entonces un software que no ofrezca

buenas capacidades de filtraje de paquetes no es un gran problema. Este tipo de arquitectura es más ventajosa que la anterior debido a que presenta mas redundancia en seguridad. Sin embargo, el host bastion esta mas expuesto a Internet, así que habría que tomar un cuidado extra para protegerlo.

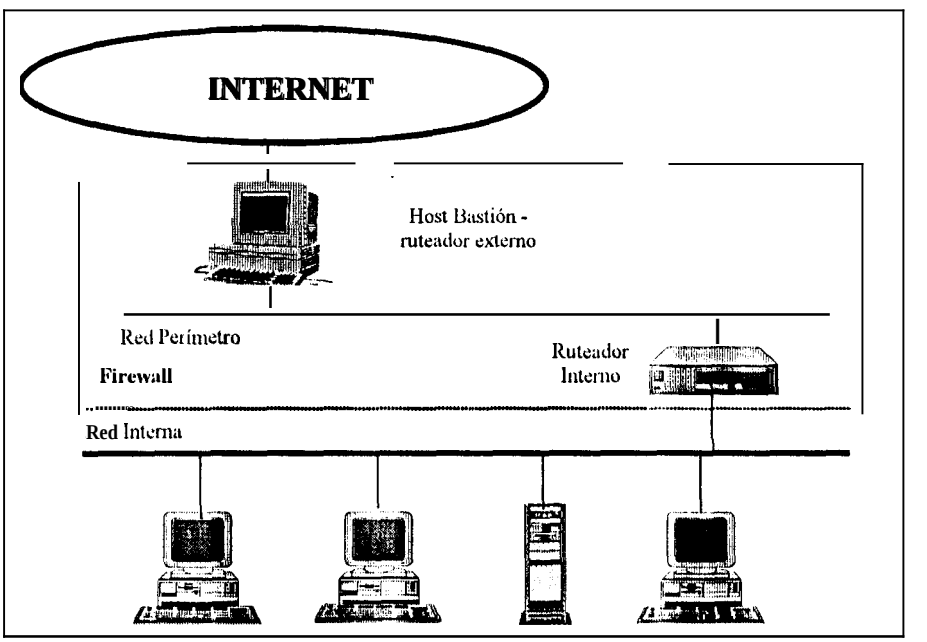


Figura No. 3-9. Arquitectura de firewall con fusión del host bastión y ruteador externo

3.3.6.2. Variaciones inseguras de Arquitecturas

a. Fusion del Host bastion y el ruteador Interno

Mientras es aceptable la fusion del host bastion y el ruteador externo, como se trato en la sección anterior, no es aconsejable fusioriar el host bastion con el ruteador interno como se ve en la figura No. 3-10

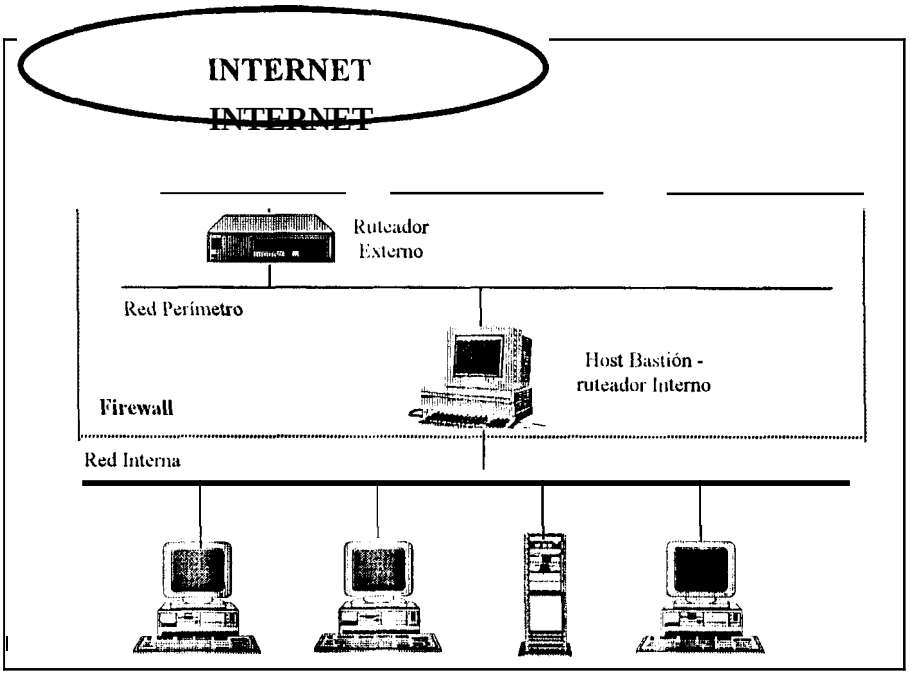


Figura NO. 3-10. Arquitectura de firewall con fusión de ruteador interno y host bastión

Si se une el host bastion con el ruteador interno, se habrá cambiado fundamentalmente la configuración del firewall. Cuando se unia un host bastion con un ruteador externo se configuraha una arquitectura screened subnet, y en la red perimetro circulaba un trafico qus no era precisamente el interno por lo que la red interna estaba protegida de curiosos en el caso de que el host bastion haya sido cornprometido. Cuando se une un host bastion con un ruteador interno se obtiene una arquitectura screened host, y si el host bastion es comprometido no hay ningun otro mecanismo de seguridad para proteger la red interna.

El principal proposito de la red perimetro es prevenir que el host bastion no tenga acceso directo al trafico de la red interna. Colocar el host bastion en el ruteador interno hace que todo el trafico interno sea accesible a la red externa o Internet.

b. Varios ruteadores Internos

Este esquema consiste en colocar varios ruteadores internos que comunican a la red interna con la red perimetro como se observa en la figura No. 3-11. El problema basico de utilizar varios ruteadores internos es el que el software de ruteo en un sistema interno puede decidir que el camino mas rapido para llegar a otro sistema interno es mediante la red perimetro permitiendo que la información de la red interna fluya a traves de la red perimetro.

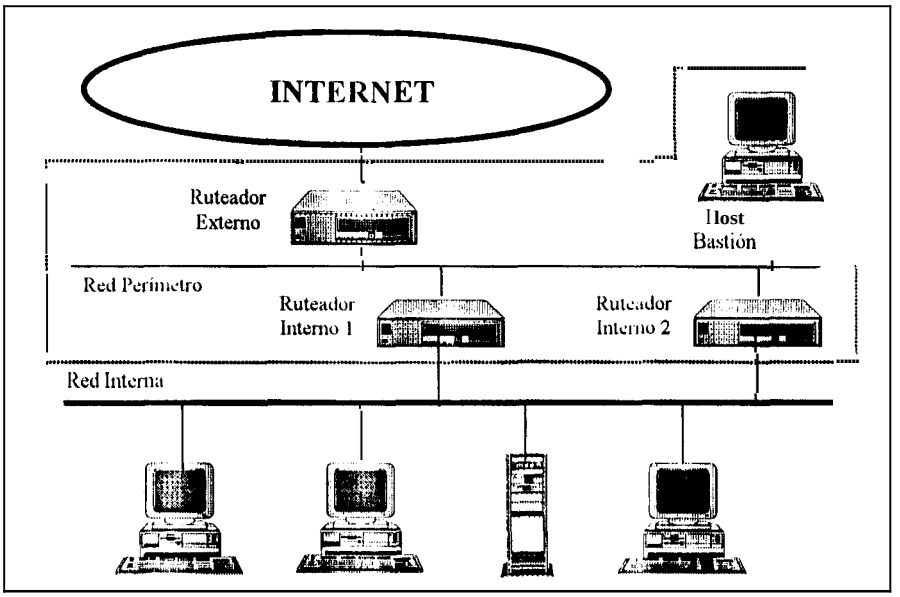


Figura No. 3-11. Arquitectura de firewall con dos ruteadores internos

Resulta algo difícil mantener multiples ruteadores internos correctamente configurados. Hay que considerar que el ruteador interno es el mas importante porque involucra un conjunto de reglas muy complejas para el filtraje de paquetes y mantener algunos de ellos incrementa la posibilidad de error.

Para una red interna grande, el tener un solo ruteador interno puede provocar problemas en el perfomance y confiabilidad ya que tiene que atender muchos requerimientos. Para solucionar

estos problemas se puede cambiar el ruteador interno por uno mas rapido o colocar mas de un ruteador. La segunda opción es la mejor ya que en caso de que el ruteador interno falle, lo mas seguro es disponer de varios ruteadores internos, pero cada uno conectado a una red perimetro separada como se ve en la figura No 3-12. Para cada red perimetro se colocan host bastiones según sea la necesidad de la organización. Sin embargo, esta configuracion es muy costosa y compleja porque implica obtener dos ruteadores de similares caracteristicas y reglas de configuracion diferentes; pero incrementara la redundancia y el perfomance haciendo muy improbable que el trafico fluya de un ruteador interno a otro.

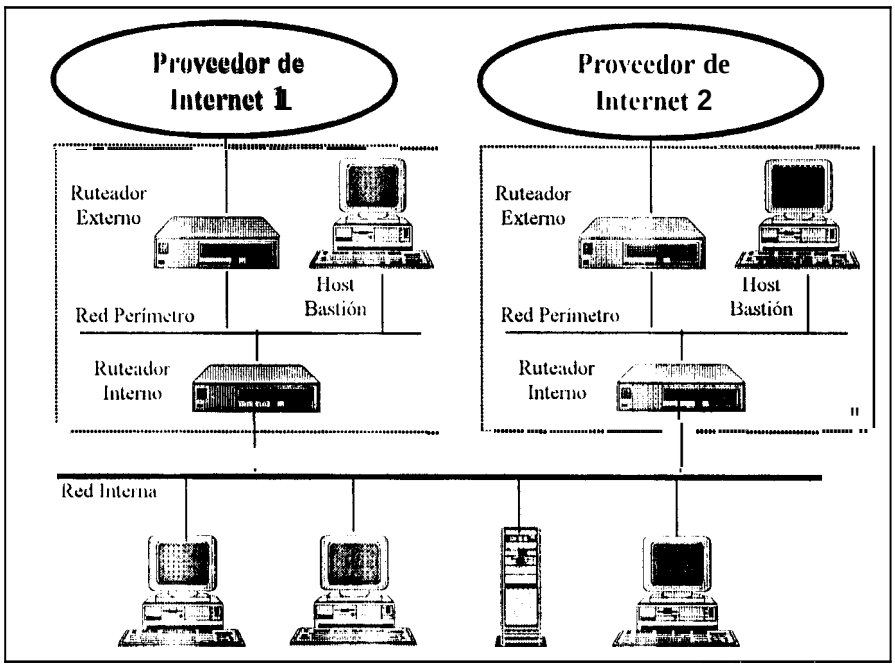


Figura No. 3-12. Arquitectura de Firewall con dos redes perímetros

En la mayoría de los casos un sólo ruteador interno no representa un cuello de botella, si así sucede, pueden estar sucediendo los siguientes casos:

- **Problema:** existe alyun trafico que sale a la red perimetro y no sale a la red externa. Este problema puede ser detectado "olfateando" todos los paquetes de la red perimetro cuando la

red interna no este en operación. De esta manera, si existen paquetes de la red interna es porque hay problemas.

Solucion: es posible que haya problemas de configuracion; la red perimetro ocasionalmente toma el trafico destinado al mundo externo en alguna parte de la configuracion. Se recomienda una revision en la configuración.

- **Problema:** el ruteador externo es rnucho mas rapido que el ruteador interno. Para determinar este problema se pueden hacer pruebas transfiriendo archivos desde la red externa o Internet hasta la red interna. El tiempo de respuesta entre la red perimetro y la red interna no debe ser demasiado grande. Si lo es, existe este problema.

Solucion: hay que considerar seriamente aumentar la capacidad del ruteador interno para alcanzar al externo.

Otra razon para colocar varios ruteadores internos es cuando la organización cuenta con varias redes internas, la cuales por razones tecnicas, organizacionales y politicas no deben compartir un solo ruteador. Una manera simple de solucionar este problema es reubicar estas redes y darles interfaces por separado en un sólo ruteador, como se ve en la figura No. 3-13. Esto complica considerablemerite la configuracion del ruteador pero no produce los riesgos de una configuracibn con multiples ruteadores.

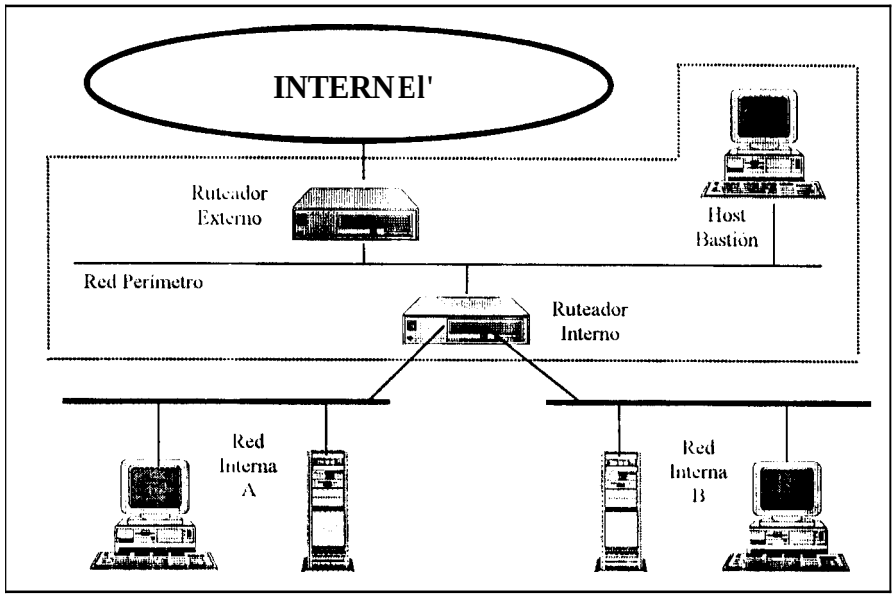


Figura No. 3-13. **Arquitectura de firewall con un sólo ruteador interno**

Si existen muchas redes internas dentro de la organización, es imposible usar un solo ruteador. La solución en este caso es utilizar una red backbone y conectarla a la red perimetro mediante un ruteador, así lo ilustra la figura No. 3-14.

3.3.6.3. Firewalls internos

Muchas organizaciones cuentan con multiples redes internas y para proteger ciertas redes de otras es necesario colocar mecanismos de seguridad entre ellas.

En un ambiente educativo, algunas razones para hacer esto pueden ser:

- Si existen redes de laboratorios donde no existe control de las actividades de los usuarios.
- Si existen redes menos seguras como por ejemplo redes de demostracion o enseñanza (usuarios extraños, no internos)
- Si existen redes que requieren mas seguridad que otras como redes para desarrollo de proyectos, redes administrativas etc.

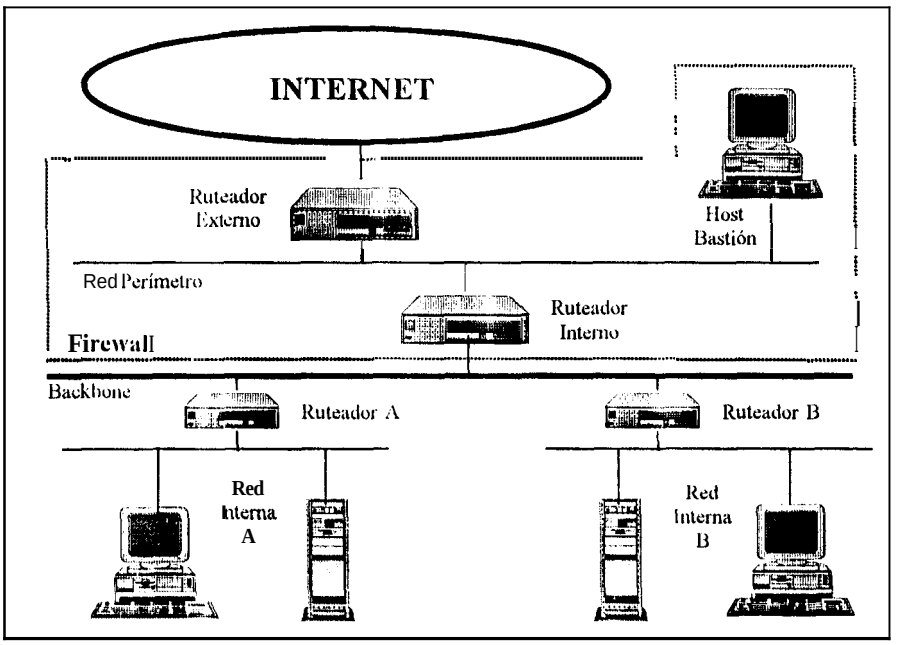


Figura No. 3-14. Arquitectura de firewall con un backbone

En algunos casos es necesario utilizar la tecnologia de firewalls para construir firewalls internos entre dos partes de una misma organización o entre organizaciones diferentes que comparten una red (figura No. 3-15). Muchas de las mismas herramientas y tecnicas que se usan par construir firewalls para Internet tambien son utilizadas para estos firewalls internos.

Luego de analizar todas las arquitecturas de firewalls, es preciso analizar con mas detenemiento las tecnologias de firewalls: host bastion, filtraje de paquetes, sistemas proxy, autenticación y encriptacion.

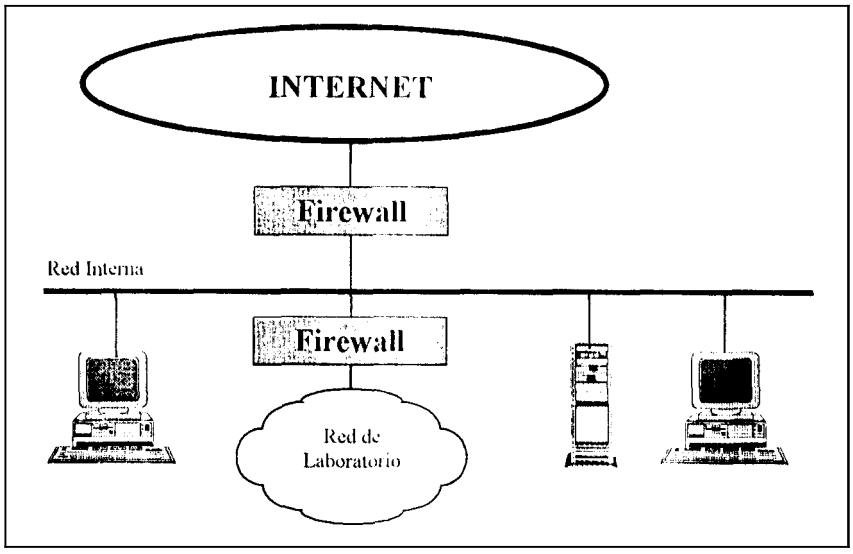


Figura No. 3-15. Arquitecturas de firewalls internos

3.4. Host Bastión

Un host bastión es una máquina cuya existencia es conocida por Internet, por lo tanto está altamente expuesta a los peligros que involucra una conexión con Internet (ver sección 1.2.). Su propósito principal es el de ser proveedor de cualquier programa de seguridad: filtradores o sistemas proxy. Habitualmente más se lo involucra con sistemas proxy. También puede brindar servicios de Internet que más tarde, en la sección 4.4., podrán ser analizados.

Los principios y procedimientos para construir un host bastión sirven para asegurar cualquier host y por lo tanto se pueden utilizar en cualquier otra máquina interna dependiendo del grado de seguridad que necesite.

Un host bastión debe ser diseñado teniendo en mente estos dos principios generales:

- **Simplicidad:** Mientras mas simple sea un host bastion más fácil sera asegurarlo (ver sección 1.5.8 Estrategia de simplicidad). Puede darse el caso de que algun servicio que ofrece el host bastion tenga errores o problemas de configuración que puedan constituirse en una posible brecha en la seguridad del mismo. Por lo tanto, se requiere mantener al host bastion tan sencillo como sea posible, es decir, que el host bastion provea la menor cantidad de servicios con el menor privilegio posible.
- **Vulnerabilidad:** Aun teniendo bien configurado un host bastion es muy posible que este sea cornprometido debido a que es la máquina mas accesible al estar expuesta ante Internet. No se puede asegurar que el host bastion nunca sea violado, la pregunta que hay que mantener en mente es ¿Qué pasa si el host bastion es comprometido?, jatectara la seguridad en todo el firewall? .Teniendo siempre presente esto se debe configurar el host bastion de tal manera que si es violado no afecte a la seguridad que provee el firewall.

3.4.7. Tipos de host bastion

Un host bastion puede configurarse de divcrsas formas:

3.4.1.1. Host dual-homed

Un host dual-homed es una maquina que tiene como mínimo dos interfases de red que conecta a dos redes pero que no rutea directamente el trafico de la una a la otra, es decir, lo hace previo a un análisis de la inforrnacion que recibe. Este tipo de host puede ser por sí solo un firewall o ser una parte de un firewall mas complejo..

3.4.1.2. Máquina víctima

Si una organización desea ofrecer servicios que son difíciles de asegurar o servicios que son nuevos y se desconoce su real funcionamiento y sus implicaciones en seguridad, es muy recomendable utilizar una maquina víctima. Esta maquina por lo regular es conectada fuera de una red interna o en una red perimetro de tal manera que si un intruso llega a comprometerla, este no podra accesar a la red interna debido a los mecanismos de seguridad que la protegen.

En estas maquinas víctimas no se colocan datos sensitivos o servicios que son de mucha importancia para los usuarios internos. Los datos sensitivos y servicios importantes de la red interna deben ser colocados en la red interna. De esta forma, si una maquina victima llega a ser comprometida, el intruso no podra robar o modificar información.

Una maquina victirna bien configurada y colocada correctamente puede proporcionar otro nivel de redundancia en la seguridad de un sistema de redes de computadoras.

3.4.1.3. Host bastión interno

En todas las arquitecturas de firewalls estudiadas, el host bastion tiene comunicación con los hosts internos quienes a su vez son clientes del host bastion. Estos hosts internos realmente son hosts bastiones secundarios que deben protegerse y configurarse mas como hosts bastiones que como hosts normales.

3.4.2. Aspectos preliminares para construir un host bastion

Antes de construir un host bastion es necesario elegir el tipo de maquina que se utlizara. Para esto hay que revisar una serie de aspectos importantes.

3.4.2.1. Sistema operativo

El sistema operativo de un host bastion debe ser familiar para los usuarios de una red de computadoras en una organización. Sin embargo, se necesita una maquina confiable que ofrezca un amplio rango de servicios de Internet para proveer a los usuarios, con multiples conexiones simultaneas y activas. Es por esto que el sistema operativo debe ser multiusuario capaz de ejecutar todas los servicios de Internet y las herramientas que constituirán el firewall tales como servidores proxy, sistemas de filtraje de paquetes, etc.

3.4.2.2. Rendimiento de la máquina

Un host bastion no debe ser una máquina rápida, es mejor que no sea tan poderosa por diversas razones:

- Una maquina lenta invita menos a ser víctima de un ataque. Por lo general los atacantes de Internet no adquieren mucho prestigio si comprometen una maquina lenta. Se gana mas prestigio si se compromete una maquina con gran hardware de por medio. El secreto esta en no hacer del host bastion una maquina poderosa y con fama [CHAP95].
- Si es comprometida, una maquina lenta sera menos usada para atacar los sistemas internos de otros lugares, ya que toma mucho tiempo compilar codigo, ejecutar programas que rompen contraseñas, etc. Todas las actividades que los intrusos buscan realizar cuando violan un sistema requieren de un gran hardware.

En realidad un host bastion no tiene mucho trabajo que hacer. Las funciones del host bastion son mayormente limitadas por la velocidad de la conexión con Internet, mas no por la velocidad de su CPU.

Se necesitaría mas poder de procesamiento si se ejecutaran programas de compresion y descompresion, programas de busquedas, o si se instalaran servicios proxy para cientos de usuarios que pueden conectarse simultaneamente. La instalacion de todos estos programas adicionales en un host bastion depende de las necesidades y recursos de las organizaciones.

3.4.2.3. Configuración del Hardware

Se necesita un hardware que brinde contiabilidad en su configuración. Uno de los objetivos de un host bastion es rnantener un rastro de un numero de conexiones simultaneas. Para esto se requiere memoria y probablemente espacio de swap en el disco. El utilizar sistemas proxy involucra la necesidad de una cantidad de espacio libre en el disco para usarse como cache.

No hay ninguna necesidad de utilizar dispositivos perifericos especiales a no ser los mas comunes que todos los distribuidores proveen: ratón, teclado, CD-ROM, tapes, etc. Un host bastion no necesita ambiente grafico ya que es un host de servicios de red y nadie (a no ser el administrador) necesita verlo. Utilizar ambiente yrafico puede animar a las personas a usar esta maquina para otros propósitos e incluso instalar programas adicionales que puedan resultar inseguros e innecesarios para la funcion del host bastion.

3.4.2.4. Cuentas de usuarios

Es muy recomendable no otorgar cuentas de usuarios en el host bastion debido a que:

- Involucra vulnerabilidad de las cuentas: Una cuenta de usuario representa una via de acceso para alguien que desea penetrar en un sistema. Las cuentas se manejan a traves de contraseñas las cuales pueden ser "olfateadas" por medio de busquedas de diccionario (comparar con palabras de un diccionario personalizado hasta que logra penetrar) o capturadas mediante sniffers cuando estas se encuentren viajando a traves de una red.

- Involucra vulnerabilidad en los servicios requeridos para soportar las cuentas: Al tener cuentas en un host bastion se habilitan servicios para los usuarios de estas cuentas. Cada servicio disponible en un host bastion constituye una avenida de ingreso por donde perpetrar un ataque.
- Reduce la estabilidad y confiabilidad de la maquina: Una maquina que no posee cuentas de usuarios tiene un comportamiento muy estable y predecible, mientras que una maquina que posee cuentas de usuarios tiene un comportamiento muy indefinido lo que produce inestabilidad [CHAP95].
- Produce una subversion inadvertida por parte de los usuarios: Los usuarios de las cuentas intrinsicamente pueden contribuir sin intención a producir un ataque a un host bastion mediante acciones tales como descuidar su contraseña, descuidar los permisos de archivos, etc. Además, un usuario puede accidentalmente cambiar la configuración de un host bastion que tiene falencias en su configuracion.
- Incrementa la dificultad de detectar ataques: Es rnuy difícil establecer el comportamiento de un host bastion con cuentas de usuarios, el administrador puede pensar que todo esta bien y sin embargo estar ocurriendo un ataque.

3.4.3. Pasos para construir un host bastion

Una vez elegidos el sistema operativo y la configuracion del hardware, estos son los pasos a seguir para implementar un host bastion:

1. Asegurar la maquina
2. Desabilitar los servicios no requeridos
3. Instalar o modificar los servicios que se desean proveer
4. Reconfigurar para la producción

5. Ejecutar un auditoreo de seguridad para establecer una linea base
6. Conectar la maquina a la red donde va a ser usada

Hay que tener cuidado de no conectar un host bastion a Internet, sin antes haberlo configurado. Se corre mucho peligro cuando se conecta un host bastion debido a que se puede perpetrar un ataque cuando sus defetisas estan aun bajas. Es muy difícil detectar a un intruso que perpetra un ataque cuando un host bastion todavia no ejecuta una revision; posiblemente el intruso podra leer todo el tráfico de la red. Cuando se implementa un host bastion el ultimo paso es conectarlo y hacerlo accesible a Internet.

3.4.3.1. Asegurar la máquina

Para asegurar una máquina se deben tomar en cuenta las siguientes consideraciones:

1. **Comenzar** con una **instalación mínima** del sistema operativo: Se recomienda instalar **el** sistema operativo en un modo rninimo para así saber exactamente con que se esta trabajando y no hacer conjeturas de que si existe uria brecha de seguridad es por una sección "desconocida" del sistema opcrativo.
2. Arreglar **los errores** conocidos **del** sistema operativo: Se deben instalar parches de seguridad que existen para el sistema operativo de acuerdo con los distribuidores de cada sistema operativo.
3. Usar una **lista** de chequeo: Estar en contacto con distribuidores y usuarios del sistema operativo seleccionado es importante. En Internet existcn listas de correo, páginas de web, newgroups, etc., que sirven para este proposito y proveen mucha información de cada software y sus versiones liberadas.
4. Guardar archivos **de log** : Un host bastion requiere de un considerable espacio para archivar la infoririacibn de log. Estos archivos de log son irnportantes para saber si todo lo

que se esta ejecutando en el host bastion esta correcto. Además, si un ataque llegara a suceder se podrá hacer un seguimiento de quien lo hizo y como se produjo este ataque. El archivo de log no necesariamente tiene que físicamente estar en el host bastion, puede ubicarse en cualquier maquina dentro de la red interna, pero hay que tomar en cuenta que el contenido del un archivo de log es el reflejo de lo que sucede solo en el host bastion.

3.4.3.2. Desabilitar los servicios no requeridos

Una vez asegurado el host bastion, el siguiente paso es desabilitar todos los servicios que el host bastion no va a proveer. Cualquier servicio que provea un host bastion puede tener errores o problemas de configuración que pueden originar problemas de seguridad.

Obviamente se tendrá que proveer todos los servicios que los usuarios necesitan para ejecutar sus tareas adecuadamente y segun lo dictaminen las politicas de seguridad de una organización. Pero si un servicio no es absolutamente necesario, no hay que habilitarlo.

Criterios para desabilitar un servicio

Existen tres reglas simples que se deben aplicar:

1. Si no lo necesita, desabilítelo.
2. Si no conoce que es o como trabaja, desabilítelo. Probablemente no lo necesita.
3. Si al desabilitarlo causa problemas, se conoce que realmente es lo que hace y se puede habilitarlo o bien descubrir como trabajar sin este.

Para entender mejor estos criterios se analizara un ejemplo basado en un sistema operativo UNIX.

Sevicios que deben ser habilitados en Unix:

Ciertos servicios son indispensables para operar un host bastion, y probablemente hay que habilitarlos. En un sistema operativo UNIX los procesos quc hay que hablitar son:

- **init, swap, page:** los tres procesos usados para manejar otros procesos
- **cron:** para correr procesos en tiempos fijos
- **syslogd:** registra toda la información de lo que sucede en el kernel y otros demonios
- **inetd:** para correr servicios de red cuando estos son requeridos por otras maquinas

Además de estos, habilitar los procesos servidores para los servicios que la organización necesita ofrecer a sus usuarios tales como Telnet, FTP, SMTP, etc.

Servicios que deben ser desabilitados en Unix:

En un sistema UNIX por lo general no siempre se distingue cuáles son los servicios que deben ser desabilitados debido a que los nombres de los servicios no son tan informativos [CHAP95]. Los servicios que deben ser desabilitados son:

NFS y servicios relacionados: (Network File System) Ninguna maquina interna confiaria en un host bastion lo suficiente como para permitir que este monte discos de maquinas internas via NFS. NFS es muy conveniente pero es muy inseguro. Los servicios NFS son provistos por un conjunto de servidores, varian dependiendo de la version de UNIX. Los principales son:

nfsd

biod

mountd

statd

lockd

automount

keyserv

rquotad

amd

Servicios **RPC:** (Remote Procedure Call) El mas crítico de estos es NIS/YP el cual es provisto por los siguientes servidores:

ypserv

ypbind

ypupdated

Servicios de booteo: Estos servicios tampoco deben ser provistos por un host bastion ya que no se desea que algun usuario bootee el host bastion. Los servicios a desabilitar son:

tftpd

bootd

bootpd

Comandos **BSD 'r':** Los comandos remotos no deben ejecutarse en un host bastion. Los servidores para estos servicios son:

rshd

rlogind

rexecd

Servidor de ruteo: Un host bastion probablemente no utiliza el servidor *routed* debido a que este se localiza en una red perimetro donde el ruteo es simple. Una alternativa es crear rutas estaticas hacia las redes internas y al ruteador que conecta a Internet.

Servicio fingerd: El servicio finger suministra informacion de las cuentas de usuarios existentes. Esta informacion es de mucho valor para intrusos ya que pueden conocer cuantas cuentas existen, informacion personal de los usuarios, cuantas cuentas estan en uso, cuantos usuarios se conectaron recientemente. Sin embargo, la informacion que brinda el comando

finger puede ser muy valiosa para los usuarios internos ya que pueden obtener direcciones de correo electronico, numeros de telefono, puntos de contacto, etc. Por lo tanto se requiere hacer un balance entre estas ventajas y las desventajas anteriormente descritas [GARF96].

Otros servicios: Pueden incluirse dentro de este grupo:

uucpd (UUCP, UNIX to UNIX Copy Protocol)

rwhod (igual que fingerd)

lpd (demonio de impresora)

3.4.3.3. Identificar y modificar los servicios

Algunos de los servicios que se desean proveer quizás no estén disponibles con el sistema operativo de un host bastion. Otros si están disponibles en el sistema operativo pero son muy inseguros en este ambiente o pierden ciertas caracteristicas que se desean.

Es aconsejable utilizar programas adicionales que hagan seguros a los servicios. En el caso de sistemas UNIX se utilizan programas como TCP Wrapper o netacl para proteger los servicios y al host que los provee. A continuación una breve explicación de estos dos programas:

TCP Wrapper: Este paquete de software monitorea todo el tráfico entrante a una maquina y controla su actividad. El TCP Wrapper provee de una lista de control de acceso para cada servicio y guarda información de log de los mismos. Para instalarlo se modifica el archivo inetd para correr un servicio llamado tcpd en vez del verdadero servidor. Así, cuando se produce un requerimiento, inetd ejecuta el servicio tcpd el cual evalua el requerimiento contra los archivos de configuración del TCP Wrapper.

Netacl: Es parecido al TCP Wrapper, controla todo el tráfico entrate a un maquina. A traves de una lista de control de acceso en un archivo de configuracioii, manipula y registra la información de log de cada servicio. La instalación es igual que el TCP Wrapper, se levanta otro demonio llamado netacl en lugar del verdadero sel-vidor. Tan solo basta modificar el archivo inetd del sistema operativo.

Con programas como estos, se puede configurar la máquina para que permita solo las conexiones en base a servicios y direcciones fuentes. Por ejemplo, se puede configurar estos programas para que el host bastion permita conexiones Telnet tan solo desde una maquina determinada.

3.4.3.4. Reconfiguración para produción

Despues de habilitar y modificar todos los servicios que se requieren, es necesario adoptar una configuracion apropiada para poner en opcracion a un host. Esta configuracion consiste en:

- Reconfigurar y reconstruir el kernel: El primer paso para reconfigurar un host bastion es reconstruir el kernel del sistema operativo para remover las capacidades que no se necesitan. Además de reducir el tamaño del kernel, y por lo tanto contar con mas memoria disponible para otros propositos, la reconstrucción del kernel niega la oportunidad a los intrusos de explotar capacidades existentes en un host bastion.
- Remover todos los programas innecesarios: Un host bastion es enteramente un proveedor de servicios de Internet y no necesariamente tiene que representar un ambiente confortable y amistoso para los usuarios internos. Es por esto que todos los programas que no son escenciales para el normal desenvolvimiento de una red deben ser removidos. En el caso de sistemas UNIX los tipicos programas que son innecesarios y que representan un gran blanco para atacantes son los programas setuid/getid. Los programas que suelen ser mas atractivos

para los atacantes son los compiladores y sistemas windows (ambientes graficos). Los cornpiladores sirven a los intrusos para coinpilar sus propios programas para violar sistemas y los sistemas windows por lo regular traen sus propios agujeros de seguridad.

- **Colocar permisos de "solo** lectura" a **la mayoría de** archivos **del sistema:** Los archivos del sistema operativo son muy importantes para la ejecución correcta del mismo. Si un intruso tiene acceso a uno de estos archivos, puede llegar a controlar el sistema de un host bastion y llegar a la red interna. En sistemas operativos multiusuarios como UNIX, se configuran permisos de acceso en modo lectura, escritura y ejecución para archivos de acuerdo a usuarics internos, grupos definidos de usuarios, y los propietarios. Todos los archivos que se consideren importantes para la ejecucion correcta del sistema debeii ser restringidos y por lo tanto sus permisos de acceso deben ser configurados en modo solo lectura

3.4.3.5. Auditoreo de seguridad

Una vez reconfigurado un host bastion, el siguiente paso es ejecutar un auditoreo de seguridad para establecer una base que sirva para tuturas comparaciones de auditoreo; y tambien para probar la seguridad de un host.

Existen paquetes publicos de auditoreo en Internet, los cuales se ejecutan en un sistema para revisar las debilidades y falencias en la red. Estos paquetes tiene dos propositos:

1. Investigar los agujeros de seguridad bien conocidos por los administradores de sistemas, explotados por atacantes o docurnentados en libros y reportes de seguridad para eliminarlos.
2. Establecer una base de datos de checksums de todos los archivos de un sistema, de esta manera se permite al administrador reconocer cambios futuros (por lo regular no autorizados) en los archivos. El manejo de estos checksurns depende del administrador.

En su mayoría, estos paquetes son gratuitos y compatibles con UNIX y los mas comunmente usados son: COPS, Tiger, Tripwire, SATAN, etc.

3.4.3.6. Conectar la máquina

Una vez efectuados los cinco pasos anteriores, el host bastion ya esta listo para ser conectado a una red y ejecutarlo. No se descarta la posibilidad que el host bastion falle, por lo tanto es necesario estar atento a cualquier cambio que se produzca en el host para detectar el posible agujero de seguridad para arreglarlo.

3.5. Filtraje de paquetes

Los filtradores de paquetes son mecanismos, normalmente provistos por los ruteadores, que controlan el trafico que fluye desde y hacia una red interna. En un ruteador se examinan, de cada paquete que ingresa a una red, las direcciones fuentes y destinos; si a esto se añade un conjunto de reglas en las cuales se acepte o rechace (en base a un conjunto de criterios que concuerden con las politicas de seguridad de una organización) un paquete determinado, entonces se obtiene un filtrador de paquetes.

Un filtrador de paquetes controla la transferencia de datos en base a:

- La dirección de red de origen del paquete
- La dirección de red destino del paquete
- Las sesiones o protocolos que estan sicndo usados en la transferencia de datos.

La mayoría de filtradores de paquetes no examinan ni toman decisiones en base a los datos dentro de cada paquete.

3.5.1. Ventajas del filtraje de paquetes

Dentro de las ventajas se enumeran las siguientes:

3.5.1.1. Un filtrador de paquetes puede proteger a toda una red

Un filtrador de paquetes colocado estrategicamente en una red puede proteger enteramente a esa red. Si se cuenta como un dispositivo de seguridad a un filtrador de paquetes se gana un nivel de seguridad de red sin observar el tamaño de la organización.

3.5.1.2. Un filtrador de paquetes no requiere del conocimiento o cooperación del usuario

A diferencia de los sistemas proxy, un filtrador de paquetes no requiere de software personalizado, de configuración especial por maquinas clientes, o de un entrenamiento especial de los usuarios. En realidad, un filtrador de paquetes es transparente a los usuarios, pues estos no se dan cuenta del trabajo que realiza el filtrador hasta que algo es prohibido, probablemente porque se trata de un problema de seguridad.

Esta transparencia que ofrece el filtraje de paquetes se debe a que no hace falta la cooperacion ni el conocimiento de los usuarios.

3.5.1.3. Filtradores de paquetes son ampliamente disponibles en ruteadores

La mayoría de filtradores de paquetes estan disponibles en muchos ruteadores implementados tanto en software como en hardware. Esto representa una gran ventaja debido a que los ruteadores son el mejor lugar para poner un filtrador. La localización de un ruteador es clave para un filtrador ya que un ruteador esta entre dos redes y controla el trafico que fluye entre ambas.

3.5.2. Desventajas del filtraje de paquetes

Los filtradores de paquetes tambien tienen desventajas. Entre las mas importantes estan:

3.5.2.1. Las herramientas de filtración no son perfectas

Las herramientas de filtracion tienen, unas menos que otras, limitaciones que no les permite cubrir todas las expectativas. Entre las limitaciones se encuentran:

- Dificultad para configurar las reglas de filtracion. Muchos filtradores poseen una interfase poco intuitiva, y un lenguaje muy difícil de interpretar por lo que resulta complicado configurar las reglas que implementan las politicas de seguridad de una organización.
- Una vez configurado el filtrador de paquetes, las reglas tienden a ser difíciles de probar. Cuando la configuracion es bastante complicada y quedan ciertos vacios, los resultados de las pruebas quizás no cumplan con las expectativas creadas.
- Como cualquier otro producto, un filtrador de paquetes tambien esta sujeto a errores de programacion por mala configuracion. La existencia de un error en un filtrador es más crítica que en un proxy debido a que si un proxy falla deja colgado el servicio y no permite que fluya mas trafico; en cambio si un filtrador de paquetes falla permite que todo el trafico fluya a traves de el.

3.5.2.2. Algunos protocolos no son apropiados para ser filtrados

No todos los servicios estan bien asegurados con un filtrador. Aún si la implementación de las reglas es efectiva y el filtrador es perfecto existen servicios que siendo filtrados igual abren agujeros o brechas en el sistema de seguridad. Por ejemplo entre estos protocolos se encuentran los que incluyen los comandos remotos BSD (rcp, rlogin, rdist, etc.), los protocolos RPC tales como NFS y NISNP, etc. En la sección **4.4.** se dan recomendaciones de como proteger los servicios de Internet mas comunes a traves de filtradores de paquetes.

3.5.2.3. Algunas politicas de seguridad no pueden ser cubiertas con los filtradores de paquetes

Existen politicas de seguridad que no pueden ser implementadas por filtradores de paquetes. La información que maneja un filtrador de paquetes en ciertos casos no permite cubrir las expectativas de seguridad de un sistema. Un ejemplo podría ser cuando una politica de seguridad desea proteger a un determinado servicio controlando la direccion que origina la conexión y el usuario, algunos filtradores manejan la direccion del host que originó el paquete pero no el usuario, de esta manera el filtrador no cubre esta política de seguridad.

3.5.3. Aspectos preliminares para configurar un filtrador de paquetes

Antes de configurar un filtrador de paquetes es necesario establecer que servicios se van a permitir o negar y luego trasladar todas las decisiones de las politicas de seguridad en reglas para filtrar paquetes.

Sin embargo, para configurar estas reglas, independientemente del filtrador (marca, hardware, software, etc.), existen conceptos que deben mantenerse en mente al hacerlo. Estos conceptos son los siguientes:

3.5.3.1. Los protocolos usualmente son bidireccionales

Cuando se configuran reglas para filtrar paquetes hay que recordar que los paquetes fluyen en dos vias. Los protocolos en Internet usualmente son bidireccionales, es decir, involucran un emisor que envía un requerimiento y un receptor que atiende y resuelve este requerimiento.

3.5.3.2. Semántica "entrsnte" y "saliente"

En un filtrador de paquetes hay que prestar mucha atencion en los terminos "entrantes" y "salientes". Por ejemplo un servicio "saliente" involucra paquetes "salientes" (paquetes de requerimiento de clientes internos) y paquetes "entrantes" (los datos que transmite el servidor externo). Para configurar un filtrador de paquetes se debe pensar en terminos de paquetes y no de servicios. Un filtrador de paquetes se configura en base al ingreso y salida de paquetes.

3.5.3.3. Permitir por defecto vs. negar por defecto

Entre las estrategias de seguridad explicadas en el capítulo I, se encuentra la de fallas seguras, la misma que establece dos puntos de vista para desarrollar las politicas de seguridad de una organización. Estos puntos de vista son: ***permitir por defecto*** (todo lo que no esta explicitamente prohibido es permitido) y ***negar por defecto*** (todo lo que no esta explicitamente permitido es prohibido). Para alcanzar simplicidad en el sistema de seguridad es mejor utilizar el ultimo punto de vista ya que es mas facil controlar solo aquellos servicios que la organización necesita y que se puedan proteger lo suficiente. De por sí las reglas de un filtrador de paquetes

guardan cierta dificultad para configurar y si no se conoce un servicio determinado el grado de dificultad para configurar las reglas aumentara.

Para fines prácticos elegir la instancia ***negar por defecto*** significa que las reglas de filtración se basaran solo en los servicios que se van a habilitar, haciendo que estas sean simples y reducidas en número.

3.5.4. Funcionamiento de un filtrador de paquetes

Un filtrador de paquetes basicamente examina la información del "header" en cada capa de la arquitectura TCP/IP. En una arquitectura TCP/IP se tienen las siguientes capas:

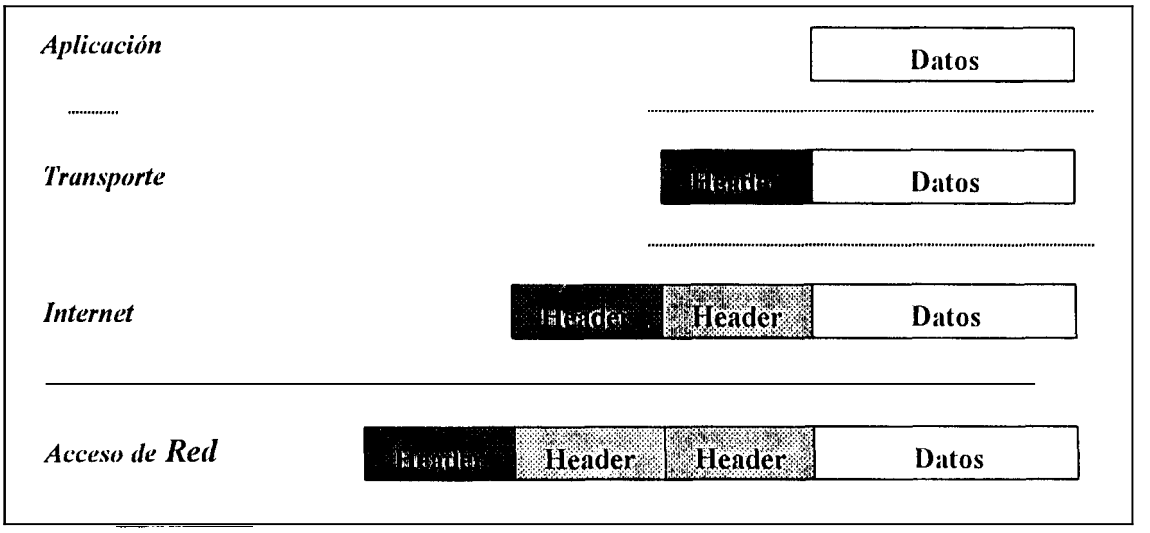


Figura NO. 3-16. Capas de la Arquitectura TCP/IP

Para describir mejor que es lo que hace un filtrador de paquetes se analizara su actividad por las capas citadas anteriormente.

3.5.4.1. Capa de Acceso de Red

En esta capa la parte del header contiene la siguiente informacion:

- Tipo de paquete cuando este disponible: Por ejemplo IP, IPX.
- La direccion fisica fuente del paquete: Si se trata del mismo segmento de red es la direccion fisica de la maquina que origina el paquete. Si se trata de otra red es la direccion fisica del ultimo ruteador por el que pasó el paquete.
- La direccion destino del paquete: Si se trata del mismo segmento de red es la direccion fisica destino de la maquina. Si se trata de otra red es la direccion fisica del siguiente ruteadoi para llegar a su destino.

En teoria es posible filtrar la informacion proporcionada en el header de esta capa; sin embargo, en la practica no es muy facil. Todos los paquetes que vienen desde Internet tienen la misma direccion fisica fuente (la direccion del ruteador que maneja la conexión con Internet). Además, muchos ruteadores mantienen conexiones con diferentes protocolos de bajo nivel, de esta manera filtrar a bajos niveles requiere configurar diferentes interfaces con diferentes tipos de reglas para diferentes protocolos de bajo nivel. Esto hace que filtrar en esta capa sea muy complicado y tedioso. Lo mas recomendable es empezar a filtrar paquetes a partir de la capa de Internet.

3.5.4.2. Capa de Internet

En la capa de Internet se encuentran los protocolos IP e ICMP. Se analizaran cada uno de ellos por separado.

Protocolo IP

Desde el punto de vista del filtrador de paquetes, el header de la capa de Internet contiene la siguiente informacion:

- La dirección lógica fuente del paquete: Con cuatro bytes de longitud. Ejm: 192.188.59.2
- La direccion lógica destino del paquete: De las mismas caracteristicas que la anterior.
- El tipo de protocolo: Identifica si el cuerpo del paquete transporta paquetes TCP, UDP o algun otro tipo de paquete.
- Campo de opciones IP: Por lo regular esta vacío; sin embargo, a veces se lo utiliza para guardar la informacion de la ruta que va a seguir el paquete desde la fuente.

Con esta informacion disponible, un filtrador ya puede aceptar o negar el flujo de un paquete determinado.

Problemas con el campo de opcion IP

El campo de opciones IP casi siempre se encuentra vacio. En su diseño su proposito fue colocar informacion especial o permitir manipular instrucciones que no tengan un campo especifico en el header. Pero este campo de opciones puede ser utilizado para llevar a cabo un ataque cuando se lo utiliza para colocar la informacion de la opcion de ruta del paquete.

La opcion de ruta permite colocar la ruta que debe seguir un paquete desde la fuente hasta su destino, de esta manera no permite que algun ruteador decida su ruta en base a sus tablas. En teoría la opcion de ruteo es muy utilizada para trabajar sin ruteadores que fueron comprometidos o que contienen tablas de ruteo incorrectas, si el emisor del paquete conoce la ruta que debe seguir el paquete se puede contrarrestar la informacion de las tablas de ruteo especificando las opciones de ruteo del paquete. En la practica, la opcion de ruteo es muy

utilizada por los atacantes quienes intentan desviar medidas de seguridad generando paquetes con rutas preestablecidas.

Para contrarrestar esta posible incursion a una red interna, un firewall que se basa en filtradores rechaza todo paquete que contenga la opción de ruteo activada sin importar cual sea la fuente o de que servicio se trata.

Problemas con la fragmentacion IP

Una de las caracteristicas de la capa IP es la habilidad para dividir paquetes grandes que no pueden atravesar algun enlace de red. Este proceso se lo conoce con el nombre de fragmentacion. Cuando llegan a su destino final los paquetes nuevamente son unidos, lo cual se conoce con el nombre de reensamblado.

El problema con la fragmentacion es que solo el primer subpaquete contiene la informacion del header de los protocolos de alto nivel (TCP, UDP, RPC) y el filtrador necesita esta informacion para examinar todos los paquetes.

La tecnica que utiliza un filtrador de paquetes es permitir la entrada de todos los paquetes fragmentados y examinar el primer paquete, que es el que contiene toda la informacion de los headers. Esta tecnica es segura ya que si el filtrador rechaza el primer paquete, la maquina destino no sabra como reensamblar el resto de paquetes, sin importar cuantos fragmentos haya recibido; y si no puede reconstruir el paquete original el paquete reensamblado no sera aceptado.

Protocolo ICMP

Dentro de la capa de Internet tambien se halla el protocolo ICMP, el cual es utilizado para manipular mensajes a traves de Internet. El protocolo ICMP no maneja un esquema propio de direcciones. Sin embargo, los filtradores de paquetes si estan en capacidad de filtrar paquetes de este protocolo examinando y evaluando el contenido de los mensajes. Este protocolo no representa un problema para los filtradores de paquetes.

3.5.4.3. Capa de transporte

Desde el punto de vista de un filtrador de paquetes, la capa de transporte contiene:

- Puerto fuente: un número de dos bytes, el cual especifica de que proceso (cliente o servidor) fue originado el paquete
- Puerto destino: similar al puerto fuente
- Campo de banderas (flags): depende del protocolo: TCP, UDP, etc.

Para estudiar mejor la capa de transporte se detallaran los dos protocolos mas comunmente usados: TCP y UDP.

Protocolo TCP

El protocolo TCP representa una conexion bidireccional y confiable entre dos puntos. Es bidireccional porque una vez que la conexion es establecida, un servidor puede replicar a un cliente sobre la misma conexion. La confiabilidad la otorgan tres garantias para la capa de aplicacion:

- El destino recibira los datos en el orden en que fueron enviados
- El destino recibira los datos completos
- El destino no recibira datos duplicados

TCP desactivara cualquier conexion que no cumpla con estas garantias. En base a esto, para bloquear una conexion TCP solo basta bloquear el primer paquete de la conexion. Sin el primer paquete, el receptor no podra reensamblar los datos completos y la conexion se desactivara.

El primer paquete se reconoce por el bit del ACK dentro del campo de banderas del protocolo TCP. Si el bit del ACK esta en cero quiere decir que se trata del primer paquete, y si esta en uno, se trata de los subsiguientes paquetes.

Identificar el comienzo de una conexion puede ayudar al filtrador de paquetes a permitir conexiones entre clientes internos y servidores externos y a prevenir conexiones entre clientes externos y servidores internos. Simplemente se examina que el bit del ACK este seteado con cero solo para conexiones salientes y seteado con uno solo para conexiones entrantes. Lo descrito se puede observar en la figura No. 3-17.

Las implementaciones de filtradores de paquetes dependen en su gran mayoría de como estos manipulen el bit del ACK. Algunos otorgan acceso directo a este bit de tal manera que se pueda incluir en las reglas de configuración [CHAP95].

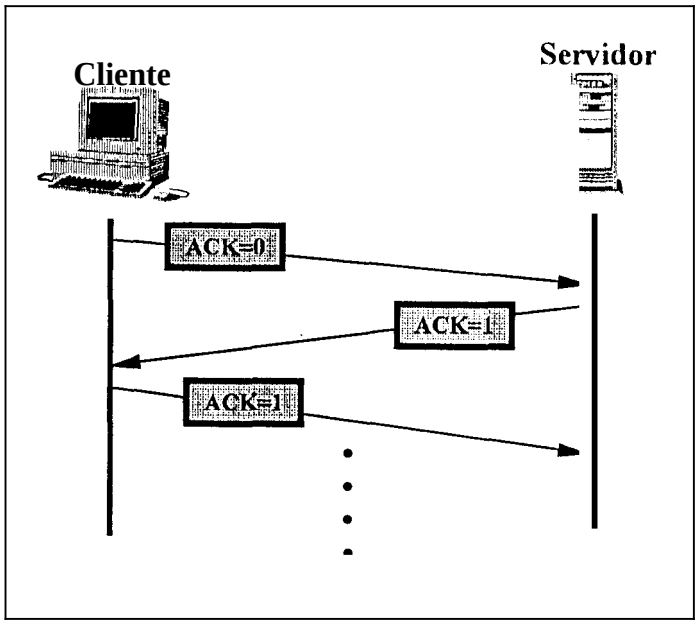


Figura No. 3-17. Reconocimiento del inicio de una conexión

Protocolo UDP

El protocolo UDP es diferente a TCP ya que no goza de las tres garantias del protocolo TCP. Cada paquete UDP es independiente y no forma parte de un circuito virtual como es el caso del protocolo TCP.

En el protocolo UDP, un paquete puede arribar a su destino mas de una vez cuando un ruteador piensa que un paquete se ha perdido.

Un paquete UDP contiene información de la direcciones fuentes y destino del paquete y los puertos que indican los servicios al igual que un paquete TCP, es decir son iguales en estructura. Sin embargo, no contiene el bit de ACK como en TCP. En TCP el bit del ACK

determina el inicio de una sesion; en UDP, al no poseerlo, no es posible saber cuando se inicia una sesion.

Para solucionar este problema algunos filtradores de paquetes poseen la capacidad de registrar la informacion de un paquete UDP saliente para luego solo permitir la entrada de la respuesta a ese paquete UDP. Es decir, el paquete entrante tiene que tener como direccion y puerto fuente la direccion y puerto destino del paquete saliente como se muestra en la figura No. 3-18. Esta capacidad se denomina ***filtraje dinámico.***

3.5.4.4. Capa de Aplicación

Los mas recientes filtradores de paquetes proveen la habilidad de filtrar protocolos de la capa de aplicacion para ciertas aplicaciones muy conocidas. Este tipo de filtraje compara el contenido de un paquete con la informacion de la capa de transporte a fin de que ambas sean consistentes. Por ejemplo, un filtrador podría asegurarse que los paquetes direccionados a un puerto DNS correspondan al protocolo DNS.

3.5.5. Acciones de un filtrador de paquetes

Una vez examinado un paquete, un filtrador tiene dos opciones:

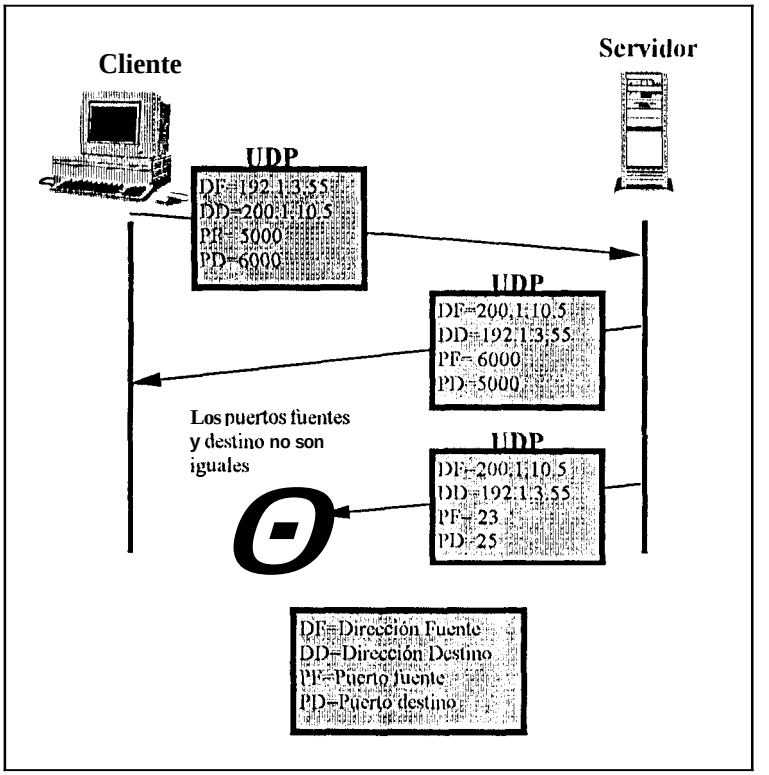


Figura NO. 3-18. Representación del filtraje dinámico

- Permitir el ingreso del paquete si curnple con las reglas de configuracion. En este caso un filtrador se comporta como un ruteador normal, recibe el paquete y lo retransrnite.
- Rechazar el paquete si no cumple con las reglas de configuracion. En este caso lo mas aconsejable es registrar en un archivo la informacion del porque este paquete fue rechazado.

Dentro de la segunda opción se dan varias recornendaciones de como se puede registrar la informacion y si se debe o no retornar mensajes de error.

3.5.5.1. Registro de información

Es importante guardar un registro de todos los paquetes que intentan ingresar a un sistema de redes de cornputadoras, ya sea si los paquetes fueron aceptados (cumplieron con las reglas de configuración) o rechazados (no cumplieron con las reglas).

Aunque no es muy práctico registrar el primer tipo informacion (paquetes aceptados) debido a la cantidad de paquetes que en realidad van a ser aceptados, es practica común de muchos administradores, al menos registrar los paquetes TCP que indican el inicio de una sesion (primer paquete con bit del ACK igual a 1) para llevar un control de que sesiones TCP fueron activadas.

Para el segundo caso (paquetes rechazados), es importante guardar un registro completo de ellos porque así se puede observar que o quienes intentan ingresar paquetes para abrir sesiones no permitidas por las politicas de seguridad.

El registro de informacion a este nivel es importante porque en caso de que se perpetre un ataque, es muy probable hallar el origen de los daños y determinar la magnitud de los mismos examinando este registro

3.5.5.2. Respuestas con codigos de error (ICMP)

Cuando un ruteador rechaza a un paquete, este puede enviar un paquete con codigo de error ICMP mediante el cual indica que el paquete no llegó a su destino. Este proceso tendría como objetivo dar aviso a la maquina emisora para que no intente mandar otro paquete de ese mismo tipo porque de igual manera sera rechazado.

Los dos grupos de mensajes dentro de los codigos de error de ICMP son:

- **"Destino inalcanzable":** "host inalcanzable","red inalcanzable";
- **"Destino** administrativamente inalcanzable": "host administrativamente inalcanzable","red administrativamente inalcanzable";

El primer tipo de mensajes indica un serio problema: que el host destino esta apagado o algún ruteador en el camino esta inhibido. El problema con este tipo de mensaje es que algunos sistemas (especialmente **UNIX)** asumen que el host involucrado es totalmente inalcanzable y cerrara todas las conexiones que actualmente mantiene con este aun si existiese otra conexión permitida por el filtrador de paquetes. Además, utilizar este tipo de mensaje es tecnicamente incorrecto por que no refleja la verdadera situacion de una red interna.

El segundo tipo de mensajes especifica una situación real de una red interna y pareceria tecnicamente correcta. Sin embargo, este codigo advierte la presencia de un filtrador de paquetes, y la informacion de que es lo que permite o rechaza. Esta informacion podria ser de mucha valia para un atacante. Por ejemplo, un atacante sabiendo que tipo de paquetes rechaza el filtrador, podria inundar la red con este tipo de paquetes produciendo un gran trabajo para el filtrador y así producir una ataque de negacion de servicio (sección 1.2.2. Ataque de negacion de servicios).

Cada uno de estos tipos de mensajes conlleva problemas. Lo recomendable en el caso de rechazar paquetes es no retornar ningun codigo ICMP a sistemas externos (donde puede estar un atacante y colectar la informacion del paquete ICMP para provocar un ataque), pero sí para los sistemas internos si es que los usuarios internos son confiables.

3.5.6. Configuracionde Reglas

Para entender mejor como configurar las reglas de un filtrador, es necesario llegar a una convención estandar de escritura.

Primero hay que recordar que los protocolos en Internet son bidireccionales, es decir que por cada sesión activa se configuran dos reglas: una para los paquetes que ingresan y otra para los paquetes que salen.

Para referirse a direcciones de red (por ejemplo 192.188.59.3) se van a utilizar las palabras "interno" o "externo" dependiendo si las direcciones son internas (dentro de la misma red interna) o externas (en la mayoria de los casos Internet).

En la mayoria de filtradores de paquetes, para cada paquete se revisan una a una las reglas de filtraje hasta encontrar la primera que satisfaga la condición del paquete y que le permita o rechace el acceso; caso contrario el paquete es rechazado.

El lenguaje en que se configuran las reglas del filtraje varia dependiendo de cada filtrador de paquetes. Muchos filtradores poseen una interfase de programacion bastante amistosa al usuario, mientras otros son complejos y tediosos.

He aqui un ejemplo de una posible configuración de reglas de filtraje en seis campos:

Regla	Rumbo	Dirección fuente	Dirección destino	ACK	Acción
A	Entrante o hacia adentro	host externo	Interna	cualquiera	Permitir
B	Saliente o hacia afuera	interna	host externo	cualquiera	Permitir
C	cualquiera	cualquiera	cualquiera	cualquiera	negar

La opción "cualquiera" significa que no importa el valor que tome el campo.

3.5.6.1. Filtrar por dirección

Este método simplemente se limita a permitir o rechazar cualquier paquete que proviene de una direccion a la cual el administrador considera hostil o no confiable. El filtrador, en este caso, lo unico que analiza en la cabecera del paquete son las direcciones lógicas fuente y destino. El uso mas recomendable de este tipo de filtrador es para habilitar conexiones de ciertos hosts con la red interna.

Filtrar por direccion evita el ataque de spoofing (paquetes forzados), ya que el filtrador puede detectar la direccion fuente del paquete. Si la direccion fuente del paquete es una direccion interna, el filtrador estara en capacidad de detectar que el paquete ha sido forzado y que se intenta perpetrar la red.

Con la siguiente regla se evita que cualquier paquete ingrese clarnando ser una direccion fuente

Regla	Rumbo	Dirección fuente	Dirección destino	Acción
A	hacia adentro o entrante	interna	cualquiera	negada

Riesgos

Si solo se utiliza filtración por direccion se corren dos grandes riesgos. El primero es que no se esta completamente seguro si el host externo con el que se establece la conexion es quien clama ser, y segundo que una maquina intermedia, entre el host externo y la red interna, intercepte y examine toda la conexion.

El hecho de filtrar por direccion evita establecer conexiones de hosts externos que claman ser hosts internos (cambio de direccion externa a interna), pero en realidad no evitan que los hosts externos sean quienes claman ser. Este tipo de ataque es llamado **"ruta fuente"** (ver seccion 1.2.1.3. Explotacion e infraestructura), y permite que un atacante cambie la direccion lógica de su maquina por la de una maquina que la red interna considera confiable. Incluso, los potenciales atacantes pueden interceptar las respuestas que otorgue la red interna antes que el verdadero host las intercepte.

El segundo riesgo el ataque llamado "hombre en la mitad" (man in the middle) o Hjacking (ver seccion 1.2.1.3. Explotacion e infraestructura) . Se trata de colocar una maquina en el camino entre un host interno y un host externo confiable. Como los paquetes de esta conexión fluyen a traves de la maquina intermedia, entonces esta ultima esta en capacidad de capturar todos los paquetes por medio de un "sniffer", e incluso interferir con respuestas al host interno antes de que el host externo confiable lo haga.

Estos dos tipos de ataques que se puederi sufrir, pueden ser prevenidos utilizando encriptacion (ver seccion 3.7 Autenticacion y encriptacion) para establecer un canal de comunicacion seguro y asegurarse que el host externo confiable sea el unico en recibir todo lo que se le envía.

3.5.6.2. Filtrar por servicio

La mayoría de filtradores de paquetes involucran filtración por servicio, lo cual resulta algo mas complicado pero eficiente. Para explicar mejor este tipo de filtraje, se utilizará un ejemplo con el servicio Telnet saliente de una red interna.

Para configurar los paquetes salientes de una sesion de Telnet hacia Internet, el adminitrador debe conocer la siguiente inforrnacion:

- La direccion fuente de los paquetes salientes es de un host interno
- La direccion destino de los paquetes salientes es de un host externo
- El puerto TCP destino es el 23 (estandar para Telnet)
- El puerto TCP fuente es un numero entre 1024 y 65535 (estandar para un puerto TCP fuente)
- Solo el primer paquete saliente (el que establece la conexion) no tendra seteado en 1 el bit del **ACK.**

Para configurar los paquetes entrantes de una sesion de Telnet hacia Internet, el adrninitrador debe conocer la siguiente inforrnacion:

- La direccion fuente de los paquetes entrantes es de un host externo
- La direccion destino de los paquetes salientes es de un host interno
- El puerto TCP fuente es **23,** el puerto que el servidor utiliza
- El puerto TCP destino es un numero mayor que 1023 (el mismo del caso anterior).
- Todos los paquetes tendrán el bit del ACK seteado en 1.

Observando esta inforrnacion, se encontrara que en ambos casos las direcciones fuente y destino son intercambiadas al igual que los puertos fuente y destino. La configuración de las

Regla	rumbo	d.fuente	d.destino	protocolo	p.fuente	p.destino	bit ACK	acción
A	afuera	interna	cualquiera	TCP	>1023	23	no	permitir
B	adentro	cualquiera	interno	TCP	23	>1023	si	permitir

Existe un riesgo al filtrar por puerto fuente, y es que el puerto fuente es tan confiable como lo es el host externo. Muchos hosts no tienen un estandar para puertos clientes, muchas veces el

administrador de un host cambia los puertos clientes. Ante esto es rnuy posible desabilitar, en lugar de habilitar, un servicio debido a que el puerto cliente no coincide con el que se estimo en las reglas. Lo recornendable en estos casos es utilizar rangos de puertos **(1024** .. 56535: quiere decir mayor que 1024 y menor que 56535) siempre y cuando el filtrador lo permita. Estos son los valores que se utilizan para los puertos clientes en los servicios **de** Internet.

3.6. Sistemas Proxy

Un sistema proxy habilita en forrna directa a un host o un numero reducido de hosts internos a Internet, y en forma indirecta a todos los demas hosts internos de una red. El host que tiene acceso directo a Internet actua como interrnediario de los demas, mientras que los clientes internos tienen la sensacion de interactuar directamente con Internet.

Un servidor proxy es instalado en un host bastion o en un host dual-homed, o en cualquier otro host que tenga comunicacion tanto con el usuario interno como con Internet. El programa del cliente primero establece una conexión con el proxy en lugar de hacerlo con el servidor real, el servidor proxy evalua el requerimiento del cliente y si lo aprueba envía el requerimiento hacia el servidor real y recibe las respuestas del servidor real para enviarlas al cliente original.

3.6.1. Ventajas de los sistemas proxy

3.6.1.1. Accesar a Internet "directamente"

En toda configuración un usuario para conectarse a Internet tiene que primero conectarse a un host para utilizar los servicios de Internet. Este es un gran inconveniente que frustra a los

usuarios y provoca que estos traten de buscar otras vías de acceso a Internet (ver sección 3.4. Host bastion).

Si se utiliza un servidor proxy en un host dual-homed, para el usuario es transparente la conexion entre el y el host, y piensa que esta interactuando directamente con Internet. Sin embargo, en realidad la conexion con Internet es indirecta, todo el trafico primero pasa por el proxy.

3.6.1.2. Proporciona un buen registro de acciones

Debido a que los servidores proxy trabajan con los protocolos de la capa de aplicacion, estos pueden permitir registrar en un archivo (archivos de log) todas las acciones de una manera muy efectiva. Por ejemplo, en lugar de archivar todos los datos transferidos durante una sesion FTP, un servidor proxy puede archivar solo los comandos ejecutados durante esa sesion FTP.

3.6.2. Desventajas de los sistemas proxy

3.6.2.1. Los servicios proxy demoran en liberarse

Para los servicios mas antiguos de Internet, tales como: FTP, Telnet, etc., existen servidores proxies ampliamente disponibles. Sin embargo, para los servicios de Internet que nacen recientemente, existe un retardo de tiempo para que salgan los correspondientes servidores poxies. Este retardo se debe principalmente a la dificultad que ofrezca el diseño de cada nuevo servicio. Existiran nuevos servicios que por su concepción sean faciles de construirles un servidor proxy, mientras que para otros quizás no.

3.6.2.2. Requieren de diferentes servidores para cada servicio

Se requiere de un servidor proxy para cada protocolo o servicio debido a que un servidor proxy examina cada protocolo para determinar que acciones son permitidas y para enmascararse como un cliente para el servidor real y viceversa.

Para obtener una configuracion con servidores proxies hay que primero buscar la disponibilidad de los mismos para los servicios deseados, instalarlos y configurarlos. Esto puede resultar un proceso muy dificil debido a que cada producto tiene sus propios manuales de instalacion y configuracion.

3.6.2.3. Requieren de modificaciones en los clientes y en procedimientos normales

Muchos servidores proxies requieren de ciertas modificaciones a los prograrnas clientes o modificaciones a los procedimientos (ver la siguiente sección para mayor entendimiento). Estas modificaciones tienen desventajas principalmente para los usuarios quienes estan acostumbrados a utilizar de cierta forma los servicios de Internet (como transferir archivos, como iniciar una sesion rlogin, etc)

Dependiendo del servicio, existen servidores proxy que sí son transparentes para el usuario. Es decir que la introducción de ese servidor proxy no altera los procediemientos a que esta acostumbrado a trabajar el usuario.

3.6.2.4. Los servidores proxy son limitados

No existen servidores proxy para todos los servicios, ya que algunos servicios no fueron diseñados con la idea de poder obtener de ellos un servidor proxy.

3.6.2.5. No protege de todas las debilidades de los protocolos

Como solución de seguridad, los servidores proxy tienen la habilidad de determinar que operaciones son seguras en un determinado protocolo. Sin embargo, no todos los protocolos dan las facilidades para esto. Por ejemplo HTTP fue diseñado para operar con servidores proxy, pero tambien fue diseñado para transmitir datos mientras es ejecutado. Si estos datos contienen virus o son comandos de ejecucion, al proxy de HTTP le es dificil proteger al servicio.

3.6.3. Funcionamiento

Los detalles de como funciona un proxy dependen de cada servicio. Para la mayoría de servicios el proxy requiere un programa servidor en el lado del servidor y en el lado del cliente uno de los siguientes metodos:

3.6.3.1. Software de cliente personalizado

Este primer método se da cuando el programa cliente conoce como contactar al servidor proxy sin necesidad de que el usuario se entere de que esta "hablando" con el servidor proxy. Para ello, estos programas clientes requieren de una configuración adicional. Además el programa cliente internamente envía al servidor proxy la dirección del servidor real al cual quiere conectarse.

Estos programas de clientes personalizados no existen en todas las plataformas (hardware/software). Aun si existiesen, estos tienen limitaciones. Por ejemplo, si un usuario esta acostumbrado a trabajar con interfases graficas, entonces rechazara utilizar un programa cliente que funcione solamente en modo texto. Sin embargo, muchos de los programas clientes

de WWW (Netscape, Mosaic, etc.) soportan proxy debido a que la mayoría de estos programas fueron creados despues que los firewalls llegaron a Internet.

3.6.3.2. Procedimiento personalizado del usuario

El usuario utiliza programas estandares para conectarse a un servidor proxy para luego "decirle" a cual servidor real quiere conectarse.

Es necesario instruir a los usuarios de los nuevos procedimientos especificos a seguir para cada protocolo. Por ejemplo, en un proxy FTP se siguen los siguientes pasos:

1. Conectarse al servidor proxy (un host bastion probablernente) en lugar del servidor FTP anonirno.
2. Ingresar la direccion de correo electronico del usuario anonimo, la cual esta compuesta por el nombre del usuario FTP seguido el nombre del servidor FTP al que se requiere conectar (por ejemplo "goliat.espol.edu.ec). Es decir, la direccion completa quedaria de la siguientu manera: "anonymous@goliat.espol.edu.ec".

Este metodo requiere de ciertas rnodificaciones a los procedimientos usuales. Estas modificaciones dependen del producto (proxy) que se utilice.

La principal desventaja de este metodo es que hay que enseñarles a los usuarios los nuevos procedimientos. Si se tienen pocos usuarios, no representa un gran problema, pero si se habla de 500 a 1000 usuarios, es un gran inconveniente.

3.6.4. Tipos de servidores proxy

A continuación se describe la terminología utilizada para catalogar a un proxy:

3.6.4.1. Proxy a nivel de aplicación o dedicados

Un proxy a nivel de aplicacion es un proxy que conoce, entiende e interpreta los comandos de una aplicacion especifica. La mas extrema version de un proxy a nivel de aplicacion es el programa Sendmail, el cual es implementado con un protocolo de "almacenar-enviar", es decir guarda momentaneamente los mensajes para luego enviarlos a su destino. Al cumplir con estas funciones, el programa Sendmail se comporta como un intermediario (proxy) entre los clientes internos y el servidor externo (Internet) para el protocolo SMTP (aplicacion). Por lo tanto, Sendmail es un proxy a nivel de aplicacion

En general los proxies a nivel de aplicacion utilizan procedimientos modificados. Hasta ahora no se conocen proxies a nivel de aplicacion que utilicen clientes modificados.

La ventaja de este tipo de proxy es que ejerce un mayor control sobre el protocolo de aplicacion, puede examinar la ocurrencia de ciertos comandos, usuarios permitidos, etc. Mientras que su gran desventaja es que solo sirve para una aplicacion en particular.

3.6.4.2. Proxy a nivel de circuito o genéricos

Un proxy a nivel de circuito es un proxy que crea un circuito entre el cliente y el servidor sin interpretar el protocolo de aplicacion, es decir no tiene tanto alcance en lo que a protección se refiere. La mas extrema version de un proxy a nivel de circuito es un **proxy híbrido**, el cual es un proxy desde el punto de vista de Internet porque sirve de intermediario, pero un filtrador de paquetes desde el punto de vista de la red interna ya que solo controla direcciones y puertos

fuente y destino. En realidad un proxy hibrido resulta de la combinación de las tecnologias de filtraje de paquetes y sistemas proxy.

En general los sistemas proxy a nivel de circuito utilizan clientes modificados. Sin embargo existen proxy que utilizan procedimientos modificados, tales es el caso del "plug-gw" del conjunto de herramientas proxy de TIS (Trusted information system).

La ventaja de utilizar sistemas proxy a nivel de circuito es que estos proveen servicios para una amplia variedad de protocolos. Por esta razon son tambien llamados genericos. La desventaja de estos sistemas proxy es que proveen de poco control sobre la aplicacion, resultan ser como los filtradores de paquetes, es decir, controlan las conexiones en base a sus direcciones y puertos fuente y destino.

3.6.4.3. Proxy inteligente

Los sistemas proxy inteligentes son aquellos sistemas proxy que pueden hacer algo mas que servir de intermediarios. Por ejemplo, cuando el cliente HTTP lanza un mismo requerimiento varias veces, aumenta el ancho de banda de la red. Para evitar esto, el servidor proxy HTTP maneja la memoria cache de la maquina donde esta instalado de tal manera que lleva el registro de las respuestas de los últimos requerimientos a fin de contestar a los requerimientos repetidos del cliente HTTP sin necesidad de consultar al servidor real.

Los sistemas proxy a nivel de aplicacion tienden a ser inteligentes ya que cada version que sale en Internet le añade ciertas habilidades especiales.

3.6.4.3. Proxy por defecto

Los servicios que son implementados con protocolos de “almacenar-enviar”, son sistemas proxy por naturaleza. Dentro de estos servicios, los mas importantes son: SMTP, NNTP, NTP. Estos servicios son considerados sistemas proxy ya que los mensajes son recibidos por un servidor y luego almacenados hasta que finalmente son enviados a otro servidor (destino final). En este esquema cada servidor intermediario actua efectivamente como un proxy para el servidor que origina el mensaje.

3.7. Autenticacion y Encriptacion

Diversos son los problemas que conlleva permitir servicios entrantes (de Internet o red externa a una red interna). Sin embargo, para muchas organizaciones es necesario tener una amplia apertura a Internet, tal es el caso de una universidad, colegio o academia.

Para permitir servicios entrantes es necesario optar por mecanismos extras que hagan seguras las conexiones. Estos mecanismos son: la autenticacion y la encriptacion.

Pero antes de analizarlos, es necesario reconocer que tipos de riesgos se corren si no se utilizan estos mecanismos. Existen tres tipos de riesgos asociados a los servicios entrantes:

- **Hijacking:** Se trata de un ataque de personficacion. Se da cuando un atacante roba una sesion terminal o login sobre un usuario que ya ha sido autentificado por un sistema sin que este se de cuenta.
- **Packet sniffing o sniffing:** Definido brevemente en la sección 1.2.1.2. Personificación. Un atacante puede “observar” toda la información que fluye sobre una red interna a traves de programas olfateadores que examinan todos los paquetes. Se pueden descubrir las contraseñas

(por ejemplo, obteniendo los primeros paquetes de una sesion Telnet) o informacion confidencial de la organizacion (datos sensibles y secretos).

- **falsa autenticacion:** Cuando un atacante puede confundir al sistema clamando ser un usuario autorizado. Esto puede suceder si un atacante toma un paquete de inicio de sesion y lo reenvía su destino original pero con una dirección fuente cambiada (la del atacante).

Las tecnicas para evitar los riesgos de los servicios entrantes detallados anteriormente son: la autenticacion y la encriptacion. Para cada tipo de riesgo se utilizan estas tecnicas de la siguiente manera:

- **Hjacking:** La mejor manera de evitar este tipo de ataques es a traves de la codificación de datos para que sólo el receptor de la comunicacion tenga acceso a la informacion, es decir que las maquinas intermedias en la comunicacion no puedan abrir sesiones sobre sesiones autorizadas.
- **packet sniffing:** Para evitar el robo de contraseñas se utilizan tecnicas de autenticacion que usan contraseñas no reusables, es decir que las contrasenas cambian en base a un criterio (tiempo, claves, etc., ver sección 3.7.1. Autenticacion) y no se mantienen siempre iguales. Para evitar el robo de informacion secreta de una organizacion se utiliza encriptacion para proveer canales seguros de comunicacion, así un paquete capturado no puede ser interpretado por que esta codificado.
- **falsa autenticacion:** Para evitar problema de falsificación de identidad se utilizan mecanismos de autenticacion que hacen que la informacion que fluye por la red (las contrasenas) no sean reusables, para de esta manera el atacante no la pueda volver a usar.

3.7.1. Autenticación

Autenticacion es el proceso por el cual se comprueba que una persona es quien clama ser. Los mecanismos de autenticacion pueden ser categorizados en base a uno o mas de las siguientes clasificaciones:

- **Algo que es:** Se refiere a dispositivos biometricos tales como detector de huellas digitales, examinadores de retinas, etc. Este rnecanismo resulta muy costoso e irnpractico ya que se requiere de software y hardware especializado, que hoy en dia todavia no es muy comun. Se lo utiliza para controlar el acceso fisico a algun lugar (laboratorios, sala de investigaciones, etc.)
- **Algo que se conoce:** El tradicional uso de una contraseña en un sistema. Este mecanismo es mas comunmente usado, especialmente en Internet, debido a que es facil de implementar, barato y práctico pues solo requiere de software mas no de hardware. Para proteger las contraseñas de posibles ataques en Internet, estas necesitan ser no reusables, es decir que una contraseiia no vuelva a ser utilizada por segunda vez.
- **Algo que se tiene:** Se trata de dispositivos tales como tarjetas magneticas, etc. Se lo utiliza para dar acceso fisico o remoto a un laboratorio o sistema. Utiliza hardware y software.

Los mecanismos de autenticacion que de diseñen pueden resultar de una combinación de las clasificaciones anteriores. Por ejernplo, se puede cornbinar "algo que se tiene" con "algo que se conoce" utilizando tarjetas electronicas con codigos secretos. El mecanismo del ejemplo puede ser utilizado para dar acceso fisico a un lugar importante, laboratorio, etc.

3.7.1.1. Esquema de contraseñas de un sólo tiempo (one-time password)

Las contraseñas de un solo tiempo, como su nombre lo indica, son contraseñas que solo pueden ser usadas una vez. Existen diferentes sistemas que proveen este esquema; algunos de ellos requieren dispositivos de hardware tales como tarjetas y calculadoras especiales, otros en

cambio son programas que estan basados en la criptografia, es decir, codifican las contraseñas actuales para generar nuevas contraseiias que solo el usuario correcto debe de conocer.

Las contraseñas de un sólo tiempo pueden funcionar de dos maneras:

- Una lista de contraseñas generadas por el sistema, la cual solo la conoce el usuario
- Una lista de contraseñas que puede ser generada dependiendo de la demanda del usuario.

Existen herramientas de software que proveen contraseiias de un solo tiempo, para un mayor detalle se tomara como ejemplo la solución "S/Key" del conjunto de herramientas de firewall de TIS (Trusted Information System).

Las solución "S/key" trabaja iterativamente aplicando un algoritmo de encriptacion, llamado MD4 (Message Digest function #4), el cual a partir de un valor inicial para producir un nuevo valor que sera la futura contraseña. El algoritmo tiene dos caracteristicas fundamentales:

- Del valor final no se puede regresar al valor inicial, es decir la encriptacion es en un solo sentido, no se puede desencriptar
- La probabilidad de que dos valores iniciales produzcan un mismo valor final es extremadamente pequeña.

S/Key funciona generando una lista de n-contraseñas como se muestra en la figura No. 3-19. Una vez generadas las n-contraseñas el proceso de validación se realiza de la siguiente manera: el sistema conoce la contraseña n (la última generada por el algoritmo MD4), el usuario debe ingresar como contraseña actual la contraseiia n-1, el sistema le aplica el algoritmo MD4 y obtiene una nueva contraseña la cual es comparada con la contraseña n que tiene en memoria. Si ambas contraseñas coinciden, el usuario sera el correcto y el sistema ahora mantendra en

memoria la clave n-1 para la siguientes validacion del usuario; de tal manera que para la siguiente ocasion que el usuario es utenticado, este tendra que surninistrar al sistema la contraseña n-2, y así sucesivamente [CHES94], [CHAP95].

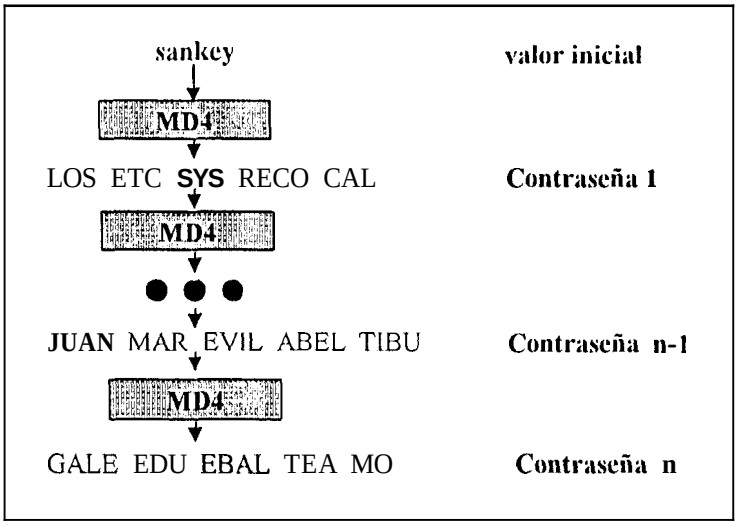


Figura No. 3-19. Esquema one-time password con S/Key

3.7.1.2. Esquema de desafio-respuesta

El esquema de desafio-respuesta es otra manera de implementar contraseñas no reusables. A igual que en el esquema anterior, existen diferentes sistemas que proveen este esquema a traves de hardware especializado: tarjetas electronicas, dispositivos perifericos, etc., o de software que emula los dispositivos de hardware.

Básicamente funciona de la siguiente manera:

- El sistema servidor al que el cliente necesita conectarse le envía un numero llamado desafio
- El cliente encripta el numero desafio otorgado por el sistema servidor y la envio de regreso al servidor

- El sistema servidor encripta el numero desafio generado por el y lo compara con el numero desafio encriptado por el cliente. Si las dos son iguales, el usuario que inició la comunicacion es quien dice ser; en caso contrario el servidor niega la conexion.

Como ejemplo se explicara el mecanismo SNK-004 de los productos de Digital Pathways (empresa dedicada a proveer mecanismos de autenticacion en sistemas). SNK-004 utiliza una tarjeta y una clave (combinación de "algo que se tiene" con "algo que se conoce"). El servidor genera un numero desafio y lo envía al cliente, la tarjeta SNK-004 es desbloqueada digitando la clave (en un dispositivo externo apropiado) y luego encripta el numero desafio para enviarlo al servidor. El servidor compara los dos numeros y verifica la autenticidad del usuario que quiere iniciar la comunicacion.

3.7.2. Encriptacion

La encriptacion es un proceso en el cual un mensaje (llamado texto plano) es transformado en otro mensaje (llamado ciphertexto) utilizando una funcion matematica y una contraseña de encriptacion (llamada clave). La desencriptacion es el proceso inverso; es decir, el ciphertexto es transformado a su formato original (texto plano) a traves de una funcion matematica y una clave.

3.7.2.1. Elementos de la encriptación

Los sistemas de encriptacion poseen los siguientes elementos en comun:

- Algoritmo de encriptacion: Es la funcion maternatica que ejecuta la tarea de encriptar y desencriptar la información.

- **Claves de encriptacion:** Son aquellas utilizadas por el algoritmo de encriptacion para determinar como los datos son encriptados o desencriptados. Son parecidas a las contraseñas de computadoras, ya que cuando un mensaje es desencriptado, se necesita la clave correcta para accesar a la informacion del mensaje. Si la clave de desencriptacion es incorrecta, el algoritmo desencriptara el mensaje de forma incorrecta haciendolo ilegible e intendihle [GARF96].
- **Longitud de la clave:** Al igual que las contraseñas, las claves poseen tambien una determinada longitud. Mientras mayor sea la longitud de una clave, es mas difícil para un atacante adivinarla a traves de algoritmos que realicen las posibles combinaciones de letras y numeros.
- **Texto plano:** Es la informacion que se desea encriptar.
- **Ciphertexto:** Es la informacion despues de haber sido encriptada.

En la figura No. 3-20 se muestra como un mensaje puede ser encriptado utilizando una clave en el emisor y otra clave en el receptor.

3.7.2.2. Alcance

- Puede proteger la informacion almacenada en un host de un acceso no autorizado ya que si se mantiene encriptada la informacion, tan solo los usuarios autorizados pueden accesarla.
- Puede proteger la informacion en tránsito mientras esta es transmitida de una red a otra. Si se encripta la informacion en transito, esta por mas que haya sido "olfateada" no podra ser interpretada.
- Puede ser usada para detectar algun cambio o alteración en la informacion y verificar el origen de la misma. Si la informacion desencriptada por el usuario autorizado no es entendible,

entonces la información ha sufrido algún cambio seguramente en tránsito o el origen (emisor de mensaje) no es verdadero [GARF96].

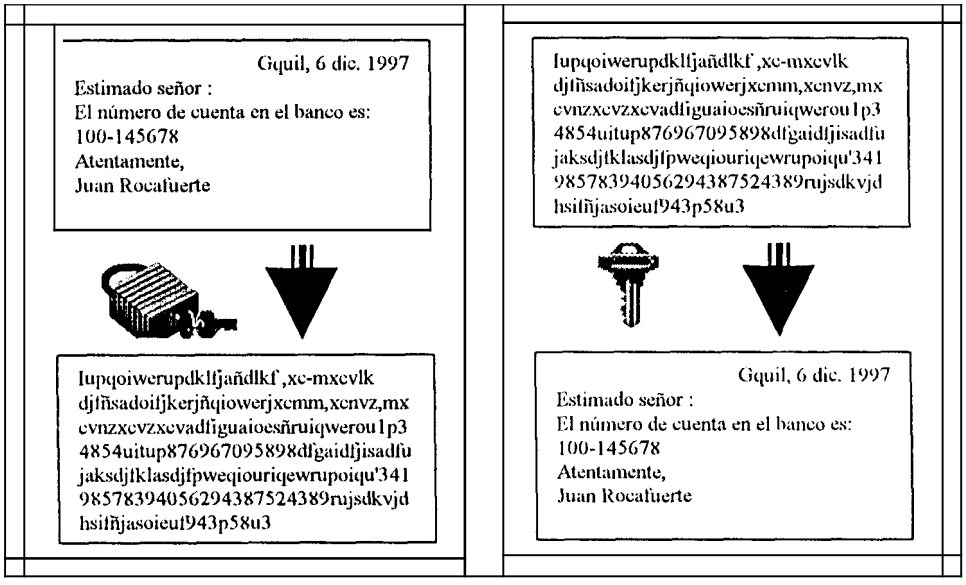


Figura No. 3-20. Encriptación de mensajes

3.7.2.3. Limitaciones

- No previene eliminaciones de datos, ya que la información encriptada que es interceptada en una red insegura puede ser eliminada y no llegar a su destino final.
- Un atacante puede comprometer el programa de encriptación ya que puede modificar el programa de encriptación y adaptarle una nueva clave o función matemática
- Un atacante puede encontrar la forma de desencriptar la información a través de un algoritmo que decodifique el mensaje probando todas las posibles combinaciones de la clave que desencripta.
- Un atacante puede accesar a la información antes que sea encriptada o después de ser desencriptada.

3.7.2.4. Encriptación en capas de TCP/IP

La encriptacion sobre Internet puede tomar lugar en varios niveles, siendo lo mas común aplicarla a nivel de aplicacion, enlace y red.

a. Encriptacion a nivel de aplicacion

Requiere de un soporte para todas las aplicaciones que se desean encriptar. Se trata de una encriptacion a muy alto nivel, requiere de versiones de criptosistemas tanto para clientes como para servidores y de modificaciones de procedimientos, lo que lo torna dificil de instalar y configurar.

b. Encriptacion a nivel de red

Este tipo de encriptacion se encuentra entre los dos anteriores esquemas. Con este tipo, los datos son encriptados desde la fuente que los origina hasta el destino cruzando por cualquier red considerada insegura. Al llegar los datos son desencriptados por el unico que puede desencriptarlos, el destino. Así se muestra en la figura No. 3-21. Este tipo de encriptación proporciona dos garantias:

- **Privacidad:** ya que los datos son encriptados, enviados a traves de redes inseguras y desencriptados en el destino final sin que nadie hay podido descifrar el contenido de la informacion.
- **Autenticacion:** en forma indirecta, el sistema destino al que llega el mensaje debe ser el unico que posea la clave para desencriptar la informacion. De otra manera la informacion no sera desencriptada. Así se asegura que el host destino sea el verdadero.

c. Encriptacion a nivel de enlace

Este tipo de encriptacion protege a un simple enlace de red. Por ejemplo, en líneas que utilizan los modems, la encriptacion protegera solo los datos cuando pasen a traves de esas lineas, no tiene capacidad para hacerlo si los datos luego pasan por ruteadores o hosts intermedios. Este tipo de encriptacion es a muy bajo nivel, por lo que no es muy popular en Internet.

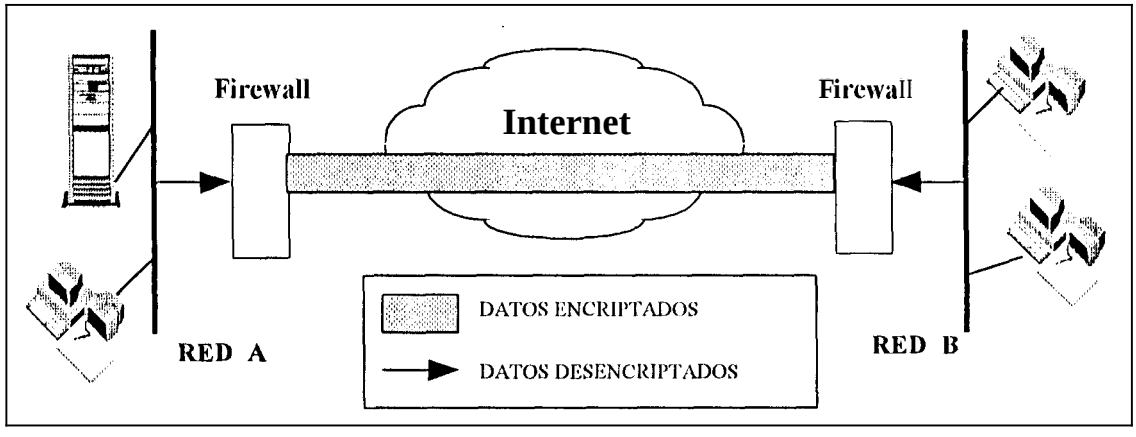


Figura No. 3-21. Encriptación a nivel de capa de RED (IP)

3.7.2.5. Algoritmos criptográficos comunes

Existen dos tipos basicos de algoritmos de encriptacion [GARF96], y son:

Clave privada

Utiliza la misma clave para encriptar y desencriptar el mensaje. Tambien es llamado algoritmo de clave simetrica. Es mayormente utilizado para proteger la informacion almacenada en la memoria secundaria de los computadores (discos duros) o para encriptar la informacion que transita entre dos maquinas. Entre los mas populares sistemas que utilizan claves privadas se encuentran:

- **DES:** (Data Encryption Standard) Es un algoritmo diseñado en la decada de 1970 por la National Bureau of Standards and Technology e IBM. Utiliza claves de 56 bits de longitud.
- **IDEA:** (International Data Encryption Algorithm) Es un algoritmo diseñado en Zurich en 1990. Utiliza claves de **128** bits. Es bastante fuerte si se considera que claves de 40 bits son vulnerables a ataques.

Clave publica

Utiliza una clave publica para encriptar el mensaje y una privada para desencriptarlo. La clave publica puede ser conocida por todos, sin comprometer la confidencialidad de la clave de desencriptacion. Tambien es llamado algoritmo de clave asimetrica. Es mayormente utilizado para crear firmas digitales en la informacion para certificar el origen y la integridad del mismo. Entre los mas populares se encuentran:

- **Diffie-Hellrnan:** Desarrollado por **B.** Diffie y M. Hellman, es un sistema para intercambiar claves criptograficas para un enlace seguro de comunicacion. La claves pueden tener cualquier longitud, pero se recomienda claves largas porque son mas dificiles de adivinar o forzar.
- **RSA:** Desarrollado por los profesores del MIT (Massachusetts Institute of Technology): **R.** Rivest, Adi Shamir y **L.** Adelman; es un sistema que puede ser utilizado para encriptar la informacion y para crear firmas electronicas digitales. La claves pueden tener cualquier longitud pero se recomienda claves largas porque son mas dificiles de adivinar o forzar.
- **DSA:** (Digital Signature Algorithm) Desarrollado por NSA (National Security Agency); es un algoritmo que solo permite claves entre 512 y **1024** bits de longitud. **Es** utilizado para crear firmas digitales.

3.7.2.6. La encriptación y la ley de U.S.

La encriptacion esta sujeta a la ley de los Estados Unidos por dos apectos:

Los criptosisternas estan sujetos a patentes

La patente de un artículo o experimiento es un documentos que certifica los derechos del autor sobre el mismo. Las patentes tambien son aplicadas para los programas de computadoras (llamados patentes de software) y han creado controversia entre la industria de software y el Congreso de U.S.

La Oficina de Patentes y Marcas de U.S. ha tenido problemas por otorgar patentes a muchos productos que no son considerados nuevos especialmente en el caso de software debido a que muchos programas de computadoras se basan en ideas utilizadas en programas anteriores. Además hasta el momento la constitucionalidad de otorgar patentes a productos de software no ha sido tratada legalmente por una corte [GARF96].

Controles de exportacion en criptosistemas

Segun la ley de Estados Unidos, la criptografia es considerada como una munición al igual que los materiales nucleares y armas de guerra. Por esta razon, la exportacion de sistemas de encriptacion es controlada por la entidad reguladora de comercio de Defensa (conocida como ITAR: International Traffic in Arms Regulation).

Para exportar un programa que encripta, es necesario que los distribuidores del programa adquieran un permiso especial o licencia de la oficina de control del comercio de Defensa (DTC: Defense Trade Control). Los distribuidores del programa deben liberarlo primero a la DTC para que ellos lo evaluen para otorgar o no la licencia. Historicamente los criptosistemas con claves de logitud menor a **40** bits han sido aprobados sin ningun problema; los criptosistemas con claves de longitud mayor a **40** bits tienen problemas para obtener la licensia.

En 1992, la Asociacion de Publicadores de Software y el Departamento de Estado de USA lograron un acuerdo que permita la exportacion de programas con esquema de seguridad **RSA** con **40** bits o menos de longitud de claves. A medidados de 1995 dos grupos independientes rompieron la seguridad de un criptosistema con claves de **40** bits, de esta manera se demostro que un criptosistemas con claves de **40** o menos bits son considerada inseguros.

3.7.2.6. Secure Socket Layer (SSL)

Secure Socket Layer es un protocolo implementado por Netscape Corporation que encripta la informacion a traves del Web.

SSL se basa en una combinación de los esquemas de clave publica y privada. SSL en realidad usa tres claves:

- Clave **publica:** Es una clave conocida por todos y que utiliza el browser para encriptar la informacion que envía al servidor.
- Clave privada: Es una clave generada aleatoriamente a partir de la clave publica y que utiliza el servidor para desencriptar la informacion que ha sido encriptada utilizando la clave publica.
- Clave **de** sesion: Las dos anteriores claves en realidad todavia no encriptan la información que se desea transmitir, sino que sirven para encriptar una tercera clave llamada clave de sesion. Esta clave de sesion es la que se utilizará para encriptar la innformacion confidencial que se desea transmitir.

Al ocupar las dos primeras claves se utiliza un esquema de clave publica, y al tener una sóla clave para encriptar la informacion confidencial a transmitir se utiliza un esquema de clave privada.

CAPÍTULO IV

POLÍTICAS DE SEGURIDAD PARA LA ESPOL

4.1. Introducción

Antes de elegir un firewall para la ESPOL, es necesario establecer las politicas de seguridad que van a controlar las redes de la universidad. Para realizar esto, de acuerdo con el capitulo II, es necesario saber que es lo se va a proteger, de quien se los va a proteger y cómo se los va a proteger.

En este capítulo primero se recopila la informacion acerca del funcionamiento del backbone de la ESPOL: los recursos conectados a el, los servicios de Internet que ofrecen sus servidores y las necesidades de la Jefatura de redes de CESERCOMP. Con esta inforrnacion se establecen las politicas de seguridad a traves de un análisis de riesgo de los recursos y el uso y responsabildades en las redes, para luego diseñar un modelo de seguridad que satisfaga las necesidades de protección de la ESPOL. Finalmente, se establece un plan de acción en caso de que se violen las politicas de seguridad.

4.2. Distribución y Funcionamiento de los recursos conectados al backbone de la ESPOL

Con la culminación del plan Informatico, la ESPOL cuenta con una espina dorsal o backbone que une a todas sus redes de cornputadoras de las unidades academicas y administrativas con otras redes nacionales e internacionales.

Este backbone provee muchos servicios y beneficia a las redes que se conecten a el. [PLAN95], [NORM96]. Los servicios mas importantes que estan disponibles son: el acceso a aplicaciones de administración académica y financiera, y el acceso a Internet desde cada una de las estaciones y servidores.

4.2.1. Recursos conecfados al Backbone y politicas de funcionamiento

- El Backbone interconecta principalmente a la redes de las unidades academicas y administrativas. Sin embargo se espera, a medida que avance el tiempo, mejorar la conectividad al backbone a traves de fibra óptica.
- Las unidades son responsables de administrar y operar sus redes, de colocar en ellas todos los recursos que consideren necesarios: servidores de servicios de Internet, servidores de información interna, estaciones, impresoras, etc.
- El backbone cuenta con dos servidores SUN SPARC 20 (Goliat) y SUN SPARC 2 (David) para brindar servicios de Internet. Mas tarde en este capitulo se detallaran los servicios que brindan estos hosts.

- Existen servidores de aplicaciones (administrativas y academicas) y bases de datos, los cuales representan las herramientas de trabajo tanto para las unidades administrativas como para las academicas. Debido a la confidencialidad que deben tener los datos, estos servidores son considerados de alto riesgo e importantes para el funcionamiento de la ESPOL. Por lo tanto, surge la necesidad de utilizar mecanismos de protección que garanticen la integridad de los datos para otorgar confiabilidad a los sistemas .
- El backbone continua fisicamente en el campus Peñas a traves de un enlace de radio con el campus Prosperina.
- La Jefatura de Redes dispone de una maquina de administración con la que pueda monitorear los sucesos en el backbone.
- Actualmente el backbone posee una conexion a Internet a traves de un proveedor local.
- La ESPOL provee acceso remoto dial-up tipo terminal a los servidores del backbone mediantc los servidores de comunicaciones ubicados fisicamente en CESERCOMP.

En el análisis de riesgo se conoceran mas detenidamente todos los recursos disponibles. En la figura No. **4-1** se aprecian todos los recursos anteriormente descritos.

4.2.2. Servicios de Internet

Por disposición de la Jefatura de Redes de CESERCOMP las maquinas SUN SPARC (David y Goliat) proveeran:

- Servidor de control de dominio (DNS, Domain Name Server)
- Correo electronico (SMTP, Simple Mail Transfer Protocol)
- Servidor de World Wide Web (HTTP, Hypher Text Transfer Protocol)
- Servidor FTP anonymous (FTP, File transfer Protocol)

- Servidor de NEWS (NNTP, Net News transfer Protocol)

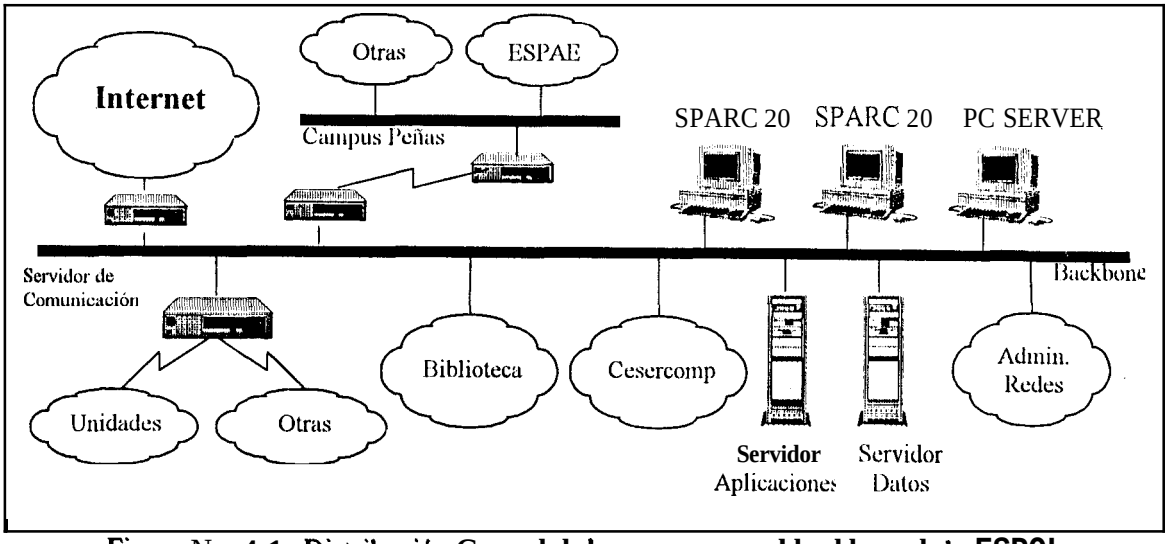


Figura No. **4-1. Distribución General de los recursos en el backbone de la ESPOL**

Las unidades conectadas al backbone que posean servidores podrán proveer de todos los servicios de Internet; sin embargo, mas adelante en este capítulo se detallaran los servicios de Internet mas comunes, sus vulnerabilidades y los metodos mas efectivos para protegerlos.

4.2.3. Necesidades de la Jefatura de Redes de CESERCOMP

La Jefatura de Redes de la ESPOL es la entidad encargada de proporcionar seguridad al backbone. Para esto todas las unidades deberan colaborar proporcionando toda la información requerida por la Jefatura de Redes [NORM96].

Además, la Jefatura de Redes requiere mecanismos (archivos de log) que le reporten todas la actividades dentro de las maquinas para que en caso de que se perpetren violaciones a la

seguridad, tener conocimiento de quien o quienes son los responsables y si los daños son criticos o salvables.

4.3. Análisis de Riesgo

En base al análisis de riesgo revisado en el capítulo II, sección 2.3.1., los recursos de la ESPOL son evaluados en base al producto de dos factores: riesgo de perdida **(R)** e importancia (W), siendo el metodo de evaluacion escogido el de lógica difusa en lugar del metodo numerico.

En el metodo tradicional numérico es difícil establecer valores para cada uno de los recursos de la ESPOL, además el resultado de una multiplicación (para obtener el riesgo total) es muy artificial y quizás no refleja lo que se quiere expresar. Por estas razones se eligio un metodo menos artificial que utiliza terrninos lingüísticos en lugar de valores y evaluacion de reglas en lugar de multiplicaciones.

Para una mayor visualización de los dos factores involucrados, el factor de riesgo (**R**) se obtiene a partir del promedio de tres posibles amenazas; y la importancia (W), a partir de tres caracteristicas intrinsecas que distinguen al recurso.

Las amenazas analizadas para el factor de riesgo son:

- Accesos **no autorizados:** Solo aquellos usuarios perrnitidos deben tener acceso a un recurso. Esta es una medida de cuan probable es que un usuario no autorizado ingrese o tome el recurso.

- **Robo de informacion:** ¿Es necesario que se ponga a disposición informacion importante?.

Esta es una medida de cuan probable es que un usuario obtenga informacion calificada como confidencial.

- **Negación de servicio:** Cuan probable es que un servicio este fuera de operación.

Las caracteristicas analizadas para el factor de importancia son:

- **Disponibilidad:** Cuan importante es tener disponible un recurso todo el tiempo.
- **Integridad:** Cuan importante es que el recurso o los datos que contiene sean consistentes.
- **Confidencialidad:** Cuan restringido debe ser el acceso a un recurso.

Para calificar a cada una de estas variables se utilizó la siguiente terminologia:

Riesgo			Importancia		
Acceso no autorizado	Robo de Info.	Negación de Servicios	Disponibili-dad	Integridad	Confidencia-lidad
Ningun	Ningun	Ningun	Ninguna	Ninguna	Ninguna
Bajo	Bajo	Bajo	Baja	Baja	Baja
Moderado	Moderado	Moderado	Moderada	Moderada	Moderada
Alto	Alto	Alto	Alta	Alta	Alta

Tabla IV. Terminos lingiiisticos para el analisis de riesgo

Cada uno de estas calificaciones fueron proporcionadas por el Dr. Enrique Pelaez, Director de CESERCOMP, y por el Msc. Guido Caicedo, Jefe de redes de CESERCOMP. Cabe destacar que se consideraron los criterios de las personas anteriormente nombradas debido a que han participado activamente en el plan informatico de la ESPOL y por lo tanto son las mas idóneas para proporcionar este tipo de informacion. Por cada fuente se realizó un analisis de riesgo por separado para luego contrastar los resultados de ambos.

Solo se han analizado los recursos que estan conectados directamente en el backbone, ya que cada subred (redes de las unidades) es libre de colocar los recursos que consideren necesarios.

Por esta razon todo administrador de una subred debe considerar un estudio de analisis de riesgo similar para construir los mecanismos de seguridad necesarios

A cada recurso conectado al backbone se le ha asignado un numero identificador y una pequeña descripción, las cuales se pueden observar en la figura No. 4-2.

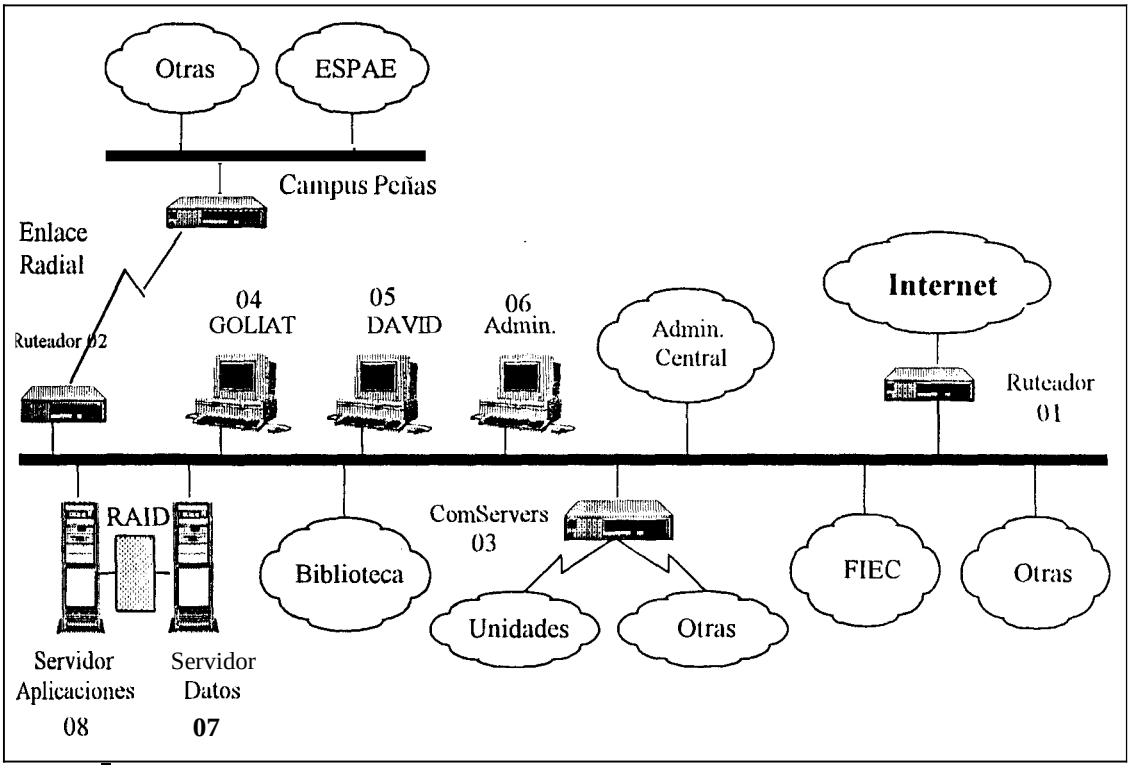


Figura No. 4-2. Distribución detallada de los recursos *en* el backbone de la ESPOL.

El desarrollo de los procedimientos del analisis de riesgo se encuentran en el apendice A.

Los resultados de riesgos totales por cada recurso conectado en el backbone del la ESPOL son:

Por esta razon todo administrador de una subred debe considerar un estudio de analisis de riesgo similar para construir los mecanismos de seguridad necesarios

A cada recurso conectado al backbone se le ha asignado un numero identificador y una pequeña descripción, las cuales se pueden observar en la figura No. 4-2.

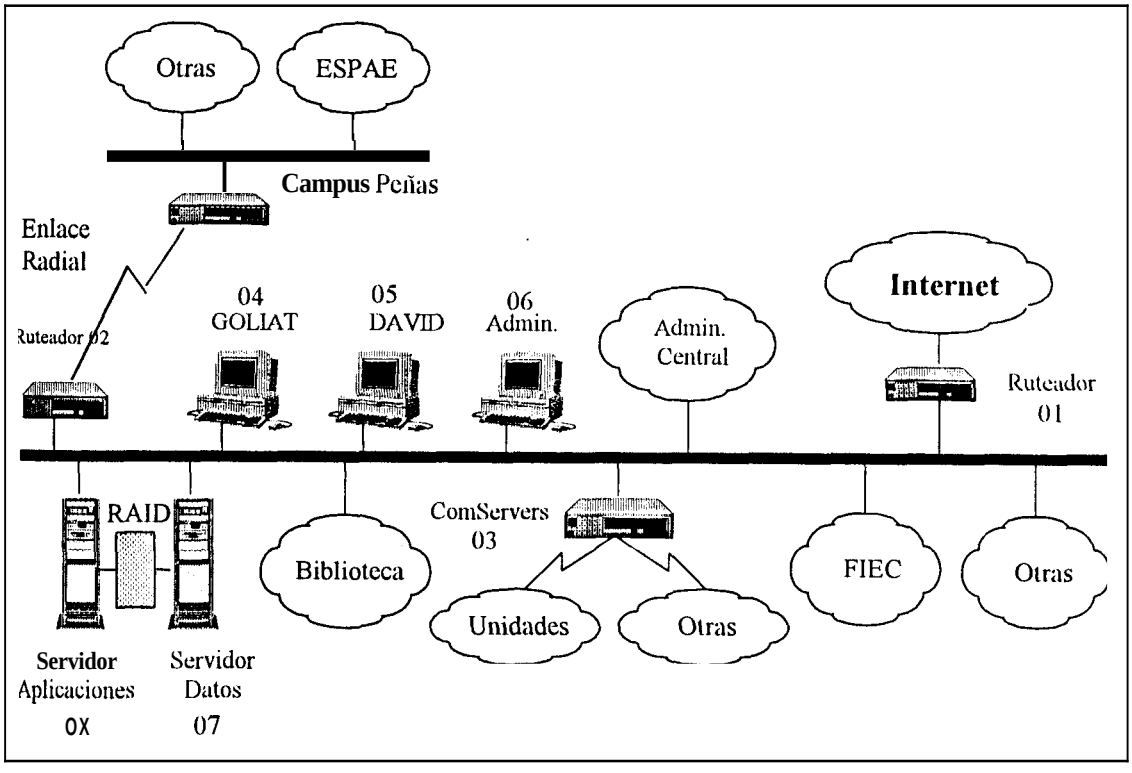


Figura No. 4-2. Distribución detallada de los recursos en el backbone de la ESPOL.

El desarrollo de los procedimientos del analisis de riesgo se encuentran en el apendice A.

Los resultados de riesgos totales por cada recurso conectado en el backbone del la ESPOL son:

Recursos		Riesgo Total
No	Nombre o descripción	R x W
01	Ruteador IBM 2210 Enlace con Ecuanet	ALTO -
02	Ruteador IBM 2210 Enlace con Las Peñas	ALTO -
03	ComServers TELEBIT	ALTO -
04	goliat.espol.edu.ec	
a	SPARC 20	ALTO +
b	S.O.: Solaris	ALTO +
	Servidores:	
c	DNS	ALTO +
d	SMTP (SendMail)	ALTO -
e	FTP (anónimo)	MODERADO -
f	HTTP	ALTO -
g	Telnet	ALTO -
05	David.espol.edu.ec	
a	SPARC 2	ALTO -
b	S.O.: Solaris	ALTO -
06	Maquina Administración	
a	RISC 6000	ALTO -
b	UNIXAIX	ALTO -
c	NetView	ALTO -
07	Servidor de bases de datos	ALTO -
a	RISC 0000	ALTO -
b	S.O.: UNIX AIX	ALTO -
c	DB/2	
0X	Servidor de aplicaciones	ALTO -
a	RISC *6000*	ALTO -
b	S.O.: UNIX AIX	ALTO -
	Servidoras:	
c	Presupuesto	ALTO -
d	Contabilidad	ALTO -
e	Tesorería	ALTO -
f	Académica	ALTO -

Tabla V. Resultados del análisis de riesgo de los recursos conectados en el backbone

4.2.1. Conclusiones de los resultados

Los riesgos han sido calificados en base a tres categorias:

ALTO $_{+}$: El riesgo es muy alto.

ALTO $^{-}$: El riesgo es alto, pero tiene un grado de moderado que lo hace menos alto. A esta categoria se la puede denominar "riesgo alto"

MODERADO $^{-}$: El riesgo es moderado con un grado de bajo. A esta categoria se la puede denominar "riesgo casi bajo".

El detalle de la obtencion de un criterio para la calificación final de los recursos se encuentra en el apendice A.

La mayoría de los recursos conectados al backbone poseen un "riesgo alto", es decir no existe alguno que no posea ningun riesgo y que no sea importante. De acuerdo a la tabla anterior, los recursos hallados mas críticos, es decir de muy alto riesgo, son el recurso goliat.espol.edu.ec: hardware, sistema opertaivo y servidor DNS. El recurso de riesgo moderado es FTP (anonimo) de Goliat.

Dado estos resultados, todos los recursos necesitan protección, unos mas que otros dependiendo de la categoria en que se encuentren. Las medidas de proteccion que se pueden tomar para cada uno de los recursos se encuentran en el modelo de seguridad.

4.4. Uso y responsabilidades en las redes de la ESPOL

Al igual que en el capitulo II, para establecer el uso y responsabilidades en las redes de la ESPOL es necesario seguir los siguientes pasos:

4.4.1. Idenfificando a los usuarios

Básicamente existen 2 tipos de usuarios: usuarios internos y externos. Dentro de los usuarios internos existen los siguientes tipos:

Administrador: Las personas que laboran para el departamento de redes de CESERCOMP. Estos son usuarios con privilegios especiales sobre todos los sistemas de la ESPOL conectados al backbone. Cada red conectada al backbone tambien tiene un usuario administrador pero con privilegios solo para su red. Para diferenciarlos, al usuario administrador del backbone se lo llamara administrador central y al otro tipo, administrador seccional.

Personal docente: Se refiere a todos los profesores de la universidad. Pueden subdividirse de acuerdo al area al que pertenecen. Ejm: facultades e institutos, etc.

Personal administrativo: Se refiere a todas las personas vinculadas a la ESPOL que no se dedican a la docencia. Dentro de este grupo pueden existir subgrupos dependiendo de las necesidades de los mismos. Ejm: rector, vicerrectores, jefes de unidades, secretarias, asistentes, etc.

Estudiantes: Todas las personas que estudian en la ESPOL. Tambien pueden tener subgrupos de acuerdo a las especializaciones a las que pertenecen. Ejm: ingenieria en computación, ingenieria en electrónica, en potencia, en mecanica, etc.

Los usuarios externos son aquellos usuarios que provienen de Internet.

Pueden existir casos de usuarios que caen en más de un tipo, como por ejemplo el personal docente que desarrolla actividades de administración para la ESPOL; en estos casos estos

administrativa de la ESPOL tiene mas privilegios sobre las aplicaciones administrativas que una secretaria; un profesor (personal docente) tiene mas privilegios sobre la aplicacion académica que un estudiante, etc.

En la tabla VI se puede observar a los tipos de usuarios que tienen acceso a los recursos conectados en el backbone.

Los tipos de acceso posibles son:

- **lectura:** el usuario solo puede leer
- **escritura:** el usuario puede escribir
- **ejecución:** el usuario puede ejecutar cualquier programa.
- **total:** acceso fisico, archivos del sistema: lectura, escritura y ejecucion

Cuando se habla de acceso a todo tipo de usuarios, se incluye al usuario administrador con todo tipo de acceso.

4.4.2. Uso apropiado de los recursos

En todos los recursos a los que solo tiene acceso el usuario administrador central o seccional, este debe detallar cuál es el uso apropiado de los mismos. Por su propia naturaleza, todos estos recursos son restringidos para los demas usuarios, es decir, no deben estar al alcance de los usuarios no autorizados ya que segun los resultados del análisis de riesgo son de mucha importancia y alto riesgo.

Para el caso de los usuarios de las SUN SPARCs (David y Goliat), se define como uso aceptable de estos recusos a lo dispuesto en las normas y reglamentos que la ESPOL ha

dispuesto para el correcto uso de los servicios de Internet. Las contravenciones a estos reglamentos seran considerados como usos inaceptables y propios para sanciones.

Recursos		Tipo de acceso	Tipo de usuario
No	Nombre o descripción		
01	Ruteador IBM 2210 Enlace con Ecuanet	total	administrador central
02	Ruteador IBM 2210 Enlace con Las Peñas	total	administrador central
03	ComServers TELEBIT	sólo los hosts que determine la jefatura de redes: Goliat, David	todos los tipos de usuarios
04	goliat.espol.edu.ec		
a	SPARC 20 (hardware)	total	administrador central
b	S.O.: Solaris	escritura y lectura en el directorio del usuario	todos los tipos de usuarios, excepto el usuario externo
	Servidores:		
c	DNS	total	administrador central
d	SMTP (SendMail)	escritura y lectura	todos los tipos de usuarios excepto el usuario externo
e	FTP (anónimo)	lectura	todos los tipos de usuarios
f	HTTP	lectura, ejecución	todos los tipos de usuarios
g	Telnet	escritura y lectura en el directorio del usuario	personal administrativo y docente
05	David.espol.edu.ec		
a	SPARC 2 (hardware)	total	administrador central
b	S.O.: Solaris	escritura y lectura en el directorio del usuario	todos los tipos de usuarios excepto el usuario externo
06	Maquina Administración		
a	RISC 6000 (hardware)	total	administrador central
b	UNIX AIX	total	administrador central
c	NetView	total	administrador central
07	Servidor de bases de datos		
a	RISC 6000	total	administrador seccional
b	S.O.: UNIX AIX	lectura	administrador seccional
c	DB/2	lectura	administrador seccional
08	Servidor de aplicaciones		
a	RISC 6000	total	administrador seccional
b	S.O.: UNIX AIX	lectura	administrador seccional
	Aplicaciones Servidoras:		
c	Presupuesto	escritura, lectura y ejecución	personal administrativo
d	Contabilidad	escritura, lectura y ejecución	personal administrativo

e	Tesorería	escritura, lectura y ejccucion	personal administrativo
f	Académica	personal docente y administrativo: cscritura, lectura, ejccucion. estudiantes: lectura	personal docente, administrativo y estudiantes

Las aplicaciones administrativas son de uso restringido, tan solo usuarios de tipo administrativo tienen acceso, y estos a su vez, tienen acceso de acuerdo a los modulos de seguridad (tipos de usuarios) de las aplicaciones. La aplicacion académica es de uso semi-restringido, ya que los usuarios docentes, administrativos y estudiantes tienen acceso al mismo. El usuario estudiante solo tiene acceso de tipo lectura. Cualquier acción en contra de la confidencialidad e integridad de los datos que manejan estas aplicaciones sera considerada inaceptable y propia para sancion.

Para las redes conectadas al backbone, los administradores de las mismas se encargaran de dictar el uso apropiado de cada uno de sus recursos teniendo como objetivo no causar problemas que afecten a los recursos del backbone. Por ejemplo, el uso no apropiado de una rnaquina cliente de una aplicacion administrativa puede ocasionar accesos no autorizados al servidor de la aplicacion y causar un perjucio a la ESPOL.

4.4.3. Determinación de quien esfa autorizado para otorgar acceso y aprobar el uso

Las unidades podrán disponer de sus redes y proveer a sus usuarios de todos los servicios que ofrece el backbone. Cada unidad tiene un(os) administrador(es) seccional(es) encargado(s) de

las redes que manejan, el o los cuales definen a los usuarios de sus servidores, sus caracteristicas y privilegios.

La jefatura de redes de CESERCOMP es la entidad encargada para otorgar acceso de las redes de las unidades al backbone y aprobar el correcto uso de estas redes.

4.4.4. Determinación de las responsabilidades de los usuarios

Como se indicó anteriormente todos los usuarios de las maquinas SUN SPARCs deben atenerse al reglamento para los servicios de Internet que posee la ESPOL.

Las aplicaciones administrativas y académica poseen modulos de seguridad en los cuales se definen los tipos de usuarios y las responsabilidades de cada uno de acuerdo a la funcion que desempeñan. Por ejemplo, el usuario director de una unidad administrativa tiene mas responsabilidades sobre la secretaria de la misma unidad.

Todas las unidades tendrán que acatar las normas y reglas para conectarse al Backbone segun el documento "Normas de acceso al Backbone e Internet" publicado por CESERCOMP en junio de 1996.

La unidades seran responsables de proteger todos los recursos en sus redes, publicar su propia política de seguridad y proceder ante posibles violaciones de seguridad, de acuerdo siempre con las politicas de la jefatura de redes de CESERCOMP.

4.4.5. Determinación de las responsabilidades de los administradores

La Jefatura de Redes de CESERCOMP es la entidad encargada de determinar cual es el alcance del usuario administrador central. El usuario administrador central tiene acceso a todos los recursos conectados al backbone y a los recursos de cada red conectada al backbone. Para esto, el administrador central debe poseer la cuenta y contraseña de cada uno de los administradores seccionales.

Los administradores de las redes de las unidades (administradores seccionales) tienen que notificar, a la jefatura de redes de CESERCOMP, la distribución, uso de sus recursos y todos los futuros carnbios que realicen a sus redes.

4.4.6. Información sensible

Las maquinas que contienen información sensible son los servidores de las aplicaciones y base de datos, a las cuales tienen acceso solo los usuarios autorizados de las aplicaciones administrativas y académica. Estos usuarios son divididos en varios subtipos dependiendo de las funciones que realizan y el grado de accesibilidad a los datos (escritura, lectura, ejecucion de procesos). Pero como se advirtio anteriormente, estas aplicaciones poseen modulos de seguridad en los que se definen a los usuarios autorizados y las acciones que estos pueden realizar.

4.5. Modelo de seguridad para el backbone de la ESPOL

Segun el capitulo II, los temas a tratar en esta sección son:

- Identificación de posibles problemas

- Controles en el modelo de seguridad
- Monitoreo
- Procedimientos generales

De estos tres temas, solo los tres primeros han sido desarrollados debido que el cuarto tema involucra definiciones de procedimientos establecidos por la Jefatura de Redes.

4.5.1. Identificando los posibles problemas

Los posibles problemas que debe afrontar el backbone son:

4.5.1.1. Accesos al backbone

Los servicios de acceso directo al backbone son:

Acceso dedicado: Si una unidad utiliza un acceso dedicado al backbone tiene conexion a los sistemas de informacion de la ESPOL y es considerada como un nodo de Internet. Además tiene incluido el servicio de acceso dial-up tipo terminal a los servidores de la ESPOL. Al ser un nodo de Internet, cualquier maquina corre riesgo de ser atacada, por lo tanto se sugiere que estas sean protegidas con seguridad de host. La conexion puede realizarse via fibra óptica o a traves de enlaces seriales utilizando los dispositivos apropiados (modems o taus).

Acceso remoto dial-up tipo terminal a los servidores: El acceso remoto dial-up tipo terminal implica que un usuario desde un lugar remoto, solo podra conectarse a aquellos servidores en los que se le haya creado un cuenta. Estos servidores pueden ser: servidores de su unidad, servidores de sistemas de informacion, o servidores de acceso a Internet. Este tipo de acceso involucra peligro si los usuarios que se conecten no son autenticados. Es recomendable la autenticacion en los servidores de la ESPOL.

Acceso rernoto dial-up TCP/IP: El acceso romoto dial-up TCP/IP se dara en caso de que la ESPOL llegue a ser proveedor local de Internet. Este tipo de acceso sí genera peliyro (ver sección 2.5.1.1. Puntos de acceso)

Acceso via Inernet: El acceso via Internet se realiza mediante la apertura de una sesion desde Internet a un servidor interno a traves de los servicios de Internet que la ESPOL brinda. Este tipo de acceso, si no es adecuadamente protegido con autenticacion, puede convertirse en una brecha de seguridad. Lo recomendable es proteger a los servicios entrantes via autenticacion y encriptacion.

4.5.1.2. Sistemas mal configurados

Los recursos a los que solo tiene acceso el administrador deben ser configurados de tal manera que cumplan con esta condición y no dejen posibilidades de peligro que posteriormente pueden ser descubiertas.

Solo los servidores de Internet (David y Goliat) conectados al backbone permiten cuentas de usuarios, lo cual puede producir brechas en la seguridad si los sistemas son mal configurados. Por esta razon existe la necesidad de brindar "seguridad de host" tanto a David como a Goliat.

Los servidores de aplicaciones y base de datos no deben permitir cuentas de usuarios en el sistema operativo debido a que los usuarios autorizados podrían producir lesiones graves (eliminaciones y cambios de archivos) al sistema operativo. Las cuentas de usuarios deben ser a nivel de la aplicacion y con contraseñas difíciles de adivinar para evitar accesos no autorizados. Tambien se sugiere brindar seguridad de host para estos dos servidores.

4.5.1.3. Errores en software

Entre los servidores de Internet el programa que puede constituirse en un peligro es el SendMail. A lo largo del capítulo I, se ha señalado las falencias de este programa. Los demas programas servidores de Internet tambien tienen problemas, menos criticos que SendMail, pero al fin y al cabo problemas de seguridad. Por esta razon, estos servicios deben ser resguardados con mecanismos de firewalls y configurados de manera segura. En la sección 6.2. Firewall externo, se trataran los problemas de cada servidor y la manera de solucionarlos.

En cuanto a las aplicaciones de servicios internos de la ESPOL, estas ya cuentan con sus propios módulos de seguridad que brindan protección a los datos.

4.5.1.4. Amenazas de usuarios internos

En la ESPOL, los usuarios internos constituyen una amenaza a la seguridad debido a que pueden intentar accesar sin permiso algún servidor del backbone. Los usuarios internos en su mayoría son estudiantes, los cuales con fines investigativos o maliciosos y despues de muchos intentos, pueden lograr accesar a algun servidor prohibido para ellos (ejemplo: servidor de aplicaciones administrativas), y ocasionar daños a la ESPOL. En estos casos se pueden utilizar mecanismos de autenticacion para evitar accesos no autorizados.

4.5.1.5. Seguridad Física

El backbone y todos los recursos del mismo estan fisicamente a salvo debido a que se encuentran en CESERCOMP, donde no es permitido el paso de personas no autorizadas.

4.5.2. Controles en el modelo de seguridad

La ESPOL como una organización académica mantiene una conexión abierta con Internet, lo cual hace que sea blanco de ataques por parte de hackers. Además, debido a la alta importancia en la confidencialidad, integridad y disponibilidad de los servidores de informacion interna de la ESPOL, es necesario colocar mecanismos de seguridad a fin de salvaguardar los intereses de la universidad.

Una vez identificados todos los recursos sensibles e importantes que se conectan al backbone, se evalúa toda la teoría de seguridad revisada anteriormente: metodos y estrategias de seguridad, tecnologías y arquitecturas de firewalls, para satisfacer las necesidades de protección de los mismos. Para entender mejor el modelo de seguridad planteado, este se divide en: niveles de seguridad, seguridad de la informacion en transito, firewall externo y firewalls internos.

4.5.2.1. Niveles de seguridad

En el area de ataques a sistemas de redes de computadoras ningun mecanismo de seguridad es invulnerable [CHES94]. A medida que los firewalls se fortalecen, los hackers buscan nuevas maneras para violar los sistemas. Por lo tanto, es importante otorgar diferentes niveles de seguridad a los recursos del backbone. Los niveles de seguridad representan los obstaculos que tendría que vencer un hacker para llegar a un recurso. Mientras mas niveles de seguridad tenga un recurso es mas dificil llegar a comprometerlo. Un ejemplo se muestra en la figura No.4-3.

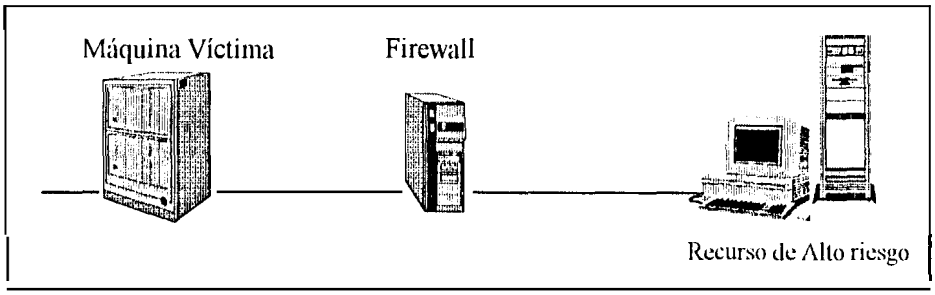


Figura No. 4-3. Niveles de seguridad p a n un recurso de alto riesgo

En la figura anterior se utiliza corno primer mecanismo de seguridad una maquina victima la cual puede ser un servidor de inforrnacion que no tiene rnucha seguridad por considerarse un recurso sin ningun riesgo (ver sección 3.4 Host bastion). El segundo mecanismo puede tratarse de un firewall con reglas que nieguen el acceso al recurso de alto riesgo; y finalrnente el recurso de alto riesgo con proteccion de host. Entonces para que un intruso pueda alcanzar el recurso de alto riesgo tiene que atravesar prirnero la rnaquina víctima luego el firewall y finalmente comprometer al recurso de alto riesgo. En total tres niveles de seguridad para el recurso de alto riesgo de la figura No. 4-3.

Se debe enfatizar que la ESPOL corno universidad debe rnantener un esquerna abierto y perrnitir arnplia conectividad con Internet. Como existe una sóla conexión a Internet, se debe proveer, como primer nivel de seguridad, un firewall entre el backbone e Internet. Las especificaciones del firewall en este punto seran tratadas mas adelante (4.5.2.3. Firewall externo).

Como segundo nivel de seguridad este modelo brinda proteccion en los hosts conectados al backbone (seguridad de host) utilizando el punto de vista de "negar por defecto": ***Todos los servicios estan prohibidos excepto aquellos que están explicitamente permitidos.***

Para los servidores SUN SPARC solo habria que habilitar los servicios que la jefatura de redes dispone y que fueron detallados anteriormente (ver sección **4.2.2.** Servicios de Internet). En el caso de los servidores de aplicaciones y bases de datos, desabilitar todos los serivicios, dejar una cuenta para el administrador y permitir las sesiones login dentro de las aplicaciones. Las aplicaciones poseen rnodulos de seguridad con una fuerte autenticacion al inicio de cada sesion. Además, en los servidores de aplicaciones y base de datos se puede aplicar algun producto de software (TCP Wrapper) que controle los prograrnas servidores en base a las direcciones fuentes de las maquinas clientes, para así habilitar de una forrna segura a ciertas maquinas de las unidades para utilizar las aplicaciones. El servidor de administracion es de uso exclusivo de la Jefatura de redes de **CESERCOMP,** por lo tanto no corre mucho riesgo ya quc no posee cuentas de usuarios excepto la cuenta root. Si existieren servidores de informacion internos se les proporcionaria la misma seguridad de host anterior.

Como se trata de una topologia muy descentralizada y los usuarios internos no son confiables, es muy recomendable utilizar firewalls por cada red interna que se conecte al backbone. Esto proveeria un segundo nivel de seguridad para los recursos dentro de las redes internas, ya que el primero es el firewall externo. Si se coloca cualquier host del backbone en una red interna, este ganaria un tercer nivel de seguridad: firewall externo, firewall interno y la seguridad del host. Por lo tanto es rnuy aconsejable colocar los servidores de aplicaciones y bases de datos en una red interna que podría ser la red de administracion central, biblioteca, etc.

4.5.2.2. Seguridad de la información en tránsito

Por el rnedio de transrnision fluiran paquetes ya sea entre redes internas, en el caso de las aplicaciones e inforrnacion interna; o, entre Internet, los servidores del backbone y las redes

internas. Por lo que los paquetes en el backbone pueden ser capturados por cualquier usuario interno o externo.

Por esta razon, existe la necesidad de proveer un mecanismo de encriptacion que proteja la informacion en tránsito como se observa en la figura No. 4-4. La region mas sombreada representa un tunel virtual que comunica los servidores de aplicaciones y bases de datos con las redes de las unidades academicas y administrativas.

La encriptacion puede ser de firewall interno a firewall interno entre subredes o tambien de firewall a maquina cliente, dependiendo del grado de importancia y riesgo que le den las subredes a los recursos en el análisis de riesgo. En el caso de la figura No. 4-4, la encriptacion es de firewall interno a firewall interno.

Con esta medida tambien se gana autenticacion para los usuarios de las aplicaciones administrativas y académica ya que solo los verdaderos usuarios pueden desencriptar la informacion de los servidores.

4.5.2.3. Firewall Externo

El firewall externo representa el primer nivel de seguridad para el backbone frente a Internet. La idea básica del firewall externo es dar un amplio acceso a las redes internas, pero siempre otorgando seguridad a ciertas direcciones y servicios que ofrece el backbone.

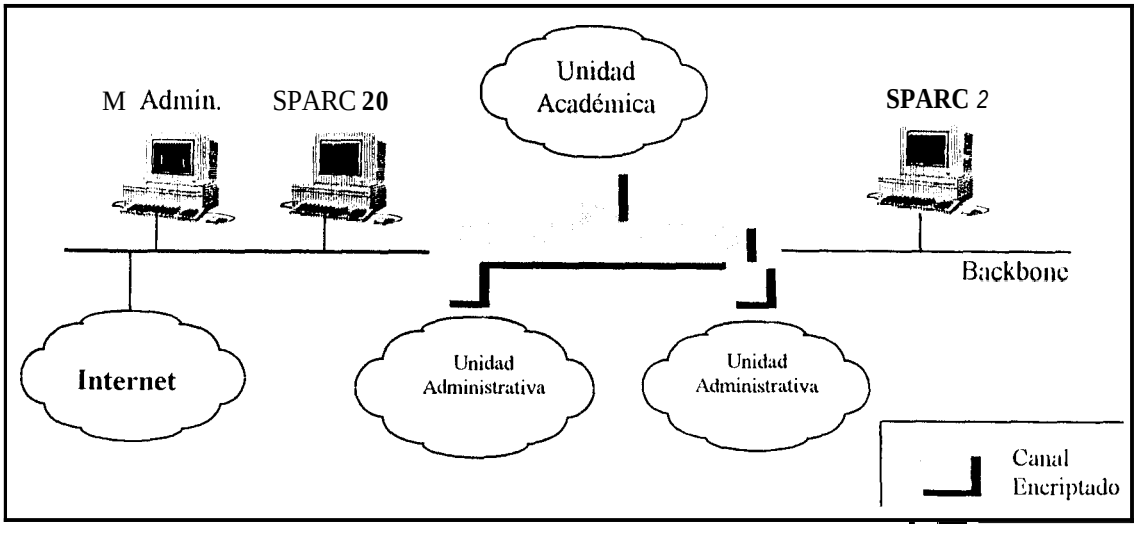


Figura No.4-4. Encriptación de datos *en* el backbone

Como la ESPOL necesita de un esquema abierto, las reglas de este firewall no serian tan estrictas con relación a las redes internas ya que estas seran protegidas por firewalls internos. Sin embargo, se pueden configurar reglas fundamentales o básicas a fin de otorgar un mínimo grado de seguridad a aquellas redes que no posean un firewall.

El firewall externo debe controlar las conexiones en base a las direcciones lógicas fuente y destino de la conexión y en base a los puertos fuente y destino del servicio. Muchos firewalls utilizan el "Address Translation" para cambiar las direcciones en los paquetes salientes de tal manera que los usuarios de Internet no conozcan la fuente de los paquetes. Este método podría ser de mucha utilidad en el firewall externo. Los requerimientos del firewall externo seran detallados en el siguiente capitulo.

Configuración del firewall externo

- La arquitectura de firewall mas segura, segun el estudio del capitulo III, es la screened subnet que utiliza dos ruteadores, una red perimetro y un host bastion. La principal razon para contar con una red perimetro es para que la informacion interna no pueda ser capturada y solo se mantenga en la red interna. Esta arquitectura sería muy apropiada para una organizacion pequeña con pocos servidores y pocos usuarios. Pero para la ESPOL, una organizacion grande y descentralizada, resultaría impractica debido a que cada subred puede poseer varios servidores de Internet y de información interna, los cuales mezclan el trafico proveniente de Internet y el trafico de los servidores de informacion internos a traves del backbone.
- Al colocar una red perimetro en la conexion con Internet se estaria desaprovechando la velocidad del medio de transmision.
- La tecnologia de red usada actualmente es ATM, lo que garantiza que el trafico no puede ser olfateado ya que por cada conexion la red ATM abre un canal seguro.
- La arquitectura que este modelo recomienda es la screened subnet pero sin red perímeto, es decir el ruteador externo conectado directamente con un host bastion (donde se coloquen programas de firewalls) y este a su vez al backbone. De esa manera todo el trafico que trate de ingresar al backbone via Internet tiene que pasar por el host bastion. Esta arquitectura es una variación insegura presentada en el capitulo III. Sin embargo, la inseguridad que presenta es el hecho de que la informacion interna puede ser olfateada, pero en la ESPOL se mezcla la informacion de Internet y la interna, por lo tanto puede ser olfateada . Así se puede observar en la figura No. **4-5.**

- El ruteador que se coloque ante Internet debe tener capacidades de filtración. El actual ruteador cumple con lo minimo que debe hacer: filtrar por direcciones para evitar el ingreso de paquetes provenientes de redes consideradas no confiables (de donde se ha sufrido algun tipo

de ataque). Se sugiere que el ruteador posea filtración por puertos fuentes y destino para distinguir los servicios permitidos. Las reglas de configuración de este ruteador varian dependiendo de los servicios de Internet que la ESPOL desee proveer. En la seccion **4.4.2.5.** se dan las reglas de filtraje para los servicios que va a proveer la ESPOL. La minima regla que debe poseer este ruteador es la siguiente:

Dirección	D. Fuente	D. Destino	Protocolo	P. Fuente	P. Destino	Acción
Adentro	Interna	Interna	Cualquier	Cualquier	Cualquier	Negar

Esta regla evita el ataque spoofing (ver seccion 1.2. Tipos de ataques); es decir, no permite el paso de todo paquete que quiera ingresar a la ESPOL utilizando una direccion fuente interna en lugar de su direccion fuente verdadera, sin importar que protocolo, puertos fuente y destino.

El host bastion, como se establecio en la seccion **3.4.**, es la maquina donde residen todos los programas de firewalls (filtradores, sistemas proxy, programas de autenticacion y encriptacion). Dependiendo de los servicios de Internet que la **ESPOL** brinde, el host bastion puede actuar como servidor de Internet. En la seccion **4.4.2.5.** se analizan los servidores de Internet mas comunes y su conveniencia o no de ubicarlos en el host bastion. El programa de firewall que se debe instalar en el host bastion debe cumplir con los requerimientos establecidos en el capítulo V.

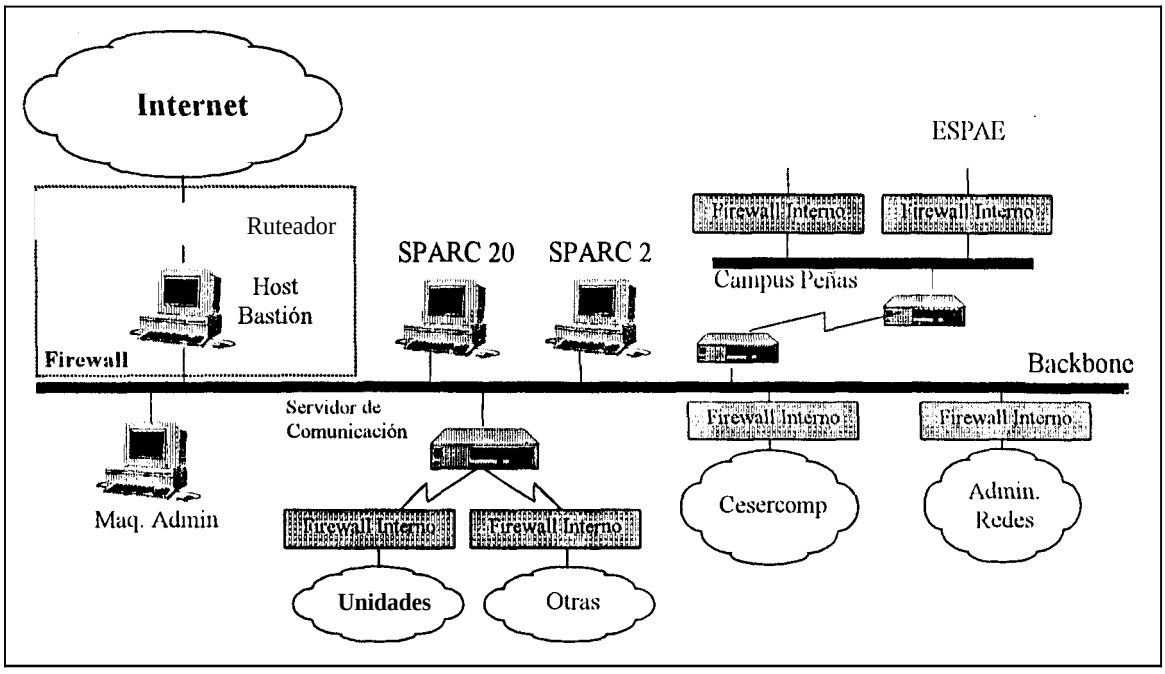


Figura No. 4-5. Arquitectura del firewall externo aplicada al backbone de la **ESPOL**

4.5.2.4. Firewalls Internos

Debido a que el backbone puede contar, en el peor de los casos, con 500 (o mas en el futuro) sesiones simultaneas (segun el Dr. Entrique Pelaez, Director de CESERCOMP) se podría pensar en problemas de trafico en el medio de transmision si se cuenta con un solo firewall entre Internet y el backbone. Muchas organizaciones que fabrican firewalls anuncian que sus productos no ocasionan problemas de embotellamiento en una red, ya que poseen un alto nivel de rendimiento.

Muchos de los firewalls utilizan mecanismos de autenticacion y archivos de logs por cada sesion levantada, los cuales incrementan el retardo en la red. Si un servicio es muy vulnerable se

necesitaran nuevos mecanismos para implementar en el firewall y quizás estos mecanismos afecten aun mas al rendimiento de la red.

Al utilizar una arquitectura de firewalls internos se descarga el trafico de la red, se obtiene una arquitectura distribuida y los monitoreos son mas eficientes. La figura No.4-6 ilustra un esquema de firewalls internos.

El firewall entre Internet y el backbone, o firewall externo, ya no necesitaria proveer tanto control en los recursos de las redes internas, debido a que este control lo proporciona el firewall interno. Con esta medida se reducen las reglas de seguridad implementadas en el firewall externo y mejorara el trafico de la red.

Cada administrador de una red interna implementaria su propio conjunto de reglas en el firewall dependiendo de su política de seguridad local y de las politicas generales de la ESPOL. Así se adquiere autonomía para que cada red interna elija los servicios de Internet que va a proveer y los riesgos que corren.

Con un firewall interno se provee una via de monitoreo para la jefatura de redes. La jefatura puede hacer uso de la cuenta del administrador en el firewall para observar si la red interna esta cumpliendo con las politicas establecidas, tener control sobre los recursos de la red, y accesar a los archivos de log. De esta forma, en caso de que suceda algún ataque o algo sospechoso, la jefatura puede localizar donde se origin6 y cuales son exactamente los daños.

Configuración de un firewall interno

Como todas la estaciones de una red interna tendrán acceso a Internet, el firewall interno tiene que proteger todos los recursos de la misma. Dentro de los recursos de mas alto riesgo que cada red interna posee se encuentran las maquinas clientes y servidores de las aplicaciones administrativas y académica.

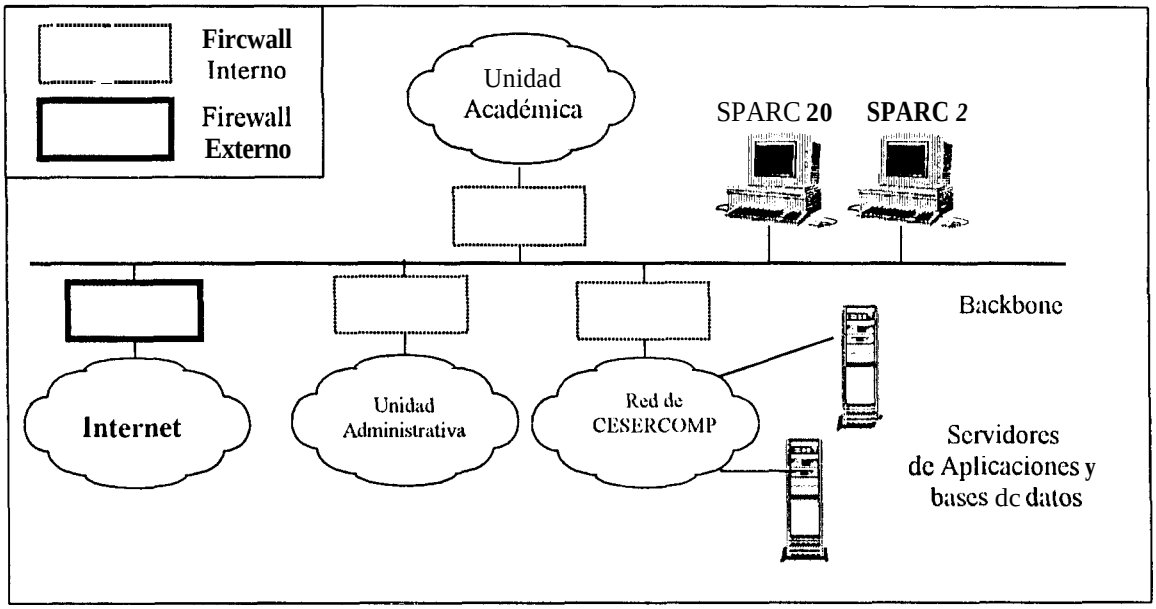


Figura No.4-6. Arquitectura de firewalls internos *en* el backbone

Como se trató anteriormente, es recomendable colocar los servidores de aplicaciones y bases de datos dentro de cualquier red interna que posea un firewall para darle un mayor nivel de seguridad. Por lo tanto, se recomienda que estos servidores se coloquen en la red de administración central o de CESERCOMP debido a que estan bajo la dirección de la Jefatura de Redes de CESERCOMP y sería mas facil ejercer control. Tambien se los puede colocar en cualquier otra red interna que sea segura.

El firewall de la red de administración central debe utilizar filtraje de paquetes y autenticacion para dar acceso solo a las maquinas clientes permitidas y comprobar que los usuarios son quienes dicen ser. Además, se puede comprobar que la información recibida este encriptada. De esta manera se provee a los servidores con un tercer nivel de seguridad.

Las direcciones IP de ciertas redes internas podrian configurarse de tal manera que no sean reconocidas por Internet. Es decir que los usuarios de Internet solo podrian ver la dirección del firewall interno. Es aconsejable adoptar este mecanismo para la red que contenga los servidores de aplicaciones y bases de datos debido a que es peligroso que los usuarios de Internet conozcan de estos servidores.

En el caso de clientes de aplicaciones administrativas, las maquinas contarán con seguridad física ya que se hallaran en las oficinas de las unidades. Las maquinas clientes de la aplicacion academica estaran tanto en las oficinas de las unidades como en los laboratorios, estas ultimas consideradas inseguras y abiertas. En las redes de laboratorio, se corre un mayor riesgo de acceso no autorizado a la aplicacion academica que en las redes ubicadas en las oficinas de las unidades, por esta razon la aplicacion academica deberia contar con un mecanismo de autenticacion extra entre el servidor y el cliente.

Por las mismas razones que el caso del firewall externo, para el firewall interno es aconsejable utilizar la arquitectura screened subnet sin red perimetro como en la figura No. **4-7.** El firewall interno posee dos mecanismos de control: el ruteador y el host bastion. Lo recomendable en este caso es que el host bastion tenga minimo tres interfases para separar las redes seguras de las inseguras.

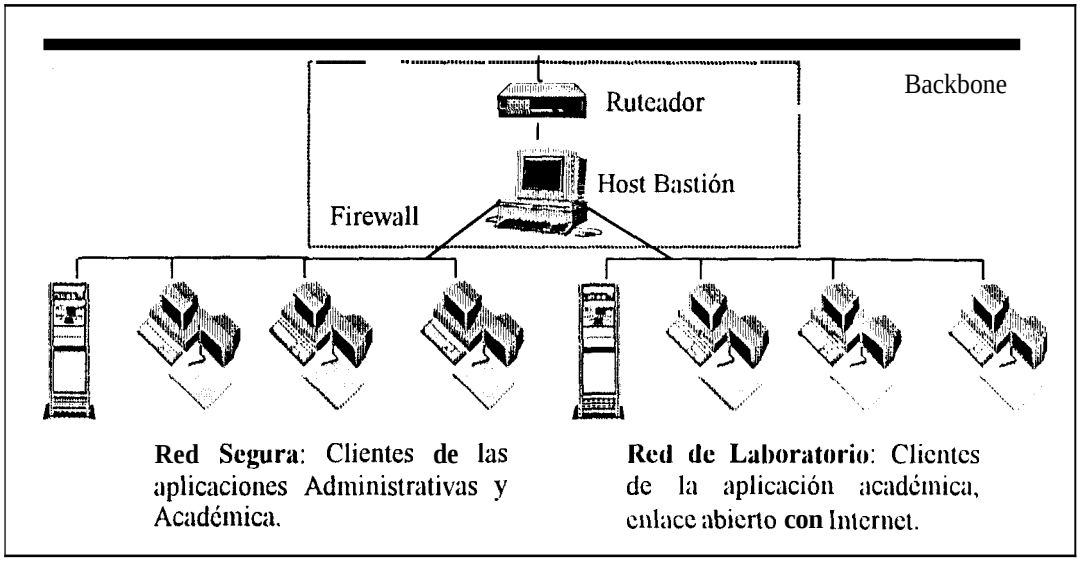


Figura No. 4-7. Configuración para un firewall interno

Este modelo trata en lo posible de otorgar el mayor nivel de seguridad a los recursos que poseen información confidencial de la **ESPOL,** dar una gran apertura a las redes de las unidades para que se conecten a Internet y proveer una topología distribuida para controlar y monitorear las actividades dentro del backbone.

4.4.2.5. Configuración de servicios de Internet

En esta sección se analizan los servicios de Internet mas comunes, sus falencias y las formas de como brindarlos con seguridad a traves de las tecnologias de firewalls estudiadas anteriormente. Estos consejos son validos tanto para el firewall externo como para los firewalls internos.

Los servicios de Internet que se analizaran son los siguientes:

- Correo electronico y SMTP (Simple Mail Transfer Protocol)
- Telnet (Terminal Access)

- FTP (File Transfer Protocol)
- NNTP (Network News Transfer Protocol)
- WWW (World Wide Web) y HTTP (Hipher Text Transfer Protocol)
- DNS (Domain Name Server)

Se han elegido estos servicios debido a que la ESPOL los proveer y es necesario que los brinde en forma segura para evitar ataques.

Correo electronico

El correo electronico es uno de los servicios de mayor riesgo debido a que un servidor de correo acepta datos de cualquier maquina externa.

Un sistema de correo consiste de tres partes:

- **Servidor:** acepta o envía mensajes. El servidor recibe comandos de servidores externos, por lo que se convierte en un canal abierto para que se susciten ataques.
- **Agente de entrega:** coloca el mensaje en la casilla de cada usuario en el servidor local. Este agente necesita de permisos especiales (privilegios de super-usuario) para escribir en cada casilla de los usuarios. Si este agente llega a ser comprometido, el intruso llega a obtener los privilegios que involucra este agente [CHAP95]
- **Agente usuario:** permite que el recipiente lea o edite un mensaje. Sencillamente se ejecuta como un usuario.

Existen tres problemas de seguridad a los que esta expuesto el servicio de correo electronico:

1. Debido a que el servidor de correo tiene contacto con el mundo externo (Internet), este puede recibir comandos que los servidores externos le envien. Asi un intruso puede intentar

ejecutar un comando para bajarse archivos de un sistema, dar de baja (shutdown) al servidor, etc.

2. El agente de entrega y el usuario no reciben comandos directamente; sin embargo son vulnerables por el contenido de los mensajes que manejan. En el contenido de un mensaje se pueden colocar comandos y el agente de entrega los interpretara y ejecutara con privilegios de super usuario.
3. Se puede colocar mensajes bombas que al abrirse se ejecutan y pueden inundar al sistema con paquetes, borrar archivos del sistema, introducir virus, etc. [CHAP95].

Para los anteriores problemas de seguridad, un firewall tiene el siguiente alcance :

- Puede evitar el primer problema restringiendo el numero de maquinas en las cuales los posibles atacantes abran canales de acceso; y dando seguridad de host al servidor de correo.
- Puede involucrarse con el contenido de un mensaje e interpretarlo a fin de encontrar programas ejecutables o comandos y evitar su ingreso.
- Al igual que el caso anterior, un firewall puede involucrarse con el contenido de los mensajes con el fin de evitar mensajes bombas.

SMTP (Simple mail transfer protocol) para **UNIX:** Sendmail

El programa mas comun de correo electronico en UNIX es el Sendmail. Se trata de un programa muy poderoso, pero con un historial de implicaciones de seguridad mas largo que el de cualquier otro. Sin embargo, las últimas versiones (versiones 8.8.7 y 8.8.8) corrigen los agujeros de seguridad conocidos.

A medida que se descubren nuevos agujeros en el Sendmail, surgen parches que tapan dichos agujeros. Es recomendable que el programa de Sendmail que se utilice en un servidor sea el

actual y contenga los parches aconsejados (no necesariamente las ultimas versiones de los parches, ya que puede ser que no esten probadas aún) [CHAP95].

Una de las razones del porque el Sendmail tiene problemas de seguridad es que es un programa muy complejo; ejecuta muchas funciones diferentes y requiere de permisos especiales para ejecutar todas sus funciones. Al utilizar privilegios de super usuario se corre un gran riesgo si es que el sistema es perpetrado. Un atacante puede explotar cualquier error en una conexión de SMTP y ganar ese privilegio de super usuario para hacer todo lo que quiera al sistema.

La solución para rnodificar el uso de privilegios de super usuario en el normal funcionamiento del Sendmail es utilizar programas llamados "wrappers", los cuales otorgan una capa extra al Sendmail y manipulan todo lo que entra o sale del programa original. De esta forma se cambian los privilegios del programa de super usuario a un usuario normal. A continuacion se analiza uno de estos programas wrappers [CHAP95].

Smap y Smapd

Uno de los wrappers mas conocido para el Sendmail es el **SMAP .** Se trata de un programa que es parte de TIS FWTK (Trusted information system firewall toolkit) y que incluye a dos subprogramas smap (cliente) y smapd (servidor) [SIYA95]. A continuacion las caracteristicas mas importantes del subprograma cliente smap:

- El programa smap es corto (alrededor de 700 líneas de codigo),
- Se ejecuta sin privilegios de super usuario.
- Se inicializa mediante inetd y toma el puerto 25.

- Ejecuta chroot para una cola de directorio en particular, por lo que no puede accesar a ningún otro directorio
- Todo lo que hace es aceptar los mensajes entrantes vía SMTP
- Obedece en un mínimo necesario los comandos de SMTP
- Almacena cada mensaje que recibe en un archivo separado en la cola de mensajes

El segundo subprograma smapd es un servidor que lo único que hace es procesar los archivos encolados en el servidor de correo, entregando los mensajes en cada casilla de los usuarios.

Tomando en cuenta el criterio de negar por defectos y desde el punto de vista de un filtrador de paquetes, para habilitar el servicio SMTP, es necesario configurar el filtrador de la siguiente manera:

No	Dirección	Fuente	Destino	Protocolo	P. fuente	P. destino	bit ACK	Nota
1	Adentro	externa	interno	TCP	>1023	25	no	mail entrante emisor a recipiente
2	Afuera	interna	externo	TCP	25	>1023	sí	mail entrante recipiente a emisor
3	Afuera	interna	externo	TCP	>1023	25	no	mail saliente emisor a recipiente.
4	Adentro	externa	interno	TCP	25	>1023	sí	mail saliente recipiente a emisor

Tabla VII. Reglas para filtrar paquetes SMTP

Utilizando el mismo estándar para las reglas de filtraje detallado en la sección 3.5. Filtraje de paquetes:

- El puerto del servidor SMTP es 25
- El puerto del cliente SMTP es mayor que 1023

- Las reglas **1** y **2** permiten el paso de mensajes desde Internet a la red interna. La regla 1 recibe el mensaje desde el emisor (servidor externo) hasta el recipiente (servidor interno). La regla **2** es la contestacion del recipiente (servidor interno) al emisor (servidor externo); ademas se controla el inicio de sesion.
- Las reglas 3 y **4** permiten el paso de mensajes desde la red interna a Internet. La regla 3 permite enviar el mensaje desde el emisor (servidor interno) hasta el recipiente (servidor externo). La regla **4** es la contestacion del recipiente al emisor; ademas se controla el inicio de sesion.
- Todo lo demas no es permitido.

Se sugiere que en el **host** bastion se coloque el servidor de correo para de esta manera permitir solo conexiones entre servidores externos y el host bastion mas no con los servidores internos. Por su concepción de ser un protocolo de "almacenar-enviar" (store-and-forward), un servidor de SMTP es un proxy por naturaleza (ver sección 3.6. Sistemas proxy). Por esto sería ilógico colocar un servidor proxy por separado para este servicio. Lo aconsejable es utilizar el mismo host bastion (proxy) como servidor de correo como en la figura **No. 4-8** [CHAP95].

Tambien *se* pueden habilitar otros servidores internos de correo de tal manera que acepten conexiones solo del host bastion y no del mundo externo. Así se evita cualquier contacto con el mundo externo para prevenir ataques de canal de comandos.

Configuración de SMTP para trabajar con un firewall

Si se envía correo a traves de un host bastion se necesita configurar el sistema de la siguiente manera:

- Especificar en el ruteador que el correo entrante debe ser direccionado al host bastion.

- Configurar el sistema de correo en el host bastion para observar la direccion destino de los mensajes que le llegan. Si el mensaje tiene direccion destino externa, el sistema debe enviarlo a su destino. Si el mensaje tiene direccion destino interno debe enviarlo hacia el servidor interno y no entregarlo localmente. Si el host bastion deja pasar correo a un servidor interno o a un conjunto reducido de servidores internos, el sistema de filtración puede restringir que las conexiones del host bastion sean solo a esos servidores, de esta manera se reduce el numero de sistemas internos que pueden ser atacados via SMTP si el host bastion llega a ser comprometido [SIYA95].
- Configurar los sistemas internos para enviar mensajes al host bastion.

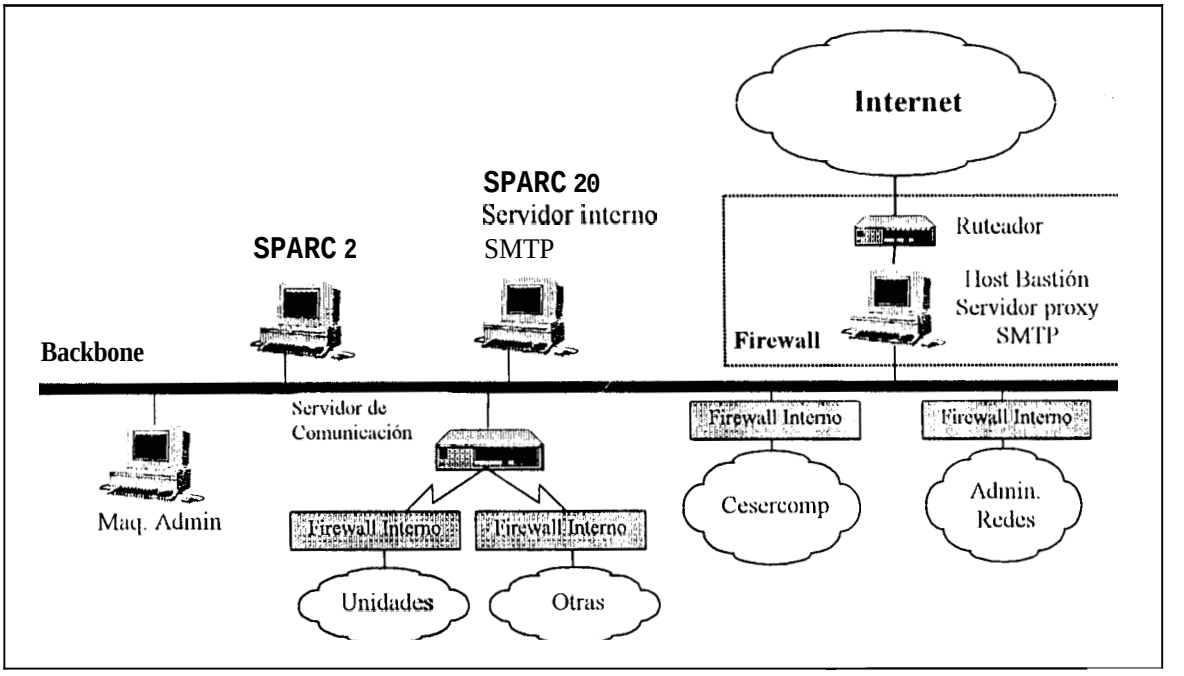


Figura No. 4-8. Configuración segura del servicio de correo electrónico

Recomendaciones para SMTP

Finalmente, para brindar el servicio de correo electronico en forma segura se debe:

- Usar filtradores de paquetes para tan solo permitir conexiones SMTP desde hosts externos con el host bastion
- Usar filtradores de paquetes para restringir conexiones SMTP desde el host bastion a los hosts internos específicos (servidores internos de correo)
- Permitir que cualquier sistema interno envíe mensajes al host bastion
- Usar SMAP o cualquier otro programa de iguales caracteristicas en el servidor de correo del host bastion
- Mantener el servidor con los parches actualizados.

Telnet

Telnet es un protocolo basado en TCP que permite a un usuario accesar remotamente a un shell de comandos de otra computadora. Este servicio tambien es muy popular en Internet, pero al igual que el correo electronico tiene muchas implicaciones de seguridad [CHAP95].

Tanto para Telnet entrante (a una maquina interna de la ESPOL) y Telnet saliente (a un servidor externo de Internet) existen serios problemas en la seguridad. La mayoría de las organizaciones permiten que sus usuarios internos accesen remotamente a otros sistemas en Internet para obtener información. Pero no permiten que usuarios externos accesen a traves de Internet a sus sistemas de redes ya que esto da origen a diversos tipos de ataques en servicios entrantes como se detallo en la seccion 3.7.

Para permitir Telnet entrante de manera segura, en la seccion 3.7.1. se analizaron diferentes esquemas de autenticacion que pueden servir para que este servicio no sea una puerta abierta a intrusos.

Para habilitar este servicio, tanto entrante como saliente, utilizando el criterio de negar por defecto y desde el punto de vista de un filtrador de paquetes, se deben configurar las siguientes reglas:

No	Dirección	Fuente	Destino	Protocolo	P. fuente	P. destino	ACK	Nota
1	Adentro	externa	interno	TCP	>1023	23	no	sesión entrante cliente a servidor
2	Afuera	interna	externo	TCP	23	>1023	sí	sesión entrante servidor a cliente
3	Afuera	interna	externo	TCP	>1023	23	no	sesión saliente cliente a servidor.
4	Adentro	externa	interno	TCP	23	>1023	sí	sesión saliente cliente a servidor.

Tabla VIII. Reglas para filtrar paquetes Telnet

Utilizando el mismo estandar para las reglas de filtraje detallado en la seccion 3.5. Filtraje de paquetes:

- El puerto del servidor Telnet es 23
- El puerto del cliente Telnet es mayor que 1023
- Telnet utiliza el protocolo TCP
- En las reglas 1 y 2 se permite la comunicacion de paquetes para Telnet entrante entre un cliente externo y un servidor interno. (Recordar que toda conexion en Internet es bidireccional, ver seccion 3.5. Filtraje de paquetes). En la regla 2, como es la respuesta del servidor interno al cliente externo, se controla el inicio de conexion (bit del **ACK).**
- En las reglas 3 y **4** se permite la comunicacion de paquetes para Telnet saliente entre un cliente interno y un servidor externo. En la regla **4,** como es la respuesta del servidor externo al cliente interno, se controla el inicio de sesion.

Por ser uno de los servicios mas populares en Internet, existeri muchos sistemas proxy para Telnet. Muchas herramientas públicas tales como **SOCKS,** a traves de un cliente modificado Telnet, y TIS FWTK, a traves de procedimientos de usuarios modificados, proveen servidores proxy para los servicios mas comunes en Internet, y entre estos se encuentra Telnet.

Recomendaciones para Telnet

Finalmente para brindar este servicio de manera segura, se sugiere lo siguiente:

- Restringir en lo posible sesiones Telnet entrantes. Si se habilita este servicio considerar la información disponible en la seccion 3.7. Autenticacion y encriptacion [CHES94].
- Telnet saliente puede ser seguro a traves de filtradores o sistemas proxy debido a que no involucra peligro como el Telnet entrante, y cualquiera de las dos tecnologias citadas puede otorgar control sobre el servicio.

FTP (File transfer protocol)

FTP es el protocolo mas usado para transferir cualquier tipo de archivo: binario, ASCII, graficos, Postscript, sonido y video de una máquina a otra. Existen dos tipos de FTP: usuario FTP y FTP anonimo. En el caso de usuario FTP, el usuario debe tener una cuenta y contraseña en el servidor, mientras que en el FTP anonimo se ingresa al sistema a traves de una cuenta especial "anonymous" y como contraseiia se usa la dirección del usuario. Si se utiliza el tipo usuario FTP entrante, se tienen los mismo problemas de seguridad que en el Telnet entrante. Para entender que problemas son estos y como solucionarlos ver la seccion de 3.7. Autenticacion y encriptacion.

El protocolo FTP utiliza dos puertos en el servidor: el 21 para control y el 20 para flujo de datos. De igual manera el cliente tambien utiliza dos puertos (arriba del 1024), uno establece la

conexion al puerto 21 del servidor enviandole el numero del segundo puerto cliente con quien va a tratar, y el segundo puerto para conversar con el puerto 20 del servidor.

Para establecer una sesion a un servidor FTP, el cliente hace un requerimiento desde uno de sus dos puertos al puerto 21 enviandole el numero del segundo puerto cliente con el cual el puerto 20 del servidor "conversara". Y así se levanta la sesion FTP. Así se observa en la figura No. 4-9.

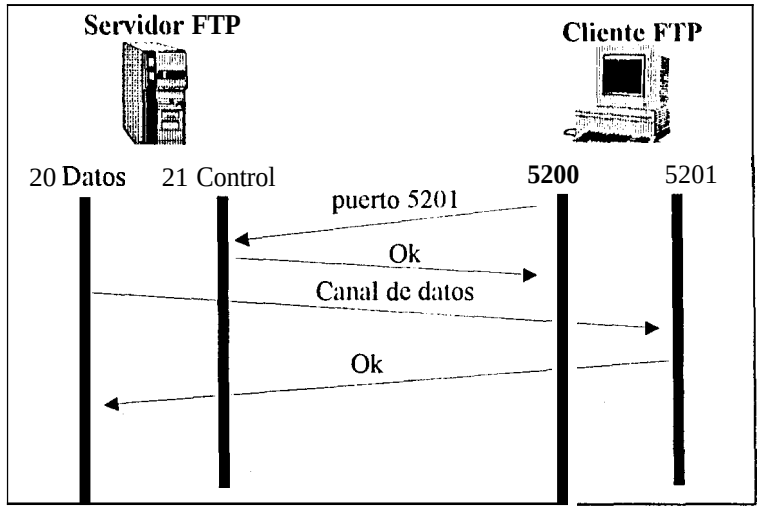


Figura No. **4-9. Modo normal de una sesion FTP**

Esta forma de conexion involucra cierto peligro debido a que el cliente FTP selecciona dinamicamente el puerto de datos y es el servidor el que inicia una conexion. Un atacante ubicado en el servidor puede abrir premeditadamente comunicacion con un puerto mayor de 1023 que no sea el seleccionado por el cliente (por ejemplo el de X windows, etc.) y perpetrar un ataque. Además, por el hecho de que el servidor FTP es quien inicia la conexion, se dificulta controlar el inicio de una conexion desde un filtrador de paquetes. Estas dos caracteristicas de este esquema representan desventajas en el modo de funcionamiento del protocolo FTP.

Actualmente, algunos servidores y clientes FTP soportan un modo alternativo que permite al cliente abrir ambos canales: el de datos y el de control. Este modo es llamado "modo pasivo". En este modo se eliminan las desventajas anteriormente citadas trabajando como lo muestra la figura No. 4-10.

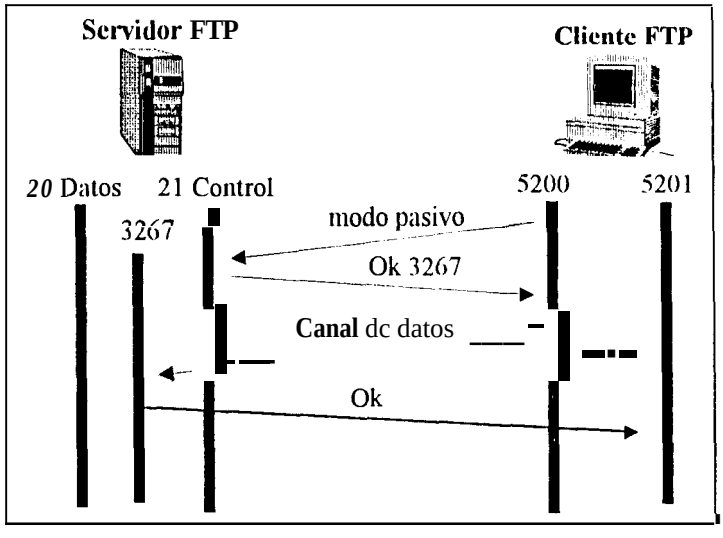


Figura No. 4-10. Modo pasivo de una sesion FTP

Para iniciar una sesion FTP en modo pasivo el cliente FTP envia un requerimiento al servidor indicandole que quiere abrir una sesion en modo pasivo. El servidor, ahora selecciona un nuevo puerto para el canal de datos (ya no el 20, sino el 3267 para este caso en especial) y se lo envia al cliente. El cliente desde su segundo puerto envia el requerimiento de datos al nuevo puerto de datos (3267) del servidor. De esta manera se elimina el contacto directo entre el puerto 20 del servidor FTP con el puerto del cliente y es el cliente quien inicia la conexion, reduciendose las posibilidades de un ataque [CHAP95].

El unico inconveniente es que este esquema es nuevo aun, y es muy posible encontrar tanto clientes como servidores FTP que no soportan el modo pasivo. En la practica los servidores que utilizan este esquema no permiten transferir datos a clientes que no lo soportan, envian

mensajes diciendo que no se puede establecer una conexión debido a que utilizan un esquema pasivo.

Para habilitar FTP usuario o anonimo, entrante y saliente, desde el punto de vista de un filtrador de paquetes, se deben configurar las siguientes reglas:

No	Direcc-ción	D. Fuentc	D. Destino	Protocolo	P.Fuentc	P.Destino	bit ACK	Notas
1	adentro	externa	interna	TCP	>1023	21	no	requerimiento FTP entrante
2	afuera	interna	externa	TCP	21	>1023	sí	respuesta la requerimiento entrante
3	afuera	interna	externa	TCP	**20**	**>1023**	no	crcacion de canal de datos para requerimientos entrantes FTP, **iiiodo** normal
4	adentro	externa	interna	TCP	**>1023**	*20*	sí	respuestas del canal de datos para requerimientos entrantes FTP, modo normal
3	adentro	externa	interna	TCP	**>1023**	>1023	no	creación de canal de datos para requerimientos entrantes FTP, modo pasivo
6	afuera	interna	externa	TCP	>1023	**>1023**	sí	respuestas del canal de datos para requerimientos entrantes FTP, iiiodo pasivo
7	afuera	interna	externa	TCP	>1023	**21**	no	requerimiento saliente FTP
8	adentro	externa	interna	TCP	**21**	**>1023**	sí	respuesta al requerimiento saliente
9	adentro	externa	interna	TCP	**20**	**>1023**	no	creación de canal de datos para requerimientos salientes FTP, **iiiodo** normal
10	afuera	interna	externa	TCP	**>1023**	**20**	sí	respuestas **dcl** canal de **datos** para requerimientos salientes FTP, modo **normal**
11	afuera	interna	externa	TCP	>1023	**>1023**	no	crcacion de canal dc **datos** para requerimientos salientes FTP, **iiiodo** pasivo
12	adentro	esterna	interna	TCP	>1023	>1023	sí	respuestas **del** canal dc datos para requerimientos salientes FTP, iiiodo pasivo

Utilizando el mismo estandar para las reglas de filtraje detallado en la sección 3.5. Filtraje de paquetes:

- Los puertos del servidor FTP son 20 (datos) y 21 (control). Para el caso de FTP modo pasivo se habilitan los puettos por encima del 1024.
- Los puertos del cliente FTP son mayores que 1023
- FTP utiliza el protocolo TCP
- Las reglas 1 y 2 permiten el inicio de una sesion FTP entrante. La regla 1 permite que el cliente externo envie el requerimiento al puerto 21 del servidor. La regla 2 permite responder del servidor interno al cliente externo; ademas se controla el inicio de sesion (bit del ACK).
- Las reglas 3 y 4 permiten la comunicacion de datos de una sesion FTP entrante en modo normal. La regla 3 permite crear el canal para transferir datos (puerto 20). La regla 4 permite responder a los requerimientos del cliente externo; ademas se controla el inicio de sesion.
- Las reglas 5 y 6 permiten la comunicacion de datos de una sesion FTP entrante en modo pasivo. La regla 5 permite que el cliente externo envie el requerimeinto a un puerto mayor que 1023. La regla 6 permite responder a los requerimientos del cliente externo; además se controla el inicio de sesion [CHAP95].
- Las reglas 7 y 8 permiten el inicio de una sesion FTP saliente. La regla 7 permite que el cliente interno envie un requerimiento a un servidor externo. La regla 8 permite responder a los requerimientos del cliente interno; ademas se controla el inicio de sesion (bit ACK).
- Las reglas 9 y 10 permiten la comunicacion de datos de una sesion FTP saliente en modo normal. La regla 9 permite la creacion del canal de datos para los requerimientos salientes. La regla 10 permite que el servidor externo responda al cliente interno; ademas se controla el bit del ACK.
- Las reglas 11 y 12 permiten la comunicacion de datos de una sesion FTP saliente en modo pasivo. La regla 11 permite la creacion del canal de datos (>1023) para los requerimientos del

cliente interno. La regla 12 permite que el servidor externo responda al cliente interno; además se controla el inicio de sesion.

En el caso de que los usuarios internos o los servidores externos no soporten FTP en modo pasivo y solo se dispone de un filtrador de paquetes para proteger a la organización es recornendable que el filtrador tenga la capacidad de filtrar dinamicamente (ver sección 3.5 Filtraje de paquetes) a fin de proteger los puertos que dinamicamente han sido seleccionados.

Desde el punto de vista de un sistema proxy no interesa si se utiliza o no el modo pasivo, ya que todas las transacciones FTP pasan por el host bastion sin tener contacto directo con el servidor o cliente real. Por esta razon la utilización de un proxy para FTP resulta muy conveniente ya que se puede tener un esquema de FTP normal o modo pasivo y brindarle la seguridad apropiada. Hay una gran variedad de sistemas proxy tanto del tipo de clientes modificados como de procedimientos modificados [CHAP95].

Accesibilidad en un servidor FTP

Para el FTP anonimo o usuario FTP, el desafio es asegurar que el servidor solo proporcione la información que desea el administrador que se le muestre al cliente FTP. La medida de control que se tome es muy importante ya que se limita el acceso de un cliente FTP a algun archivo que involucre agujeros de seguridad [CHAP95].

Muchos servidores FTP ejecutan ***chroot*** para FTP anonimos antes que el servidor FTP comience a procesar comandos de un usuario anonimo. Sin embargo, para soportar ambos tipos de FTP (usuario y anonimo), los servidores necesitan accesar a todos los archivos. Esto

significa que chroot no garantiza mucha seguridad para un servidor FTP debido a que el servidor no siempre se ejecuta en un ambiente chroot.

Para solucionar este problema se modifica la configuración del archivo inetd.conf para que en lugar de levantar el servidor FTP se levante primero el chroot y luego el servidor FTP. Normalmente un servidor FTP limita el acceso para los usuarios anonimos, pero los usuarios normales sí pueden tener acceso ilimitado. Levantando el chroot antes del servidor FTP se limita tambien el acceso a los usuarios no anonimos.

Otro problema que involucra el FTP es que los usuarios internos de un sistema confian sus archivos en zonas que pueden ser accesadas por un usuario anonimo de FTP. Los usuarios confian en la seguridad a traves de obscuridad y piensan que nadie notara sus archivos. Pero precisamente los atacantes estan pendientes de que canal puede abrirse para penetrar. Lo recomendable en este caso es indicarles a los usuarios propietarios de archivos que nieguen los permisos de escritura, lectura y ejecucion para los demas.

Demonio wuarchive

Para evitar los problemas citados anteriormente existen programas servidores FTP modificados, tales como wuarchive, que permiten accesos semi-anonimos; es decir, que el usuario anonimo requiere de una contraseña adicional para ganar el acceso a ciertos directorios. Dentro de las caracteristicas de este demonio se encuentran:

- Mejor registro de lo que sucede en cada sesion FTP
- Habilidad para definir clases de usuarios (internos o externos). Segun esta clasificación se puede determinar que archivos y directorios pueden ver estos grupos de usuarios [SIYA95].

- Restricciones para ciertas clases de usuarios. Por ejemplo se puede limitar el numero de usuarios anonimos simultaneos, el limite puede variar dependiendo del día, hora, etc.
- Habilidad para comprimir y manipular archivos automaticamente.
- Puede aplicar chroot para usuarios no anonimos, cuando se habilita el servicio FTP normal pero se requiere limitar el acceso a los usuarios.

Recomendaciones para **FTP**

- Si se tiene clientes FTP que soportan modo pasivo, los hosts internos pueden protegerse via filtraje de paquetes. Es seguro el filtraje de paquetes solo si se puede filtrar el bit del **ACK** (inicio de sesion).
- Si se tienen clientes FTP que no soportan modo pasivo, se recomienda el uso de un proxy.
- Si se habilita un servidor FTP, se recomienda utilizar filtraje de paquetes para que lleguen paquetes de requerimientos FTP solo al host bastion.
- Evitar que los usuarios coloquen sus archivos en zonas que un usuario anonimo tiene acceso.
- Si se habilita un servidor FTP no anonimo se recomienda utilizar los mecanismos de autenticacion analizados en la sección 3.7.1. Autenticacion.

NNTP (Network news transfer protocol)

NNTP es un servicio usado generalmente para transferir noticias a traves de Internet. Un servidor de noticias es un lugar donde las noticias fluyen hacia o desde una organización, y al cual los usuarios pueden accesar para leer o enviar noticias [CHAP95].

Las dos unicas maneras en que se puede dar un ataque via NNTP son:

- Que el servidor NNTP tenga algun problema interno (software bugs) o este mal configurado.

En realidad no existen aun reportes de violaciones a traves de NNTP. El tipo de ataque que se puede dar es "orientado a datos" (ver **1.2.** Tipos de ataques) que por lo regular se produce cuando se implementan nuevos grupos de noticias automaticamente.

- Que el ataque provenga del servidor NNTP externo de alimentacion de noticias. Se dan casos en que los servidores externos NNTP alimentadores de noticias pertenecen a lugares inescrupulosos, que desean aprovecharse para enviar ataques. Es por esto que es recomendable investigar antes de suscribirse a un alimentador de noticias externo.

La solución optima en un ambiente con firewall es arreglar para que las noticias fluyan directamente desde el servidor externo a un servidor interno de noticias. Este método puede ser protegido mediante sistemas proxy o filtración de paquetes.

Por ser NNTP un protocolo de almacenar-enviar al igual que SMTP, este es capaz se desarrollar su propio proxy. Por lo tanto, se podría pensar en utilizar el servidor de noticias como proxy. Sin embargo, no es recomendable colocar el servidor proxy de NNTP en el host bastion debido a que se presentarian los siguientes problemas:

- Un servidor de noticias absorbe toda la disponibilidad de espacio en disco y tiempo de procesamiento por lo que no puede coexistir con otros servicios mas indispensables. Se puede utilizar una configuración de multiples hosts bastiones, sin embargo se estaria desperdiciando un host solo para este servicio.
- No se permitiria tener grupos de noticias para discusiones internas, ya que si el host bastion es comprometido, todos los grupos quedarian expuestos a un ataque.
- Habria que habilitar uno de los siguientes metodos para permitir a los usuarios leer las noticias:

- Cuentas de usuarios en el host bastion: Esta opción permite que los usuarios ganen acceso al host bastion y recuperen todos los mensajes provistos por el servidor de noticias. Este metodo es muy peligroso, ya que puede comprometer al host bastión y dejar vulnerable el sistema.

- Utilizando solo clientes NNTP: Permitir que los usuarios internos puedan leer las noticias del host bastion solo utilizando programas clientes NNTP y no utilizando Telnet. Para esto los usuarios internos deben utilizar la capacidad de "lector de noticias" (newsreader). El problema que se presenta es la disponibilidad de un servidor NNTP que permita la capacidad de "lector de noticias" en los clientes.

- Exportando las noticias a traves de NFS (Network File System) : Con este metodo se exportan las noticias del servidor a los clientes via NFS. Con esto se esuelve el problema del metodo anterior. Sin embargo, si los usuarios internos pueden usar NFS para accesar al host bastion, un atacante tambien lo podría hacer debido a que la seguridad de NFS es muy debil, por lo que es recornendable para un host bastion desabilitar este protocolo (ver sección 3.4. Host bastion).

- Relevando las noticias del host bastion a un servidor interno: Simplemente se relevan las noticias a traves del host bastion y hace de un servidor interno el verdadero servidor de noticias. El problema con este metodo es que requiere de mucho mantenimiento y toma gran cantidad de tiempo hacerlo.

El proposito del filtrador de paquetes es permitir solo la conexión del servidor NNTP alimentador y el servidor NNTP interno [CHAP95]. Pensando de esta manera, la configuración de las reglas seria:

No.	Dirección	D. fuente	D. destino	Protocolo	P. fuente	P. destino	bit ACK	notas
1	Adentro	Proveedor esterno	Servidor interno	TCP	>1023	119	no	noticias entrantes
2	Afuera	Servidor interno	Proveedor esteriio	TCP	119	>1023	sí	respuesta noticias entrantes
3	Afuera	Scrvidor interno	Proveedor esteriio	TCP	>1023	119	no	noticias salientes
4	Adentro	Proveedor externo	Servidor iiiterno	TCP	119	>1023	sí	respuesta noticias salientes

TP

Utilizando el mismo estandar para las reglas de filtraje detallado en la sección 3.5. Filtraje de paquetes:

- El puerto del servidor NNTP es 119
- El puerto del cliente NNTP es mayor que 1023
- NNTP utiliza el protocolo TCP
- Las reglas 1 y 2 permiten el ingreso de noticias al servidor interno. La regla 1 permite que el servidor externo envíe los mensajes al servidor interno. La regla **2** permite responder al requerimiento del servidor externo; ademas se controla el inicio de sesion (bit del ACK).
- Las reglas 3 y **4** permiten la salida de noticias a servidores externos. La regla 3 permite que el servidor interno envíe los mensajes a algun servidor externo. La regla **4** permite que el servidor externo responda al requerimiento del servidor interno; ademas se controla **el** inicio de sesion (bit del ACK) [CHAP95].

Recomendaciones para NNTP

Finalmente, las recomendaciones para brindar NNTP de manera segura son:

- No utilizar un host bastion como servidor de noticias sino servidores internos.

- Usar filtraje de paquetes o sistemas proxy para controlar las conexiones entre servidores externos e internos.
- Permitir la conexión con servidores externos considerados seguros.
- Advertir a los usuarios internos la existencia de servidores de noticias no confiables.
- Configurar el servidor NNTP correctamente, evitando errores en la configuración.

World wide web (WWW) y HTTP (Hyphertext transfer protocol)

La World Wide Web, mayormente conocida como web, es el servicio mas utilizado en Internet [CHAP95], El web nacio en 1993 y hasta ahora ha tenido un explosivo crecimiento mayor que cualquier otro servicio (Telnet, FTP, gopher, etc). El protocolo que utiliza el web es HTTP que habitualmente es direccionado en el puerto 80; se dice habitualmente porque en muchos servidores no es cierto, pues en su concepción el protocolo HTTP dejo abierta siempre la posibilidad de ocupar cualquier puerto en el servidor. Esto representa una desventaja desde el punto de vista de un filtrador de paquetes ya que tiene que verificar el puerto con quien se va a comunicar.

La solución a este inconveniente representa colocar un proxy de HTTP para permitir conexiones internas o externas. Sin embargo, se pueden configurar las reglas en un filtrador de paquetes asumiendo que la mayoría de sesiones HTTP usan el puerto 80.

Para habilitar este servicio, desde el punto de vista de un filtrador de paquetes, se deben configurar las siguientes reglas:

No.	Dirección	D. fuente	D. destino	Protocolo	P. fuente	P. destino	bit ACK	notas
1	Adentro	externo	interno	TCP	>1023	80	no	sesión entrante, cliente a servidor
2	Afuera	interno	externo	TCP	80	>1023	sí	sesión entrante, servidor a cliente
3	Afuera	interno	externo	TCP	>1023	80	no	sesión saliente, cliente a servidor
4	Adentro	externo	interno	TCP	80	>1023	sí	sesión saliente, servidor a cliente

Tabla XI. Reglas para filtrar HTTP

Utilizando el mismo estándar para las reglas de filtraje detallado en la sección 3.5. Filtraje de paquetes:

- El puerto del servidor HTTP es 80
- El puerto del cliente HTTP es mayor que 1023
- HTTP utiliza el protocolo TCP
- Las reglas 1 y 2 permiten la comunicación de clientes externos a servidores internos. La regla 1 permite el ingreso de requerimientos por parte de clientes externos a servidores internos. La regla 2 permite que el servidor interno envíe una respuesta al cliente externo; además se controla el inicio de sesión.
- Las reglas 3 y 4 permiten la comunicación de clientes internos a servidores externos. La regla 3 permite que el cliente externo envíe requerimientos a servidores externos. La regla 4 permite el ingreso de la respuesta del servidor externo al cliente interno; además se controla el inicio de sesión.

Utilizar un servidor proxy para HTTP acarrea un beneficio adicional debido a que el servidor puede cargar páginas de web de Internet previamente accesadas en su memoria caché. De esta manera, la próxima vez que se intente accesar a una de estas páginas, el servidor la

proveerá directamente desde su memoria cache. Esto significa que el servidor eleva significantemente el rendimiento para las maquinas clientes y reduce los requerimientos de ancho de banda de la red.

Aparte de estas soluciones via filtraje de paquetes y sistemas proxy, el protocolo HTTP lleva consigo algunos problemas que se escapan un poco del alcance de un firewall. Estos problemas se enfocan en dos puntos:

¿Qué daños pueden hacer los clientes a un servidor HTTP ?

¿Qué daños puede hacer un servidor HTTP a un cliente ?

Daños a un servidor HTTP

El desafio de proteger un servidor HTTP es igual al desafio de proteger un servidor FTP, lograr que los clientes puedan accesar solo a lo que el administrador desea que accesen, y que los clientes no puedan tomar alguna herramienta para cornprometer el servidor. Aqui se detallan algunos consejos para lograr este objetivo:

- Ejecutar el servidor sin privilegios de super-usuario.
- Usar el mecanismo chroot para restringir las operaciones del servidor a un determinado directorio para que no haya contacto con los archivos de configuración del sistema.
- No colocar información importante en una pagina de web. De esta manera si sucede algun ataque, no existira nada de interes para el atacante.
- Configurar el resto de la red para que en caso de que el servidor sea comprometido, no se involucre ningun otro sistema [CHAP95].

Un servidor HTTP por si mismo no ocasiona graves problemas en la seguridad. Sin embargo existe una caracteristica que utiliza el servidor HTTP que si involucra grandes riesgos. Se trata de los programas externos con los cuales interactua como por ejemplo los scripts CGI (Common

gateway interface), los cuales ejecutan ciertos procedimientos en el servidor. Por ejemplo, si alguien ejecuta consultas de base de datos a un servidor HTTP, este ejecuta un programa externo que ejecuta la consulta y genera una pagina HTML con las respuestas [CHAP95].

La existencia de estos programas externos puede originar dos tipos de problemas:

- Los programas externos, frecuentemente scripts en shells que corren sobre un servidor HTTP, se utilizan para accesar informacion y son hechos por personas que conocen algo o quizás nada acerca de seguridad. Por esta razon es muy difícil establecer que los scripts sean seguros. Lo aconsejable en estos casos es revisar estos scripts, mantenerlos en un periodo de prueba y despues ponerlos en operación. Otra medida a tomar seria utilizar algun mecanismo (chroot) para proveer de un ambiente seguro a los scripts. A pesar de tener estas soluciones, no se puede asegurar que los scripts CGI sean totalmente seguros debido a que nadie es perfecto.
- Un atacante puede cargar sus scripts o programas ya compilados via FTP y luego ejecutarlos en el servidor HTTP. Para esto se deben cumplir las siguientes condiciones:
    - El servidor HTTP y FTP se estan ejecutando en la misma maquina para que el atacante pueda subir los programas a traves de FTP y colocarlos en el servidor HTTP.
    - Si se tiene acceso a algunas areas donde se encuentran los archivos del sistema.
    - Si en algún directorio se tiene al menos permiso de escritura.

Daños a clientes HTTP

El daño que se puede hacer a un cliente HTTP es aun mas complejo que el daiio que se le puede hacer a un servidor HTTP. El problema con los clientes es que generalmente los browsers son diseñados para ser extensibles, es decir ejecutan programas externos para tratar con ciertos tipos de datos. Los servidores HTTP proveen informacion en muchos formatos: texto

plano, HTML, Postscript, video, etc. Sin embargo, los clientes HTTP comunes no entienden sino unos pocos formatos de estos, por lo tanto tienen que llamar a programas externos para interpretar los otros formatos. Estos programas externos presentan o imprimen el formato indicado.

Un atacante puede cambiar el formato original del servidor. Por ejemplo, si un servidor utiliza como formato de un archivo a Postscript, el cual es un lenguaje de programacion completo para controlar impresoras, entonces un atacante puede enviar instrucciones dentro del archivo. Al abrir el archivo en el cliente se ejecutarán las instrucciones que envio el atacante. Para dar una idea, si la instrucción fuera "borrar todos los archivos del actual directorio", se borrarian todos los archivos de ese directorio perjudicando a la maquina del cliente.

No existe una solución practica ante este problema, en realidad depende bastante del cliente HTTP si se conecta a una direccion de web que resulta sospechosa o desconocida [CHAP95]. Una solución puede ser proporcionar educación a los clientes para que no inicien conexiones a direcciones sospechosas y cuando ocurran problemas de este tipo, anotar la direccion de ese Web para evitar futuras conexiones de clientes. Las direcciones sospechosas pueden ser nombres mal escritos u homonimas de organizaciones grandes. Por ejemplo, en esta direccion http:/lwww.mycrosoft.com/ se puede deducir que no se trata de la verdadera ya que el nombre esta mal escrito.

Recornendaciones para WWW

- Es recomendable utilizar un host bastion dedicado por cada servidor HTTP interno.
- Tomar precaución con los programas externos que usa el servidor HTTP.
- Es necesario configurar el sewidor HTTP para controlar a que tiene acceso un cliente, es decir, observar si existen formas en las que un cliente pueda ejecutar sus propios programas.

- Utilizar un proxy para HTTP, así se gana mayor control sobre los puertos que maneja y se aprovechan los beneficios de la memoria cache para no aumentar el ancho de banda de la red.
- Configurar con cuidado los clientes HTTP y prevenir a los usuarios para que no cambien esta configuración y que no se conecten a lugares sospechosos.
- Actualmente existen programas de firewalls (en su mayoría comerciales) que examinan todos los datos que son transferidos desde Internet via Web, de esta rnanera se puede censar si los datos contienen virus, comandos ejecutables, etc.

DNS (Domain name server)

DNS es un mecanismo estandar de Internet que almacena informacion relativa a los hosts. **DNS** es un sistema de base de datos distribuida que traduce los nombres de los hosts a direcciones IP y las direcciones IP a nombres de hosts. Cualquier programa que usa nombres de hosts es un cliente DNS. Por ejemplo: Telnet, SMTP, FTP, etc. [CHAP95]

Existen dos tipos de actividades DNS:

"lookup" : Ocurre cuando un cliente DNS consulta informacion al servidor. Por ejemplo, la direccion IP de un host dado su nombre, el nornbre del host dado su direccion IP, el nombre de un servidor dado un dominio, etc.

Transferidores de zona: Ocurren cuando un servidor secundario DNS requiere de otro servidor DNS primario todo lo que este ultimo conoce de un pedazo de nombre de un dominio. Estas transferencias de informacion de zonas suceden a lo largo de todos los servidores en Internet y son de mucha utilidad para obtener informacion de dominios.

Para actividades de tipo "lookup" usualmente, y por razones de rendimiento, se utiliza el protocolo UDP. Si alguna informacion se pierde en el transito, se lanza un requerimiento

nuevamente pero esta vez utilizando TCP. El servidor DNS usa el puerto 53 tanto para UDP como para TCP y el cliente un puerto mayor que 1023 para TCP y UDP.

Los problemas mas comunes que se pueden originar dentro de este protocolo son:

- **Respuestas erroneas:** El primer problema de seguridad con DNS es que muchos servidores y clientes pueden ser engañados por un atacante que cambie la informacion. No es posible estar cornpletarnente seguros de que la inforrnacion recuperada es la información requerida, o de que el servidor que respondio es a quien se lanzo el requerimiento. Un atacante puede aprovecharse de esto, y por ejemplo cambiar la inforrnacion de dominio de un host al que una organizacion considera confiable y que permite acceso a la organizacion sin uso de contrasefias. De lograrlo, el atacante podría ingresar al sistema sin problemas.

La solución para el problema anterior puede ser la utilización del proceso llamado "doble-reversa", el cual consiste en los siguientes pasos: prirnero se lanza un requerimiento dada una direccion IP, el servidor responde con un nombre, y segundo se lanza un requerimiento dado el nombre de la respuesta anterior, finalmente el servidor tiene que responder con la direccion IP original, caso contrario se trata de una direccion falsa. Actualrnente existen sisternas operativos tales como Solaris que implementan este proceso para mayor seguridad.

- **Revelar mucha inforrnacion a atacantes:** Otro problema que se da muchas veces es que en DNS se habilita demasiada informacion de los servidores internos de una organizacion. Se vuelve mas crítico el problema cuando los servidores internos poseen informacion sensitiva la cual no debe por ningun motivo presentarse ante Internet. Este problema origina ataque de tipo "ingenieria social" (ver sección **1.2.** Tipo de ataques), en el cual los atacantes pueden obtener cierta informacion de los hosts internos y manipular esta inforrnacion para engafiar a los administradores, cambiar contrasefias, etc.

En el servidor DNS existen dos registros que guardan inforrnacion acerca de los hosts:

HINFO (Host information records): El nombre del hardware y sistema operativo que la maquina usa. Esta informacion es de mucha valía para un atacante ya que gracias a ella puede introducir errores de configuracion.

TXT (Textual infomation records): Nombra caracteristicas especiales de un sistema, por ejemplo si usa herramientas especiales de seguridad.

La solución a este problema es el ocultamiento de la inforrnacion DNS a traves de una configuracion especial. La manera de esconder informacion DNS es hacer que el servidor DNS le otorgue un total acceso de consultas de dominio externos a las maquinas internas y acceso restringido de consultas de dominios internos a las maquinas externas.

Para desarrollar este método es necesario establecer la configuracion de la figura No. **4-11** siguiendo los siguientes pasos:

1. **Crear un servidor DNS falso:** Este servidor DNS ubicado en el host bastion debe ser el sewidor primario en caso de que exista otro servidor DNS interno. El falso servidor DNS conoce todo el dominio interno de una red. Sin embargo, la unica informacion que debe presentarse al mundo externo es de:
   - Las maquinas que constituyen el firewall
   - Cualquier maquina interna que necesita ser reconocida por Internet (servidor de noticias por ejemplo).

   Los otros nornbres internos de las rnaquinas de la red deben ser falsos. Sin embargo, hay que tomar en consideración que esta informacion falsa debe ser consistente en caso de que se utilice el proceso doble-reversa, es decir, los nombres de los hosts deben coincidir

con las direcciones IP. Además, se necesita colocar un filtrador de paquetes entre el host bastion y la red interna a fin de filtrar la inforrnacion entre el servidor falso (host bastion) y el o los servidores verdaderos (internos).

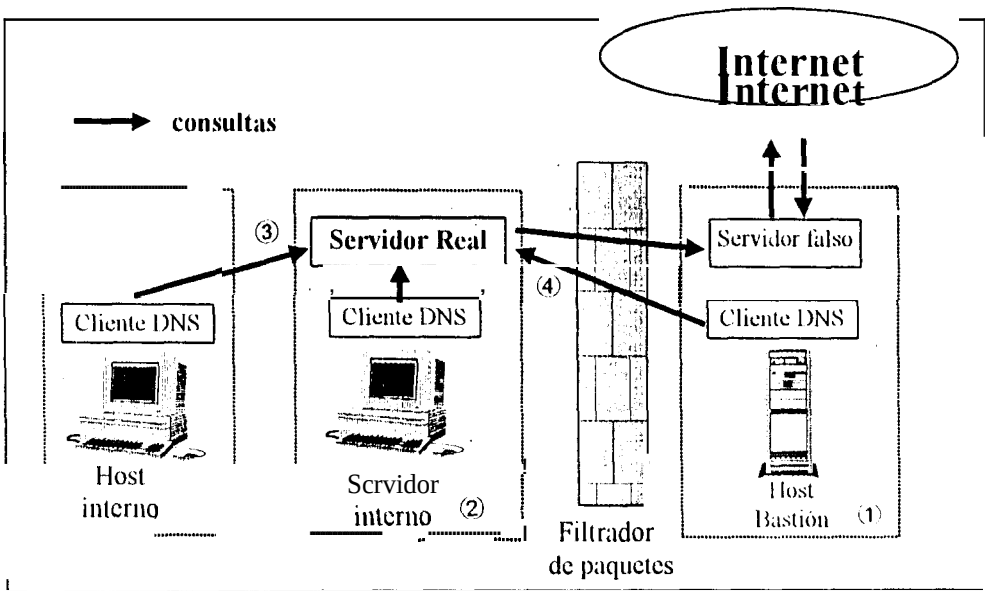


Figura NO. 4-11. Esquema de funcionamiento para esconder la información del servidor DNS

2. **Crear un servidor DNS** interno **para uso** de hosts internos: Las rnaquinas internas necesitan utilizar un servidor DNS para tener iiiforrnacion de los dernas hosts internos, y no la inforrnacion falsa que brinda el servidor DNS externo. Por esto, existe la necesidad de habilitar un servidor DNS interno confiable que incluso sirva para obtener inforrnacion de hosts externos.

La rnanera mas segura de obtener inforrnacion externa es a traves del host bastion, *es* decir tratar de que el servidor DNS interno se cornunique solo con el host bastion a fin de recoger inforrnacion externa, y no permitir la cornunicacion directa del servidor DNS interno con los demas servidores DNS en Internet. Utilizar filtradores de paquetes para hacer esto es un poco dificultoso ya que es complicado filtrar el protocolo UDP. Para sisternas UNIX

existe una alternativa para solucionar este problema, se trata del direccionador "forwarder" disponible en un archivo de configuración del servidor (/etc/named.boot). Este direccionador le dice al servidor que consulta (en caso de no encontrar la respuesta) a que otro servidor hacerle el requerimiento. Utilizando este direccionador en el servidor interno para que apunte sólo al servidor DNS externo o falso estara solucionado el problema [CHAP95]. Otra solución más práctica es utilizar un proxy en el host bastión, de tal manera que todo el tráfico saliente siempre pasara por el proxy y así se controlara que el cliente **DNS** pregunte primero al host bastion ② (ver figura 4-11).

3. Habilitar consultas desde clientes **DNS** internos al servidor DNS interno: Es necesario que las maquinas clientes de la red accesen al servidor DNS ③ (ver figura 4-11). Se pueden dar dos casos:

   - Cuando el servidor interno recibe una consulta acerca de una maquina interna o externa cuya informacion se encuentra en su cache, entonces el servidor responde directamente.
   - Cuando el servidor interno recibe una consulta acerca de una maquina externa cuya informacion no se encuentra en su cache, entonces el servidor interno envía una consulta al servidor DNS del host bastion, y se preocupa por recibir una respuesta.

4. Configurar para que un cliente en el host bastion consulte al servidor interno: Un cliente en el host bastibn (por ejemplo Sendmail) puede necesitar informacion de los nombres verdaderos de los hosts internos, para este caso especial se habilitan las consultas al servidor DNS interno ④ (ver figura **4-1**1).

Este ultimo paso es bastante arriesgado debido a que si un intruso logra comprometer el host bastion, entonces podra ver toda la información disponible en el servidor DNS interno.

El filtrador representado en la figura No. 4-11 debe contener las siguientes reglas permitidas:

lo.	Dirección	D. fuente	D. destino	Protocolo	P. fuente	P. destino	bit ACK	notas
1	Afuera	scrvidor interno	**host** bastión	UDP	53	53	no	consulta desde el servidor interno al host bastión vía UDP
	Afuera	servidor iiitcriio	host bastioii	TCP	>1023	**53**	sí	consulta dcsde **el** servidor interno al **host** bastión vía TCP
		host bastión	scrvidor interno	UDP	53	**53**	no	respuestas desde el host bastión al scrvidor interno vía UDP
4	Adentro	host bastión	**servidor** interno	TCP	53	>1023	si	respuestas dcsde el host bastión al servidor interno via TCP
5	Adentro	host bastión	scrvidor interno	UDP	>1023	53	no	consultas dcsdc clientes del host bastion al scrvidor iiitcriio vía UDP
6	Afuera	host bastión	scrvidor interno	TCP	>1023	**53**	no	consultas dcsdc clientes del host bastión al scrvidor iiitcriio vir TCP
7	Adentro	scrvidor interno	host bastion	UDP	53	>1023	no	respuestas dcsdc el scrvidor interno a los clientes del host bastiór vía UDP
8	Afuera	scividor interno	host bastion	TCP	53	>1023	sí	respuestas desde c scrvidor interno a lo! clientes del host bastiór vía TCP

Tabla XII. Reglas para filtrar DNS escondiendo la informació n

Utilizando el mismo estandar para las reglas de filtraje detallado en la sección 3.5. Filtraje de paquetes:

- El puerto del servidor DNS es 53
- DNS utiliza el protocolo TCP y UDP

- El puerto del cliente DNS es mayor que 1023
- Las reglas 1 y *2* permiten las consultas desde el servidor interno al host bastion. La regla 1 permite la consulta del servidor interno al host bastion via UDP. La regla *2* permite la consulta del servidor interno al host bastion via TCP.
- Las reglas 3 y **4** permiten la respuesta desde el host bastion al servidor interno. La regla 3 permite que el host bastion responda al requerimiento del servidor interno via UDP. La regla **4** permite que el host bastion responda al requerimiento del servidor interno via TCP.
- Las reglas ***5*** y 6 permiten las consultas desde el host bastion al servidor interno. La regla 5 permite la consulta desde los clientes del host bastion al servidor interno via UDP. La regla 6 permite la consulta de los clientes del servidor interno al host bastion via TCP.
- Las reglas 7 y ***8*** permiten la respuesta desde el servidor interno al host bastion. La regla 7 permite que el servidor interno responda al requerimiento del host bastion via UDP. La regla **8** permite que el servidor interno responda al requerimiento del host bastion via TCP.

Una configuracion alternativa, pero menos segura que la anterior, es no ocultar la informacion DNS. Con esta otra configuracion se habilita toda la informacion de los hosts internos de una organización y se justifica en el caso en que no exista informacion relevante en los sistemas. De igual manera es aconsejable utilizar al host bastion con servidor DNS externo pero sin falsear la informacion. En este caso el servidor interno es primario y el servidor externo ubicado en el host bastion es secundario. Esto se observa en la figura No. **4-12.**

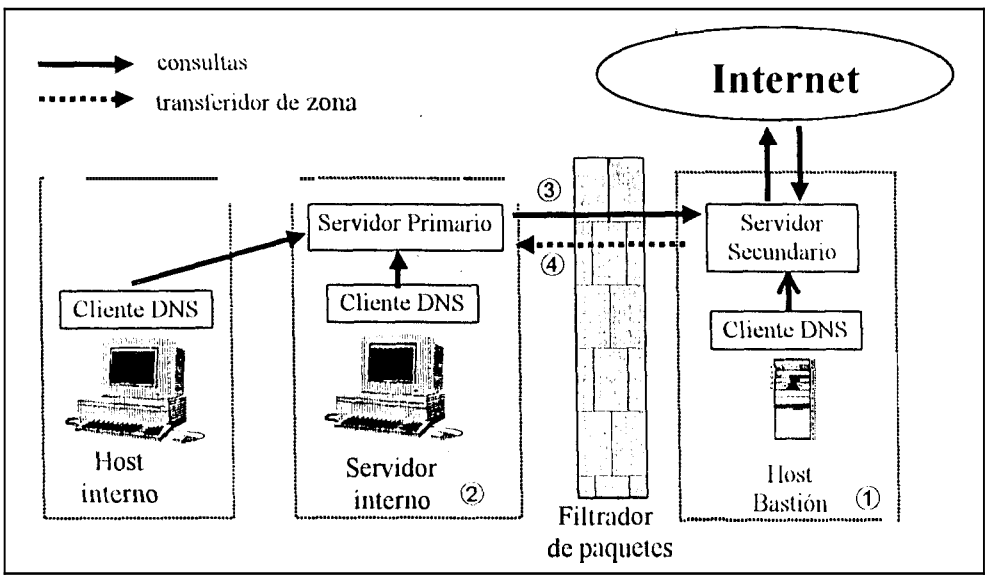


Figura No. 4-12. Esquema de funcionamiento sin esconder la información del servidor DNS

Para implementar esta configuración hay que seguir los siguientes pasos:

1. **Habilitar un servidor secundario en un host bastión:** En esta ocasión el servidor ubicado en el host bastión posee información verdadera acerca de los hosts internos. La razón del servidor en el host bastión es para que los usuarios de Internet no tengan contacto directo con la red interna ① (ver figura No. 4-12)
2. **Crear un servidor primario en la red interna:** A fin de que los usuarios internos obtengan información de los hosts internos sin necesidad de consultar al host bastión ② (ver figura No. 4-12) [CHAP95].
3. **Habilitar consultas del servidor primario al secundario:** De esta manera los usuarios internos pueden hacer consultas de hosts de Internet. ③ (ver figura No. 4-12).

4. **Habilitar transferidores de zona entre el servidor secundario y el primario:** De esta manera la información es transferida del servidor primario al secundario para que este pueda responder a las consultas de usuarios de Internet ④ (ver figura No. **4-12).**

El filtrador de paquetes colocado entre el servidor secundario y el servidor primario debe permitir las siguientes reglas:

No.	Dirección	D. fuente	D. destino	Protocolo	P. fuente	P. destino	bit ACK	notas
1	afuera	servidor interno	host bastión	UDP	*53*	53	no	consultas desde el servidor interno al host bastión vía UDP
2	afuera	servidor interno	host bastion	TCP	>1023	**53**	no	consultas desde el servidor interno al host bastion vía TCP
3	adentro	host bastión	servidor interno	UDP	*53*	53	no	respuestas desde el host bastión al servidor interno via UDP
4	adentro	host bastión	servidor interno	TCP	**53**	>1023	si	respuestas desde el host bastion al servidor interno via TCP
5	adentro	host bastión	servidor interno	TCP	>1023	53	no	requerimiento de transferidor de zona desde host bastión al servidor interno
6	afuera	servidor interno	host bastión	TCP	*53*	>1023	sí	respuestas de transferidor de zona desde el servidor interno al hos bastión

Tabla XIII. Reglas para filtrar paquetes DNS sin esconder la información

Utilizando el mismo estándar para las reglas de filtraje detallado en la sección **3.5.** Filtraje de paquetes:

- **El** puerto del servidor DNS es 53

- DNS utiliza el protocolo TCP y UDP
- El puerto del cliente DNS es mayor que 1023
- Las reglas 1 y **2** permiten las consultas desde el servidor interno (Primario) al host bastion. La regla 1 permite que el servidor primario consulte al secundario via UDP. La regla **2** permite que el servidor primario consulte al secundario via TCP.
- Las reglas 3 y **4** permiten las respuestas desde el host bastion al servidor interno. La regla 3 permite que el host bastion conteste al servidor interno via UDP. La regla **4** permite que el host bastion conteste al servidor interno via TCP.
- Las reglas 5 y 6 permite la comunicacion de requerimientos de transferidores de zona entre el host bastion y el servidor interno. La regla 5 permite que el host bastion envíe un requerimiento al host interno via TCP. La regla 6 permite que el servidor interno responda al requerimiento de host bastion via TCP.

Recornendaciones para DNS

Finalmente, para proveer el servicio DNS es necesario tomar en cuenta las siguientes recomendaciones:

- Desabilitar transferencias directas entre servidores internos e Internet. Las consultas tienen que ser hechas a traves de un servidor DNS externo.
- Configurar un servidor DNS externo en el host bastion [CHAP95].
- Desabilitar registros que contengan informacion de cada maquina (HINFO, TXT).
- Utilizar el mecanismo doble-reversa evitar respuestas erróneas que ocasionen ataques.
- Considerar el ocultar informacion del dominio interno a traves de falsos servidores DNS.

4.5.3. Monitoreo

Dentro de las necesidades de la jefatura de Redes de CESERCOMP se encuentra la de monitorear constantemente los recursos y las redes conectadas al backbone. Hay que recordar que al tener un firewall por cada subred conectada al backbone se contempla que el usuario administrador central (Jefatura de Redes) pueda accesar a los archivos de log de cada uno de estos firewalls internos a fin de monitorear todos los sucesos que han sido registrados por este. Con esto se gana un mayor control sobre las redes internas desde cualquier punto del backbone.

Es preferible que tanto los firewalls internos como el firewall externo posean intrinsecamente capacidades de registro para generar consultas y reportes; caso contrario, habria que recurrir a los archivos de log que ofrecen los sistemas operativos. Para mayor informacibn referirse a la sección 2.5.3.1. Mecanismos de monitoreo.

4.5.4. Resumen de las politicas de seguridad

De acuerdo a la Tabla I del capítulo II, la informacibn de las politicas de seguridad de red para la ESPOL es la que se presenta en la tabla XIV.

Recursos		Probabilidad riesgo	tipo de usuario de quienes protegerse	Medidas protectoras
No	Nombre o descripción			
01	Ruteador IBM 2210 Enlace con Ecuanet	ALTO	usuarios externos	seguridad propia y física
02	Ruteador IBM 2210 Enlace con Las Peñas	ALTO -	usuarios internos	seguridad propia y física
03	ComServers TELEBIT	ALTO -	usuarios internos	seguridad propia y física
04	goliat.espol.edu cc			

a	SPARC 20:	ALTO	usuarios iiitcriios	scguridiid física
b c	S.O.:Solaris DNS	ALTO	usuarios iiitcriios y csteriios	scgiiridiid dc Iiost y Firewall externo
d	SMTP (SendMail) SMTP (SendMail)	ALTO ALTO	usuarios internos y externos	scguridad dc host y Firewall
e	FTP (anónimo)	MODERADO	usuarios externos	
f	HTTP	ALTO	usuarios iiitcriios y cstcrnos	
g	Telnet	ALTO	usuiirios estcriios	cstcriio
05	David.espol.edu cc			
a	**SPARC 2**	ALTO	usuarios iiitcriios	scguridiid física
b	S.O.: Solaris	ALTO	usuarios iiitcriios y cstcriios	scguridiid dc host y Firewall externo
06	Maquina Administración			
a	RISC 6000	ALTO	usuarios iiitcriios	scguridad física
b	UNIX AIX	ALTO	usuarios iiitcriios y cstcriios	scguridiid dc host, firewalls esterno
c	NetView	ALTO	usuarios iiitcriios y cstcriios	scgiiridiid dc host y firewall cstcriio
07	Servidor de bases de datos			
a	RISC 6000	ALTO	tisuarios iiitcriios	scguridad física
b	S.O.: UNIX AIX	ALTO	usuarios iiiteriios y cstcrnos	scgiiridiid de **Iiost,** firewalls externo c interno
c	DB/2	ALTO	iisuarios iiitcriios y externos	scguridiid dc host, firewalls cstcriio c interno
08	Servidor de aplicaciones			
a	RISC 6000	ALTO.	usuarios iiitcriios	scgiiridiid física
b	S.O.: UNIX AIX	ALTO.	usuarios iiiteriios y cstcriios	seguridad de host, firewalls cstcriio e interno
d	Presupuesto	ALTO	usuiirios	scgiiridiid de host,
d	Contabilidad	ALTO	iiitcriios	firewalls
e	Tesorería	**ALTO**	y	cstcriio c
f	Académica	ALTO	cstcriios	iiitcriio

Tabla XIV. Cuadro de resumen c **las** politicas de seyuridad de redes de la E ')OL

El significado de los terminos utilizados en el campo de probabilidades de riesgo fue analizado en la seccion **4.3.** Análisis de riesgo; para resumir, los tipos de usuarios han sido presentados como usuarios internos y externos segun la seccion **4.4.1.** Identificando a los usuarios; y para las medidas protectoras se ha eligido la siguiente terminologia:

- Seguridad propia: Significa asegurar al recurso con mecanismos propios del recurso que se desea asegurar (ruteadores y servidores de comunicacion)
- Seguridad fisica: Significa aislar al recurso en un lugar de acceso restringido. Para mayor información ver seccion **2.5.1.5.** Seguridad fisica .
- Seguridad de **host:** Significa sólo habilitar los servicios estrictamente requeridos y brindarles seguridad con mecanismos propios o programas extras acoplados en el sistema. Para mayor referencia de cómo construir un host bastion ver la seccion 3.4. Host bastion.
- Firewall externo: Mecanismo de primer nivel de seguridad. Para mayor referencia de los requerimientos de este tipo de firewall, ver la seccion *5.2.* La configuracion de servicios de Internet se encuentra en la seccion **6.2.** Firewall externo.
- Firewall interno: Mecanismo de segundo nivel de seguridad. Los requerimientos para este firewall dependen de las necesidades de las redes internas. Sin embargo, la configuracion del firewall interno puede ser la misma que la del firewall externo.

Hasta este punto la configuracion de los recursos conectados en el backbone cambia de la siguiente forma:

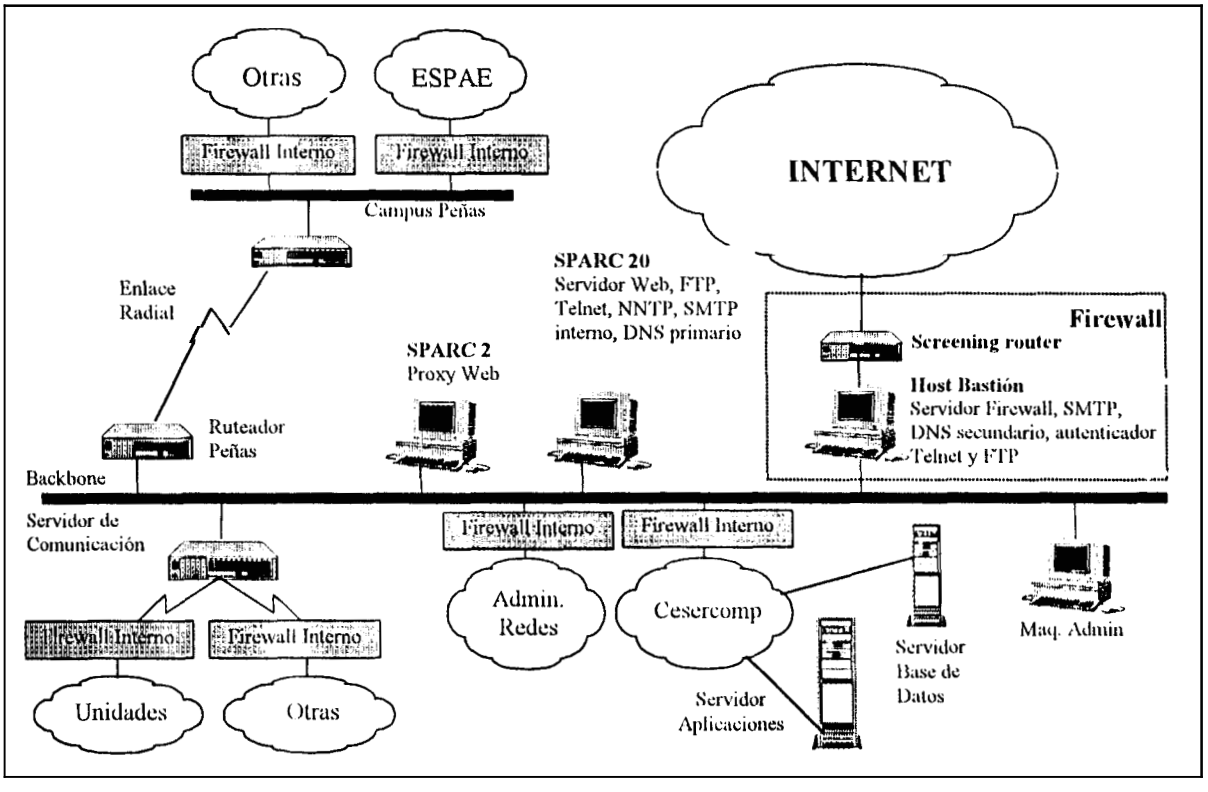


Figura No. 4-13 Configuración del Modelo de seguridad

El primer mecanismo de seguridad es el firewall externo, el cual está constituiído por el ruteador filtrador (screening router) y el host bastión. El ruteador filtrador debe ser configurado utilizando el criterio de negar por defecto: "Todo está prohibido excepto lo expresamente permitido". El host bastión es la máquina residente del servidor firewall y de otros servidores. Algunos programas o paquetes de Firewalls traen consigo soluciones para los problemas de seguridad de todos los servicios de Internet anteriormente descritos. Por lo tanto, las características del producto de firewall que la ESPOL adquiera, básicamente deben cubrir las necesidades de seguridad de los servicios que la ESPOL brinda. De acuerdo a esto, no se necesitaría de servidores adicionales en el host bastión. Sin embargo, si la ESPOL no adquiere un producto de

firewall, entonces sera necesario instalar productos gratuitos disponibles en Internet y seguir las recomendaciones en cada una de las configuraciones de los servicios de internet que la ESPOL brinda.

La maquina Goliat como principal servidor de Internet contiene los servidores de FTP, Telnet, SMTP, Web y DNS primario. En la maquina David se recomienda colocar exclusivamente un servidor proxy web para aprovechar toda su memoria cache y disminuir el ancho de banda de la red. Ambos hosts deben contar con serguridad de host.

Los servidores de aplicaciones y bases de datos deben colocarse en una red interna, en este caso la red interna es la de CESERCOMP pero puede ser cualquiera otra que contenga un firewall interno de por medio. La configuración de un firewall interno depende de las necesidades y de los servicios de Internet que va a brindar la red interna.

Los detalies de todas las configuraciones finales de los servidores se definira en un documento exclusivo para la Jefatura de Redes de CESERCOMP por razones de seguridad.

4.6. Plan de accion ante violación de politicas de seguridad

En esta seccion se asume que las redes interconectadas en el backbone poseen la protección adecuada. De acuerdo con la seccion 2.6. Plan de accion, cuando las politicas de seguridad son violadas, una organización se puede acoger a dos estrategias:

- Proteger y proceder
- Perseguir y acusar

Antes de presentar un plan de acción ante una eventual violación de politicas de seguridad en la ESPOL es necesario evaluar las condiciones para ambas estrategias:

4.6.7. Condiciones para proteger y proceder

Esta estrategia consiste en proteger los recursos de la red y restaurar cualquier daño ocasionado por un ataque. Se debe adoptar esta estrategia si se cumplen las siguientes condiciones aplicadas para las redes de la ESPOL:

Que los recursos esten desprotegidos: Para el caso de la ESPOL no se cumple esta condicion debido a que los recursos si estan bien protegidos de acuerdo al modelo de seguridad presentado. Los recursos del backbone mas importantes poseen hasta 3 niveles de redundancia (servidores de aplicaciones y bases de datos).

Que una actividad intrusa continuamente ocasione un gran daño y riesgo financiero: Si se presentasen actividades intrusas en los recursos del backbone, estas ocasionarian daños que pudieran ser fácilmente recuperables (por ejemplo: servidor de HTTP, Gopher, SMTP, etc.). En el caso de los servidores de aplicaciones y bases de datos, los riesgos financieros serian cuantiosos. Esta condicion se cumple a medias.

Que exista un considerable riesgo para los usuarios de la red: Los usuarios internos de la ESPOL, en su mayoría estudiantes, siempre van a estar expuestos a las capturas de contraseñas de cuentas. No se cumple esta condicion.

Que el costo de una persecusion a un intruso sea muy alto: El costo de persecusion es alto debido a que los firewalls internos y externo deben poseer mecanismos o trampas para capturar a un intruso. Sí se curnple esta condicion.

4.6.2. Condiciones para perseguir y acusar

Esta estrategia consiste en perseguir a los intrusos, obtener pruebas de los ataques que han ocasionado y acusarlos ante una agencia de leyes. Se debe adoptar esta estrategia si se cumplen las siguientes condiciones aplicadas para las redes de la ESPOL:

Que los recursos y sistemas esten bien protegidos: Los recursos conectados al backbone son bien protegidos. Se cumple esta condicion.

Que la red haya sido centro de ataques de intrusos y estos no dejan de hacerlo: Por su concepción de entidad académica abierta a Internet, la probabilidad de ser blanco de ataques es alta. Se cumple esta condicion.

Que el local sea apropiado para incurrir el riesgo de un acceso no autorizado: Al poseer redundancia en seguridad para cada recurso, sí se puede correr el riesgo de permitir a los intrusos continuar. Se cumple con la condicion.

Que las herramientas de monitoreo y registro puedan archivar bastante información: Capacidades de registro y monitoreo son requerimientos para el firewall que la ESPOL decida adquirir. Se cumple con la condicion.

Que exista disponibilidad para acusar: En Ecuador no existe ninguna ley para condenar las actividades intrusas realizadas por medios computacionales. Sin embargo, existen entidades internacionales que ayudan dando consejos a las partes involucradas para resolver este tipo de problemas. Estas entidades no tienen jurisdicción en Ecuador, pero no se puede descartar las posibles soluciones que estas planeen. La condicion se cumple parcialmente.

4.6.3. Conclusiones

Se podría pensar que la estrategia "perseguir y acusar" es la estrategia mas adecuada para la ESPOL debido a quc se cumplen la mayoría de sus condiciones; sin embargo, no sirve de

mucho adquirir mecanismos sofisticados para capturar a hackers si no existen leyes que condenen estas acciones. Estos mecanismos servirían nada mas para obtener información de como penetraron, quienes son y cuales fueron sus intenciones.

En el caso eventual de que la violación suceda por mala configuración del firewall, se corren peligros a pesar de tener redundancia de seguridad en los recursos. Estas brechas pueden producir otras brechas y así sucesivamente hasta que un recurso quede totalmente desprotegido. En este caso seria urgente adoptar una estrategia de "proteger y proceder".

Dado lo anterior, no se puede pensar en adoptar una sola estrategia de respuesta para la ESPOL. Es necesario llegar a un punto de equilibrio entre ambas estrategias de tal manera que se protega y recupere, pero tambien se persiga y acuse. Entonces, en el caso de incidentes que violen las politicas de seguridad en el backbone, las actividades a realizar serían las siguientes:

1. Determinar que politicas han sido violadas y evaluar la situación.
2. Investigar como y cuando se violó la o las politicas de seguridad.
3. Descubrir quien violó las politicas de seguridad.
4. Corregir los daños y aplicar las sanciones respectivas al o a los culpables dependiendo del tipo de violación y del tipo de usuario.

En el caso de que los atacantes sean usuarios internos, las sanciones son determinadas en base a los reglamentos que dispone la ESPOL. En el caso de que usuarios externos violen los sistemas internos es necesario tener soporte por parte de entidades (agencias de leyes) encargadas de resolver este tipo de problemas. Estas organizaciones pueden ser: CERT (Computer Emergency Response Team; e-mail: cert@cert.sei.cmu.edu), CIAC (Computer

Incident Advisory Capability; e-mail: ciac@tiger.llnl.gov) y CNSRT (Computer Network Security Response Team; cnsrt@ames.arc.nasa.gov).

En el caso de que usuarios internos violen sistemas de organizaciones externas, y estas lo notifiquen y prueben estas acciones ante la jefatura de redes, sera necesario establecer nuevas sanciones en los reglamentos de la **ESPOL** en común acuerdo con las sanciones que las agencias de leyes recomienden.

CAPÍTULO V

EVALUACION DE FIREWALLS

5.1. Introducción

Luego de plantear un modelo de seguridad en base a las necesidades de la ESPOL, es preciso establecer las características del elemento que constituye el primer nivel de seguridad ante Internet: el firewall externo. Para elegir el producto de software con el que se implementara el firewall externo es nrtcesario conocer el modelo de seguridad y la tecnologia contemporanea que ofrece el mercado de productos para firewalls.

Los productos de sottware para firewalls o paquetes de firewalls a evaluar son seis: cuatro publicos disponibles en Internet; y dos comerciales o privados. Los paquetes de firewalls publicos han sido soleccionados en base a la tecnologia que ofrecen, para cada tipo de tecnologia *se* ha escogido al menos dos, para poder efectuar una comparacion real entre ellos. Es decir, se comparán dos filtradores de paquetes y dos sistemas **proxy.** Los paquetes de firewalls comerciales o privados a evaluar han sido seleccionados por que hasta el año de 1996

(fecha en que se inició esta tesis) presentaban las mejores caracteristicas y por que han sido premiados y certificados por organizaciones de seguridad de acuerdo a la National Computer Security Asociation (http://www.ncsa.com).

Los paquetes de firewalls en el mercado incrementan rapidamente por lo que no causaria sorpresa si en este momento existen paquetes de firewalls con mejores caracteristicas de los aqui presentados

En este capitulo, primero se establecen los requerimientos del paquete de firewall para la ESPOL mediante las caracteristicas que debe ofrecer: seguridad, rendimiento, interfase, plataforrna, soporte, garantia y costos. A partir de estos criterios se procede a evaluar los diferentes productos de firewalls, de acuerdo a su condición de publicos o privados, para luego seleccionar el mejor firewall para la ESPOL.

Despues de seleccionar a la rnejor alternativa de paquete de firewall, se procede a evaluar la plataforma mas segura en la que se lo debe colocar de acuerdo a los criterios proporcionados por libros y revistas serias que continuamente realizan evaluaciones entre sisternas operativos.

5.2. Criterios para evaluar a un firewall

En esta sección se establecen los requerimientos minimos de un firewall para la ESPOL y luego la rnanera en que se llevara a cabo la evaluación.

5.2.1. Requerimientos minimos de un firewall para la ESPOL

Para analizar los requerimientos de un firewall para la ESPOL, se dividen las caracteristicas de un firewall en las siguientes categorias:

- Seguridad
- Rendimiento
- Interfase
- Plataforma
- Soporte
- Garantia
- Costo

5.2.1.1. Seguridad

Filtros a conexiones

Si el producto de firewall se basa en filtraje de paquetes, estas son las caracteristicas que debe poseer para brindar protección a la ESPOL:

- Filtros por direcciones IP y puertos tanto fuentes y destino: Esto es lo mas basico que debe tener un firewall, de esta manera se protegen las direcciones de los recursos mas importantes del backbone y se desabilitan todos los servicios entrantes a estos recursos en base a las direcciones y puertos de los paquetes de origen. Con esta medida la ESPOL debe implementar el punto de vista de negación por defecto. (ver sección 1.5.5.1. negar por defecto).
- Filtración en ambos sentidos: Es decir que el firewall reconozca la red interna de la externa para tener mayor control y filtrar direcciones y servicios tanto de afuera hacia adentro como de adentro hacia afuera. Con esta caracteristica la ESPOL restringe el acceso tanto a los usuarios de Internet al backbone como los usuarios de la ESPOL a Internet. Además, se logra

evitar los ataques via spoofing, donde los paquetes ingresan teniendo una dirección fuente de la red interna (ver seccion **1.2.** Tipos de ataques).

- **Filtros a servicios basados en los protocolos TCP, UDP, ICMP:** El paquete de firewall debe ser capaz de reconocer los paquetes de acuerdo al protocolo que manejan. Solo se piden estos tres protocolos debido a que la ESPOL solo manipula aplicaciones sobre estos protocolos. Sin embargo, si el firewall provee filtros aplicables para otros protocolos sera mejor.
- **Filtros en conexiones establecidas FTP, Telnet, HTTP:** El firewall tiene que levantar demonios o programas de estas aplicaciones para poder manipular el ambiente en que se desarrollan los usuarios de estas aplicaciones. Por ejemplo, no permitir que los usuarios FTP ejecuten comandos de eliminación, etc. El paquete de firewall debe proveer filtros a conexiones establecidas a los servicios FTP, Telnet y HTTP debido a que la ESPOL los acepta como servicios entrantes.
- **Filtros por datos:** Los firewalls contemporaneos filtran el campo de datos dentro de los paquetes que se transmiten, precisamente para evitar que los datos sean corruptos, contengan virus o sean comandos a ejecutar.
- **Filtraje dinamico:** Esta es una caracteristica que permite al software del firewall configurar reglas cuando esta en operación. Esta condición ayuda a filtrar con mayor seguridad los paquetes basados en el protocolo UDP (ver seccion 3.5. Filtraje de paquetes).

Sistemas Proxy

Para los paquetes de firewalls que se basan en sistemas proxy, estas son las caracteristicas mínimas para la ESPOL:

- **Aplicaciones soportadas Telnet, FTP, HTTP:** Estas son las mas importantes ya que la ESPOL brinda estos servicios a usuarios externos. Sin embargo, el paquete de firewall debe

contar con mas sistemas proxy en caso de que la ESPOL a futuro necesite brindar mas servicios.

- Las aplicaciones proxy deben filtrar a usuarios, direcciones IP fuentes y destinos. Al igual que los filtros, los servidores proxy deben considerar estos datos para tomar decisiones (permitir o negar el acceso a la red).
- El servidor proxy debe permitir manipular el ambiente en que los usuarios de las aplicaciones FTP, Telnet y HTTP se desenvuelven. De esta manera se restringe los directorios, comandos o programas que los usuarios puedan ejecutar indebidamente y con fines rnaliciosos.
- Programas modificados: La ESPOL posee muchos usuarios, los cuales no se acostumbraran a cambiar los procedimientos normales de conexión con las aplicaciones (servicios de Internet). Es aconsejable que se utilicen programas modificados, de tal manera que sean transparentes al usuario.
- Examinar datos: Al igual que en un filtrador, el proxy debe ser capaz de observar que es lo que esta fluyendo por el. De esta forma se evitan virus, programas maliciosos, etc.

Cabe destacar que las caracteristicas de los filtradores de conexiones y sistemas proxy son equivalentes, es decir, se puede tener un producto firewall que utiliza solo filtrador de paquetes o solo sistemas proxy que cumplen con los requerimientos de seguridad para la ESPOL. Algunos productos fusionan estas dos tecnologías para compensar las carencias del uno con las bondades del otro.

Monitoreo: registro, notificación y reportes

Una medida importante para evitar y detectar problemas en la seguridad es el monitoreo. El firewall de la ESPOL debe proveer las mejores herrarnientas existentes para monitorear las

sesiones que maneja ya que en su concepción, la universidad maneja un esquema muy abierto hacia Internet, y esto facilita que se originen ataques. Además se satisface la necesidad de monitoreo de la Jefatura de Redes.

Las características mínimas que necesita el producto de firewall para la ESPOL son:

- Registro en tiempo real: Mediante un visor de sucesos en tiempo real se pueden observar tanto los paquetes que entran como los que salen. Esta es una medida para probar al firewall y verificar si esta cumpliendo con las reglas con que fue configurado.
- Registro detallado en base a direcciones IP y puertos tanto fuentes y destinos, usuario, fecha y hora. Es importante, en caso de que suceda un ataque, tener información completa acerca del origen, servicio, fecha y hora en que sucedio, de esta manera se puede detectar una brecha de seguridad no contemplada.
- Notificación de situaciones sospechosas en tiempo real via correo electronio o a traves de ventanas de alarma. Una de las ventajas de tener registro de sucesos en tiempo real, es que cuando suceda una situacion sospechosa o un ataque, el firewall pueda notificar a traves de un mensaje de alarma en correo electronico o a traves de ventanas con sonidos incluidos.
- Ejecucion de programas o trampas para atrapar al intruso en caso de violación. Por tener la ESPOL un esquema abierto, es muy probable que se den ataques. Ante esto, el administrador tiene que optar por mecanismos que engañen a los intrusos, haciendoles pensar que han violado a un sistema cuando en realidad no lo han hecho. Esto proporcionara una medida de seguridad y lograra registrar al usuario y/o las actividades que realizó. Estos registros pueden constituirse en pruebas para sancionar al atacante.

- Reportes: El firewall preferiblemente debe manejar una herramienta que le permita al administrador consultar e imprimir reportes de los archivos de registro para manejar estadisticas.

Aotenticación

Al brindar servicios entrantes: Telnet, FTP y HTTP, es necesario contar con mecanisrnos extras sobre los filtros, que puedan autentificar a los usuarios de estas aplicaciones. Existen variedades de esquemas para autentificar las contrasefias de los usuarios. Las caracteristicas que debe poseer el paquete de firewall son:

- Aplicaciones soportadas: Telnet, FTP y HTTP
- Implementación de autenticacion soportadas: Para implernentar esquernas de contraseñas de un solo tiempo y desafio-respuesta para los usuarios autorizados desde Internet. Los esquemas disponibles y mas estandares son:
    - UserID: Es el esquema típico de contrasefias por usuario.
    - SecurID: Permite implementar contrasenas basadas en tiempo, es decir que cambian cada cierta unidad de tiempo (minutos, horas, días).
    - S/Key: Permite implementar contraseñas de un solo uso o un solo tiempo, es decir que cada vez que el usuario se conecte a un sistema, tendra una nueva contrasefia (ver sección 3.7.1. Autenticacion).
- Autenticacion en conexiones dial-up: Esta tambien es una medida adicional que puede implementarse en los sewidores de comunicacion.

Encriptacion

El backbone maneja informacion promiscua (conexiones libres a Internet) e informacion confidencial (de las aplicaciones administrativas y academicas). Para proteger la informacion

confidencial en tránsito es necesario utilizar encriptacion. Para ello cada subred debe contar con los mecanismos de encriptacion de emisor y receptor (ver seccion 3.7.2. Encriptacion). Las caracteristicas mínimas que el software de firewall para la ESPOL debe poseer son:

- Encriptacion entre firewalls (firewall-firewall): Esta caracteristica permite la comunicacion firewall a firewall, en el primer firewall se encripta y en el otro se desencripta.
- Encriptacion en conexiones rernotas **(firewall-usuario):** Si una subred no posee un firewall, esta puede encriptar y desencriptar cualquier informacion a traves de un modulo o programa que tiene la capacidad de encriptar o desencriptar. Este modulo, disponible en el paquete de firewall, puede ser ubicado físicamente en cualquier maquina cliente y le permitira comunicarse con el firewall sin necesidad de tener otro firewall (interno). Basicamente se encripta la informacion entre el usuario y el firewall.
- Tipos de encriptacion soportados: El esquema de encriptacion debe ser estandar, de tal manera que exista interoperabilidad con otros firewalls. Los esquernas considerados mas estandares son: DES y RSA (ver seccion 3.7.2. Encriptacion).

Traduccion de direcciones IP

Una caracteristica opcional que ofrecen los paquetes de firewalls y que la ESPOL podría utlizar es la traduccion de direcciones IP. La necesidad de traduccion de direcciones IP nace cuando:

- Por razones de seguridad, el administrador decide ocultar de Internet alguna direccion IP interna.
- Una direccion IP interna no es valida para Internet, es decir, esta direccion IP pertenece a alguna otra red en Internet.

Por su concepción, los sistemas proxy permiten traducir las direcciones internas por la direccion del host donde estan instalados **estos.** Sin embargo, existen algunos paquetes de

firewalls basados en proxies o en filtradores que permiten cambiar las direcciones internas por otras direcciones y no solo por la dirección del hosts donde este instalado.

Con esta caracteristica la ESPOL podra esconder las direcciones de los recursos mas importantes (redes administrativas, servidores de informacion internos) para que los usuarios externos no tengan conociemiento de estos. La traduccion de direcciones IP debe soportar las aplicaciones: FTP, Telnet, HTTP, DNS, SMTP y NNTP debido a que son las aplicaciones que la ESPOL brinda.

5.2.1.2. Rendimiento

Para evitar el cuello de botella que se produciria en la ESPOL entre el backbone e Internet, debido a la cantidad de usuarios conectados al mismo tiempo, el modelo de seguridad plantea que cada subred utilice su propio firewall interno para protegerse; así el firewall externo, ubicado en la conexión del backbone con Internet, quedara mas libre de carga. El firewall externo debe ser transparente en terminos de rendimiento, es decir que los usuarios no se percaten del retardo producido por el firewall.

El rendimiento de un firewall se evalua calculando la tasa de transacciones por minuto (tpm) o la tasa de bytes por segundo (bps), que este pueda transmitir de una red a otra. Cuando se transmiten datos de una red a otra por medio de un ruteador, el tiempo que demora una transacción desde que se inicia un proceso (aquel que hace posible la transmision de datos) hasta que este termina, es menor al tiempo que tomaría el mismo proceso si en lugar del ruteador se utilizara un firewall. Esto se debe a que el ruteador debe analizar la informacion la informacion y tomar decisiones: chequea direcciones lógicas de destino, aplica un algoritmo de ruteo y en base a la informacion disponible en la tabla de ruteo se retransmite la informacion por

una de sus interfases. En cambio el firewall debe a mas de escoger una ruta, filtrar de acuerdo a ciertas politicas.

La tasa de transacciones por minuto se obtiene del cociente entre el numero total de transacciones y el tiempo en minutos que demoro en procesarlas. Por ejemplo, una transaccion puede ser la transmision de un archivo desde un servidor al cliente; y el tiempo de procesamiento es el tiempo contado desde que se inició el requerimiento (del cliente al servidor) hasta cuando se transmitio todo el archivo. De esta manera, la formula para obtener las transacciones por minuto de un firewall es:

$$tp/t = \frac{n}{T_t} \qquad \text{[NEWM95]}$$

donde:

tp / t : transacciones por unidad de tiempo

n: numero de transacciones

T_t : tiempo total de transacciones (minutos); $T_t = t_1 + t_2 + t_3 + \ldots + t_n$

donde t_i es el tiempo que demoro la transaccion i

Como en el caso del plan de pruebas en la siguiente sección, si las transacciones que se ejecutan son de longitud constante, por ejemplo, si el archivo del ejemplo anterior es constante y la transacciones se repite n veces, se puede obtener la medida en bytes por segundo a traves de la siguiente formula:

$$\text{Byteslsegundo} = \frac{\text{n x número dc bytes de cada transacción}}{T_t}$$

donde:

n: número de transacciones

T_t: tiempo total de transacciones (segundos); $T_t = t_1 + t_2 + t_3 + \ldots + t_n$

donde t_i es el tiempo que demoro la transaccion i

Los firewalls a compararse deben estar configurados de igual manera, así el tiempo que demore cada transaccion dependera del tiempo que tome el firewall para procesar los paquetes, del hardware de la maquina, del tiempo que tome el sistema operativo en encargarse del proceso y del trafico de la red [NEWM97].

Cada software de firewall contara con el mismo ambiente, es decir la misma rnaquina, interfase de red y sistema operativo, por lo tanto a estas variables se las considera constantes. Sin embargo, el trafico de la red es una variable muy cambiante ya que depende mucho de la carga que soporte la red en el momento especifico en que se emite una transaccion. Es por esta razon que la red tiene que estar vacía o por lo menos considerarse estable con un flujo de paquetes constante. Además, con una muestra de varias mediciones se puede obtener una media de tiernpos, la cual es mas representativa y confiable.

Mientras mayor grado de rendimiento obtenga un firewall, sera mejor. Sin embargo, la medición de rendimiento, explicado con mayor detenimiento en el plan de pruebas descrito en la siguiente sección, es relativa mas no absoluta. Es decir, no se puede establecer que los datos obtenidos

representan al firewall y que siempre se van a obtener los mismos en otras configuración, estos datos tan solo son para efectos de comparacion.

El siguiente plan de pruebas se realizó solo con los firewalls públicos seleccionados debido a que no se pudo conseguir los instaladores de un producto de firewall comercial.

Plan de pruebas

Objetivo: Obtener la media de las tasas de transacciones por minuto que maneja un firewall.

Condiciones generales:

La maquina cliente se halla en la misma maquina del firewall, así todas las transacciones pasan por el firewall. El sistema de firewall esta configurado de la siguiente manera:

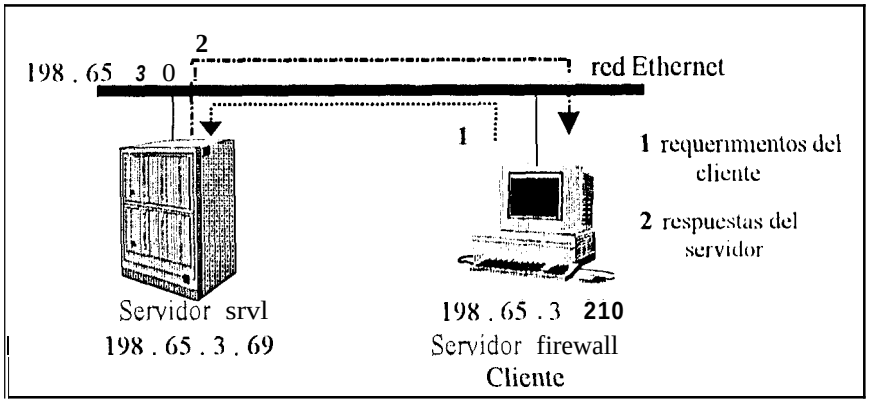


Figura No. 5-1 Configuración del firewall en plan de pruebas

Las características de los dispositivos que actuan son:

Caracteristicas	srv1	firewall / Cliente
Procesador	Pentium/66 Mhz	Pentium 100 Mhz
Memoria RAM	128 MB	32 MB
Sistema operativo	UNIX SCO	Linux Red Hat 4.0 (1.3)
Interfase de red	10 Mbps	10 Mbps

Se asume:

- Que la unica manera en que el cliente pueda llegar al servidor es a traves del firewall. En este caso se cumple ya que el mismo cliente es el firewall. Además, antes de iniciar las pruebas de rendimiento se probo que las conexiones siempre pasaban por el cliente.
- Que el servidor no se comunique directamente con el cliente sino a traves del firewall. Tambien se cumple debido a la misma razon anterior.
- Que las maquinas utilizadas sean las mismas en todas las pruebas.
- Que la red esté vacía o que la lectura de paquetes sea constante, es decir la tasa de incremento de paquetes debe ser constante en las horas en que se ejecutan las pruebas. Ver apendice B, donde consta la lectura de paquetes en el segmento de red durante las horas en que se realizaron las pruebas.
- Que los firewalls a probar tengan las mismas reglas de configuración.
- Que el firewall configurado funcione correctamente, es decir, debe cumplir con las caracteristicas que ofrece.

Estrategia

Para probar el rendimiento de un determinado firewall, el cliente (firewall) emite requerimientos al servidor. Para provocar estos requerimientos el cliente emula sesiones FTP para obtener un archivo de aproximadamente 350 KB, manteniendo primero 5 y luego 10 sesiones al mismo

tiempo dando la apariencia de 5 y 10 clientes físicos pero que en realidad son virtuales (dentro de la misma maquina). Este proceso se repite 5 veces para obtener un tiempo promedio de cuanto se demora el firewall procesando 5 y 10 sesiones al mismo tiempo respectivamente. Es decir, que en total se emiten 25 y 50 requerimientos FTP al servidor.

Para implementar esta estrategia se genero un script en korn shell que al ejecutarse en la maquina cliente crea clientes virtuales que lanzan requerimientos al servidor. El programa se ejecuta y envía los resultados (tiempo que demoro la transaccion) a ciertos archivos de salida. Este script es mayormente explicado en detalle en el apendice B, al igual que los archivos de salida.

Resultados Esperados

El tiempo que demore cada transaccion utilizando un firewall de por medio sera mayor que el tiempo que demore esa misma transaccion sin un firewall de por medio.

Los tiempos que registren los paquetes de firewalls basados en filtradores de paquetes seran menores que los tiempos que registren los firewalls basados en sistemas proxies, por la concepción de estos tipos de firewalls que fueron analizados en el capítulo III. Es decir, la tasa de transacciones por unidad de tiempo de los firewalls basados en filtradores de paquetes sera mayor que la tasa de transacciones por unidad de tiempo de los firewalls basados en sistemas proxy.

La siguiente tabla modelo puede ser utilizada para efectos de comparacion y tambien para construir graficos de transacciones por unidad de tiempo versus numero de clientes virtuales.

Transacciones	Sin firewall				Producto X			
	tiempo (seg)	varianza	tpm t/min	Kb/s	tiempo (seg)	varianza	tpm t/min	Kb/s
5 (350Kb cada una)								
10 (350Kb cada								

Para cada producto se tienen las siguientes columnas:

- **tiempo (segundos):** El tiempo que demora el producto de firewall en procesar 5 o 10 transacciones. Este valor es un promedio de los tiempos arrojados en las pruebas.
- varianza: Para todos los valores resultantes de las pruebas se obtiene la varianza, es decir un grado de dispersion con respecto al promedio.
- **tpm (transacciones por minuto):** La tasa de transacciones por minuto obtenida a partir del campo anterior.
- **Kbytes/s (Kilobytes por segundo):** El numero de kilobytes por segundo que demora el producto de firewall en procesar las transacciones. Para esto es necesario que las transacciones sean de la misma longitud.

De esta manera se podra observar claramente la degradación del rendirniento de cada firewall comparado con la tasa real del rendimiento sin firewall ya que esta es la tasa ideal por que no tiene retardo.

5.2.1.3. Interfase

Esta categoria representa las caracteristicas de la interfase del software de firewall ante el usuario. En el caso de un producto firewall, el usuario es el administrador de la red, y por lo

tanto es quien se encargara de instalarlo, configurarlo y mantenerlo. Para facilitar estas tareas se requieren analizar las siguientes caracteristicas:

- **Facilidad de instalacion:** La instalacion del firewall debe ser natural e intuitiva. De esta forma, aunque el firewall posea una teconologia nueva para el administrador, este sera facil de instalar y no requerira de conocimientos especializados.
- **Facilidad de configuracion:** La configuracion de reglas en un firewall debe ser clara y facil de entender. Muchos firewalls ofrecen interfases graficas representando objetos que intervienen en la red a protegerse. Las reglas de filtración deben ser sencillas de manipular para que el administrador pueda probarlas.
- **Mantenimiento:** Este factor no es menos importante que los anteriores. El firewall debe ser capaz de proveer seguridad a los nuevos servicios de Internet que aparezcan.
- **Información disponible:** Otro factor importante es la calidad de la informacion disponible tanto en manuales como ayuda en línea, documentación en web sites, etc. El firewall seleccionado para la ESPOL debe poseer abundantes fuentes de informacion accesibles.

5.2.1.4. Plataforma

Dentro de la categoria plataforma se considera:

- **Hardware / sistema operativo:** El hardware y el sistema operativo que soportan al programa de firewall deben ser seguros. En esta sección solo se evaluara la operabilidad del producto con algunas plataformas y luego una vez seleccionado el mejor producto de firewall para la ESPOL se evaluara la plataforma mas segura.
- **Interfases de red:** El backbone de la ESPOL es de teconologia ATM; sin embargo, se dispone de un convertidor de Ethernet a ATM. Por lo tanto, el software del firewall debe soportar como minimo interfases de red Ethernet o ATM; si soporta mas tipos de interfases sera mejor. El número de interfases puede variar con el tiempo, inicialmente se requieren como mínimo

dos, pero puede ser que en el futuro el administrador decida proteger otras redes (a mas del backbone) con el mismo host bastion utilizado para el firewall externo; entonces necesitara mas de dos interfases.

5.2.1.5. Soporte

El soporte constituye un aspecto secundario dentro de la selección pero es importante ya que en caso de que se den problemas en el firewall, las personas capacitadas y con experiencia seran de mucha utilidad. Dentro del soporte a usuarios se analizaran los siguientes aspectos

- **Soporte local:** ¿Quiénes son los soportes autorizados para el producto?, ¿En que lugares han instalado el producto?, ¿Tienen experiencia como soporte autorizado del producto?
- **Soporte externo:** ¿Existe soporte a nivel de Latinoamerica?, ¿Existe una línea de soporte a traves de Internet?

5.2.1.6. Garantía

Para la garantia es necesario analizar dos aspectos tanto para software como hardware:

Tiempo de garantia: Mientras mayor tiempo de garantia ofrezcan mejor sera.

Confiabilidad del distribuidor: Es deseable que sea una empresa responsable la que distribuye el producto.

Aiios de permanencia en el rnercado: La cantidad de años que tenga un distribuidor indica el grado de experiencia.

5.2.1.7. Costo

El costo es el ultimo factor que interviene en la evaluación, no porque se considere menos importante, sino porque no se pueden disponer multiples criterios para evaluarlo. Simplemente

la primera opción la tendra el de menor costo. El costo tiene que detallarse en cuanto a lo que respecta al hardware como al software.

5.2.2. Evaluación

La evaluación se concentrara en 3 fases. La primera fase se basara en las caracteristicas de protección del firewall. Si un firewall no cumple con los requerimientos mínimos de seguridad de la ESPOL, sera descartado. Si el firewall cumple con los requerimientos, sera una alternativa potencial.

En la segunda fase se someterá a los productos firewalls (los descartados y los no descartados) a la prueba de rendimiento. A traves de un cuadro comparativo se podrán apreciar los diferentes firewalls en acción. Se reitera una vez mas, que esta medida no es absoluta, no identifica al firewall, tan solo es para efectos de comparacion.

En la tercera fase, se analizaran los aspectos denominados secundarios. Como son: interfase, plataforma, soporte, garantia y costos.

5.3. Firewalls a evaluarse

Los productos de firewalls escogidos para evaluar pueden ser categorizados en publicos, aquellos productos gratuitos disponibles en Internet, y los productos privados o comerciales, aquellos distribuidos por empresas y que tienen un costo.

Dentro de la categoria de software de firewalls publicos a evaluar se encuentran:

- SINUS o SF version 0.2.9, http://www.switch.edu/
- IPFWADM version 1.2.0, http://www.xos.nl/
- FWTK (Firewall Toolkit, de Trusted Information System), http://www.tis.com/
- SOCKS version 5.0, http://www.socks.nec.com/

Cada uno de estos productos ha sido obtenido en Internet, compilado, instalado y configurado sobre una plataforma LINUX (Red Hat 4.0). Toda la informacion que se dispone de estos firewall fue hallada tanto en los textos guías como en Internet.

En la categoria de productos de firewalls privados se encuentran:

- Firewall-? version 2.1 de Checkpoint, http://www.checkpoint.com/
- Secured Network Gateway version 2.2 de IBM, http://www.ibm.com/

Solo del primer producto se pudo obtener los instaladores. Se instaló en una plataforma Solaris 2.5 con el mismo hardware de los firewalls publicos. Lastimosamente Firewall-1 no tiene instaladores para Linux, es por esta razon que se eligio una plataforma UNIX estandar como Solaris. El firewall de IBM fue estudiado a traves de sus especificaciones y caracteristicas tecnicas halladas en las páginas de los web sites de IBM y de NCSA (National Computer Security Association) y de revistas tales corno: Data Comunications y Network Computing.

Antes de evaluar cada una de estas alternativas, se daran a conocer aspectos importantes de cada uno a fin de familiarizarse con la informacion disponible. De cada firewall se analizara la tecnologia que utiliza (filtradores de paquetes, sistemas proxies o ambos), que es lo que ofrece, como funciona y un ejemplo de configuracion.

5.3.7. *Firewalls publicos*

5.3.1.1. SINUS

SINUS es un programa experimental academico del instituto federal de tecnologia de Zurich que utiliza la tecnologia de filtraje de paquetes.

El programa fuente disponible en Internet solo es valido para una plataforma Linux, ya que el origen de este programa es academico y experimental.

El firewall SINUS (tambien llamado SF) comprende:

- un lenguaje de configuracion propio y sencillo
- implementación de reglas dinamicas
- capacidad de registro de acciones
- capacidad de alerta
- filtración de protocolos: RIP, FTP, ICMP, IGMP, UDP y TCP

Basicamente este producto opera en base a:

- Un usuario y grupo <<firewall>> que debe ser creado por el administrador en los archivos /etc/passwd y /etc/group respectivamente.
- Un modulo llamado <<sfc>> que es creado al compilar el código fuente, el mismo que debe ser añadido al kernel del sistema operativo.
- Un demonio llamado <<sf>> que debe ser ejecutado una vez que se insertó el modulo anterior. Es aconsejable que este demonio se ejecute al momento de iniciar el sistema.
- Un archivo de configuracion llamado <<firewall.conf>> donde se programan las reglas que reflejen las politicas de seguridad.

- Un archivo de log llarnado <<firewall.report>> donde se respaldan todas las acciones que se prograrnaron en el archivo firewall.conf.

El archivo de configuracion (firewall.conf) cornprende tres partes:

- Seccion de configuracion: contiene toda la inforrnacion de la topologia interna de la red
- Seccion de reglas: contiene las reglas de filtración de paquetes
- Sección de notificacion: especifica lo que tiene que hacer el dernonio del firewall en caso de que coincida con una regla de filtración.

Ejemplo de configuracion de reglas:

Seccion de configuracion interna, se pueden especificar tanto rnaquinas como redes internas.
Además, detallar la direccion e-mail a la cual se quiere enviar los reportes de alertas a peligros.

setup

internalnets 193.194.195.0 #red interna 193.194.195.0

mail–default "root@firewall.espol.edu.ec" # direccion e-mail por defecto

#sección de reglas en las que *se* perrnite, bloquea o rechaza conexiones.

rules

accept tcp from 192.188.59.6 port 1024..6000 to 192.188.59.3 port 21 notification_level 1;

#Esta regla especifica se acepte una conexión TCP desde una direccion 192.188.598.6, cuyo
puerto es mayor que 1024 y menor que 6000, hacia la direccion 192.188.59.3 con puerto 21
y un nivel de notificacion 1 (detallado en la sección de notificacion).

#Sección de notificacion, se especifican los niveles de notificacion.

notification

level 1: #archiva la acción, envía un #mensaje a la dirección de # defecto y ejecuta un #comando

message “sesion entrante FTP al goliat.espol.edu.ec” #mensaje aparece en el archivo de log

mail

exec ifconfig eth0 down # desabilita la interfase

end #marca el final del archivo de #configuracion.

5.3.1.2. IPFWADM

IPFWADM version 1.2.0 es un filtrador de paquetes que sirve para administrar los servicios de firewall que ofrece el kernel de Linux version 1.2.1. Este sistema operativo guarda en su kernel un modulo de firewall que se habilita al momento de instalarlo.

IPFWADM version 1.2 reemplaza al modulo de firewall llamado IPFW, que presentaban versiones anteriores de kernels. IPFWADM fue realizado para ser mas completo y de mas facil configuracion que IPFW.

Este producto de firewall ofrece las siguientes caracteristicas:

- un lenguaje de configuracion propio
- capacidad de registro de acciones
- filtración de protocolos:ICMP, UDP y TCP

- capacidad de traducir direcciones (solo con los protocolos TCP y UDP en sesiones salientes).
- reglas de configuracion que incluyen direcciones y nombres (DNS)

IPFWADM trabaja con un modulo del mismo nombre ya insertado en el kernel del sistema operativo. El demonio ipfwadm se lo puede iniciar manualmente o al inicio del sistema. Lo mas recomendable es configurar un archivo cualquiera con todas las reglas del filtración y ejecutarlo cuando se inicia al sistema.

Reglas de configuracion

La sintaxis de las reglas de configuracion en este firewall se asemejan a la sintaxis de comandos en Unix.

Ejemplo de configuracion de reglas:

```
# Enviar el correo electronico al servidor interno
ipfwadm -F -a accept -P tcp -S 0.0.0.0 1024:65535 -D 192.188.59.325
# opcion -F: para activar el modo de operación de envío
# opcion -a accept: añade esta regla al kernel y acepta la siguiente conexión
# opcion -P tcp: para especificar el tipo de protoclo
# opcion -S: para especificar la fuente del paquete y los puertos
# opcion -D: para especificar el destino del paquete y los puertos

# Enviar el correo electronico a servidores externos con las mismas especificaciones que la
# regla anterior
ipfwadm -F -a accept -P tcp -S 192.188.59.3 25 -D 0.0.0.01024:65535
```

```
# Enmascaramiento de la red interna
ipfwadm -F -a accept masquerade -S 192.188.59.0 -D 0.0.0.0
# opcion -F: para activar el modo de operación de envio
# opcion -a accept: añade esta regla al kernel y acepta la siguiente conexión
# opcion masquerade: para enmascarar o traducir las siguientes direcciones
# opcion -S: para especificar la direccion fuente a enmascarar y el servicio
# opcion -D: para especificar la direccion destino enmascarada
```

5.3.1.3. FWTK

El FWTK (Firewall toolkit) es un conjunto de programas y practicas de configuracion para facilitar la construcción de firewalls para Internet. Se trata de un compendio de servidores proxy de varios tipos que funcionan a traves de procedimientos modificados. El objetivo de este producto es usar programas pequeños por separado con un archivo de configuracion en comun.

Para ejecutar este producto hay que seguir los siguientes pasos:

- Editar el archivo /etc/inetd.conf desabilitando todos los servicios estandares. Matar el proceso inted anterior y habilitar el nuevo proceso inetd habilitando los servidores proxy.
- Desabilitar la capacidad de envio (IP forwarding) del host
- Configurar los servidores proxy a traves del archivo <<netperm-table>>

El archivo de configuracion <<netperm-table>> comprende los siguientes servicios:

- **Smap, servicio de SMTP: El** protocolo SMTP es implementado utilizando dos herramientas: smap y smapd, cliente y servidor respectivamente (ver sección **4.4.2.5.** Configuracion de servicios de Internet). El programa smap es el cliente que acepta los mensajes de una red y los envía al disco para una posterior entrega a los directorios de los usuarios. El

smap esta diseñado para correr como un proceso sin privilegios aplicando el chroot, es decir previene de potenciales riesgos hallados en el Sendmail. El smapd es el servidor que se encarga de revisar periodicamente la cola de mensajes para entregar aquellos que han sido almacenados [SIYA95].

- **Proxy FTP (ftp-gw):** Este servidor proxy utiliza procedimientos modificados. Es ejecutado cuando recibe un requerimiento en el puerto FTP del firewall. El servidor proxy ejecuta un prograrna que restringe los comandos que habitualmente pueden ejecutar un demonio ftpd (mkdir, remove, put, etc). Ademas el servidor ftp-gw puede:
  - restringir el acceso en base a usuarios y direcciones
  - restringir el acceso a ciertos archivos y ejecucion de comandos del sistema (chroot)
  - autenticar a usuarios
- **Proxy Telnet y Rlogin (tn-gw, rlogin-gw):** De igual manera que el proxy FTP, los servidores Telnet y Rlogin tienen el mismo alcance, y modo de operación.
- **Proxy HTTP y Gopher (http-gw):** Este programa soporta clientes modificados o procedimientos modificados. Tiene el mismo alcance que los servidores proxy anteriores. Ademas, al recibir un requerimiento de una sesion HTTP tambien examina las reglas de configuración del proxy FTP. Para usarlo con clientes modificados tales como Netscape o Mosaic, es necesario agregar la dirección del proxy en la especificacion del URL.
- **Proxy X Windows (x-gw):** Este programa permite una interface a nivel de usuario de X Windows que opera sobre el proxy tn-gw o rlogin-gw. Este proxy funciona dejando que los clientes comiencen una sesion desde otros hosts al programa X Windows de un sistema interno.
- **Proxy plug-gw:** Se trata de un proxy genérico que puede personalizarse para cualquier servicio de Internet. El servicio mas utlizado con este proxy genérico es NNTP.
- **Servidor de autenticacion:** FWTK provee de algunos mecanismos de autenticacion. Este servidor mantiene una base de datos de usuarios, guardando la siguiente información: nombre,

grupo, cuenta y la ultima autenticacion exitosa (ultima contraseña). Soporta algunas plataformas para la autenticacion entre ellas: userID, S/Key, SecurID, SNK004 (ver secciones 5.2.1.1. Seguridad, 3.7.1. Autenticacion).

- **Wrapper Netacl:** Este wrapper es utilizado para proteger al servidor firewall (ver sección 3.4. Host bastion). Se maneja en base a nuevos demonios para todos los servicios en lugar de los tradicionales. A traves del archivo netperm-table se configuran los servicios y listas de acceso en base a direcciones IP.

FWTK además, posee algunas herramientas administrativas:

- **portscan:** Lista los puertos (servicios) disponibles en cualquier maquina interna. Esto es un mecanismo que le permite al administrador observar que puertos están disponibles en sus sistemas.
- **netscan:** Es un programa que permite ejecutar el comando ping para saber que hosts estan "vivos" en la red interna.
- **reporteador:** A traves de syslog.conf el FWTK puede archivar todo tipo de información que pasa por el proxy: usuarios, servicios, direcciones, etc. Además, permite obtener reportes por aplicaciones, por ejemplo del servidor de autenticacion todas las personas autenticadas y no autenticadas, etc.

Ejemplo de configuracion de reglas

Para cada proxy existen reglas particulares de configuracion, para efectos de este ejemplo se tomara la configuracion para el proxy FTP:

```
ftp-gw: denial-msg          /usr/local/etc/ftp-deny.txt
# esta línea permite presentar un mensaje de negación del servidor proxy al usuario
ftp-gw: welcome-msg         /usr/local/etc/ftp-welcome.txt
```

esta linea permite presentar un mensaje de bienvenida del servidor proxy al usuario

ftp-gw: timeout 3600

esta linea permite establecer el tiempo que debe durar la conexion al servidor proxy

ftp-gw: permit-hosts 206.72.133.* -log

esta linea permite el acceso al servidor proxy desde cualquier maquina de la red 206.72.133.*

5.3.1.4. SOCKS

SOCKS es un sistema proxy genérico que se coloca en un host bastion y que comunica a todos los usuarios internos con Internet. Al tratarse de un proxy genérico, SOCKS utiliza clientes modificados en lugar de procedimientos modificados.

SOCKS consiste de dos partes:

Servidor SOCKS: Conjunto de programas servidores que se ejecutan en un host que puede comunicar directamente a una red con Internet (host bastion).

Programas **clientes:** Conjunto de programas clientes especiales que conocen como conectarse con el servidor SOCKS en lugar de enviar directamente los requerimientos a Internet.

El cliente SOCKS basicamente reemplaza las llamadas de las funciones sockets: connect( ), getsocketname( ), bind( ), accept( ), listen( ) y select( ), con su propia version de las mismas. Cuando un cliente modificado envía un requerimiento, este busca al servidor SOCKS, el cual recoge toda la informacion que es enviada a traves de las funciones sockets. En base a la informacion suministrada al servidor este decide, segun las politicas de seguridad, si establece o no una conexion con Internet.

La version de SOCKS 5.0 trabaja a traves de dos archivos de configuracion: <<socks5.conf>>, para la configuracion del servidor y <<libsocks5.conf>> para la configuracion de los clientes modificados. Estos dos archivos son creados por el administrador luego de haber examinado los manuales de configuracion disponibles con el programa.

El servidor proxy de SOCKS ofrece:

- Filtración por usuarios, por direcciones IP y por puertos.
- Autenticacion de usuarios para servicios entrantes
- Ruteo para diferentes direcciones en caso de maquinas que utilicen diferentes interfases.
- Control de comandos que pueden ejecutar los usuarios autorizados.

El cliente del SOCKS o tambien llamado cliente SOCKS - ified ofrece dos tipos de conexiones: directa, cuando la conexidn se establece directamente con el servidor real sin que el proxy la examine y la conexidn proxy, cuando es examinada por el proxy.

Reglas de configuracion

Ejemplo de configuracion del archivo socks5.conf:

permit gmazzari, mocana 192.188.59.3 255.255.255.255 192.188.59.2 255.255.255.255. eq 25

Con esta regla se esta permitiendo que los usuarios gmazzari y mocana puedan conectarse desde la direccion 192.188.59.3 a la direccion 192.188.59.2 via e-mail (puerto 25).

deny monsalve 192.188.59.3 255.255.255.255 0.0.0.0. lt 1023

En esta regla se niega la posibilidad que el usuario monsalve desde la maquina 192.188.59.3 accese a cualquier otra red utilizando los puertos menores a 1023.

Ejemplo de configuracion dei archivo libsocks5.conf:

Esta confiyuracion varía dependiendo del programa cliente, sin embargo el estandar es asi:

sockd @=david.espol.edu.ec 0.0.0.0 0.0.0.0

Con esta regla se establece que todos los usuarios del programa cliente que quieran conectarse a cualquier red, tienen que pasar por el servidor socks david.espol.edu.ec.

direct grnazzari 192.188.59.3 255.255.255.255 0.0.0.0

En esta regla se especifica que el cliente gmazzari desde la dirección 192.188.59.3 puede accesar a cualquier red sin pasar por el proxy.

5.3.2. Firewalls privados o no publicos

5.3.2.1. FireWall-1

FireWalt-1 de Checkpoint es un firewall que combina las ventajas de la filtracion de paquetes con las ventajas de los sistemas proxy. La filtración de paquetes examina la información (cabeceras) de todas las capas desde la capa de red hasta la capa de aplicacion. Los sistemas proxy para proteger a los servicios entrantes mediante autenticacion y encriptacion. Checkpoint, la empresa creadora de este firewall, denomina a esta tecnica "Tecnica de inspección total multicapa".

Firewall-1 esta disponible en diversas plataformas de sistemas operativos. Inicialmente fue diseñado para sistemas Unix estandares y luego llevado a NT.

Firewall-I ofrece:

- **Ambiente cliente/servidor para la administración:** Desde cualquier maquina de la red se puede administrar al firewall a traves de un programa o modulo especial colocado en el cliente.
- **Filtración de conexiones por protocolos, direcciones IP y por usuarios:** Como un filtrador de paquetes, Firewall-1 puede filtrar en base direcciones IP y protocolos.
- **Autenticacion para los usuarios de los servicios Telnet, FTP, HTTP:** FW-1 reemplaza los demonios estandares de FTP, Telnet y HTTP con unos demonios especiales. Estos demonios se ejecutan una vez que el inicio de sesión es permitido, luego estos demonios se encargan de levantar al servidor de autenticacion.
- **Autenticacion para clientes (aplicaciones):** Este mecanismo provee autenticacion por aplicacion. No existe necesidad de modificar a la aplicacion. El administrador configura cuales son los servicios (aplicaciones) disponibles, que dias, que horas, y cuantas sesiones al mismo tiempo pueden ser permitidas.
- **Encriptación entre nodos. (VPN, Virtual private net):** Firewall-1 se introduce al termino de redes virtuales privadas, que en realidad significa disponer de Internet como una red privada en donde el trafico de informacion entre redes privadas este a salvo. Para esto los firewalls tienen que poseer mecanismos de encriptacion. Firewall-1 utiliza esquernas de encriptacion DES, RSA, (ver sección 3.7.2. Encriptacion) FWZ1 (esquema propio de firewall-1 que se basa en el algoritmo de Deffie-Hellman) [SIYA95].
- **Traduccion de direcciones IP:** Firewall-1 esta en capacidad de traducir direcciones IP internas por cualquier otra dirección a fin de proteger los recursos internos.
- **Encriptacion en conexiones remotas (dial-up):** Protege la informacion en conexiones remotas entre un usuario (administrador) y el firewall a traves de la encriptacion de datos.
- **Interfase grafica para la configuracion:** Firewall-1 introduce un propio lenguaje visual para la configuracion de las reglas que reflejaran las politicas de seguridad.

- **Modulo para manejar ruteadores:** Este producto incluye un módulo para fortalecer las reglas de configuración en los ruteadores de una red. Trabaja solo con ruteadores Cisco y Wellfleet, no posee capacidad para rnanejar a otros ruteadores.
- **Capacidad de registro y alarma a tiempo real:** La informacion que registra es en base al tiempo, protocolos y servicios, acciones tomadas (rechazar, aceptar, bloquear, encriptar), fuentes y destinos, usuarios conectados, longitudes de los paquetes, claves de encriptacion y nombres de usuarios.
- **Administración centralizada:** Esta capacidad le permite a la organización, configurar y adrninistrar todas las políticas de seguridad de multiples servidores (hosts) a traves de una estacion centralizada. Esto elimina la necesidad de configurar cada servidor independientemente.

Arquitectura interna

La tecnica de inspección total multicapa establece que las decisiones de control deben ser tomadas en base a lo siguientes factores:

- **Comunicacion:** Toda la inforrnacion desde la capa IP hasta la capa de aplicacion.
- **Comunicacion de estado derivado:** No es suficiente examinar los paquetes aisladamente. Es necesario registrar la informacion derivada de las comunicaciones pasadas para saber si la conexion actual es valida. Por ejemplo, cuando se utiliza el protocolo **UDP,** es necesario verificar si la informacion del paquete actual entrante coincide con la informacion del paquete pasado saliente. (ver capitulo No. 3, filtraje de paquetes).
- **Aplicaciones de estado derivado:** La informacion derivada de las aplicaciones anteriores en una conexion. Por ejemplo, un usuario previamente autentificado puede accesar solo a los servicios autorizados.

- **Manipulación de información:** La evaluación de todas las expresiones basadas en todos los factores anteriores

Funcionamiento

Basicamente FireWall-1 se maneja a traves de dos modulos:

1. Modulo de control
2. Modulo firewall

Estos modulos pueden residir en el mismo host o por separado, es decir, operan independientemente. Si los dos son colocados en diferentes maquinas, la comunicacion entre estos es autentificada por razones de seguridad.

Modulo de control

El modulo de control es el encargado de la adrninistracion y configuracion del firewall. Incluye el GUI (Graphical user interfase) y un submodulo de administracion. El GUI es la interfase final con el usuario y el submodulo de administracion es el encargado de manejar las reglas de configuracion, usuarios, servicios, etc.

El modulo de control es implernentado en un modelo cliente/servidor. El cliente interactua con el usuario via el GUI para manejar al servidor de administracion, el cual interactua con el submodulo de administracion descrito anteriormente.

Modulo de firewall

Este modulo es el que se encarga de ejecutar todas las reglas configuradas en el modulo de control. Comprende basicamente programas (demonios) que se ejecutan cuando ingresan o egresan paquetes en el firewall.

En este modulo se aplica la tecnica de inspección total multicapa, en la que se analizan toda la informacion del paquete y se registra la informacion de estado derivado de las conexiones.

Dentro de los aspectos del modulo del firewall se encuentran:

- Objetos de red
- Políticas de seguridad
- Base de reglas
- Servicios
- Monitor de estado

Objetos de red

En el ambiente de Firewall-I todo se define como objeto. Por ejemplo, hosts, redes, servicios y usuarios, Cada uno de estos objetos tiene su conjunto de atributos: direcciones de red, mascara, etc. Algunos necesitan ser especificados por el administrador y otros son extraídos desde las bases de datos de la red: arhivos de hosts y redes, NIS (Network information services), DNS, etc. Los agentes SNMP son usados para extraer informacion adicional incluyendo la configuración de interfases de red de hosts, ruteadores y compuertas (gateway).

Politicas de seguridad

Las politicas de seguridad estan definidas en terminos de hosts, servicios, usuarios y las reglas que gobiernan las interacciones entre ellos. Una vez que los objetos de red han sido verificados, para instalar las reglas, Firewall-1 permite generar un codigo especial llamando "codigo de inspeccion", el cual puede ser instalado en cualquier host donde sea necesario enforzar las politicas de seguridad. El codigo de inspeccion o INPECT es muy entendible en formato ASCII y tambien puede ser instalado directamente usando un editor de texto.

Base de reglas

Una base de reglas es un conjunto ordenado de reglas que definen una política de seguridad especifica. Una regla describe una comunicacion en terminos de su fuente, destino, servicio, acción a tomar (aceptar o rechazar) y el registro de información.

Servicios

Firewall-1 define todos los servicios conocidos y usados en las politicas de seguridad. Todos los servicios son examinados y controlados, aun aquellos que no estan definidos. Dentro de los servicios definidos se encuentran:

- Servicios estandar arpa: Telnet, FTP, SMTP, etc.
- Servicios remotos: rlogin, rsh, rftp, etc.
- Protocolos avanzados como HTTP, Gopher, Archie.
- Servicios IP: ICMP, RIP (Routing Internet protocol), SNMP, etc.

Los nuevos servicios pueden definirse en base a los siguientes protocolos: TCP, UDP, RPC, ICMP, Otros

Monitor de Estado

Este producto dispone de un visor o monitor de todos los modulos firewalls instalados a lo largo de una red. Este visor presenta estadisitcas de todos los paquetes recibidos en los modulos, cuales han sido rechazados y cuales aceptados.

5.3.2.2. SNG (Secured network gateway) de IBM

SNG es un producto de firewall que combina las tecnologias de filtraje de paquetes y sistemas proxy, pero por separado; es decir, posee un modulo de filtración y un modulo de proxies. Además agrega caracteristicas de redes privadas virtuales, autenticación y translacion de direcciones, entre otras.

SNG trabaja sobre una sóla plataforma de hardware: servidor Risc 6000 con sistema operativo Unix AIX.

Observando en general las caracteristicas ofrecidas por este firewall:

- **Filtraje de paquetes:** En base a direcciones IP y puertos tanto fuentes como destinos. La version beta 3.01 ofrece filtros por dias y horas .
- **Servidores proxy:** Para las aplicaciones estandares mas populares en Internet, tales como Telnet, FTP, HTTP, Real Audio, etc. Contiene servidores a nivel de circuito (genericos) y a nivel de aplicacion.
- **Autenticacion:** Con varios mecanisos de autenticacion como: SecurID, S/Key, etc. (ver secciones 3.7.1. Autenticacion y **5.2.1** _ Seguridad).
- **Encriptacion:** IBM introduce el concepto de redes privadas virtuales. Utiliza los esquemas de encriptacion **DES** y **RSA** (ver sección 3.7.2. Encriptacion)

- **Encriptacion en conexiones remotas:** De esta manera el firewall puede ser operado desde cualquier estacion en modo seguro.
- **Traduccion de direcciones IP:** Cambia las direcciones IP de los recursos de la red interna.
- **lnterfase grafica:** La version **2.2** ofrece la interfase grafica para el sistema operativo **AIX** (SMITH), pero las reglas de configuración son ingresadas como texto. La version beta 3.01 ya ofrece una interfase en HTML para que el administrador pueda cargarla en cualquier examinador (browser) de web.
- **"Hardening":** Proceso en el cual el firewall desinstala todos los servicios considerados peligrosos en el servidor firewall.
- **Capacidad de registro y alarma a tiempo real:** A traves de un registro de acciones en tiempo real en base a los usuarios, servicios, fecha y hora. Es capaz de notificar cuando suceda alguna acción sospechosa, previarnente determinada por el administrador. Además, puede ejecutar comandos o programas para hacer trampas para capturar a un posible atacante.
- **Servidor DNS:** Para uso de clientes externos, de esta manera el administrador puede esconder la información de la red interna
- **Manejador de correo:** SNG evita que haya contacto directo, via correo electronico, con los servidores internos.

Arquitectura interna

Basicamente SNG de IBM trabaja con las tecnologias de filtraje de paquetes y sistemas proxy. Sin embargo, no las combina, al contrario, las maneja como modulos que trabajan por separado aprovechando las ventajas que ofrecen cada uno de ellos.

La administración y los modulos que conforman al firewall estan centralizados en un solo punto, es decir en la maquina en donde se instala el producto.

En el siguiente gráfico se puede observar su diseño:

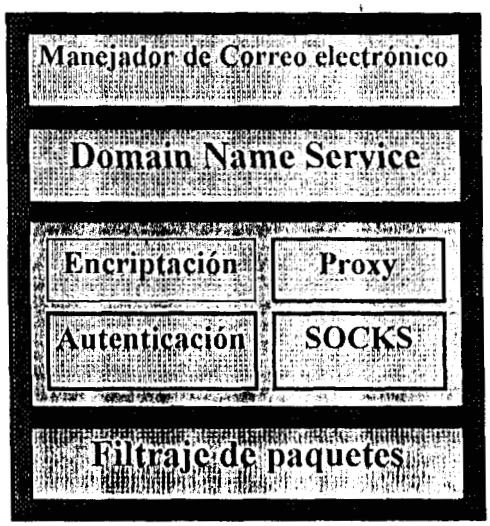


Figura No. 5-2 Diseño interno de SNG de IBM

Funcionamiento de SNG

Para entender el funcionamiento de este firewall es necesario conocer el alcance de todas sus características:

Filtraje de paquetes: Este es el mecanismo de protección inicial que brinda el firewall. De esta forma, a nivel de la capa IP (red) se filtran los paquetes en base a direcciones IP fuente y destino, protocolos, puertos fuente y destino, interfase de red.

Autenticación: SNG permite al administrador aplicar autenticación para los usuarios. Provee de algunos métodos de autenticación y la oportunidad de crear un propio método. Permite

implernentar la tecnica de contraseñas de una sóla vida, para que en caso de que una contraseña sea robada, no pueda ser utilizada.

SOCKS: SNG contiene el programa SOCKS (analizado anteriormente), el cual es un proxy genérico con clientes modificados. Principalmente SOCKS, por su concepción de proxy con clientes modificados, interconecta a los usuarios internos con Internet otorgando simplicidad y transparencia. Tambien brinda la ventaja de esconder las direcciones IP de los recursos de la red interna, ya sea por razones de seguridad o por que se tratan de direcciones no reconocidas por Internet. SOCKS es utilizado para brindar protección a los servicios salientes.

Servidores proxy: SNG a mas de SOCKS, contiene servidores proxy de procedimientos modificados: FTP y Telnet, los cuales se utilizan para sesiones entrantes a la red interna. Estos servidores proveen de autenticacion para los usuarios.

Encriptacion: IBM utiliza el concepto de redes privadas virtuales para generar canales seguros de datos a traves de redes consideradas inseguras (Internet). SNG utiliza esquemas estandares para permitir la interoperabilidad con otros firewalls y permite refrescar las claves de encriptacion dinamicamente para evitar el caso en que un atacante descubra el algoritrno de encriptacion y la clave. Para el caso de usuarios remotos, SNG provee un modulo que es instalado en la maquina cliente, para encriptar la información entre el usuario remoto y el firewall.

Servidor de control de dominio: SNG posee un servidor DNS (Domain name service) que solo brinda información a las maquinas de la red interna mas no a las maquinas de redes

externas consideradas inseguras. De esta manera SNG ofrece un servidor de dominio para la red interna.

Manejador de correo electronico: Llamado "Correo seguro" (SafeMail), se trata de un servidor de correo que no almacena el correo y no se ejecuta con privilegios de super usuario. Este servidor para correos salientes a Internet cambia la dirección del usuario por la del firewall. De esta manera los mensajes salientes a Internet pareceran salir del firewall mas no del servidor de correo interno. Soporta SMTP (Simple mail transfer protocol) y MIME (Multipurpose Internet mail extensions).

5.4. Evaluacion de Firewalls

La evaluacion de productos o paquetes de firewalls se divide en dos grupos, uno para los productos publicos y otro para los privados. La evaluacion termina con la selección del mejor producto de firewall para la ESPOL.

5.4.7. Evaluación de firewalls *públicos*

Dentro de la primera fase o fase de análisis de seguridad, los primeros paquetes de firewalls publicos fueron analizados de la siguiente manera:

5.4.1.1. Seguridad

a. Filtros a conexiones

Solo SINUS e IPFWADM utilizan filtradores de paquetes, por cuanto solo a estos es factible calificar en esta sección.

Características	SINUS	IPFWADM
Direcciones IP y puertos	Sí	Sí
Filtro en ambos sentidos	Sí	Sí
Aplicaciones basadas en TCP, UDP, ICMP	Sí	Sí
A conexiones: FTP, Telnet, HTTP	No	No
Por datos	No	No
Filtraje dinámico	No	No

Tabla XVI. Cuadro cornparativo de filtros a conexiones en productos de firewalls publicos

Las tres primeras caracteristicas son cubiertas por ambos firewalls. Estas tres caracteristicas marcan un enorme grado de seguridad; sin embargo, las tres ultimas tambien son necesarias. Estas tres ultimas caracteristicas hacen que ninguno de los dos productos cumplan los requerimientos minimos para lo que necesita la ESPOL.

b. Sisternas Proxy

En este caso tan solo FWTK y SOCKS utilizan servidores proxy, seria impractico en esta sección calificar a SF e IPFWADM ya que no los poseen. A continuación el análisis y comparacion de las caracteristicas de los sistemas proxy:

Caraterísticas	FWTK	SOCKS
Aplicaciones soportadas Telnet, FTP, HTTP	Sí, y tambien soporta rlogin, SMTP, Xwindow y plug para cualquier otra aplicacion	Sí, ademas soporta todas las aplicaciones que puedan ser socks-ified
Reglas por usuario, direcciones y puertos	No, solo permite o niega acceso en base al destino y al usuario	No porque no filtra en base a puertos fuentes
Manipular el ambiente de usuarios FTP, Telnet y HTTP	Sí, puede restringir el acceso a una rama de directorio del sistema (chroot).	Depende de la aplicacion cliente ya que trabaja con programas clientes moditicados
Programas modificados	Sí, cada usuario debe aprender los nuevos procedimientos para cada aplicacion. No es transparente.	La transparencia a los usuarios depende de los programas clientes.
Examinar datos	No	No

FWTK no puede tomar decisiones en base a direcciones IP y puertos fuentes como destinos, como lo hace SOCKS (excepto puertos fuente). FWTK utiliza procedimientos modificado, lo

cual representa una desventaja desde el punto de vista del usuario internos, en cambio SOCKS, al ser un proxy a nivel de circuito, hace que los procedimientos no cambien y sea transparente para el usuario interno. Una posible desventaja de SOCKS es que depende de la aplicacion cliente, ya que si esta no puede ser socks-ified, el firewall no funcionara. Ante las desventajas que presentan ambos sistemas proxy, ninguno de ellos esta en calidad de afrontar las necesidades de seguridad en la ESPOL.

c. Monitoreo: registro, **notificación y** reportes

Esta característica la poseen todos los firewalls, entonces se puede obtener un cuadro comparativo con la siguiente informacion:

Caracteristica	**SINUS**	**IPF**WADM	**FWTK**	**SOCKS**
Registro a tiempo real	Si	Si	Si	Si
Registro detallado: direcciones IP, usuarios, fecha y hora, servicios	No, ya que no registra usuarios	Registra direcciones, puertos, tamaño de paquetes, bit del ACK.	Si	Si
Notificación	Via e-mail y mensaje de alerta al archivo de registro	No	No	Si
Ejecucion de programas c trampas	Sí, puede ejecutar cualquier comando en el ambiente, además tiene una funcion de espiar para obtener informacion de atacante	No	smlO permite ejecutar programas en el servidor HTTP.	No
Reportes	No posee ninguna herramienta que genere consultas o reportes. Los datos se registran en un sólo formato.	No	No posee ninguna herramienta que genere consultas o reportes. Los datos se registran en un sólo formato.	Sí

Tabla XVIII. Cuadro comparativo de monitoreo en productos de **firewalls** públicos

Cada firewall presenta desventajas. Los firewalls que presentan mejores caracteristicas de monitoreo son FWTK, SF y SOCKS 'ya que poseen capacidad de registro a tiempo real y los datos registrados son bastante completos.

SF notifica situaciones peligrosas y puede ejecutar cualquier comando o programa (trampa) mientras que FWTK y SOCKS no poseen esas cualidades. Por lo tanto SF es la mejor alternativa en esta categoria; sin embargo, este no cumple con todas las expectativas de lo que se requiere.

d. Autenticacion

Estas son las caracteristicas de autenticación que poseen los firewalls públicos:

Caracteristicas	SINUS	IPFWADM	FWTK	SOCKS
Aplicaciones Telnet, FTP y HTTP	No	No	Sí	Sí
Esquemas soportados	Ninguno	Ninguno	contraseiias de texto, S/key, securid, snk	contraseñas de texto, Kerberos
Autenticacion en conexiones dial-up	No	No	No	No

Tabla XIX. Cuadro comparativo de autenticacion entre productos publicos

Tan solo los sistemas basados en proxy poseen mecanismos de autenticacion para las aplicaciones Telnet, FTP y HTTP. Sin embargo, ambos proxies no autentifican en conexiones dial-up. FWTK ofrece la mejor opción ya que soporta mas esquemas de autenticacion.

e. Encriptacion

Ninguno de los firewalls publicos soporta encriptacion. FWTK es un programa abierto a otros para poder colocar modulos de encriptacion, pero por sí solo no lo provee.

f. Traduccion de direcciones **IP** ,

Característica	SF	IPFWADM	FWTK	SOCKS
Aplicaciones: FTP, Telnet, HTTP, DNS SMTP, NNTP	No	Sí	Sí por su concepción de proxy.	Sí, por su concepción de proxy.

Tabla XX. Cuadro comparativo de traduccion de direcciones entre firewalls públicos

Los firewalls basados en sistemas proxy, por su concepción, pueden traducir o cambiar las direcciones IP internas. Las direcciones internas siempre se traducen por la dirección del servidor proxy; es decir, para los usuarios de Internet todos los paquetes de la red interna provienen del proxy. Esta es una gran ventaja sobre los filtradores.

IPFWADM tambien posee una capacidad llamada "IP masquerade", la cual permite traducir direcciones IP.

Conclusion de la **evaluación** de la categoria de seguridad (primera fase)

En cuanto a la protección que debe brindar un producto de firewall para la ESPOL, ninguno de los presentados aquí, por sí solos, representan una solución total.

Dentro de los firewalls basados en la filtración de paquetes, SF presenta la mejor alternativa ante IPFWADM. Ambos, dentro de las caracteristicas de filtros, ofrecen lo mismo; sin embargo, SF ofrece mejores capacidades de monitoreo, notificación y registro de acciones que IPFWADM.

Dentro de los firewalls basados en sistemas proxy, no existe una diferencia tangible que haga prevalecer a un ganador. A lo largo de esta primera fase, ambos firewalls han presentado

ventajas y desventajas. Al poseer mejores caracteristicas en autenticacion y la posibilidad de acoplar un sistema de encriptacion, FWTK se convierte en una buena alternativa para utilizarlo para los servicios entrantes que requieren autenticacion: Telnet y FTP. Debido a !a transparencia para los clientes que 'ofrece SOCKS, este puede controlar los servicios salientes que ofrece la ESPOL a sus usuarios.

Una solución parcial para la ESPOL podría ser la union del mejor filtrador de paquetes: SINUS con ambos proxies: SOCKS para servicios salientes y FWTK para servicios entrantes. Asi las desventajas de unos pueden ser solucionadas con la ventajas de otros. Aun asi, el producto firewall final tendría falencias y no serviria como una solucion total.

En la segunda fase de la evaluación se considera el rendimiento, en el cual se comparan transacciones con los productos de firewalls y sin ellos.

5.4.1.2. Rendimiento

A pesar de que todos los productos publicos de firewalls estan descartados en la primera fase, se evalua su rendimiento para efectos de comparacion. Siguiendo la metodologia explicada en la sección 5.2.1.2., prirnero se presentan los productos de firewalls basados en filtradores de paquetes y luego los sistemas proxy de acuerdo con la tabla XV:

Tran sacc.	Sin firewall				SF				IPFWADM			
	t seg	varian	tpm	Kb/s	t seg	varian	tpm	Kb/s	t seg	varian	tpm	Kb/s
5	7.65	0.71	39.2	228.6	9.32	0.33	32.1	187.8	8.78	0.197	34.1	199.3
10	14.5	0.23	41.3	241.3	17.0	0.305	35.1	204.8	16.56	0.152	36.2	211.3

Tran sacc.	Sin firewall				FWTK				SOCKS			
	t seg	varian.	tpm	Kb/s	t seg	varian.	tpm	Kb/s	t seg	varian.	tpm	Kb/s
5	7.65	0.71	39.2	228.6	13.26	0.089	22.68	131.9	12.87	0.057	23.3	147.4
10	14.5	0.23	41.3	241.3	21.28	0.051	28.19	164.4	19.80	0.157	30.3	176.7

Tabla XXI. Cuadro cornparativo de rendimiento entre firewalls publicos
Fuente Pruebas de rendirniento hechas por el autor de **la** tesis, Apendice B

Comparando los resultados de los firewalls con los resultados de las transacciones sin firewall, estos ultimos poseen un menor tiempo de retardo ya que no se cuenta con el retardo que introduce un firewall para tomar una decision (permitir o negar el acceso). Como se esperaba los filtradores de paquetes tienen un menor retardo con respecto a los sistemas proxy, ya que estos ultimos examinan los paquetes hasta la capa de aplicacion y por lo tanto demoran mas que los filtradores de paquetes para decidir si permiten o niegan una conexion.

Entre los productos orientados a sistemas proxy que han sido evaluados, el que mejor rendimiento presenta **es** SOCKS. Las razones por las cuales SOCKS presenta mayor rendimiento que FWTK son:

- El cliente **SOCKS** se comunica con el servidor a traves de sockets, los cuales envian la suficiente inforrnacion para que el servidor evalue y tome decisiones. El servidor no necesita examinar cada paquete para extraer informacion.
- FWTK es un proxy que utiliza procedimientos modificados, es decir el cliente debe primero manualmente conectarse al proxy antes de conectarse con el recurso deseado. El servidor

necesita exrnaminar cada paquete que le llega, sea externo o interno, para obtener información y tomar decisiones.

Entre los filtradores de paquetes SINUS e IPFWADM, este ultimo logro ser superior al SINUS con poca diferencia.

En la figura No. **5-2** se puede apreciar la grafica KB/s versus numero de transacciones. Los filtradores se acercan mas a la curva de rendimiento del sistema sin firewall (situación ideal). Los sistemas proxy se alejan mas de la situacon real, entre ellos SOCKS muestra mejor rendimiento.

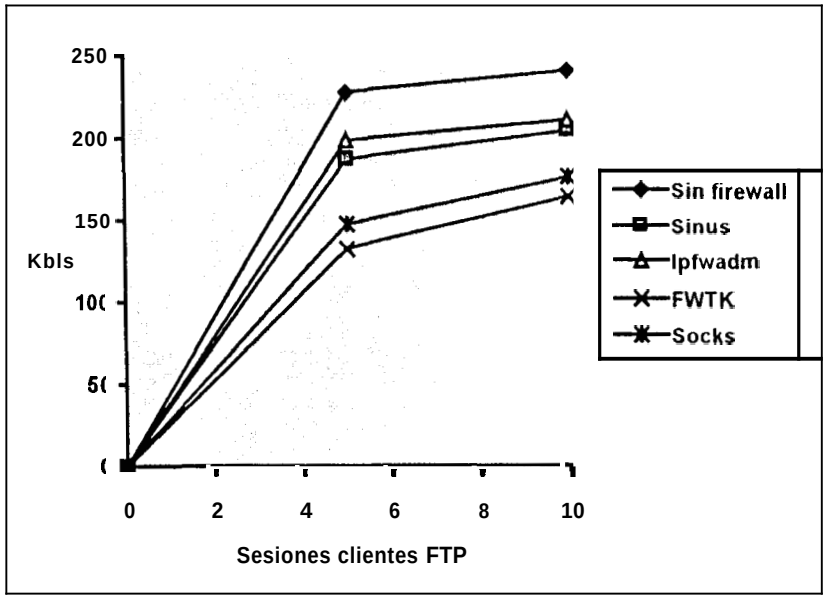


Figura No. 5-2 Cuadro de rendimiento de productos de firewalls publicos

Luego de observar el rendimiento de los productos de firewalls, se puede comprobar las conclusiones de la sección 5.2.1.2. Rendimiento. Todos los firewalls publicos no pasaron la primera fase, y en la segunda fase el firewall que mostro mejor rendimiento es IPFWADM

Dentro de la tercera fase de evaluación se encuentran los siguientes aspectos:

Interfase

Plataforma

Soporte

Garantía

Costos

Para los paquetes de firewalls publicos hay que tomar en cuenta las siguientes consideraciones:

- No tienen garantias
- Son gratuitos
- No hay soporte.

Por lo tanto no se puede evaluar estas categorias.

5.4.1.3 Interfase

Las caracteristicas de los productos de firewalls evaluados se presentan en la tabla XXII.

La interfase con el usuario que presentan todos los firewalls publicos evaluados es muy pobre. Las compilaciones de estos productos no son complicadas, dependen del sistema operativo y el hardware de la maquina donde se instalen, además de la pericia de la persona que los instala.

Tanto SINUS, IPFWADM y FWTK otorgan facilidad en el mantenimiento. Los dos primeros como filtradores de paquetes pueden brindar seguridad a nuevos servicios en base a los puertos que estos utilicen. FWTK ofrece un proxy genérico de procedimiento modificado que se puede adaptar a cualquier nuevo servicio. Sin embargo, la protección que ofrece este ultimo es muy básica, ya que no tiene el alcance que tiene un proxy a nivel de aplicación.

Característica	SF	IPFWADM	FWTK	SOCKS
Facilidad de instalacion	Se levanta el demonio e inserta un modulo en el kernel	Tiene que compilarse en el kernel de LINUX.	Modificar inetd.conf para levantar los demonios modificados	Sí, solo hay que ejecutarlo (levantar el demonio). Los clientes deben soportar SOCKS.
Facilidad de configuracion	Reglas en texto, son faciles de entender y manipular	Reglas con muchas opciones a traves de letras. (-o, -i, -v, etc), poco entendibles y dificiles de manejar	Reglas en texto con palabras que interpretan funciones. Son claras y bien definidas.	Reglas en texto, faciles de entender y manipular.
Mantenimiento	Sí puede brindar proteccion a un nuevo servicio basado en el puerto maneja	Si puede brindar proteccion a un nuevo servicio basado en el puerto que maneja	A traves del proxy generico plug-gw, puede brindar seguridad a cualquier servicio nuevo.	Depende, si el cliente soporta socks, se puede brindar proteccion, en caso contrario, no
Información disonible	Existe poca informacion. Los creadores disponen de un foro para que los clientes les notifiquen errores o consejos.	Solo se dispone de una pagina del manual en linea de LINUX. No existe mucha informacion	Si dispone informacion, pero es muy superficial. Para la configuración es necesaria mas informacion.	Si dispone informacion, al igual que FWTK, para la configuración deberia otorgar mas informacibn.

Tabla XXII. Comparación de interfase entre productos de firewalls públicos
Fuentes: Web sites de todos los productos

Para cada firewall, la informacion es escasa e insatisfactoria en lo que a configuracion de reglas se refiere. Solo SF y **SOCKS** poseen ejemplos de configuraciones de reglas, para FWTK e IPFWADM hay que probar cada regla para verificar lo que hace.

Existen foros y listas de mensajes, donde personas con experiencia en estos productos dart consejos de instalacion, configuracion y pruebas. La desventaja de esto es que no hay garantia de que los consejos y recomendaciones que brindan estas personas sean los mas adecuados. En la bibliografía se provee datos para accesar a estos foros y listas.

5.4.1.4. Plataforma

Caracteristicas	SF	IPFWADM	FWTK	SOCKS
Hardware/SO	SO: LINUX, Hardware: cualquiera que soporte LINUX.	SO: LINUX, Hardware: cualquiera que soporte LINUX.	SO: SunOS, Solaris, Solaris Intel, LINUX, SCO, BSDI, HP/UX, IBM/AIX, ULTRIX, CMU MACH, BSD/386. Cualquier hardware que soporte a estos sistemas operativos	SO: SunOS, Solaris, Linirx, SCO, BSDI, HP/UX, IBM/AIX, ULTRIX, CMU MACH, BSD/386, Windows NT. Cualquier hardware que soporte a estos sistemas operativos
Interfases de red	Maximo dos interfases. Soporta cualquier tipo de interfase que soporte LINUX.	Maximo dos interfases. Soporta cualquier tipo de interfase que soporte LINUX.	Soporta cualquier numero y tipos de interfase que soporten los SO's	Soporta cualquier numero y tipos de interfase que soporten los SO's

Tabla XXIII. Comparacion de plataformas entre productos de firewalls publicos
Fuente: Web sites de todos los productos públicos

La información de la plataforma de estos firewalls es bastante imprecisa. No existen requerimientos de memoria en el hardware, la capacidad en disco duro, interfases de red soportadas, etc. En mensajes de respuestas enviados al autor de esta tesis por parte de los diseñadores de cada uno de estos firewalls, señalan que las interfases de red soportadas por su producto dependen del sistema operativo sobre el que esta instalado. Entre las interfases de red mas populares que soportan los sistemas operativos aquí nombrados se encuentran: Ethernet, Token Ring, ATM y FDDI.

SF e IPFWADM son firewalls que se utilizan exclusivamente sobre LINUX, el cual es un sistema operativo cuyo origen es académico y experimental. Su principal ventaja es que es publico y puede ser instalado en cualquier PC con escasos requerimientos de memoria (16 MB). Sin embargo, no existe garantía ni soporte en caso de que se produzca alguna falla.

FWTK y SOCKS son los firewalls que mas variedad de plataformas basadas en UNIX ofrecen. SOCKS es el unico firewall que puede ser instalado sobre una plataforma Windows NT a mas de las plataformas basadas en UNIX.

Las otras categorías no se evalúan porque para los productos publicos en Internet, no hay garantia ni soporte y además son gratuitos.

5.4.2. Evatuacion de firewalls privados

5.4.2.1. Seguridad

a. Filtros a conexiones

Características	Firewall-1	SNG/IBM
Direcciones IP y puertos, fuentes y destinos	Sí	Sí
Filtro en ambos sentidos	Si	Si
Protocolos TCP, UDP, ICMP	Si	Si
A conexiones: FTP, Telnet, HTTP	Sí	No
Por datos	Si	No
Filtraje dinámico	Sí	No

Firewall-1 basa su seguridad en un filtraje de paquetes en la información de todas las capas de la arquitectura TCP/IP. No utiliza sistemas proxy, por lo que toda la seguridad que ofrece se encuentra dentro de estas características. Por otro lado, SNG posee filtraje de paquetes, pero basa mas su seguridad en sistemas proxy. La ventaja y desventajas que presentan ambos se remonta a la diferencia que presenta cada una de estas tecnologias (ver capítulo III)

Las tres primeras caracteristicas de protección que debe poseer un filtrador, las cumplen ambos firewalls. Firewall-1 es capaz de proteger las conexiones establecidas FTP, Telnet y HTTP debido a que:

- Examina la información de cada paquete concerniente a cada una de las capas de la arquitectura TCP/IP
- Ejecuta programas especiales para cada uno de estos programas.
- Tiene la capacidad de rnantener en memoria los últimos paquetes que fluyeron, a fin de crear nuevas reglas en forma dinámica. Por ejemplo, en el caso de paquetes UDP, Firewall-1 revisa que los paquetes UDP entrantes correspondan con los paquetes UDP salientes pasados. Con esta tecnica tambien protege a las conexiones FTP salientes, ver sección **4.4.2.5.**

Las caracteristicas del Firewal-1 hacen posible brindar seguridad a cualquier servicio sin necesidad de programas adicionales. El filtrador de SNG no posee estas capacidades ya que sólo filtra a nivel de la capa IP. Para controlar las conexiones establecidas SNG utiliza servidores proxy.

En la version 3.0 de Firewall-1, Checkpoint ofrece la capacidad de filtración de paquetes por datos; es decir, detectar virus, programas ejecutables, comandos, etc. En la version 3.1 beta de SNG, IBM tambien ofrece la capacidad de examinar los datos, pero a traves de los sistemas proxy.

b. Sisterna Proxy

Firewall-1 no posee servidores proxy, por lo que no entra en esta parte de la evaluación.

Soporta Telnet, I TF , I ITTF	No soporta HTTF , sólo Teln TF e

	Gopher y WAIS.
Reglas por usuario, direcciones y puertos	No.
Manipular el ambiente de usuarios FTP, Telnet y HTTP	Sí, puede restringir el acceso a una rarna de directorio del sistema (chroot).
Procedimientos modificados	Posee proxy transparentes, para los usuarios internos y no transparentes para los usuarios de Internet.
Examinar datos	No

SNG posee servidores proxy para los servicios Telnet y FTP. Para HTTP, IBM ofrece un proxy HTTP que viene con el sistema operativo AIX. Para los usuarios internos se provee de SOCKS, el cual es transparente y necesita de clientes rnodificados. Para los usuarios externos (Internet) se utilizan los servidores proxy a nivel de aplicacion con procedimientos modificados. Para conexiones basadas en UDP, **SNG** protege a estos servicios en base a los servidores proxy.

En el caso del servidor SOCKS, las reglas sí son determinadas en base a usuarios, direcciones IP y fuentes, destinos, y puertos. Pero en los servidores proxy rnodificados para los usuarios externos, las reglas solo son basadas por usuarios, los cuales son definidos por el administrador. Esta es la principal razon por la cual SNG se sustenta sobre un filtrador de paquetes ya que de esta manera puede controlar direcciones y puertos otorgando una mayor protección.

A cada usuario de una aplicacion entrante Telnet, FTP y HTTP se le puede restringir el acceso a deterrninados directorios del sistema, otorgando mas seguridad en el ambiente en que se ejecutan.

c. Monitoreo: registro, **notificación y reportes**

Esta caracteristica la poseen todos los firewalls, entonces se puede obtener un cuadro comparativo con la siguiente información:

[illegible]	Firewall-1	SNG / IBM
Registro a tiempo real	Sí	Sí
Registro detallado: direcciones IP, usuarios, fecha y hora, protocolos	Sí	Sí
Notificación	Via e-mail, ventanas de alerta.	Via e-mail, ventanas de alerta
Ejecucion de programas o trampas	Sí	Sí a traves de agentes SNMP. (Netview)
Reportes	Posee herramientas propias para generar consultas y reportes.	No posee herrarnientas propias, se respalda en DB2

En esta sección de monitoreo, ambos firewalls poseen las mismas capacidades. En primera instancia se podría pensar que como SNG se basa en proxies, el nivel de registro es mayor; sin embargo, Firewall-1 ofrece las mismas capacidades de registro.

La notificacion de sucesos sospechosos en tiempo real, para cualquiera de los dos productos, se hace por medio de mensajes de correo o a traves de ventanas de alerta con sonido incluido.

Firewall-1 posee la capacidad de ejecucion de trampas y generación de consultas y reportes por sí solo. En cambio SNG tiene que sustentarse en herramientas adicionales de IBM como Netview para crear trampas y DB2 para generar consultas y reportes. Esto es un factor de desventaja ya que si no se poseen estas herramientas adicionales, no se puede aprovechar todas las bondades que ofrece el firewall SNG. Para la ESPOL no representa desventaja ya que cuenta con estos programas adicionales.

d. Autenticacion

Características	Firewall-1	SNG / IBM
Aplicaciones Telnet, FTP y HTTP	Sí	Sí
Esquemas soportados	SecurID, Kerberos, S/key	SecureNet, SecurID, Generic autentication exit, userID
Autenticacion en conexiones dial-up	Sí	Si

Tabla XXVII. Cuadro comparativo de autenticacion entre firewalls privados
Fuentes: Web sites de ambos productas

Ambos firewalls presentan caracteristicas de autenticacion.

e. Encriptacion

Características	Firewall-1	SNG / IBM
Encriptacion firewall-firewall	Si	Sí
Encriptación en conexiones remotas	Si, los clientes (estaciones) deben tener Windows 95	No en la version 2.2. IBM lo esta ofreciendo en la versión beta 3.1
Esquemas soportados	**DES,** RSA, FWZI (esquema propio de Firewall-1)	RSA, DES

Tabla XXVIII. Cuadro comparativo de encriptacion entre firewalls pr ados
Fuentes: Web sites de ambos productos

Los dos firewalls ofrecen capacidades de encriptar la información que por ellos fluye. Primeramente los dos firewalls proveen encriptacion firewall-a-firewall, dando un canal seguro para los datos. Firewall-1 soporta los esquemas DES, SKIP y FWZ1, los dos primeros son estandares y el ultimo es un algoritmo propio de Checkpoint. En cambio SNG, provee RSA y **DES.** Todos los esquernas presentados (excepto FWZ1) son estandares y presentan buena operabilidad con firewalls de distintas marcas.

Otra opción importante es la que ofrece Firewall-1, consiste en encriptar la conexión entre el firewall y un cliente externo o remoto, de tal manera que el recipiente que debe desencriptar y encriptar sea un cliente normal (para Windows **95)** sin tener que utilizar otro firewall de por medio. SNG ofrece esta caracteristica en su version beta 3.1 con clientes Windows 95 y OS/2.

En conclusion final, ambos productos ofrecen similares caracteristicas de encriptacion.

e. Traduccion de direcciones IP

Esta caracteristica la presentan los dos firewalls. Firewall-1 puede cambiar cualquier direccion interna por cualquier otra direccion sin necesidad de usar sistemas proxy. **SNG,** en cambio utiliza a SOCKS y un manipulador de correo electronico.

Como se analizo anteriormente, **SOCKS,** por su concepción de proxy, traduce todas las direcciones de los clientes internos por la direccion del sewidor donde esta instalado. SOCKS no puede traducir las direcciones internas por otra que no sea la direccion del proxy, por lo que **SNG** no brinda la oportunidad al administrador de cambiar las direcciones IP por otras cualquiera. El otro mecanismo que utiliza **SNG** es un manipulador de correo electronico, el cual cambia la cabecera de todos los mensajes salientes a Internet que por el fluye. Esta medida es practica para organizaciones pequeñas, con pocos usuarios y con un sewidor de correo, pero en la ESPOL pueden existir n-sewidores de correo electronico con n-mensajes, y resultaria impractica esta medida ya que causaria un gran retardo en el firewall y por ende en el backbone.

La mejor opción la presenta Firewall-?, debido a que le brinda la oportunidad al adrninistrador de cambiar las direcciones IP de los recursos de la red interna por otras direcciones que no necesariamente tienen que ser la direccion IP del proxy.

5.4.2.2. Rendimiento

Para el caso de los productos de firewalls privados, no fue posible evaluar el rendimiento como se hizo para los firewalls públicos debido a que tanto el programa como la plataforma de SNG no estuvo disponible. La evaluación de rendimiento que se muestra en esta sección fue obtenido de una prueba de estres (saturación) que realizo los laboratorios NSTL (National Software Testing Laboratories) en dos ocasiones, la primera en 1995 y la segunda en 1997; y que luego fueron publicadas en la revista "Data Comunications" en marzo de 1.997.

Metodologia de pruebas en NSTL

La configuración de la red de pruebas es la siguiente:

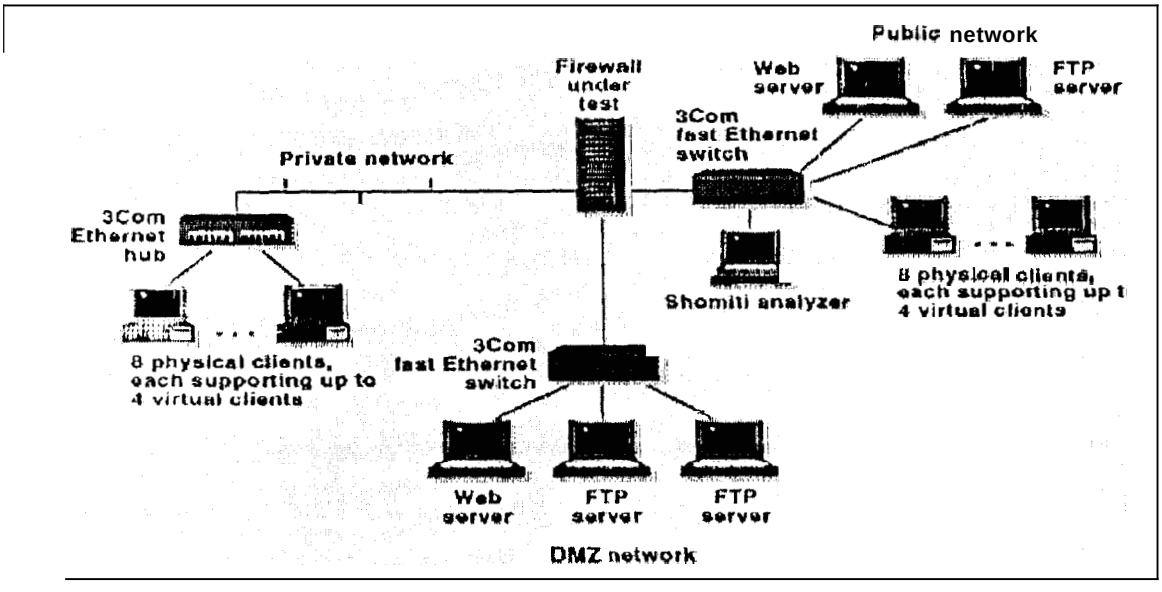


Figura No. **5-3 Configuración de pruebas de NSTL**
Fuente Data Communications. Marzo1997

En **la** figura No. .5-3 se observan tres redes: una externa o pública que simula a Internet, una perimetro (DMZ) y una interna. Para medir el rendimiento del firewall, los clientes internos (red interna) y externos (red externa) lanzan requerimientos a los servidores de la red perimetro.

Cada cliente fisico (maquina) soporta hasta **4** clientes virtuales **(4** requerimientos clientes), es decir que cada red (interna o externa) puede generar hasta 32 sesiones clientes.

Se genero trafico a traves de un programa especial elaborado por NTSL, en la que se podia variar el porcentaje de sesiones **FTP** y WWW. Se tomó registro del tiempo que tomó el firewall en procesar a 8, 16, **24, 32, 40** y **48** clientes virtuales. Este proceso se repitió 100 veces para luego obtener una tasa de transacciones por minuto como lo muestra en la figura No. **5-4** para la primera prueba en 1995 y una tasa de Bytes/segundo como lo muestra la figura No 5-5 para la prueba de 1997.

Es valido recalcar que las empresas surninistradoras de firewalls que concursaron dotaron del hardware y sistema operativo necesarios (los que recominedan para el normal funcionarniento de sus productos) para las pruebas, por lo que en realidad las transacciones por minuto obtenidas dependen del firewall y del hardware/sistema operativo que los distribuidores suministraron.

Resultados

Las curvas discontinuas significan que el firewall no pudo terminar su labor hasta las **48** sesiones clientes ya que en el punto de discontinuidad (ultimo punto) empezaron a perder las sesiones y estancarse.

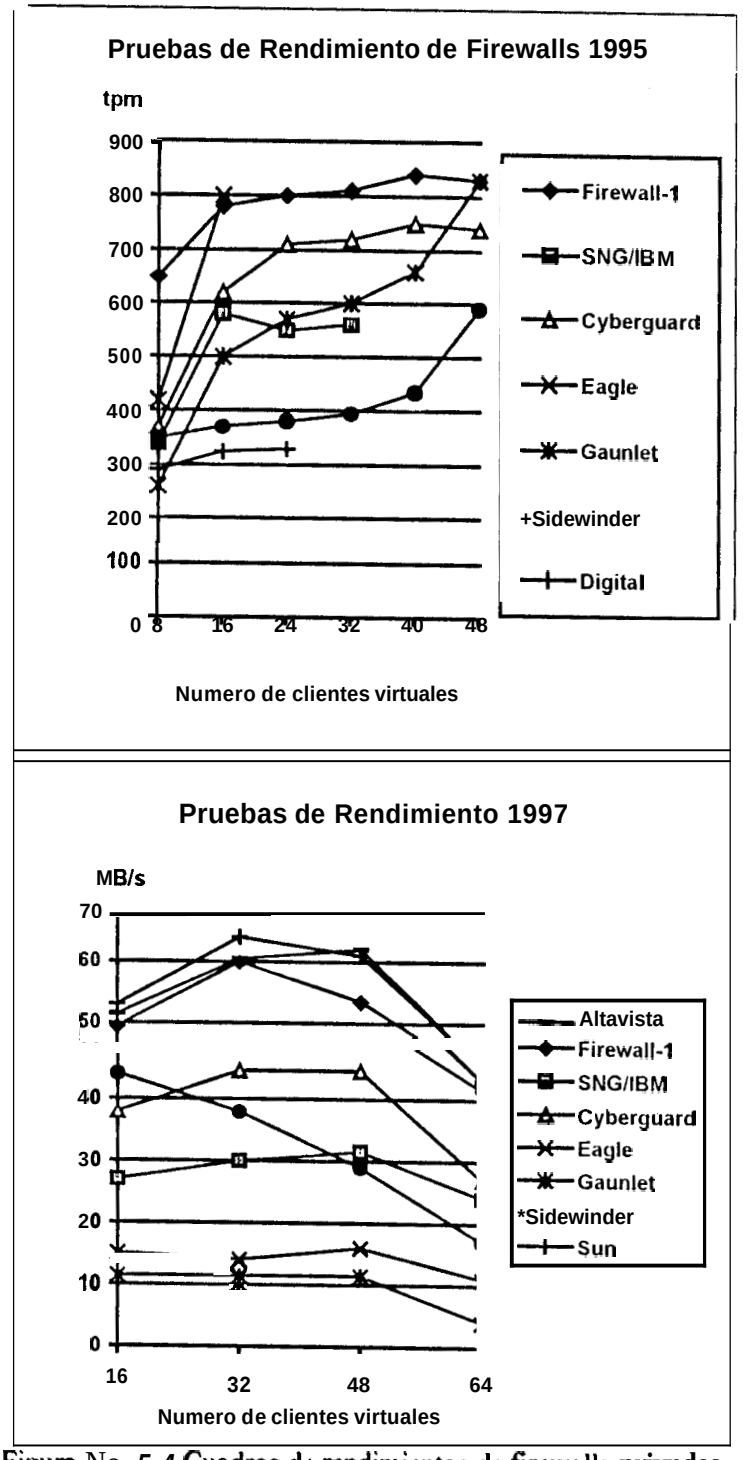


Figura No. 5-4 Cuadros de rendimientos de firewalls privndos
Fuente: Data Communications, noviembre/1995 y abril/1997

En la prueba de 1995, Firewall-1 gano el premio de "Top Performers" ofrecido por Data Communications por presentar el mayor grado de rendimiento entre todos los firewalls evaluados. En cambio SNG de IBM se presento en tercer lugar y no completo la prueba ya que soportó hasta 32 clientes virtuales.

En la prueba de 1997, ante la inclusion de otros firewalls nuevos en el mercado, Firewall-1 obtuvo un rnodesto tercer lugar entre 20 concursantes, mientras que SNG obtuvo un noveno lugar. Sin embargo, nuevamente el rendimiento de Firewall-1 fue superior al de SNG de IBM

El retardo de SNG se debe principalmente a que:

- Utiliza sistemas proxy, los cuales retardan mas el rendimiento como quedo demostrado en la evaluacion programas de firewalls publicos.
- Consume muchos recursos del sistema haciendolo retrasar.

El firewall Sun ofrecido por la Sun Microsystems como un equipo enteramente hardware que se debe colocar como ruteador entre la red interna e Internet. Especificamente se trata de un ruteador filtrador que permite o niega el acceso en base a ciertas politicas. No completa las caracteristicas de un filtrador para la ESPOL ya que no examina datos ni posee filtraje dinamico.

El firewall Altavista de la Digital Equiment es un producto basado en sistemas proxy. No completa todas las caracteristicas de los requerirnientos mínimos de seguridad para la ESPOL debido a que no tiene capacidad para examinar datos ni lo promociona en futuras versiones. Por esta razon no se lo incluye en la evaluacion

5.4.2.3. Interfase

Las caracteristicas de interfase en arnbos productos de firewalls son:

Caracteristica	Firewall-1	SNG / IBM
Facilidad de Instalacion	Sí, una sola instalación en modo texto. Se adueña de las interfases de red y desabilita todos los servicios por defecto.	Sí, puede ser en texto o gráfica. Posee "Hardening" para desabilitar todos los servicios y programas considerados peligrosos.
Facilidad de configuracion	La interfase es gráfica si se utiliza OpenWindows o Windows NT. Las reglas se configuran en base a objetos representados gráficamente y previamente ingresados. El ambiente es bastante amigable y entendible.	La interfase es gráfica si se utiliza SMIT de AIX. Las reglas para filtradores y proxies se configuran a través de menúes y el ingreso de las mismas es por texto. Existen opciones en las reglas que requieren de ayuda en línea.
Mantenimiento	Firewall-1 puede brindar seguridad a cualquier nueva aplicacion basada en TCP, UDP o RPC.	Para servicios nuevos se puede dar protección via filtraje de paquetes, pero no es eficiente (en el caso de UDP). Es necesario un servidor proxy nuevo para proteger eficienternente.
Informacion	Sí dispone de bastante inforrnacion	Sí, pero no se consiguio inforrnacion

Firewall-1 ofrece una instalacion y configuracion muy fácil e intuitiva. En la instalacion se siguen procedirnientos normales con bastante inforrnacion en cada paso; sin embargo, se requiere que la persona que lo instale tenga conocimientos del sistema operativo y sobre firewalls. La configuracion es a traves de graficos. Cada grafico representa a un objeto el cual tiene propiedades: nombre, direcciones IP, clasificación (host o gateway), modulo firewall, etc. En conclusion Firewall-1 ofrece un arnbiente rnuy entendible y amistoso.

De la instalacion y configuracion de SNG no hay mucha informacion por que no se adquirio el programa y el hardware para instalarlo. Con la inforrnacion de rnanuales y demostraciones se pudo observar que la instalacion no es complicada, es realizada en rnodo grafico (usando la herramienta de administración SMIT de **AIX)** y la navegacion de opciones es a traves de rnenues. Las configuraciones son separadas de acuerdo a la tecnologia: filtrador de paquetes,

SOCKS, sewidores proxies para Telnet y FTP, etc. El ingreso de reglas es en modo texto, algunos campos a llenar son confusos y requieren ayuda.

En terminos de mantenimiento, Firewall-1 por sus capacidades es capaz de brindar proteccion a cualquier nuevo sewicio de Internet. En cambio SNG brinda proteccion a nuevos servicios solo si estos no son basados en UDP, ya que para eso necesitaran un servidor proxy. Por esta razon IBM, por la compra de su producto, ofrece todas las versiones posteriores gratis, ya que estas actualizan los servidores proxy dependiendo de los nuevos servicios en Internet.

La informacion disponible sobre cada producto de firewall es abundante. Checkpoint e IBM ofrecen manuales de instalacion, configuración, pruebas y ejemplos. En este aspecto ambas empresas llenan las expectativas, en sus páginas de web ofrecen informacion para personas que tienen un nivel bajo de conocimiento en este tema.

5.4.2.4. Plataforma

Características	Firewall-1	SNG /IBM
Hardware/SO	**SO:** HP-UX, Solaris, SunOS, Windows NT, Solaris Intel, **AIX,** Windows 95 (cliente remoto). **Hardware:** Sun SPARC, Intel x86, HP-PA 9000, RISC 6000 **Memoria requerida:** 16 MB sobre la del sistema operativo.	**SO:** AIX **Hardware:** cualquier IBM RISC / 6000. **Memoria requerida: 64** MB incluido el sistema operativo
Interfases de red	Soporta un maximo de 16 interfases y pueden ser: Ethernet, Token Ring, FDDI, ATM, Fast Ethernet, 100VG-AnyLAN, serial up T1/E1, T3/E3, ISDN, Asynchronous.	Mínimo **2,** no existe informacion del maximo de interfases. Las interfases pueden ser: Ethernet, Token Ring, FDDI, ATM, Fast Ethernet, 100VG-AnyLAN, serial up T1/E1, T3/E3, ISDN, Asynchronous.

En esta sección se marca una diferencia notable. Ambos paquetes de firewalls soportan sistemas operativos UNIX y plataformas seguras en hardware, pero Firewall-1 ofrece diversidad

tanto de sistemas operativos UNIX como de hardware. En cambio IBM ofrece su producto para su sistema operativo y plataforma propia, no le da la oportunidad al administrador de elegir la plataforma. Adicionalmente Firewall-1 ofrece la posibilidad de ser instalado en otros sistemas operativos como Windows NT

5.4.2.5. Soporte

Características	Firewall-1	SNG / IBM
Soporte local:	Sí	Sí
Soportes autorizados	Distribuidores en Ecuador: MAINT y COMWARE (Firewall-1 para plataforma SUN).	IBM del Ecuador. Vende solución Hardware y software
Lugares donde han instalado	Han vendido el producto en BanRed, Banco del Pacifico, Banco Continental	Superintendencia de Compañias
Experiencia como soporte	Sí	Sí
Soporte externo	Brasil, Argentina, Venezuela, Chile	IBM Andino, IBM mundial

Tabla XXXI. Comparacion de soporte entre productos de firewalls privados
Fuente. Web sites de arnbos productos

Como se puede apreciar, ambos productos ofrecen soporte mediante personas expertas en el producto. En caso de ser necesario, poseen contactos con los distribuidores para traer a personas extranjeras para brindar soporte.

5.4.2.6. Garantía

Características	Firewall-1	SNG / IBM
Tiempo de garantía	Software: 3 meses Hardware: 1 año	Sofrware:No hay límite de tiempo. Hardware: 1 año
Confiabilidad del distribuidor	La empresa que distribuye a nivel mundial es Checkpoint. Actualn ente su producto abarca el 40% del mercado mundial.	IBM significa prestigio y garantía
Años de permanencia en el mercado	4 años	17 años

Tabla XXXII. Cuadro comparativo de garantía entre firewalls privados

Checkpoint es una empresa creada en 1993 y se dedica principalmente a proveer productos de seguridad para redes de computadoras. Actualmente ocupa el 40% del mercado mundial de firewalls segun la investigación realizada por IDC (International Data Corporation). Además mantiene alianzas estrategicas con empresas tales como:

- Sun Soft, Inc.
- Hewlett-Packard
- UB Networks
- Oracle
- IBM

IBM es una empresa mundial que se ha dedicado principalmente a producir hardware y recientemente software. IBM goza de buena reputación en lo que se refiere a sus productos, es sinonimo de garantia y confiabilidad.

Ambas empresas muestran garantias para su producto. A pesar de que Checkpoint es una empresa joven en comparacion con ISM, ha sabido apoderarse del mercado de firewalls debido a que su producto principal Firewall-1 ha sido la mejor opción entre sus competidores.

5.4.2.7. Costos

Para efectos de esta tesis se utilizaran cotizaciones referenciales que se obtuvieron en julio de 1997. El lector debe considerar que los precios reales fluctuan a traves del tiempo y por razones de competencia en el mercado.

Características	Firewall-1	SNG / IBM
Software	CONWARE:$14000 a $15000 MAINT: $18000 a $19000	Entre $13000 a $14000
Hardware/Sistema operativo	CONWARE: $15000 a $18000 MAINT: $2000 a $2500	Entre $16000 a $18000

Fuente: Distribuidores autorizados (CONWARE, MAINT, IBM)

El caso de Firewall-1 es especial, ya que los dos distribuidores locales presentan cotizaciones diferentes. las cuales se analizaran de acuerdo al distribuidor:

CONWARE del Ecuador.- Empresa distribuidor autorizada de productos Sun

Esta empresa ofrece este producto, a traves de un programa especial, a muy bajo precio para entidades educativas como la ESPOL. Esta empresa como distribuidora autorizada de Firewall-1 para plataforma Sun con Solaris, recomienda que esta es la mejor para llevar transacciones a traves de Internet. La máquina que aconsejan usar es una SUN ULTRA 1170 con todas las especifiaciones para trabajar con el firewall, cuyo precio oscila entre 15000 y 18000 dolares. Es decir, que si la ESPOL se decide por esta opción, incluido el hardware, gastaria hasta 33000 dolares.

MAINT.- Empresa distribuidora autorizada de Checkpoint, vende la solución Firewall-1 para todas las plataformas. Aconsejan la plataforma Windows NT por ser distribuidor autorizado de NT e inclusive solo dan soporte para esta. Esta empresa no posee el programa especial de rebaja para instituciones educativas. La plataforma de hardware y software, con las especificaciones aconsejadas para ejecutar el firewall sin problemas, costaría alrededor de 2000 a 2500 dolares. La solución Firewall-1 total sería de hasta 21500 dolares.

Como conclusion de estas cotizaciones referenciales, el costo de Firewall-1 depende de la plataforma en que se implemente. Este producto brinda a la organización la libertad de decidir el nivel de inversion en mecanismos de seguridad.

El caso de IBM es fijo. El costo total del firewall incluido el hardware, el cual debe ser siempre un RISC 6000 de IBM, es alrededor de 32000 dolares. Este costo es mas alto aún para la solucion mas cara de Firewall-1

Conclusiones de la evaluacion de firewalls privados

En la primera fase de evaluacion, ambos firewalls ofrecen soluciones a los posibles problemas que pueden presentarse en la ESPOL. La forma en que implementan estas soluciones es diferente: Firewall-1 utiliza la tecnica de inspección multicapa y SNG, filtradores y proxies por separado. Firewall-1 presenta una mejor solución en las categorías evaluadas.

En la segunda fase de evaluacion, el rendimiento mostrado por Firewall-1 es superior al mostrado por IBM en las dos pruebas realizadas por los laboratorios NSTL.

En la tercera fase de evaluacion, las caracteristicas de plataforma e interfase mostradas por Firewall-1 son superiores a las presentadas por SNG ya que este es muy limitado. En las caracteristicas de soporte y garantia, todas las empresas distribuidoras ofrecen soluciones parecidas. El costo, en el caso de Firewall-1, varia de acuerdo a la plataforma en que se desea ejecutarlo, mientras el precio de SNG es uno solo. Sin embargo, los costos de implementación de SNG siempre son superiores al de Firewall-1.

Un aspecto que no se consider6 en la evaluacion es la capacidad de administracion que ofrecen los productos de firewalls. El modulo de administracion de Firewall-1 puede controlar otros modulos colocados a lo largo de la red interna que se protege. Esta caracteristica se ajusta efectivamente al diseño de firewalls internos en que se basa el modelo de seguridad de la ESPOL, ya que para la implementación de una subred tan solo podría adquirirse un modulo firewall (y adquirir el modulo de administracion) para proteger la subred y sin embargo poder ser controlado por el modulo de administracion del firewall principal (firewall externo). SNG de IBM por sí solo no ofrece esta capacidad, sino a traves de programas externos que representan un costo adicional.

Ante todos los parametros analizados anteriormente, el firewall mas apropiado para la ESPOL es Firewall-1; sin embargo, aun es necesario establecer que plataforma es la mas apropiada: NT o Solaris. Por esta razon, en la siguiente sección se analizan los criterios para elegir a una piataforma.

5.5. Criterios para la evaluacion de plataforrnas de un firewall

La selección del hardware depende mas bien de los requerimientos mínimos que exige el firewall y el sistema operativo sobre el cual va a ser instalado. Por lo tanto surge la pregunta ¿En que sistema operativo se debe instalar un firewall?. En esta seccion solo se daran criterios para evaluar los sistemas operativos sobre los cuales se debe instalar el firewall seleccionado.

Los siguientes son los criterios que deben tomarse en cuenta:

- Estabilidad y seguridad
- Rendimiento y escalabilidad

- Disponibilidad de herramientas públicas

5.5.1. Estabilidad y seguridad

Estos son los factores mas importante de todos. El sistema operativo debe ser seguro ya que si este es facilmente comprometido, el firewall podria ser desabilitado y el atacante podria violar los sistemas de la red interna. Lo mínimo que el sistema operativo debe ofrecer es un nivel C2 de seguridad segun el Orange Book[1].

Un firewall siempre debe permanecer en operación, ya que la seguridad de la red interna depende de **el.** Si el sistema operativo es inestable, es decir se inhibe, el firewall también lo sera **y** esto puede conllevar a consecuencias desastrozas en la seguridad de la red interna. Un firewall ante Internet es en realidad un servidor de Internet ya que atiende requerimientos a servicios tanto de Internet como de la red interna. Por esta razon, el sistema operativo debe poseer capacidades de servidor. Dentro de las capacidades mas importantes se encuentran:

- **Multitarea:** Es la division del codigo de aplicaciones complejas en una coleccion de tareas distintas. Esto involucra mayor rendimiento y modularidad en los programas servidores.
- **Multiusuario:** Es el soporte de multiples tareas y protección en la integridad de los datos. El file system debe soportar la apertura de un gran numero de archivos (usuarios) al mismo tiempo sin deteriorar el rendimiento.

---

[1] Orange **book** fue creado por el Departamento de Defensa del Centro Nacional de seguridad de computadoras (NCSC), en **el** cual *se* describen los niveles de seguridad para hardware, software e información confidencial.

- **Multihilo:** Es la capacidad de dividir a los procesos dentro de un mismo programa formando hilos. Esta capacidad hace que los procesos se dividan en subprocesos con un mismo fin para mejorar el rendimiento de cada programa.
- **Protección** entre tareas: El sistema operativo debe proteger a las tareas de interferir los recursos que otras tareas estan ocupando. Una tarea no debe tener la capacidad para inhibir todo un sistema.

5.5.3. Rendimiento y escalabilidad

El rendimiento de un sistema operativo es un factor importante, sin embargo es relativo ya que depende del hardware en que se halla instalado. Por esta razon, lo que hay que tomar en cuenta en el sistema operativo es la escalabilidad o alcance en lo que a poder de servidor se refiere. Los posibles niveles de escalabilidad son:

- **PC** server: Es un solo servidor con el procesador y los dispositivos de entrada /salida mas poderosos.
- **Superserver:**También llamado multiprocesador, es un solo servidor con varios procesadores.
- **Multiservers:** Tambien llamados clusters, son varios superservers que trabajan juntos. En este nivel no hay límites en los que se refiere a poder de procesamiento.

Como medida consultiva tambien se pueden realizar pruebas con el firewall en las diferentes plataformas requeridas por los distribuidores. De esta manera, a traves del grafico bps vs. clientes, se puede notar con cual plataforma el firewall ofrece mejor rendimiento.

5.5.3. Disponibilidad de herramientas publicas

Esta es una ventaja que presentan algunos sisterna operativos. La empresa proveedora del sistema operativo tiene que hacer disponible parches y demas programas correctores como herramientas publicas para corregir los posibles errores que pueda tener.

Además para el firewall es conveniente tener herramientas publicas de seguridad instalados sobre un sisterna para otorgar redundancia en la protección de la red interna. Esta medida involucra la popularidad que tenga el sistema operativo en el medio ya que rnuchos grupos (acadernicos, investigadores, etc.) desarrollan gratuitamente productos (programas) sobre sisternas operativos rnuy utilizados.

5.6. Evaluación de la plataforma para el firewall seleccionado

El firewall seleccionado, Firewall-I, puede trabajar en plataformas Solaris y NT. De acuerdo a los criterios provistos en la sección anterior, esta es la comparacion de ambos sisternas operativos:

Criterios	Solaris 2.5.	Windows NT server 4.0
Estabilidad y seguridad		
Nivel de seguridad C2	Si	Si
Multitarea	Si	Si
Multiusuario	Si	**No,** carece la habilidad de compartir aplicaciones graficas a traves de la red[2].
Multihilo	Si	Si
Protección entre tareas	Si	No, los procesos pueden saturar recursos de memoria y hacer caer al sistema. Depende de la memoria que los procesos ocupen[2]
Rendimiento y escalabilidad		
PC server	**Si**	Si
Superserver.	Sí	Despues de los 5 procesadores degrada el poder de procesamiento[3]
Multiservers	Si	No
Prueba de rendimiento	Mayor que NT.[4]	Menor que Solaris[4]
Disponibilidad de herramientas públicas	Amplia	Escasa

5.6.1. Estabilidad y seguridad

Dentro de la categoria de estabilidad y seguridad, Windows NT 4.0 muestra debilidades frente a Solaris 2.5 : NT no es por naturaleza un sistema multiusuario ya que no puede compartir aplicaciones graficas en la red; y no protege la memoria asignada a los procesos que ya la estan utilizando.

---

[2] **Fuente:** T. **Yager, Byte, "Unix vs. NT: Head to Head",** 1996
[3] **Fuente: R. Orfali &** D. **Harkey &** J. **Edwars, The Essential Client/Server,** 1996
[4] **Fuente: Key Labs** Inc., 1996. **Es un laboratorio independiente dedicado a probar hardware y software en arnbientes de red incluyendo Internet**

5.6.2. Rendimiento y escalabilidad

Solaris 2.5 posee mayor escalabilidad que NT, ya que soporta superserver y clusters, niveles que no son alcanzados en su totatilidad por NT.

En caso que, por necesidad de mayor rendimiento, se decida colocar al firewall de la ESPOL en superservers y en clusters NT no otorgara esas facilidades.

Con la misma metodología utilizada en la evaluacion de rendimiento de firewalls realizada en la sección 5.4.2.2., KeyLabs Inc. realizó la evaluacion de Firewall-1 en las dos plataformas con las siguientes caracteristicas en el hardware:

Características	Solaris 2.5.	Windows NT 3.51
Procesador	Sun Sparc Ultra	Intel Pentium Pro 200 MHz
Memoria RAM	64 MB	64 MB
Tarjeta de Red	100Base-TX	Intel EtherExpress Pro 100Base-TX

El 75% del trafico generado para estas pruebas fue debido a sesiones HTTP y el *25%* a sesiones FTP.

El grafico resultante **Mbps** vs. numero de clientes es:

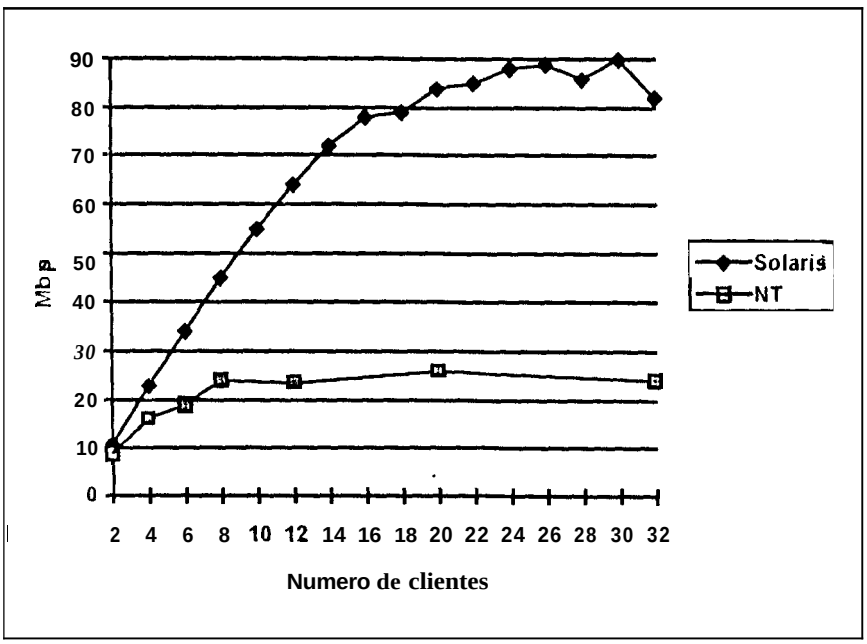


Figura No. 5-5 Cuadros de rendimiento de Firewall-1 con Unix y NT
Fuente: http://w.checkpornt.com/

En la figura No.5-5 se observa una supremacia del firewall con plataforma Unix sobre el firewall con plataforma NT. Por esta razon Solaris ofrece mejor rendimiento sobre NT.

5.6.3. Disponibiiidad de herramientas publicas

En Internet, Unix continua siendo el sistema operativo mayormente utilizado y por ende el que mas herramientas publicas dispone. Existen programas para sistemas Unix desde los mas sencillos hasta los mas sofisticados. En la rama de la seguridad, Internet provee una gran cantidad de programas en Unix estandar para construir un firewall. Estos programas al ser publicos o gratuitos carecen de garantias y soporte por parte de los distribuidores, lo que constituye una desventaja.

En cambio NT, al ser distribuido por Microsoft, no posee una gran cantidad de programas publicos que sean soportados por NT. En la rama de seguridad hasta la presente fecha no existen herrarnientas públicas que ayuden a construir un firewall.

5.6.4. Conclusiones

Ante todas las caracteristicas evaluadas y cornparadas, Solaris mantiene suprernacia sobre NT en lo que respecta a seguridad y estabilidad. En los demas factores: rendimiento, escalabilidad y disponibilidad de herrarnientas publicas, igual que en el caso anterior, Solaris rnarca ventajas sobre NT. Por lo tanto la selección de la plataforma correcta para el firewall externo de la ESPOL es Solaris.

Windows NT esta entrando con paso firme en el mercado de servidores de Internet, no sería sorpresa si algún día NT supera a los sistemas Unix. Por esta razon los distribuidores de firewalls privados ya estan ernpezando a sacar versiones compatibles con NT.

CAPÍTULO VI

IMPLEMENTACION DE UN MODELO DE SEGURIDAD

6.1. Introducción

En el capitulo IV se definió un modelo de seguridad que consiste en establecer niveles de seguridad a los recursos conectados al backbone de la ESPOL. Estos tres niveles de seguridad son: firewall externo, seguridad de hosts y firewall interno.

En este capitulo se describe la implementación de un modelo de seguridad basado en los tres niveles de seguridad. Además, se evalúa la situación actual y se dan recomendaciones adicionales para enforzar las medidas de seguridad actuales. Por razones de seguridad el modelo aquí implementado no muestra en detalle sus caracteristicas, tan sólo se limita a tratar los aspectos mas importantes y hacer recomendaciones generales. Sin embargo, como parte del trabajo de esta tesis, se entregara el detalle del modelo a la Jefatura de Redes de CESERCOMP en el documento confidencial: "Implementacion de un modelo de seguridad para la ESPOL".

6.2. Firewall Externo

6.2.7. *Implementación del modelo de seguridad*

El firewall externo representa el primer nivel' en el modelo de seguridad. Lo constituye el screening router (ruteador filtrador) y el servidor firewall, programa instalado en un host bastion, como se observa en la figura No. 6-1. Además, se utiliza un servidor proxy de web, el cual puede ser instalado en el host bastion o en el servidor David.

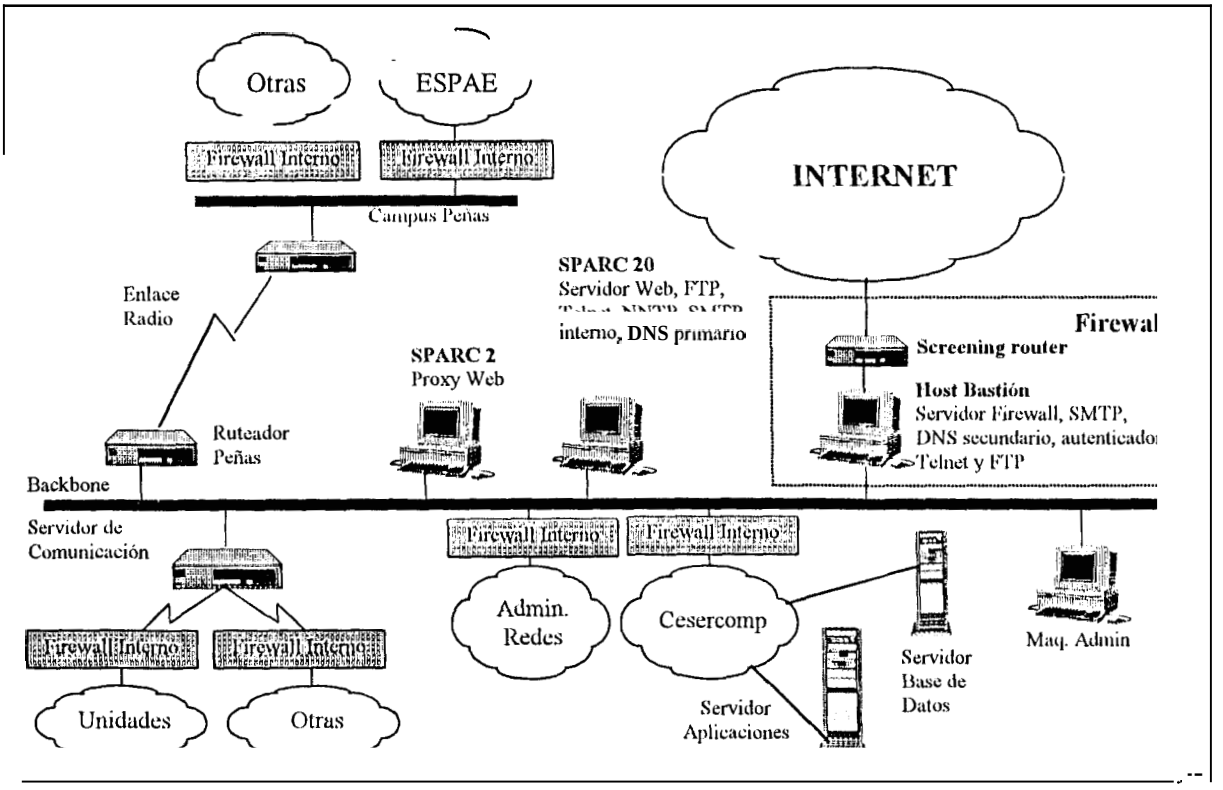


Figura No. 6-1 Configuración del firewall externo para la ESPOL

6.2.1.1. Ruteador externo

El ruteador externo (ruteador entre Internet y el host bastion) es el primer mecanismo que conforma el firewall. En el se concentran las reglas de filtraje básicas para evitar accesos no autorizados y habilitar servicios de Internet.

Actualmente la ESPOL solo habilita los siguientes servidores: correo electronico, web y popmail; y los clientes pueden utilizar cualquier servicio saliente (hacia los servidores de Internet: FTP, Web, etc.)

Para mayor seguridad se debe utilizar el criterio de negar por defecto: "Todo esta prohibido excepto lo explicitamente permitido". Las reglas de filtración en el ruteador externo estan detalladas en el documento de "Implementación de un modelo de seguridad para la ESPOL" exclusivo para la Jefatura de Redes de CESERCOMP.

6.2.1.1. Servidor Firewall: Producto Firewall-1

El host bastion es la maquina que debe ser colocada entre el ruteador externo y la red interna. En el se debe contar con un programa de firewall que cumpla con los requerimientos minimos de seguridad para la ESPOL.

El producto seleccionado en el capitulo V fue Firewall-1 porque cumple con los requerimientos minimos de seguridad para la ESPOL y por ser el mejor ante sus competidores. Antes de colocar al producto en operación se ejecuta un plan de pruebas para observar su comportamiento debido a que el host bastion donde se lo instalo, posee los requerimientos minimos de acuerdo a los fabricantes del Firewall-1.

Plan de pruebas del producto Firewall-1 en la ESPOL

Objetivos:

1. Probar la estabilidad del servidor firewall
2. Probar el rendimiento del hardware del servidor firewall

Justificación del plan de pruebas

El computador donde se instaló Firewall-1 tiene las siguientes características:

Memoria RAM:	32 MB
Procesador:	Pentium 100 MHz
Sistema Operativo:	Solaris Intel 2.5.1
2 interfases de red:	Ethernet 10 MBps

La capacidad mínima de memoria requerida para el producto Firewall-1 es de 16 MB por encima de la memoria que utiliza el sistema operativo. Por ejemplo, Solaris Intel necesita mínimo 16 MB pero se recomienda 32 MB, es decir que Firewall-1 necesita como mínimo 32 MB (16 del sistema operativo más 16 del firewall) y lo recomendable es 48 MB (32 del sistema operativo y 16 del firewall).

Según lo anterior, el computador en el que se instaló el firewall funciona con lo mínimo de memoria requerida. En consecuencia se puede traer problemas de estabilidad y rendimiento en la red.

Estrategia para el plan de pruebas

- Para probar la estabilidad del servidor firewall se simulará un ambiente típico de operación en la red de la ESPOL (carga de la red). De esta manera se puede observar el comportamiento del servidor firewal. Si se inhibe el servidor firewall, se podrá sospechar falta de memoria.

- Para probar el rendimiento de la red se simulará un ambiente típico de operacion en la red de la ESPOL como en el caso anterior y se evaluará, desde el punto de vista del usuario, si el tiempo de respuesta en transacciones permitidas por el servidor firewall es tolerable. Los usuarios no deberían percibir la existencia del servidor firewall.

El ambiente típico de operación se logró determinar mediante continuas mediciones tanto del tráfico entrante como del saliente. La tasa de tráfico entrante promedio registrada en la ESPOL en horas de mayor uso de la red es de aproximadamente 56 Kbps y la saliente aproximadamente de 3 Kbps. El tráfico en el backbone varía desde 7 a 10 MBbps.

Configuración del servidor firewall

La arquitectura del firewall a utilizar es ***screened-subnet*** (sección 3.3.5.3.) sin red perimetro. Así se ilustra en la figura 6-2:

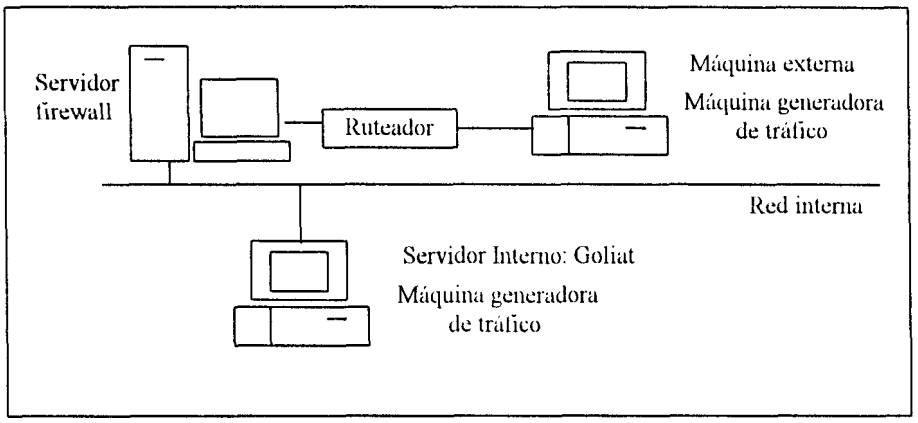


Figura no. 6-2 Configuración de pruebas del Firewall-1

Las caracteristicas de los recursos de la figura anterior son:

- Un ruteador con dos puertos LAN.
- Un hub Ethernet de 10 Mbps con 2 puertos como mínimo
- Dos computadores, uno para la red interna y uno para la red externa con las siguientes caracteristicas:
    - Servidor Interno: Procesador Pentium 32 o 28 MB de RAM, con una interfase de red Ethernet. Esta maquina tiene que simular al servidor David o Goliat de la ESPOL (ver figura No. 6-2).
    - Maquina externa: Procesador 80486 o pentium con Windows 95, mínimo 8 MB de memoria RAM, interfase de red.

Resultados de las pruebas

El trafico tanto entrante como saliente, generado por la emisión de paquetes ICMP (ping) indefinidos en varias sesiones de Windows 95, fue mayor a 65 Kbps y 3 Kbps respectivamente.

El servidor firewall nunca se inhibio. El trafico generado en la red interna no influyó en rendimiento del firewall.

Sin el servidor firewall cada paquete ICMP, en ir a su destino y regresar a su emisor, demora 8 rnilisegundos; con el servidor firewall, este demora 13 milisegundos, por lo que existe un retraso de 5 rnilisegundos por cada paquete.

Se transfirieron 5 archivos de 1 MB cada uno desde el servidor interno al cliente externo. En el tiempo que dernoro no fue mayor a 20 segundos para cada archivo. Al igual que en los paquetes ICMP, el servidor firewall no desmostro degradación en su rendimiento.

Lo que si falló en el servidor firewall fue el registro de acciones a tiempo real, ya que las acciones se iban registrando a destiempos y omitía la información del paso de algunos paquetes ICMP. Esta capacidad se vio afectada por el trafico que fue generado.

Ante estos resultados, el programa Firewall-1 demostro tener un aceptable nivel de rendimiento sin contar con el problema del registro a tiempo real. Una posible solución a este problema seria el aurnento de memoria RAM en el servidor firewall. Y si los problemas persisten consultar a la casa fabricante Checkpoint rnediante sus distribuidores autorizados.

6.2.2. *Evaluación de las medidas de seguridad actuales*

Actualrnente la ESPOL solo se protege a traves de un screeening router (ruteador filtrador) situado entre Internet y el backbone. El autor de esta tesis considera que este ruteador filtrador tiene las siguientes ventajas y desventajas:

Ventajas:

- Este filtrador posee capacidad para examinar direcciones y puertos fuente y destino. Sin embargo, no cumple con todos los requerimientos de un filtrador de paquetes de acuerdo a la sección 5.2.1.
- Las reglas de filtracion son sencillas de entender e implementar.
- Las reglas protegen tanto a recursos como a los servicios de los mismos.

Desventajas

- Las reglas configuradas son muy básicas pero algunas son redundantes.
- Las reglas no protegen direcciones de redes internas.
- No se utiliza el criterio de negar por defecto: "Todo es prohibido excepto lo explicitamente permitido".

Además de este filtrador, la ESPOL dispone de un servidor proxy para web. Sin embargo, no se aprovecha de todas las ventajas que ofrece este servidor, ya que no todas las maquinas de la ESPOL se conectan al proxy para navegar por Internet sino que salen directamente. De esta manera se esta ampliando el ancho de banda de red haciendola mas lenta.

Recomendaciones

Para las medidas actuales se recomienda:

- Utilizar el criterio de negar por defecto en el ruteador
- Hacer una revision completa de todas las reglas de filtracion en el ruteador, si es preciso documentar que es lo que hace cada regla y eliminar reglas que no se utilizan. En el documento confidencial para CESERCOMP se evalua cada regla.
- Implementar las reglas del ruteador que se describen en el documento confidencial de implementación para la Jefatura de Redes de CESERCOMP.

- Desde el ruteador dar proteccion a las redes internas mas importantes: CESERCOMP-CDA, rectorado, red de servidores de aplicaciones.
- Configurar a todas las maquinas de la ESPOL para que naveguen en el web a traves del proxy. Se recomienda aumentar la memoria del servidor proxy en caso de que presente degradación en su rendimiento.
- Colocar al servidor host bastion con el producto Firewall-1 para ponerlo en operación.

6.3. Seguridad de Host

6.3.7. Implementacion de hosts seguros

La seguridad de host representa el segundo nivel de seguridad. Los hosts considerados importantes y de alto riesgo son: Goliat, David y los servidores de aplicaciones y base de datos. Estos servidores deben utilizar seguridad de host a mas de la proteccion que brinda el firewall externo. Hay que recordar que si los hosts de aplicacion y base de datos se colocan en una red interna protegida por un firewall interno, estos adquiriran un tercer nivel de seguridad.

De acuerdo a la sección 3.4. la seguridad de host consiste en:

- **Desabilitar los servicios no requeridos:** Se debe aplicar el criterio de negar por defecto, desabilitar todos los servicios innecesarios y solo habilitar los que se necesitan.
- **Identificar y modificar los servicios:** Se debe identificar que servicios se desean brindar para aplicar programas especiales o Wrappers que ayuden a filtrar estos servicios en base a direcciones IP de los clientes.

- Reconfigurar para la produccion: Despues de los pasos anteriores es necesario reconfigurar el sistema operativo y verificar los permisos de acceso a los archivos del sistema para luego poner a los hosts en operación.

Tomando en consideración estos aspectos se establecen por cada host, en el documento exclusivo para la Jefatura de Redes de CESERCOMP, las medidas de seguridad apropiadas.

6.3.2. Evaluación de las medidas de seguridad actuales

Los hosts conectados al backbone estan protegidos mediante filtros y programas especiales (Wrappers, ver sección 3.4. Host Bastion) que niegan el acceso a ciertas direcciones IP y a ciertos servicios. En estos filtros y programas especiales si se utiliza el criterio de negar por defecto: se desabiltan todos lo puertos y luego solo se habilitan los puertos de los servidores que se necesitan.

El servidor de Internet actual, Goliat, esta protegido por un bridge con reglas de filtraje como se puede ver en la figura No. 6-3. Además, posee un ambiente restringido que inhabilta a los usuarios a ejecutar ciertos comandos. La seguridad del Goliat esta bien irnplementada a pesar de que recientemente se encontro un bug en este shell. Los detalles de este bug estan tratados en el documento confidencial de implementación.

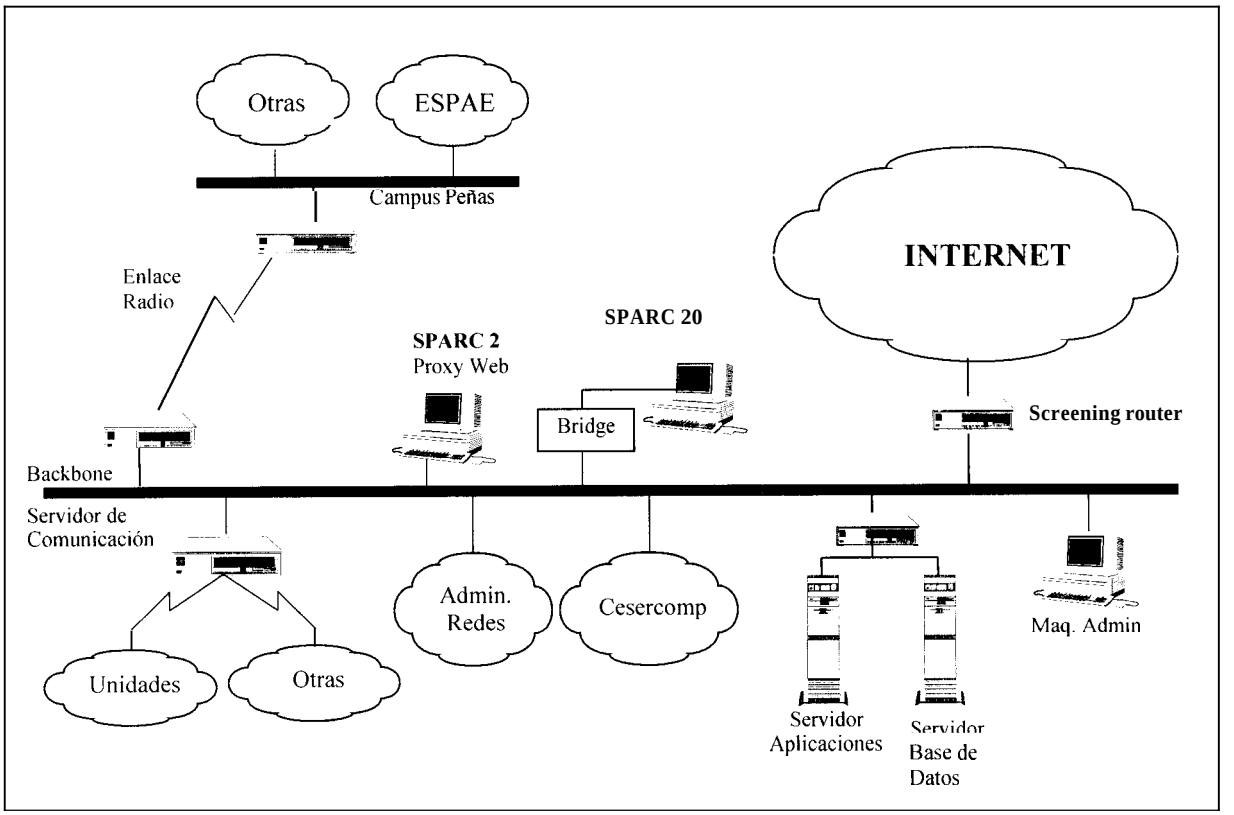


Figura No. 6-3 Configuración actual de servidores en el backbone

El servidor David que se utiliza como proxy de web, no posee cuentas de usuarios y es protegido por el ruteador externo. Su funcion es exclusivamente de servidor proxy y no corre peligros.

Los servidores de aplicaciones y base de datos se encuentran aislados en una red a traves de un ruteador, el cual posee reglas que niegan el acceso a todo, excepto a los puertos que utilizan la base de datos y las aplicaciones. La seguridad de estos hosts esta bien implementada.

Aplicar bridges entre el backbone y hosts es una medida adicional que sirve de mucho. En cuestión de seguridad es muy importante la redundancia en mecanismos; en caso de que uno falle, el otro puede suplirlo. Sin embargo, el bridge o ruteador intermedio debe poseer un buen rendimiento a fin de que no se perciba su existencia y no sea causa de una degradacion en el sistema. Hasta el momento de escribir esta tesis, el bridge ubicado entre el backbone y el Goliat no ha presentado degradacion en el rendimiento.

Recomendaciones

Para la seguridad de host se recomienda:

- Utilizar el criterio de negar por defecto: Desabilitar todos los servicios y dejar solo los que se necesitan.
- Solo permitir usuarios necesarios en los hosts de aplicaciones y base de datos
- Utilizar programas wrappers en los hosts de aplicaciones y base de datos
- En hosts que perrniten cuentas de usuarios como el Goliat, hacer uso de shells restringidos. A medida que pase el tiernpo se recomienda cambiar de shell, especialmente si ya han violado el actual.
- Utilizar como medida adicional bridges o ruteadores para conectar los hosts al backbone. Sin embargo, estos mecanismos deben poseer un buen rendimiento para no crear sobrecarga ni hacer lentos a los hosts.

6.4. Firewall interno

Un firewall interno es aquel que se encuentra entre el backbone y una red interna, y representa el tercer nivel de seguridad. El proposito de este firewall es brindar protección a los recursos de

la subred a la que esta conectado. Por lo tanto, las reglas de configuracion de este firewall dependen mucho de las politicas de seguridad que se implementen en la subred.

De acuerdo con el capitulo IV, la arquitectura recomendada para un firewall interno es la screened-subnet donde se separan la red segura (maquinas de administración en una unidad) de la red insegura (laboratorio). Por esta razon, el servidor firewall o host bastion debe poseer como minimo tres interfases de red como se observa en la figura 6-4

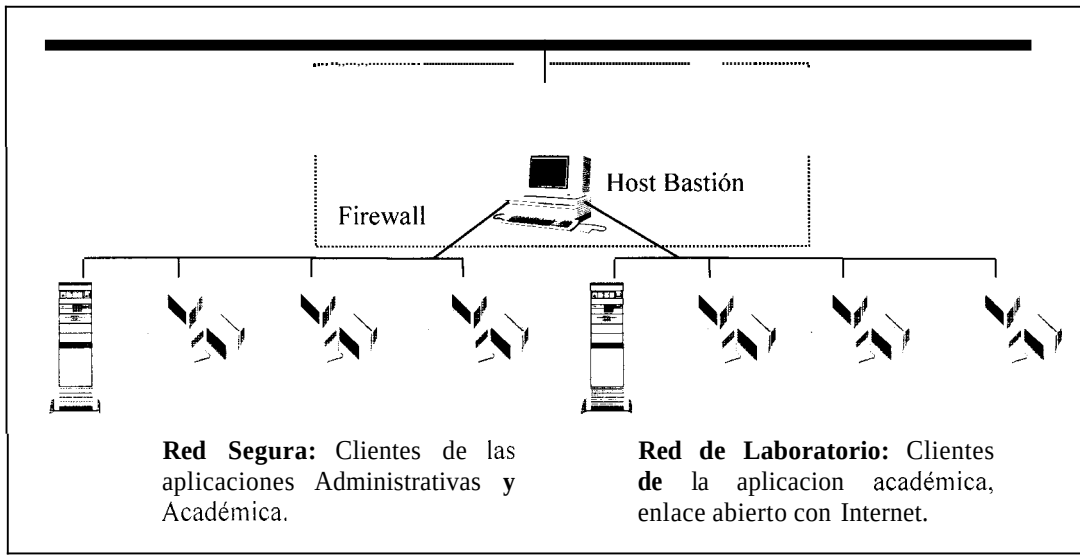


Figura NO. 6 4 Configuración de un firewall interno

La selección del mejor programa servidor de firewall debe ser realizada en base a los requerimientos minimos que debe cumplir este para proteger la subred.

Para configurar tanto al ruteador como al servidor firewall se pueden utilizar los mismos consejos y recomendaciones anotadas para el firewall externo de la ESPOL. Sin embargo, la configuracion del firewall interno no tiene que ser totalmente identica a la del firewall externo de

tal forma que si infortunadamente el firewall externo es víctima de un ataque, los atacantes no puedan tomarse los firewalls internos.

CONCLUSIONES Y COMENDACIC

De este estudio de seguridad de redes de computadores ante Internet y otras redes se pueden obtener las siguientes conclusiones y recomendaciones:

Conclusiones

1. Una red libremente expuesta a Internet, sin ningun mecanismo de protección, constituye un peligro latente para sus recursos y puede ser tambien una plataforma para violar otras redes. Si un atacante se toma una red y sus servidores, este puede tomar otras redes de otras organizaciones que permiten una comunicacion confiable (conexion sin uso de passwords) con la red violada. Por lo tanto, al diseñar un modelo de seguridad hay que pensar en la seguridad de su organizacion y la de otras que confian en su organizacion.

2. Los protocolos de Internet fueron diseñados pensando en su funcionamiento inmediato y en lo ultimo en que se pensó fue en la seguridad. Por esta razon, existen protocolos que al ser utilizados conllevan riesgo y son faciles de violar. Las primeras versiones de los programas en Internet (por ejemplo Sendmail) tienen muchas brechas en su seguridad, pero poco a poco se han ido cubriendo estas brechas en las posteriores versiones. No hay que olvidar que existen personas (atacantes) a tiempo completo que se dedican a probar todos los programas hasta hallar alguna falla. De esta manera no se puede considerar que la ultima version de un programa no va a tener errores. A medida que surgen nuevos protocolos en Internet, surgen nuevas brechas de seguridad, de esta manera se origina una carrera entre los fabricantes de firewalls, que cada año liberan productos mas poderosos, y los hackers que cada vez mas tecnifican sus ataques.

3. En materia de seguridad no se puede asegurar la invulnerabilidad de una estrategia o modelo. En Internet ningun mecanismo es invulnerable [CHES94], prueba de eso es que algunas organizaciones, teniendo poderosos sistemas de firewalls, han sido perpetrados por un ataque. La idea central que tiene que prevalecer en el administrador de una red es otorgar redundancia de seguridad por cada recurso de su red. Así, cada recurso tendra al menos un mecanismo de seguridad que le brindara protección.

4. El resultado de los analisis de riesgo con lógica difusa describe el riesgo de cada recurso del backbone de la ESPOL con mayor exactitud que el metodo numerico. El metodo numérico no representa lo que verdaderamente se quiere expresar ya que al multiplicar un numero pequeño (por ejernplo importancia) con uno grande (por ejemplo riesgo), da como resultado un numero pequeño (riesgo total) lo cual no refleja el verdadero riesgo real. En cambio el analisis de riesgo con lógica difusa conjuga reglas, otorgadas por los propios expertos, para hallar el riesgo total; y combina todas las posibilidades de sus variables (riesgo e importancia). El objeto del analisis de riesgo es descubrir cuantos recursos dispone la organizacion y cuales se deben proteger mas que otros.

5. De todas las arquitecturas de firewalls presentadas en el capítulo III, la arquitectura mas idonea para la ESPOL es la screened subnet pero sin red perimetro. Esta arquitectura es una variación considerada insegura debido a que no se cuenta con una red perimetro para separar el trafico interno del trafico de Internet, en consecuencia desde Internet se puede tener acceso a la informacion interna de la organizacion. La ESPOL como universidad posee una conectividad abierta hacia Internet, de acuerdo a esto, todas las redes internas pueden poseer sus propios servidores de Internet además de servidores de informacion interna. Entonces en el backbone de por sí se mezcla la informacion interna con el trafico

proveniente de Internet. Por esta razon es innecesario utilizar una red perimetro. La solución para evitar que desde Internet personas no autorizadas accesen a informacion interna es encriptarla entre subredes a lo largo del backbone. Con esta medida se gana tambien autenticacion ya que solo el receptor autorizado podra interpretar la informacion.

6. Ningun producto de firewall público evaluado cumple en su totalidad los requerimientos de seguridad de la ESPOL. Sin embargo, la combinación de estos puede servir de mecanismo de respaldo para el verdadero producto de firewall que la ESPOL instale. En cuanto a los firewallls comerciales, Firewall-1 al igual que SNG de IBM satisfacen las necesidades de seguridad para la ESPOL. Sin embargo, Firewall-1 ofrece mejores caracteristicas en cuanto a rendimiento y plataforma que SNG. Por lo tanto, el producto de firewall recornendado para la ESPOL es Firewall-1.

7. Para instalar los productos públicos se requiere pericia en el sistema operativo sobre el cual se desea instalar y conocimientos basicos de firewalls, de otra manera la instalacion de estos productos resulta infructuosa y tediosa. En cambio los productos comerciales son diferentes a los publicos ya que la instalacion es sencilla y amistosa al usuario.

8. En un ambiente típico en el backbone de la ESPOL, la inclusion del producto Firewall-1 instalado en un host bastion con las caracteristicas que exige el distribuidor, no afectara el rendimiento del backbone desde el punto de vista del usuario interno. Es decir, el usuario interno no se percatara de la presencia del firewall.

Recomendaciones

1. En el caso especifico de la ESPOL, es rnejor implementar un modelo de seguridad utilizando el criterio de negar por defecto: **"Todo** esta prohibido **excepto** lo explicitamente permitido", debido a que se sabe que servicios brinda el backbone y por ende cuales son las debilidades. Adernas, no se corren riesgos de ataques con los servicios que no brinda el backbone.

2. En rnateria de seguridad nadie tiene la última palabra, es decir, hasta los firewalls más poderosos y nuevos pueden ser violados si los nuevos protocolos de Internet contienen fallas en seguridad. Por lo tanto se recornienda que cuando se adquiera el producto firewall se llegue a un acuerdo con el distribuidor para que se actualice el producto con futuras versiones. Adernas, se debe innovar la configuración del firewall, actualizar el servidor proxy web, y añadir nuevos mecanismos de seguridad (por ejernplo productos de firewalls publicos) para evitar brechas de seguridad en el modelo.

3. Se recomienda tornar rnedidas de protección basadas en el rnodelo de seguridad presentsdo en esta tesis. Se debe habilitar un firewall externo (entre Internet y el backbone, Firewall-1), aplicar seguridad de host en todas las rnaquinas y sugerir a todas las redes internas utilizar algun rnecanisrno de seguridad (módulo de Firewall-1, si se ha comprado Firewall-1).

4. Se deben utilizar mecanismos de encriptacion y autenticacion (modulo de Firewall-l) para los servidores de aplicaciones y base de datos a fin de prevenir cualquier acceso no autorizado a esta inforrnacion considerada confidencial.

5. Se recomienda que se utilice como plataforma del servidor firewall un sistema basado en UNIX estandar, preferiblemente Solaris Sparc o Solaris Intel, ya que en esta tesis quedo demostrado la supremacia de Solaris sobre NT en lo que respecta a servidores seguros para Internet.

6. Antes de colocar cualquier firewall en una red interna se sugiere que se realice un estudio de sus necesidades mediante un análisis de riesgo empleando lógica difusa para lograr resultados que se acercan mas a la realidad. De esta manera se puede implementar un modelo de seguridad efectivo y eficiente.

APÉNDICES

APENDICE A

ii 1 y · ll del analisis de riesqo a l recursos de la ESPOL

Este apendice tratara principalmente el desarrollo de dos analisis de riesgo para los recursos de la ESPOL utilizando lógica difusa: el primer analisis con datos proporcionados por el director de CESERCOMP y el segundo analisis con datos proporcionados por el jefe de redes de CESERCOMP. Para ello es necesario prirnero revisar los principales conceptos de la logica difusa y el uso de variables lingüísticas aplicado al analisis de riesgo.

A.1. Introduccion a la Iogica difusa

En logica difusa un conjunto se define de la siguiente manera: Sea **A** un conjunto de elementos x tal que estos satisfacen la mernbresia definida por **A.** La funcion de mernbresia u(x) brinda un grado de pertenencia al conjunto **A** para cada elemento x. Esta funcion u(x) es definida entre 0 y **1,** donde 1 representa a los elementos que estan cornpletamente en **A, y** 0 los que no estan cornpletarnente en **A.** Es decir, no es como en la logica tradicional donde el elernento pertenece o no al conjunto, sino que existe cierto grado de pertenecia, y este grado lo determina la funcion u(x). Así, mientras x obtiene un u(x) que se aproxirna a **1** se dice que x alcanza mayor grado de pertenencia y si se aproxirna a 0 se dice que x alcanza menor grado de pertenencia. Entonces un conjunto difuso puede ser representado como el par ordenado (x, u(x)):

$$\mathbf{A} = \{ (x,u(x)) \mid \mathbf{x} \in X, 0 \leq u(x) \leq 1 \}$$

donde X es un conjunto definido de objetos

En otras palabras un valor difuso consiste en aproximaciones a ese valor. Por ejemplo, en el caso de variables numericas se puede definir un numero difuso 3 como un conjunto de valores entre el 2 y el 4 cada uno con un valor u(x) como se grafica en la figura No. A-1

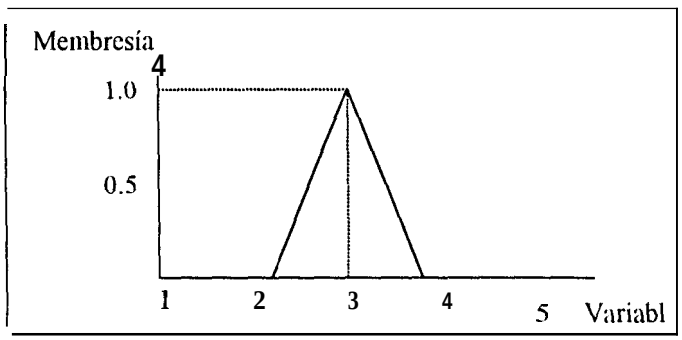


Figura No. A-1 Representación de un número difuso con una función de membresía triangular.

Este conjunto puede ser expresado semanticamente como "cercano a 3" o "acerca de 3". En la figura No. A-1 se puede observar que 2 tiene un grado de membresia igual a 0, y que a los valores posteriores a 2 adquieren un mayor grado de membresia hasta llegar al maximo punto en 3. Despues de 3, los valores siguientes adquieren un menor grado de membresia hasta llegar a 0 en el punto 4. En este caso de ejemplo la funcion de membresia es triangular, pero la funcion de membresia u(x) puede ser definida de otra forma: sinusoidal, cuadrangular, etc. La definición de la funcion de membresia depende del dominio y del comportamiento que se desea observar en la variable.

En lógica difusa se definen operaciones de conjuntos, aritméticas, lógicas, teorias de posibilidades y manejo de probabilidades, las cuales no seran descritas por que salen del alcance de este trabajo. [PELA95]

Una variable lingüística es una variable cuyos valores son palabras u oraciones, y no valores numericos. Estos valores linguisticos por lo general son definidos como conjuntos difusos. Por ejemplo, la probabilidad de fallas de un sistema puede ser representada en el grafico Membresia versus ocurrencia de fallas. La variable probabilidad u ocurrencia de fallas puede tomar los siguientes valores: Muy alta, alta, moderada, baja y remota, cada uno con sus rangos en probabilidades nurnericas. En este ejemplo el valor Muy alta tiene un rango de probabilides desde 10' hasta 1, y así sucesivamente para los valores posteriores.

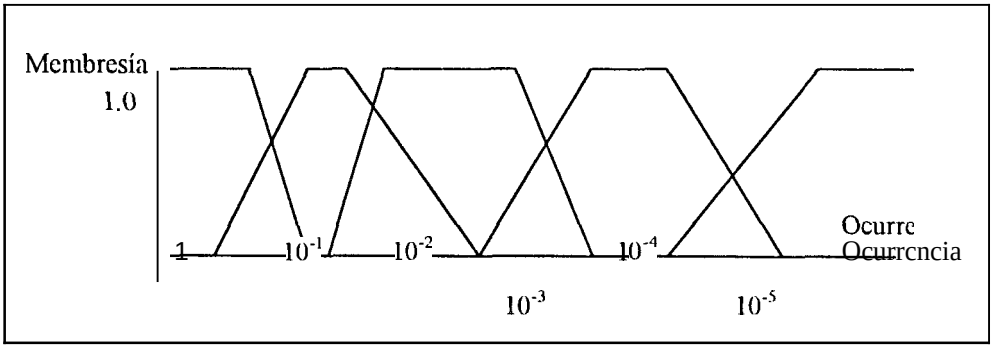


Figura No. **A-2 Definición de conjuntos difusos de probabilidad de fallas**
Fuente: Bowles & Pelaez, Application of fuzzy logic to reliability engineering, 1995

Las operaciones con valores linguisticos se pueden realizar a traves de reglas de estructura IF-THEN otorgadas por los resultados de estudios o por personas expertas en el tema. Tambien existen otros metodos [PELA95].

A.2. Acercamiento al análisis de riesgo

Para calcular el riesgo total de cada recurso se utiliza el sistema descrito en la figura No. **A-3.** Se lo puede dividir en: Entradas, procesos y salidas. Tanto las entradas como los modulos de

reglas que se pueden percibir en la figura **A-3** fueron proporcionados por las personas expertas sobre las cuales se sustento el analisis.

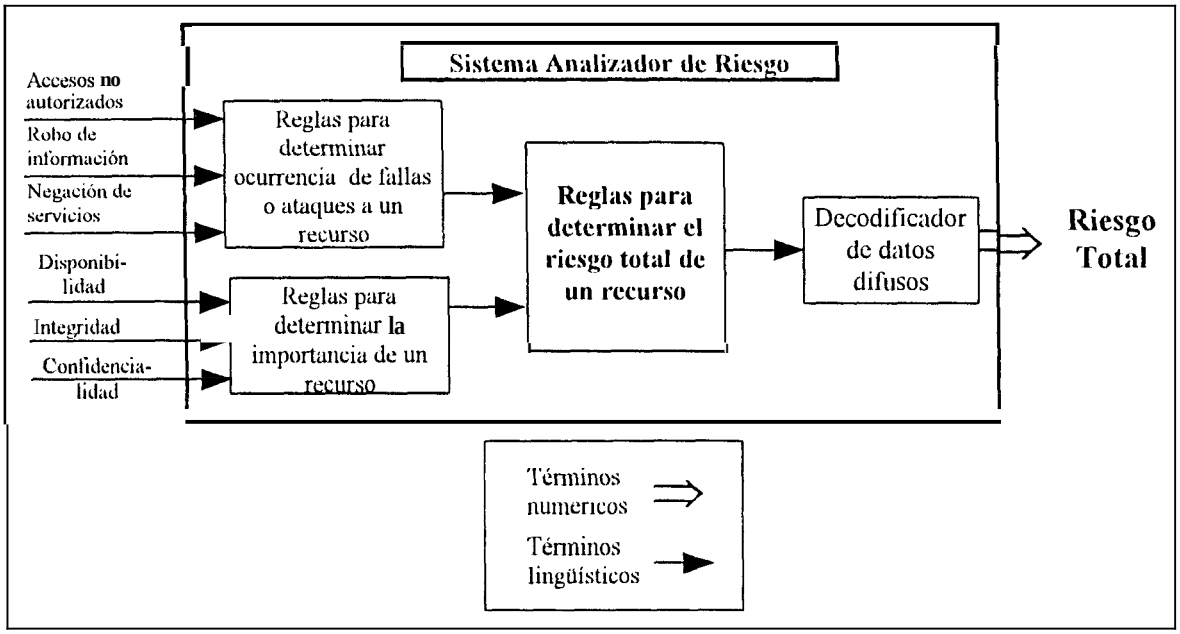


Figura No. **A-3 Analizador de Riesgo con lógica difusa**

A.2.1. Entradas

Cada recurso definido en el capitulo IV pasara por el sistema analizador de riesgo. Cada recurso contiene 6 variables, las cuales pueden contener los siguientes valores:

Variables de Riesgo			Variables de Importancia		
Acceso no autorizado	Robo de	Negación de Servicios	Disponibili-	Integridad	Confidencia-
Ningún	Nin Qn	Ningún	Nin una	Nin una	Nin una
Bajo	Ba'o	Bajo	Ba'a	Ba'a	Ba'a
Moderado	Moderado	Moderado	Moderada	Moderada	Moderada
Alto	Alto	Alto	Alta	Alta	Alta

Tabla A-1
Cuadro de variables difusas con sus valores

Es necesario que los expertos establezcan funciones de membresia de acuerdo con los valores que puede tomar. Tanto para las variables de riesgo e importancia se adoptó como dominio

numérico una escala del 0 al 10, donde 0 representa menor riesgo o importancia y 10 mayor riesgo o importancia.Los valores de estas variables, para cada uno de los recursos analizados seran otorgados por los expertos consultados: Jefe de Redes y el Director de CESERCOMP.

Tal como en las figuras **A-1 y A-2,** el cornportamiento de cada variable debe dfinirse en ternincs de sus funciones de rnernbresia (riesgo por acceso no autorizado, importancia por integridad, etc.). Estas funciones de membresia tambien fueron definidas por los expertos en base a los valores que pueden tomar las variables de acuerdo a la tabla A-I.

Definición de funciones de membresia por parte del Jefe de redes de CESERCOMP

Para **el** Jefe de Redes de **CESERCOMP estas son** las funciones de rnernbresia para cada variable:

Riesgo por acceso no autorizado

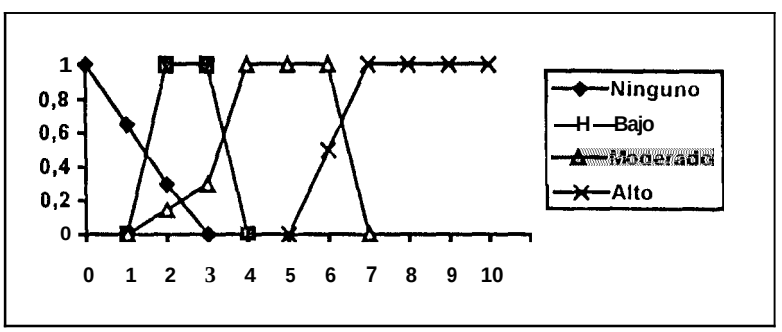


Figura No. A-4 Funciones de membresía p a n riesgo por acceso no autorizado por parte del Jefe de Redes

Riesgo por Robo de información

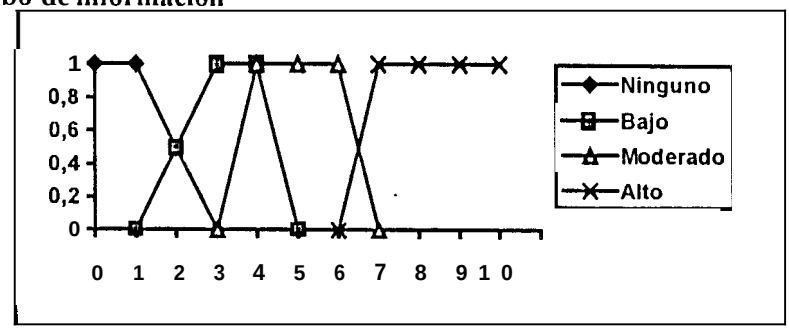
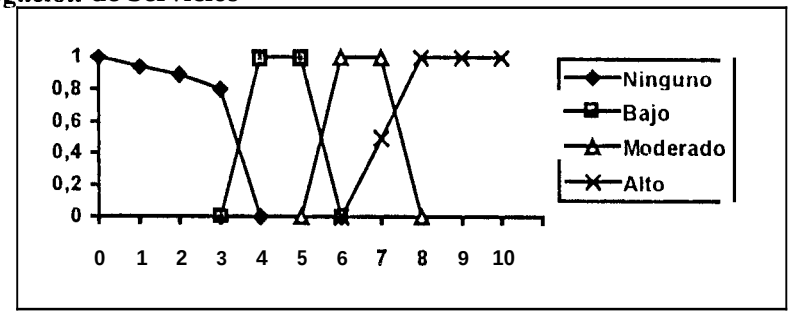


Figura No. **A-5 Funciones de membresía para riesgo por robo de información por parte del Jefe de Redes**

Riesgo por Negación de Servicios



Figum No. **A-6 Funciones de membresía p a n riesgo por acceso no autorizado por parte del Jefe de Redes**

En el campo de importancia, las funciones fueron definidas de la siguiente manera:

Importancia por disponibilidad

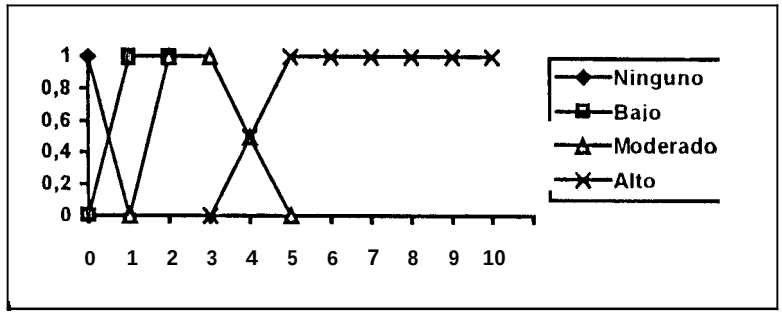


Figura No. **A-7 Funciones de membresía p a n importancia por disponibilidad por parte del Jefe de Redes**

Importancia por integridad

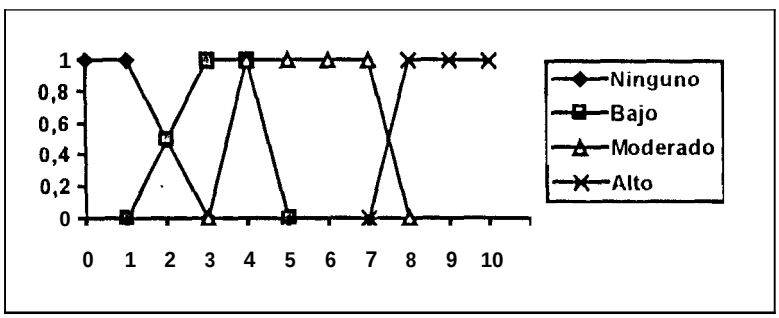


Figura No. **A-8 Funciones de membresía para importancia por integridad por parte del Jefe de Redes**

Importancia por confidencialidad

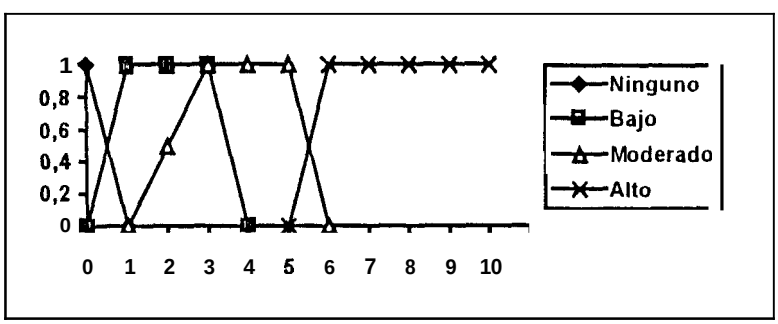


Figura No. **A-9 Funciones de membresía para importancia por confidencialidad por parte del Jefe de Redes**

Calificacion de variables por **recurso** por parte del Jefe de redes

Una vez que el Jefe de Redes definio a juicio personal las funciones de membresía se le solicitó que llenara la siguiente tabla:

Recursos		Riesgos (posibles ataques)			Importancia		
No	Nombre o descripción	Acceso no autorizado	Robo de Info.	Negación de servicios	Disponi-bilidad	Integridad	Confiden.
01	Ruteador IBM 2210 Enlace con Ecuanet	Bajo	Ningún	Bajo	Alta	Alta	Baja
02	Ruteador IBM 2210 Enlace Las Peñas	Bajo	Ningún	Bajo	**Alta**	Alta	Baja
03	ComServers TELEBIT	Bajo	Bajo	Bajo	Alta	Alta	Moderada
04	Goliat						
a	SPARC 20:	Moderado	Bajo	Bajo	Alta	Alta	Alta
b	S.O.: Solaris 2.5	Moderado	Bajo	Bajo	**Alta**	**Alta**	Alta
c	DNS	Alto	Alto	Modcrado	Baja	Alta	Ninguna
d	SMTP (SendMail)	Bajo	Bajo	Bajc	Alta	Alta	Alta
e	FTP (anónimo)	Ninguno	Ninguno	Ninguno	Ninguna	Ninguna	Ninguna
f	HTTP 1.0	Moderado	Bajo	Bajo	Moderada	Moderada	Moderad
g	Telnet	Moderado	Bajo	Bajo	Alta	Alta	Alta
05	David						
a	SPARC 2	Ninguno	Ninguno	Bajo	Moderada	Moderada	Baja
b	S.O.: Solaris	Ninguno	Ninguno	Bajo	Moderada	Moderada	Baja
06	Maquina Admin.						
a	RISC 6000	Bajo	Bajo	Bajo	Alta	Alta	Alta
b	S.O.: UNIX **AIX**	Bajo	Bajo	Bajo	Alta	Alta	Alta
c	Nc! View	Bajo	Bajo	Bqjo	Moderada	Alta	Moderada
07	S. Base dc datos						
a	RISC 6000	Bajo	Bajo	Bajo	Alta	Alta	Alta
b	S.O.: UNIX AIX	Bajo	Bajo	Bajo	Alta	Alta	Alta
c	DB/2	Alto	Alto	**Alto**	Alta	Alta	Alta
08	S. Aplicaciones						
a	RISC 6000	Bajo	Bajo	Bajo	**Alta**	**Alta**	Alta
b	S.O.: UNIX AIX	Bajo	Bajo	Bajo	**Alta**	Alta	Alta
	Aplicaciones Servidoras:						
c	Presupuesto	Alto	**Alto**	**Alto**	Alta	Alto	Alta

d	Contabilidad	**Alto**	**Alto**	**Alto**	Alta	Alta	Alta
e	Tesorería	**Alto**	**Alto**	**Alto**	Alta	Alta	Alta
f	Académica	**Alto**	**Alto**	**Alto**	**Alta**	Alta	**Alta**

Los valores que se encuentran en la tabla anterior representan lo que piensa el Jefe de Redes para cada uno de los recursos.

Definiciones de funciones de membresia por parte del director de CESERCOMP

El director de CESERCOMP estimo que las funciones de membresia eran una sóla para el riesgo y una sóla para la importancia.

Riesgo

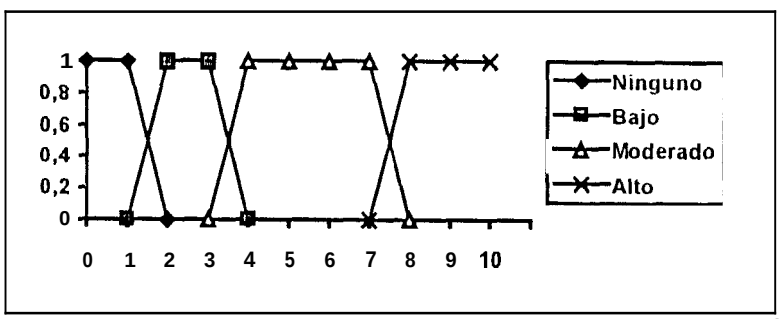


Figura No. **A-10 Funciones de membresia para riesgo por parte del Director de CESERCOMP**

Importancia

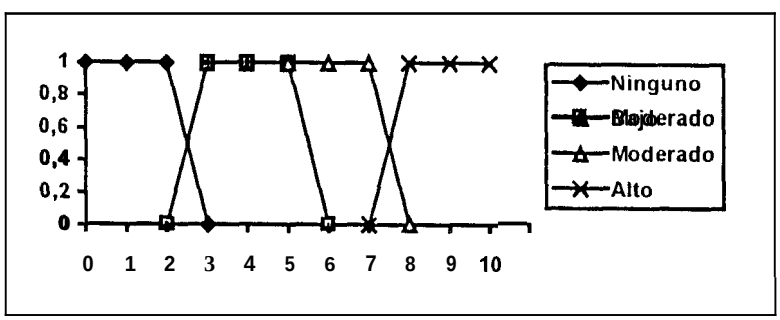


Figura NO. A-11 Funciones de membresia para importancia por parte del Director de CESERCOMP

Calificacion de variables por recurso por parte del Director de CESERCOMP

De igual manera, el Director de CESERCOMP estimo los siguientes datos para los recursos:

Recursos		Riesgos (posibles ataques)			Importancia		
No	Nombre o descripción	Acceso no autorizado	Robo de Info.	Negación de servicios	Disponi-bilidad	Integridad	Confiden.
01	Ruteador IBM 2210 Enlace con Ecuanet	Bajo	Bajo	BiIJO	Alta	Alta	Alta
02	Ruteador IBM 2210 Enlace Las Peñas	Bajo	Bajo	Bajo	Alta	Alta	Alta
03	ComServers TELEBIT	Bajo	Bajo	Bajo	Moderada	Alta	Alta
04	Gohat						
a	SPARC *20:*	Moderado	Moderado	Moderado	Moderada	Alta	Alta
b	S.O.: Solaris 2.5	Moderado	Bajo	Moderado	Alta	Alta	Alta
	Servidores:						
c	DNS	Bajo	Bajo	Bajo	Alta	Alta	Moderada
d	SMTP (SendMail)	Moderado	Moderado	Modcrado	Moderada	Alta	Moderada
e	FTP (anónimo)	Alto	**Alto**	Moderado	Baja	Baja	Baja
f	HTTP 1.0	Moderado	Moderado	Moderado	Baja	Moderada	Moderada
g	Telnet	Bajo	Bajo	Bajo	Baja	Moderada	Alta
05	David						
a	SPARC 2	Moderado	Moderado	Moderado	Moderada	Alta	Alta
b	S.O.: Solaris	Moderado	Bajo	Moderado	Moderada	Moderada	Alta
06	Maquina Admin.						
a	RISC 6000	Ninguno	Ninguno	Ninguno	Baja	Alta	Alta
b	S.O.: UNIX **AIX**	Ninguno	Ninguno	Ninguno	Alta	Alta	Moderada
c	Ncr View	Ninguno	Ninguno	Ninguno	Baja	Alta	Alta
07	S. Base de datos						
a	RISC 6000	Bajo	Bajo	Bajo	Baja	Alta	Alta
b	S.O.: UNIX AIX	Bajo	BiIJO	Bajo	Alta	Alta	Moderada
c	DB/2	Bajo	Bajo	Bajo	Alta	Alta	Alta
08	S Aplicaciones						
a	RISC 6000	Bajo	Bajo	BiIJO	Baja	Alta	Alta
b	S O UNIX AIX	Bajo	BiIJO	Bajo	Alta	Alta	Moderada

	Aplicaciones Servidoras:						
c	Presupuesto	Bajo	Bajo	Bajo	Alta	Alta	Alta
d	Contabilidad	Bajo	Bajo	Bajo	Alta	Alta	Alta
e	Tesorería	Bajo	Bajo	Bajo	Alta	Alta	Alta
f	Académica	Bajo	Bajo	Bajo	Alta	Alta	Alta

Tabla A-3
Cuadro de calificación de recursos por parte del director de CESERCOMP

A.2.2. Procesamiento

El procesamiento comprende los tres primeros bloques o modulos de la figura **A-3.** Estos bloques son: reglas para determinar ocurrencias de ataques, eglas para determinar la importancia y reglas para determinar el riesgo total de un recurso. Los dos primeros bloques son para determinar un solo factor de importancia y riesgo respectivamente a partir de las entradas y el ultimo es para hallar el riesgo total.

A.2.2.1. Módulos de Riesgo e importancia

Cada uno de los datos de entrada se evaluan en los modulos de riesgo e importancia respectivamente. Estos modulos contienen reglas que califican el riesgo y la importancia otorgadas por los expertos, estas reglas constituyen la base de conocimiento apta para evaluar los diferentes terminos lingüísticos de entrada. Cada base de conocimiento arroja un solo resultado para el riesgo e importancia reflejados en terminos linguisticos y con nuevas funciones de membresia para ellos.

Reglas para determinar el riesgo segun el jefe de Redes de **CESERCOMP**

Las siguientes reglas conjugan los tres tipos de riesgo para obtener un solo factor de riesgo. El numero de reglas depende de las combinaciones de los valores otorgados por el jefe de Redes de CESERCOMP en la tabla **A-2.**

No.	Acceso no autorizado	Robo de Info.	Negación de servicio	Factor de riesgo
1	Alto	alto	alto	Alto
2	alto	alto	moderado	Alto
3	moderado	bajo	bajo	moderado
4	bajo	bajo	bajo	bajo
5	bajo	ninguno	bajo	bajo
6	ninguno	ninguno	bajo	bajo
7	ninguno	ninguno	ninguno	ninguno

Tabla A-4
Reglas para obtener el factor riesgo por parte del Jefe de Redes de CESERCOMP

Definición de las funciones de membresía para el factor de riesgo según el jefe de redes de CESERCOMP

Para hallar la función de membresía, el experto determinó en base a su criterio que ésta debe ser el resultado de sumar las funciones de membresía de riesgo no autorizado en una proporción de 1, robo de información en una proporción de 0.5 y negación de servicios. en una proporción de 0.5. Luego llevar las funciones a una escala de 0 a 1. Después de todo este procedimiento, fue necesario suavizar las curvas ya que en algunos casos las funciones resultantes no llegaban a 1 y los puentes eran muy dispersos. En la figura A-12 se puede observar las funciones de membresía para el riesgo en un gráfico membresía versus riesgo(rango 1 a 10).

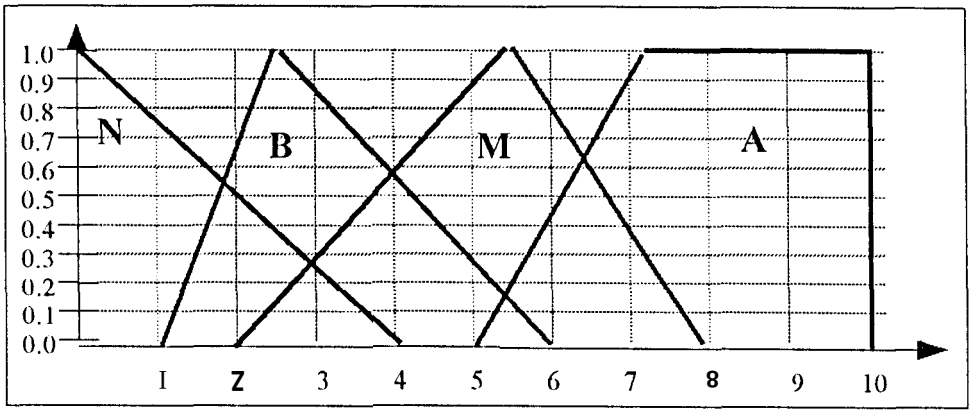


Figura No. A-12 Funciones de membresía para el factor riesgo por parte del Jefe de Redes

Reglas para determinar la importancia segun el jefe de Redes de CESERCOMP

Al igual que en el caso de riesgo, se solicitó al Jefe de Redes que dictaminara las siguientss reglas a fin de calcular un solo factor de importancia a partir de las entradas. Se solicitó solo 8 reglas ya que estas son las posibles combinaciones de las entradas otorgadas por el experto en la tabla **A-2.**

No.	Disponibilidad	Integridad	Confidencialidad	Factor de Importancia
1	Alta	alta	alta	alta
2	alta	alta	moderada	alta
3	alta	alta	baja	alta
4	moderada	moderada	moderada	moderada
5	moderada	moderada	baja	moderada
6	moderada	alta	moderada	moderada
7	baja	alta	ninguna	moderada
8	ninguna	ninguna	ninguna	ninguna

Tabla A-5
Reglas para obtener el factor importancia por parte del Jefe de Redes de CESERCOMP

Para el factor de importancia tambien es necesario que el experto defina funciones de membresia.

Definición de las funciones de membresia para el factor de importancia segun el jefe de redes de CESERCOMP

Para hallar la funcion de membresia, el experto determino que esta debe ser producto de sumar las graficas de disponibilidad en una proporcion de 1, integridad en una proporcion de 0.5 y confidencialidad en una proporcion de 1. Despues de todo este procedimiento, fue necesario suavizar las curvas porque estas no llegaban a 1 sus puntos eran dispersos. En la figura No. A-13 se representa las funciones de membresia para la importancia.

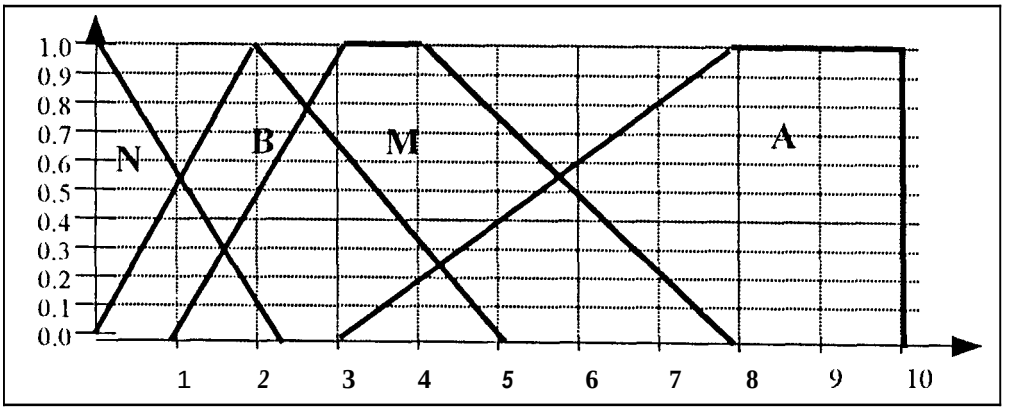


Figura No. A-I3 Funciones de membresia para el factor importancia por parte del Jefe de Redes

Reglas para determinar el riesgo segun el Director de CESERCOMP

Se solicit6 las siguientes reglas al director de CESERCOMP ya que estas son las posibles combinaciones de las variables de riesgo de los recursos calificados por el de acuerdo a la tabla A-3.

No.	Acceso no autorizado	Robo de Info.	Negación de servicio	Factor de riesgo
1	alto	alto	alto	Alto
2	alto	alto	moderado	Alto
3	alto	moderado	alto	moderado
4	alto	moderado	moderado	moderado
5	moderado	moderado	alto	moderado
6	moderado	moderado	bajo	moderado
7	bajo	moderado	bajo	moderado
8	ninguno	ninguno	ninguno	ninguno
9				
10	Moderado	Bajo	Moderado	moderado
11	Bajo	Bajo	Bajo	Bajo
12	Moderado	Moderado	Moderado	Moderado
13	Moderado	Bajo	Moderado	moderado

Reglas para obtener el factor riesgo por parte del Director de CESERCOMP

Estas reglas son numeradas porque van a ser referenciadas en el analisis.

Definición de las funciones de rnembresia para el factor de riesgo según el Director de redes de CESERCOMP

El experto estimo que las funciones de membresia para el factor de riesgo son las mismas que se definieron en la figura No.A-10

Reglas para deterrninar la importancia segun el Director de CESERCOMP

Se solicitó las siguientes reglas al director de CESERCOMP ya que estas son las posibles combinaciones de las variables de riesgo de los recursos calificados por el de acuerdo a la tabla A-3.

No.	Disponibilidad	Integridad	Confidencialidad	Factor de Importancia
1	Alta	alta	alta	alta
2	alta	alta	moderada	alta
3	moderada	alta	alta	alta
4	moderada	alta	moderada	moderada
5	moderada	moderada	alta	moderada
6	baja	alta	alta	alta
7	baja	moderada	moderada	moderada
8	baja	moderada	alta	moderada
9	baja	baja	baja	baja
10	ninguna	baja	baja	baja

Tabla A-6
Reglas para obtener el factor importancia por parte del Director de CESERCOMP

Estas reglas son numeradas porque van a ser referenciadas en el analisis.

Definición de las funciones de rnernbresia para el factor de importancia segun el Director de redes de CESERCOMP

El experto estimo que las funciones de membresia para el factor de riesgo son las mismas que se definieron en la figura No.A-11

A.2.2.2. Modulo de riesgo Total

Este es el tercer bloque de procesamiento del sistema propuesto en la figura No. A-3. Una vez calculado ambos factores riesgo e importancia y obtenidos sus funciones de rnembresia correspondientes (figuras A-12, A-13, A-10, A-11), las salidas de los modulos anteriores ingresa

a un nuevo modulo que los procesara para obtener un resultado de riesgo total. Este nuevo modulo al igual que los anteriores contiene reglas que constituyen una base de conocimiento para evaluar los datos de entrada. Al igual que en la fase anterior, estas reglas son otorgadas por los expertos.

Reglas para el riesgo total por parte del Jefe de Redes de CESERCOMP

De acuerdo a las posibles combinaciones de los factores de riesgo e importancia de acuerdo a las tablas A-4 y A-5.

No.	Factor riesgo	Factor importancia	Riesgo total
1	Alto	Alta	Alto
2	Alto	Moderada	Alto
3	Alto	Baja	Alto
4	Alto	Ninguna	Bajo
5	Moderado	Alta	Alto
6	Moderado	Moderada	Alto
7	Moderado	Baja	Bajo
8	Moderado	Ninguna	Ninguno
9	Bajo	Alta	Moderado
10	Bajo	Moderada	Bajo
11	Bajo	Baja	Bajo
12	Bajo	Ninguna	Ninguno
13	Ninguno	Alta	Bajo
14	Ninguno	Moderada	Bajo
15	Ninguno	Baja	Ninguno
16	Ninguno	Ninguna	Ninguno

Tabla A-7
Reglas para obtener el riesgo total por parte del Jefe de Redes

Las reglas son numeradas debido a que seran referenciadas en el análisis posterior.

No.	Factor riesgo	Factor importancia	Riesgo total
1	Alto	Alta	Alto
2	Alto	Moderada	Alto
3	Alto	Baja	Moderado
4	Alto	Ninguna	Alto
5	Moderado	Alta	Alto
6	Moderado	Moderada	Moderado

7	Moderado	Baja	Moderado
8	Moderado	Ninguna	Bajo
9	Bajo	Alta	Moderado
10	Bajo	Moderada	Moderado
11	Bajo	Baja	Bajo
12	Bajo	Ninguna	Bajo
13	Ninguno	Alta	Bajo
14	Ninguno	Moderada	Bajo
15	Ninguno	Baja	Bajo
16	Ninguno	Ninguna	Ninguno

Tabla A-8
Reglas para obtener el riesgo total por parte del Director de CESERCOMP

En este modulo las reglas son evaluadas usando la tecnica del min-max.

1. La tecnica del min-max establece que el valor de verdad de una regla es determinada en base a la conjuncion de sus antecedentes (en este caso riesgo e importancia).
2. La conjuncion de dos valores difusos es determinado en base al minimo grado de membresia de ambos [PELA95].
3. Por lo tanto, el valor de verdad de una regla es el menor grado de verdad de sus antecedentes.
4. Si cualquier resultado es consecuencia de mas de una regla, entonces ese resultado debe poseer el maximo grado de verdad de todas las reglas que lo incluyen como consecuencia.

Para explicar mejor la tecnica, como ejemplo calculemos el riesgo del recurso 04a segun el director de CESERCOMP. En los dos primeros bloques del analizador de riesgo se obtienen como resultados el factor riesgo y el factor. importancia. Ambos resultados son **altos** de acuerdo a las reglas establecidas en las tablas A-6 y A-7.

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla
Moderado	Moderado	Moderado	Moderado	12

Alto	Alto	Alto	Alto	1

Luego las reglas que intervienen son las posibles combinaciones de los valores que pueden tomar estas variables:

No.	Factor riesgo	Factor importancia	Riesgo total	Grado Membresia
1	Alto	Alta	Alto	10
2	Alto	Moderada	Alto	0.5
5	Moderado	Alta	Moderado	0.5
6	Moderado	Moderada	Moderado	0.5
9	Bajo	Alto	Moderado	0.5
10	Baio	Moderado	Moderado	0.5

La evaluación de las reglas seria de la siguiente manera:

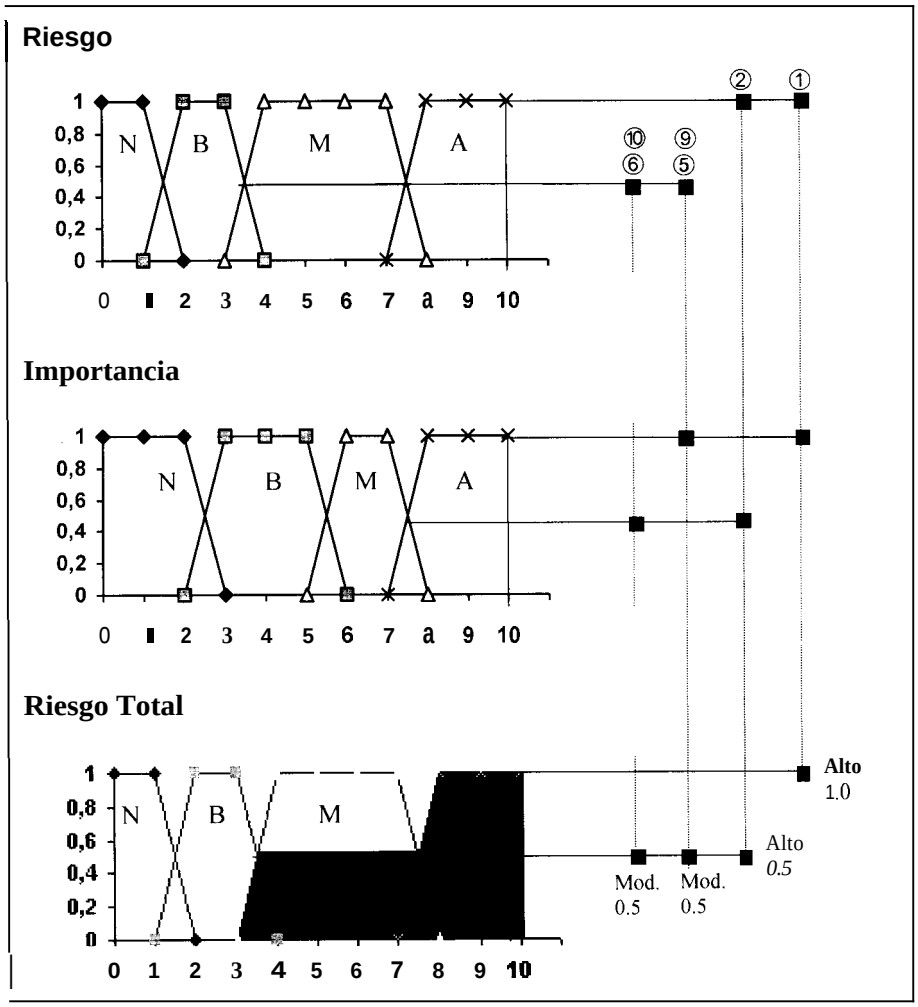


Figura No. A-14 Cálculo del riesgo total del recurso 04a con datos del Director de CESERCOMP

El resultado que arroja este modulo es un valor difuso, el cual luego ingresa a un decodificador de lógica difusa para ser convertido en un valor numérico mediante el método del maximo peso, el cual consiste en promediar los puntos de maxima posibilidad para cada conclusion difusa. Para el recurso 01, entonces el valor numérico es:

$$Z = \frac{1\,(8+9+10) + 0.5\,(4+5+6+7)}{1(3) + 0.5(4)} = 7.6$$

Este valor es el equivalente en terminos numericos sobre una escala de 1 a 10.

De acuerdo a lo anterior, se suman los puntos de la region sombreada por los valores de membresia correspondientes y se divide para el resultado de la suma de los valores de membresia por el numero de puntos que los contienen.

A.2.3. Salidas

La salida del sistema analizador de riesgo es un valor numerico, el cual nuevamente es convertido en lógica difusa interpolando el valor numerico con las funciones de membresia dependiendo del mayor grado de membresia de los valores difusos que puede tomar. En el caso del recurso 01, el valor de membresia que puede tomar es 0.51 de alto y 0.49 de moderado.

En este caso en particular, no se puede decidir si el valor numerico resultante es enteramente alto o enteramente moderado, sin embargo da una idea de que el recurso tiene un riesgo alto pero con un grado de moderado.

A.3. Desarrollo del Analisis de riesgo

Una vez explicado como se realiza un analisis de riesgo utilizando lógica difusa, para el desarrollo se van obviar ciertos pasos detallados con el fin de pasar a las conclusiones que representan lo mas importante de este estudio. Primero se desarrollaran los dos analisis por separado, para luego contrastar los resultados de ambos y obtener conclusiones.

A.3.1. Analisis de riesgo de los recursos del backbone con datos del Director de CESERCOMP

1. recurso **01**

Para el riesgo:

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla
Bajo	Bajo	Bajo	Bajo	11

Para la importancia:

Alta	Alta	Alta	Alta	1

Los grados de membresia son:

Riesgo	Moderado	1.0
	Bajo	0.5
	Alto	0.5
Importancia	Moderada	1.0
	Baja	0.5
	Alta	0.5

El riesgo total es:

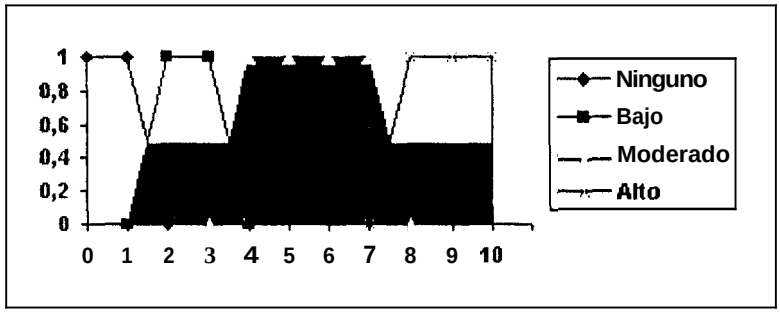


Figura No. A-15 Calculo del riesgo del recurso 01

El valor numérico que representa el riesgo total es:

$$Z = \frac{0.5(2+3) + 1(4+5+6+7) + 0.5(8+9+10)}{0.5(2) + 0.5(3) + 1(4)} = 6.08$$

El valor numérico del riesgo total es 6.08 con un grado de 10 de moderado, es decir el riesgo es totalmente moderado.

2. recurso 02

Acceso no autorizado	Robo de Info	Negacion de Sew.	Resultado	No. Regla
Bajo	Bajo	Bajo	Bajo	11

Para la importancia:

Moderada	Alta	Alta	Alta	3

Ambos factores riesgo e importancia son altos al igual que el recurso 01. Por lo tanto el riesgo total tambien es igual al riesgo total del recurso 01.

3. Recurso 03

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla
Bajo	Bajo	Bajo	Bajo	11

Moderada	Alta	Alta	Alta	3

4. Recurso 04.

04.b. Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Sew.	Resultado	No. Regla
Moderado	Bajo	Moderado	Moderado	13

Alta	Alta	Alta	Alta	3

Al poseer los mismos valores el riesgo total es igual al riesgo total del recurso 04.a..

04.c. Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla
Bajo	Bajo	Bajo	Bajo	11

Alta	Alta	Moderada	**Alta**	**3**

Ambos factores riesgo e importancia son altos al igual que el recurso 01. Por lo tanto el riesgo total tambien es igual al riesgo total del recurso 01.

04.d. Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla
Moderado	Moderado	Moderado	Moderado	12

Para la importancia:

Moderada	Alta	Moderada	Alta	4

Ambos factores riesgo e importancia son altos al igual que el recurso 04a. Por lo tanto el riesgo total tambien es igual al riesgo total del recurso 04a.

04.d. Para el riesgo

Para el riesgo: .

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla
Alto	**Alto**	Moderado	Alto	2

Baja	Baja	Baja	Baja	9

Por lo tanto la grafica del riesgo total seria:

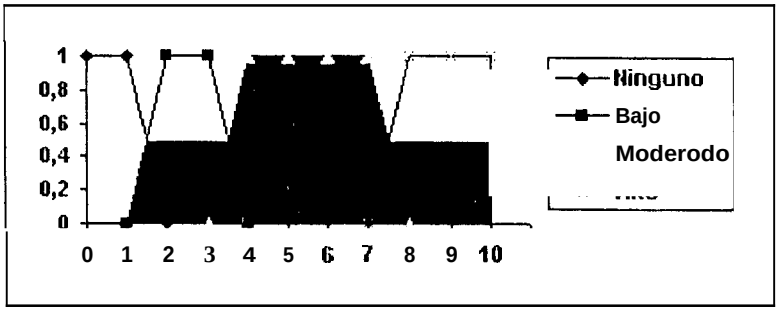


Figura No. A-16 Cálculo del riesgo total del recurso 04.e con datos del Director de CESERCOMP

El valor numérico del riesgo total es 6.08 con un grado de 1.0 de moderado, es decir el riesgo es totalmente moderado.

04.f. Para el riesgo:

Acceso no autorizado	Robo de Info	Negación de Sew.	Resultado	No. Regla
Moderado	Moderado	Moderado	Moderado	12

Para la importancia:

Los grados de membresia son:

Riesgo	Moderado	1.0
	Bajo	**0.5**
	Alto	**0.5**
Importancia	Moderada	1.0
	Baja	**0.5**
	Alta	**0.5**

Por lo tanto la grafica del riesgo total seria:

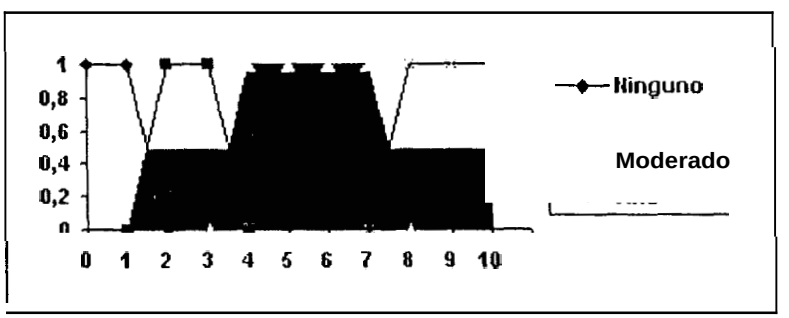


Figura No. **A-17 Cálculo del riesgo total del recurso 04.f con datos del Director de CESERCOMP**

El valor numérico del riesgo total es 6.08 con un grado de 1.0 de moderado, es decir el riesgo es totalmente moderado.

04.g.Para el riesgo:

Acceso no	Robo de Info	Negación de Serv.	Resultado	No. Regla
Bajo	Bajo	Bajo	Bajo	11

Para la importancia:

Baja	Moderada	Alta	Moderada	8

Los grados de membresia son:

Riesgo Moderado 1.0

Bajo **0.5**

Alto **0.5**

Importancia Moderada 1.0

Baja **0.5**

Alta **0.5**

Por lo tanto la grafica del riesgo total seria:

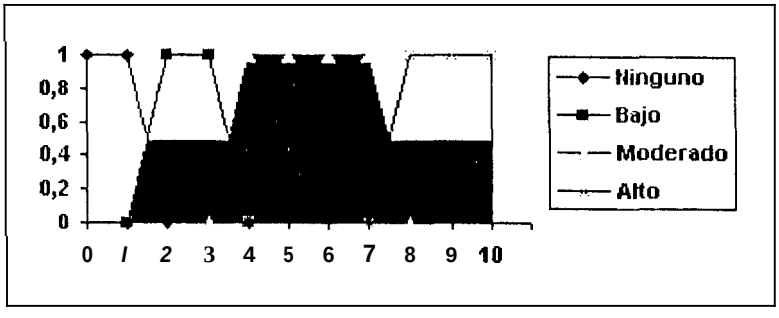


Figura NO. A-18 Cálculo del riesgo total del recurso 04.g con datos del Director de CESERCOMP

El valor numérico del riesgo total es 6.08 con un grado de 1.0 de moderado, es decir el riesgo es totalmente moderado.

5. Recurso 05

05.a. Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Sew.	Resultado	No. Regla
Moderado	Moderado	Moderado	Moderado	12

Para la importancia:

Ninguna	Baja	Baja	Baja	10

El riesgo total es igual al riesgo total del recurso 04.a.

05.b. Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Sew.	Resultado	No. Regla
Moderado	Bajo	Moderado	Alto	13

Para la importancia:

Moderada	Alta	Alta	Alta	1

Los factores de riesgo e importancia son altos al igual que los factores del recurso 04f. Por lo tanto el riesgo total es igual al riesgo total del recurso 04f.

6. Recurso 06

06.a.Para el riesgo:

Acceso no	Robo de Info	Negacion de Sew.	Resultado	No. Regla
Ninguno	Ninguno	Ninguno	Ninguno	8

Para la importancia:

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla
Moderada	Moderada	Alta	Moderada	5

Los grados de membresia son:

Riesgo Moderado 1.0

	Bajo	0.5
	Alto	0.5
Importancia	Moderada	1.0
	Baja	0.5
	Alta	0.5

Por lo tanto la grafica del riesgo total seria:

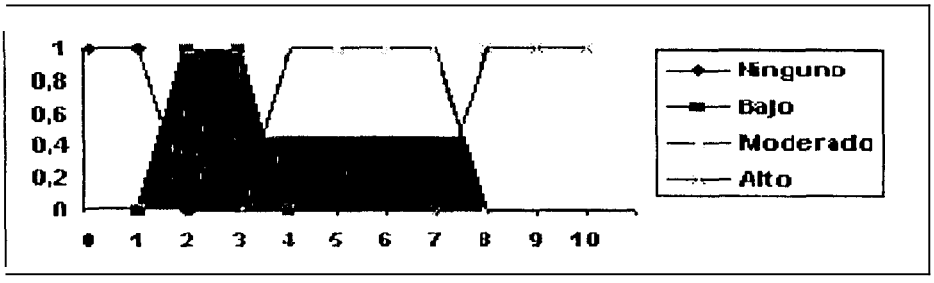


Figura No. **A-19 Cálculo del riesgo total del recurso 06.a con datos del Director de CESERCOMP**

El riesgo total seria:

$$Z= \frac{1(2+3) + 0.5\,(4+5+6+7)}{1(2) + 4(0.5)} = 4.0$$

Significa que el riesgo total del recurso 06.a. es moderado.

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla
Ninguno	Ninguno	Ninguno	Ninguno	8

Baja	Alta	Alta	Alta	6

Ambos factores son altos al igual que los del recurso 06a. Por lo tanto el riesgo total es el mismo **4.0** moderado.

Acceso no autorizado	Robo de Info	Negacion de Sew.	Resultado	No. Regla
Ninguno	Ninguno	Ninguno	Ninguno	8

Para la importancia:

Alta	Alta	Moderada	Alta	2

El riesgo total es igual al riesgo del recurso 0.6.a.

7. Recurso 07

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla
Baio	Baio	Baio	Baio	11

Baja	Alta	Alta	Alta	6

El riesgo total es igual al riesgo del recurso 01.

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla
Bajo	Bajo	Bajo	Bajo	11

Para la importancia:

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla

El riesgo total es igual al riesgo total del recurso 01.

07.c.Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla
Bajo	Bajo	Bajo	Bajo	11

Para la importancia:

Alta	Alta	Moderado	Alta	2

El riesgo total es igual al riesgo total del recurso 01.

8. recurso 08.

Todos las partes integrantes de este recurso poseen los mismos factores tanto de riesgo e importancia como el recurso 01. Por lo tanto poseen el mismo riesgo total que el recurso 01.

A.3.2. Análisis de riesgo de los recursos del backbone con datos del Jefe de redes de CESERCOMP

1. Recurso 01

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla Tabla A-4
Bajo	Ninguno	Bajo	Bajo	5

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5
Alta	Alta	Baja	Alta	3

Riesgo	Bajo	1.0
	Ninguno	0.54
	Moderado	0.56
	Alto	0.14
Importancia	Alta	1.0
	Moderada	0.55
	Baja	**0.24**

Por lo tanto la grafica del riesgo total seria:

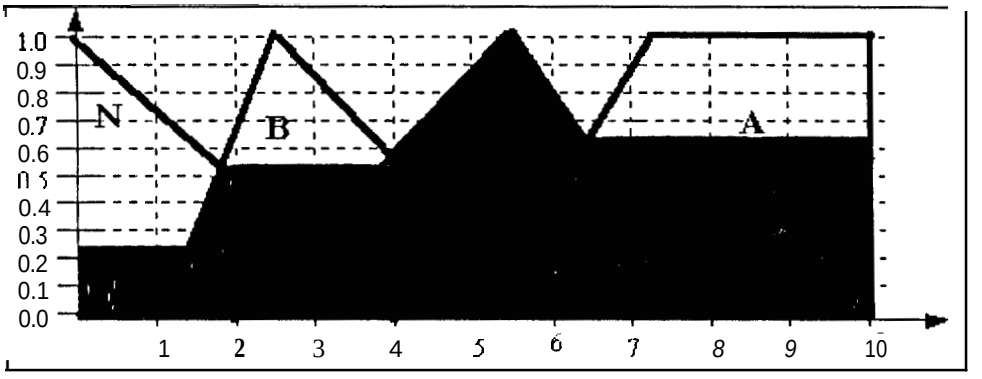


Figura No. **A-20 Cálculo del riesgo total del recurso 01 con datos del Jefe de Rede**

El valor numérico del riesgo es:

$$Z = \frac{0.55(2.5)+1(5.5)+0.56(7.2+X+9+10)}{0.55+1+0.56(4)+0.24} = 6.45$$

El riesgo total es de 6.45 con un grado 0.66 de moderado y 0.64 de alto.

2. recurso 02

Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 01, el riesgo total del recurso 02 es igual al recurso 01, 6.45 con un grado 0.66 de moderado y 0.64 de alto.

3. recurso 03

Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Sew.	Resultado	No. Regla Tabla A-4
Bajo	Bajo	Bajo	Bajo	4

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5
Alta	Alta	Moderada	Alta	2

tiene el mismo riesgo total que el recurso 01

4. recurso 04

04.a Para el riesgo:

Acceso no autorizado	Robo de Info	Negacion de Serv.	Resultado	No. Regla Tabla A-4
Moderado	Bajo	Bajo	Moderado	3

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5
Alta	Alta	Alta	Alta	1

Los grados de membresia son:

Riesgo	Moderado	**1.0**
	Ninguno	0.27
	Bajo	0.56
	Alto	0.63
Importancia	Alta	1.0
	Moderada	**0.55**
	Baja	0.24

Por lo tanto la grafica del riesgo total seria:

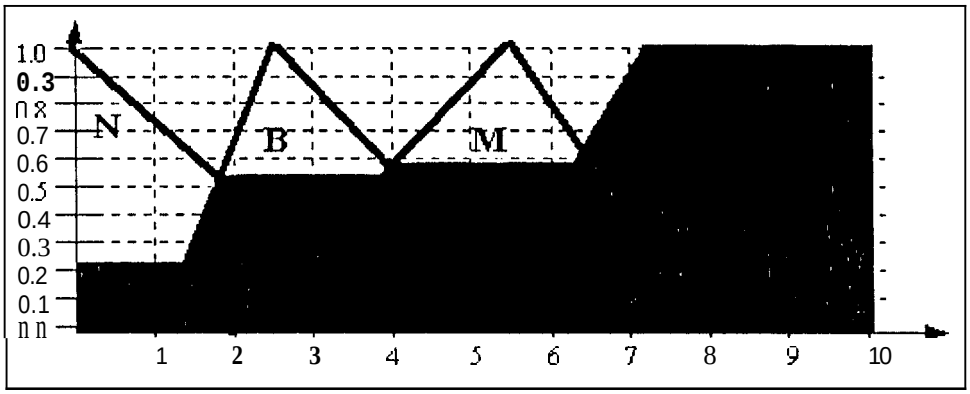


Figura No. **A-21 Cálculo del riesgo total del recurso 04.a con datos del Jefe de Redes**

$$Z = \frac{0.55(2.5)+0.56(5.5)+1(7.2+8+9+10)+0.24(0)}{0.24+0.55+0.56+1(4)} = 7.3$$

El riesgo total es 7.3 con un grado de 1.0 de alto

04.b Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 04.a, el riesgo total del recurso 04.b es igual al riesgo total del recurso 04.a.; es decir, 7.3 con un grado 1.0 de alto.

04.c Para el riesgo:

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla Tabla A-4
Alto	Alto	Moderado	Alto	2

Para la importancia:

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla
Baja	Alta	Ninguna	Moderada	7

Los grados de membresia son:

Riesgo Alto 1.0

Bajo 0.14

	Moderado	0.63
Importancia	Moderada	**1.0**
	Alta	0.55
	Baja	0.8

Por lo tanto la grafica del riesgo total seria:

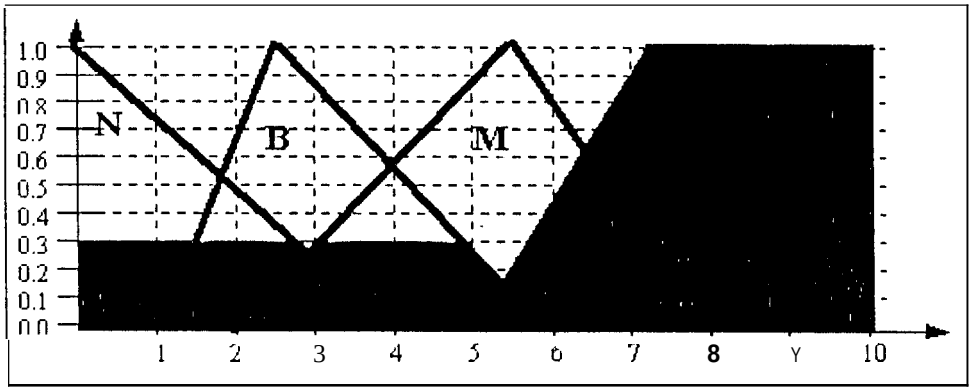


Figura No. **A-22 Cálculo del riesgo** total **del recurso 04.c con datos del Jefe** de **Redes**

El valor numérico del riesgo es:

$$Z = \frac{1(7.2+8+9+10)+0.3(0)+0.3(2.5)+0.14(5.5)}{1(4)+0.3+0.3+0.14} = 7.5$$

El riesgo total es de *7.5* con un grado de 1.0 de alto.

04.d Para el riesgo:

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla Tabla A-4
Bajo	Bajo	Bajo	Bajo	**4**

Para la importancia:

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla
Alta	Alta	Alta	**Alta**	1

El riesgo es bajo y la importancia alta al igual que en el recurso 01. Por lo tanto el recurso 04.d tiene el mismo riesgo total que el recurso 01.

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla Tabla A-4
Ninguno	Ninguno	Ninguno	Ninguno	7

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5
Ninguna	Ninguna	Ninguna	Ninguna	8

Los grados de membresia son:

Riesgo	Ninguno	**1.0**
	Bajo	**0.54**
	Moderado	*0.27*
Importancia	Ninguna	1.0
	Baja	0.52
	Moderada	0.3

Por lo tanto la grafica del riesgo total seria

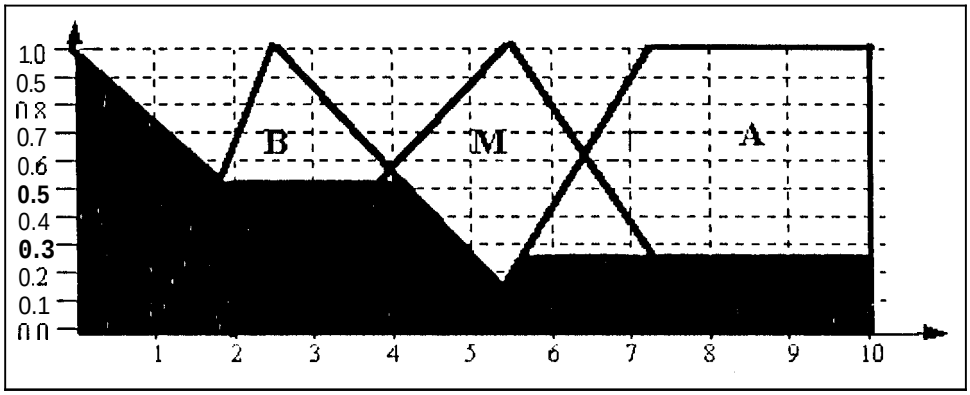


Figura No. **A-23 Cálculo del riesgo total del recurso 04.e con datos del Jefe de Redes**

El resultado numérico del riesgo total es:

$$Z = \frac{1(0)+0.25(2.5)+0.27(7.2+8+9+10)}{1+0.52+0.27(4)} = 4.05$$

El riesgo total es de 4.05 con un grado 0.65 tanto en bajo como en moderado. Este caso es especial, ya que el riesgo numérico coincide con punto de intersección entre bajo y rnoderado.

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla Tabla A-4
Moderado	Bajo	Bajo	Moderado	3

Para la importancia:

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5
Moderada	Moderada	Moderada	Moderada	4

Los grados de membresia son:

Riesgo	Moderado	1.0
	Ninguno	0.27
	Bajo	0.56
	Alto	0.63

Importancia	Moderada	1.0
	Ninguna	0.3
	Baja	0.8
	Alta	**0.55**

Por lo tanto la grafica del riesgo total sería

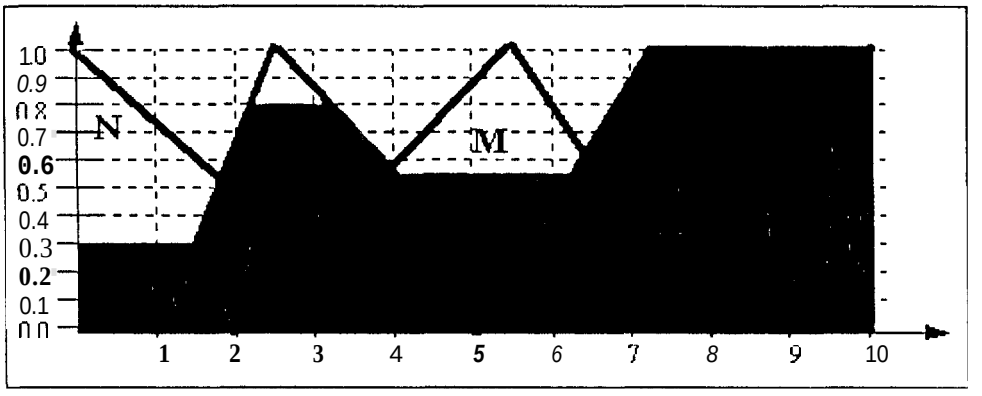


Figura No. A-24 Cálculo del riesgo total del recurso 04.f con datos del Jefe de Redes

El valor numérico del riesgo total es:

$$Z = \frac{0.3(0)+0.8(2.5)+0.55(5.5)+1(7.2+8+9+10)}{0.3+0.8+0.55+1(4)} = 6.94$$

El riesgo total es de **6.94** con un grado de 0.89 de alto y 0.41 de moderado.

04.g Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 04.a, el riesgo total del recurso 04.g es igual al riesgo total del recurso 04.a.; es decir, 7.3 con un grado 1.0 de alto.

5. recurso 05

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla Tabla A-4
Ninguno	Ninguno	Bajo	Bajo	6

Para la importancia:

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5
Moderada	Moderada	Baja	Moderada	5

Los grados de membresia son:

Riesgo	Bajo	1.0
	Ninguno	0.54
	Moderado	0.56
	Alto	0.14
Importancia	Moderada	1.0
	Ninguna	0.3
	Baja	0.8
	Alta	0.55

Por lo tanto la grafica del riesgo total seria

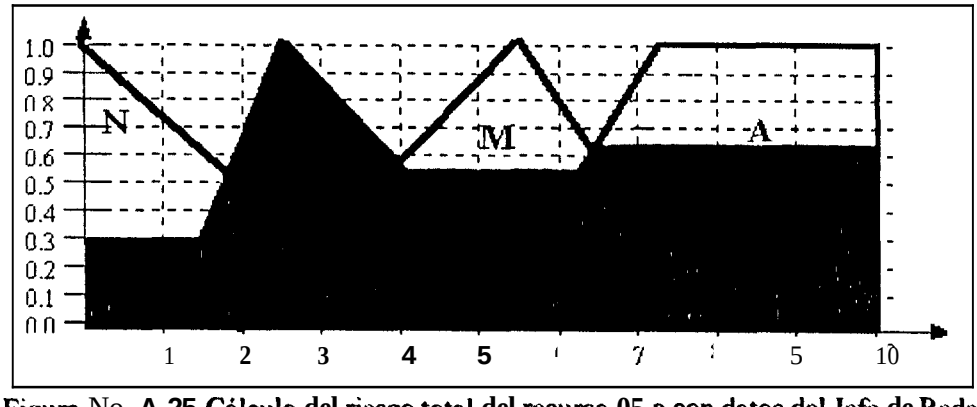


Figura No. **A-25 Cálculo del riesgo total del recurso 05.a con datos del Jefe de Redes**

El resultado numérico es:

$$Z = \frac{0.3(0)+1(2.5)+0.55(5.5)+0.56(7.2+8+9+10)}{0.3+1+0.55+0.56(4)} = 6.03$$

El riesgo total es de 6.03 con un grado de 0.42 de alto y 0.8 de moderado.

05.b Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 05.a, el riesgo total del recurso 05.b es igual al riesgo total del recurso 05.a.; es decir, 6.03 con un grado de 0.42 de alto y 0.8 de moderado.

6. recurso 06

06.a Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 04.d, el riesgo total del recurso 06.a es igual al riesgo total del recurso 04.d.; es decir, 6.45 con un grado de 0.66 de moderado y 0.64 de alto.

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla Tabla A-4
Bajo	Bajo	Bajo	Bajo	**4**

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5
Moderada	Alta	Moderada	Moderada	*6*

El factor de riesgo es bajo y el de importancia moderada, al igual que el recurso 01. Por lo tanto el riesgo total es el mismo del recurso 01, 6.45 con un grado de 0.66 de moderado y 0.64 de alto

7. recurso 07

07.a Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 04.d, el riesgo total del recurso 07.a es igual al riesgo total del recurso 04.d; es decir, 6.45 con un grado de 0.66 de rnoderado y 0.64 de alto.

07.b Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 04.d, el riesgo total del recurso 07.b es igual al riesgo total del recurso 04.d; es decir, 6.45 con un grado de 0.66 de moderado y 0.64 de alto.

07.c Para el riesgo:

Acceso no autorizado	Robo de Info	Negación de Serv.	Resultado	No. Regla Tabla A-4
Alto	Alto	Alto	Alto	1

Para la irnportancia:

Disponibilidad	Integridad	Confidencialidad	Resultado	No. Regla Tabla A-5

Los grados de membresia son:

Riesgo	Alto	1.0
	Bajo	0.14
	Moderado	0.63
Importancia	Alta	1.0
	Baja	**0.24**
	Moderada	0.55

Por lo tanto la grafica del riesgo total seria

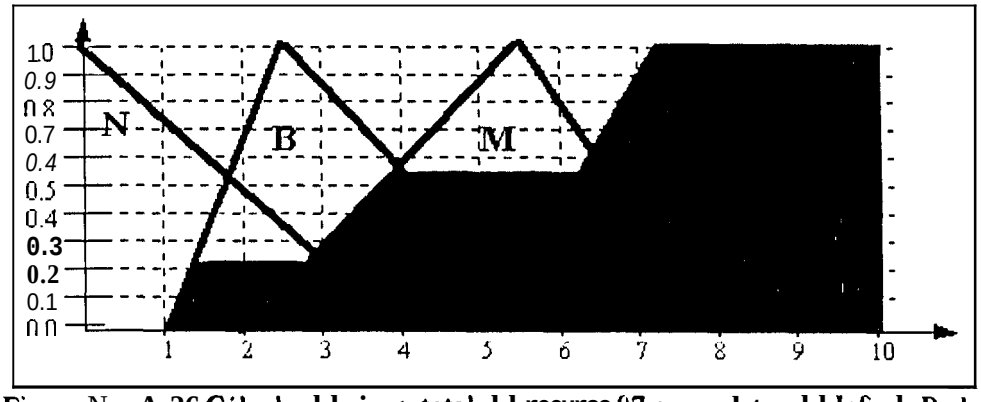


Figura No. **A-26 Cálculo del riesgo total del recurso 07.c con datos del Jefe de Redes**

El resultado numérico es:

$$Z = \frac{1(7.2+8+9+10)+0.55(55)+0.24(2.5)}{1(4)+0.55+0.24} = 7.52$$

El riesgo total es de 7.52 con un grado de 1.0 de alto.

8. recurso 08

08.a Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 04.d, el riesgo total del recurso 08.a es igual al riesgo total del recurso 04.d.; es decir, 6.45 con un grado de 0.66 de moderado y 0.64 de alto.

08.b Por tener los mismos datos de entrada (riesgos e importancias) que el recurso 04.d, el riesgo total del recurso 08.b es igual al riesgo total del recurso 04.d.; es decir, 6.45 con un grado de 0.66 de moderado y 0.64 de alto

Los recursos 08.c, 08.d, 08.e poseen los mismos datos de entrada que el recurso 07.c. Por lo tanto tienen los mismos riesgos totales.

A.3.3. Comparación y conclusión de los dos analisis de riesgos

Los resultados obtenidos en ambos analisis son parecidos, ambos expertos tienen una concepción parecida acerca del riesgo e importancia de los recursos conectados al backbone de la ESPOL.

El riesgo total a partir de los resultados obtenidos de los dos analisis, es realizado de la siguiente manera:

- Se comparan los dos valores de riesgo total y se selecciona el mayor valor lingüístico obtenido. Esta medida se basa en la union de dos valores difusos ya que el resultado de la union es el mayor valor de los terminos.
- En algunos recursos, los grados de membresia son similares y no se denota una diferencia en terminos linguisticos. Por esta razon, los terminos linguisticos han sido subdividos a traves de simbolos (+ ó -) para poder distinguir a cada recurso.
- El signo se coloca de acuerdo al mayor grado de membresia obtenido entre las dos variables de riesgo. Es "+" cuando ambos riesgos tienen el mismo valor con altos grados de membresia (mayor que 0.8). Es "-" cuando una de las variables de riesgo tiene menor valor que la otra.
- Los recursos 04.g, 08.c y 07.c muestran resultados diferentes en cada analisis efectuado. Posee un grado 1.0 de moderado segun el analisis del director de CESERCOMP y un grado de 1.0 de alto según el analisis de Jefe de Redes. Para este caso se ha considerado el valor resultante de la union de los valores difusos (el maximo valor), es decir alto, pero con signo "-" ya que, al tener un antecedente moderado, el valor resultante es alto pero con un grado de moderado.

De esta manera los resultados finales son:

Recursos		Riesgos		
No	Nombre o descripción	Riesgo Total Análisis de ricsgo con datos del Director de CESERCOMP	Ricsgo Total Análisis de riesgo con datos del Jefe de redes de CESERCOMP	Conclusión dc ambos riesgos
01	Ruteador IBM 2210 Enlace con Ecuanet	6.08 Modcrado 1.0	6.45 Alto: 0.64 Moderado: 0.66	ALTO
02	Ruteador IBM 2210 Enlace Las Peñas	6.08 Moderado 1.0	0.45 Alto: 0.64 Moderado: 0.66	ALTO
03	ComServers TELEBIT	6.08 Moderado 1.0	6.45 Alto: 0.64 Moderado: 0.66	ALTO
04	Goliat			
a	SPARC 20:	7.6 Alto: 0.51 Moderado 0.49	7.2 Alto: 1.0	ALTO
b	S.O.:Solaris 2.5	7.6 Alto: 0.51 Modcriido 0.49	7.2 Alto: 1.0	ALTO
c	DNS	7.6 Alto: 0.51 Moderado 0.49	7.53 Alto: 1.0	ALTO
d	SMTP (SendMail)	7.0 Alto: 0.51 Moderado 0.49	7.2 Alto: 1.0	ALTO
e	FTP (anónimo)	***0.08*** Moderado 1.0	4.05 Bajo: 0.56 Moderado: 0.56	MODERADO
f	HTTP 1.0	6.08 Moderado: 1.0	6.94 Alto: 0.89 Modcrado: 0.41	ALTO
g	Telnet	6.08 Moderndo: 1.0	7.2 Alto: 1.0	ALTO
05	David			
a	SPARC 2	6.08 Moderado: 1.0	6.03 Alto: 0.42 Moderado: 0.8	ALTO
b	S.O.: Solaris	6.08 Moderado: 1.0	***6.03*** Alto: 0.42 Modcrado: 0.8	ALTO
06	Maquina Admin.			
A	RISC 6000	4.0 Moderado 1.0	6.45 Alto: 0.64 Moderado: 0.66	ALTO

b	NetView	4.0 Moderado 1.0	6.03 **Alto:** 0.42 Moderado: 0.8	ALTO
07	S. Base de datos			
a	RISC 6000	6.08 Modcrado: 1.0	6.45 Alto: 0.64 Modcrado: ***0.66***	ALTO
b	S.O.: UNIX AIX	6.08 Moderado: 1.0	6.45 Alto: 0.64 Moderado: 0.66	ALTO
c	DB/2	6.08 Moderado: 1.0	7.52 Alto: 1.0	ALTO
ox	S. Aplicaciones			
a	RISC 6000	6.08 Moderado: 1.0	6.45 Alto: 0.64 Moderado: 0.66	ALTO
b	S.O.: UNIX AIX	6.08 Moderado: 1.0	6.45 Alto: 0.64 Moderado: 0.66	ALTO
	Aplicaciones Servidoras:	***6.08*** Moderado: 1.0	7.52 **Alto:** 1.0	ALTO
c	Presupuesto			
d	Contabilidad			
e	Tesorería			
f	Académica			

Tabla A-9

Con estas sencillas operaciones con terminos lingüísticos, se ha logrado cuantificar al riesgo en cada recurso conectado al Backbone de la ESPOL. Estos resultados no representan totalmente la realidad ya que los riesgos de ataques son muy variables porque cada año surgen nuevas brechas de seguridad en sistemas de redes de computadoras, y es dificil predecir el comportamiento de las personas que generan los ataques.

Con este estudio, se establece una medida estimativa del riesgo e importancia para clarificar que es lo que se necesita proteger, y cuales recursos son mas indispensables de proteger que otros. A partir de estas conclusiones ya se pueden generar politicas de seguridad.

APENDICE B

Resultados de las evaluaciones de rendimiento de firewalls publicos

En este apendice se detallan los prograrnas codificados para las pruebas, las lecturas de trafico de la red utilizada para verificar que la red estaba semi-libre (sin flujo de trafico) en los lapsos de las pruebas y los resultados de las pruebas realizadas en la evaluación de productos de firewalls públicos (referirse al capítulo V).

B.1. Programas

Este primer prograrna inicia **25** sesiones FTP al servidor de pruebas, es decir 5 clientes al rnisrno tiempo. El segundo prograrna inicia 50 sesiones FTP al servidor de pruebas, es decir con 10 clientes al rnisrno tiernpo.

```
#############################################################################
#           Programa que inicia 25 sesiones FTP                             #
#############################################################################

# Seteo de variables locales #
n=l                                          # Contador n
s=l                                          # Contador s
ruta="output"                                # arreglo que contiene el
                                              # nombre el nombre de los
                                              # arhivos de salida

sentencia="ftp -vin < script >> $ruta$n "    # arreglo que contiene la
                                              # sentencia ftp que se
                                              # ejecutará.EL ftp recibe
                                              # parametros de un script
                                              # y lanza los resultados
```

```
                                        # a un archivo de salida.

set sentencia-final                     # arreglo final

# lazo que forma la sentencia final que se ejecutara (5 sesiones ftp
# separadas por pipes)

until (( s > 5 ))
do
  sentencia-final= "'echo $sentencia-final $sentencia ` |"
  let s=s+1
done

# lazo que ejecuta la sentencia final 5 veces y envía los resultados
# a archivos de salida

until (( n > 5 ))
do
        echo Cliente Virtual $n >> $ruta$n
        echo $sentencia-final
        let n=n+1

done

################################################################################


################################################################################
#                  Programa que inicia 50 sesiones FTP                         #
################################################################################

# Seteo de variables locales #
n=1                                     # Contador n
s=1                                     # Contador s
ruta="output"                           # arreglo que contiene el
                                         # nombre el nombre de los
                                         # arhivos de salida

sentencia="ftp -vin < script >> $ruta$n "  # arreglo que contiene la
                                         # sentencia ftp que se
                                         # ejecutará.EL ftp recibe
                                         # parametros de un script
                                         # y lanza los resultados
                                         # a un archivo de salida.

set sentencia-final                     # arreglo final

# lazo que forma la sentencia final que se ejecutara (10 sesiones ftp
# separadas por pipes)

until (( s > 10 ))
do
```

```
  sentencia_final= "'echo $sentencia_final $sentencia ` |"
  let s=s+1
done

# lazo que ejecuta la sentencia final 5 veces y envía los resultados
# a archivos de salida

until (( n > 5 ))
do
        echo Cliente Virtual $n >> $ruta$n
        echo $sentencia-final
        let n=n+1

done

#################################################################################
```

El script al que invocan los programas anteriores es :

```
#################################################################################
#                parámetros de ingreso en las sesiones ftp                      #
#                     de los programas anteriores                               #
#################################################################################

open 206.72.133.69              # servidor ftp
user gmazzari goliatl           # usuario y password de conexión
cd ftp                          # cambia al directorio ftp
get pql                         # coge el archivo pql del servidor
bye                             # despide la conexión
#################################################################################
```

B.2. Lectura de trafico de red

Las lecturas de trafico de red tomadas una semana antes de las pruebas indican que entre las 5:00 AM y 7:00 AM la red se encuentra sin trafico y que por lo tanto es muy factible realizar las pruebas en estas horas.

Para leer los siguientes datos hay que tomar en consideración los siguientes aspectos:

1. En la primera línea de cada lectura, el paquete estadistica emite el dia y la hora en que se comienzari a registrar los paquetes.
2. En la segunda línea se registra el día y la fecha hasta donde se leyeron paquetes.
3. El resto de la información corresponde al tipo de paquetes leídos.

```
################################################################################

LANWatch statistics file c:\lw\prueba1.txt opened: Mon May 19 05:05:23 1997
 Packet Type Counts: Mon May 19 06:55:58 1997
IP: 279
   ICMP: 103
      port_unreachable: 66
      host-redirect: 37
   TCP: 4
      unknown: 4
   UDP: 172
      unknown: 66
      BOOTPC: 5
      netb-dg: 23
      rode: 78
ARP: 184


LANWatch statistics file c:\lw\prueba2.txt opened: Tue May 20 04:52:38 1997
 Packet Type Counts: Tue May 20 07:02:53 1997
IP: 262
   ICMP: 89
      port-unreachable: 56
      host-redirect: 43
   TCP: 15
      unknown: 6
      POP-3: 9
   UDP: 158
      unknown: 56
      BOOTPC: 10
      netb-dg: 57
      route: 35
ARP:191

LANWatch statistics file c:\lw\prueba3.txt opened: Wed May 21 05:10:55 1997
 Packet Type Counts: Wed May 21 06:58:20 1997
IP: 282
   ICMP: 126
      port-unreachable: 86
```

host–redirect: 40
TCP: 22
unknown: 22
UDP: 134
unknown: 75
BOOTPC: 15
netb-dg: 5
route: 39
ARP: 172

LANWatch statistics tile c:\lw\prueba4.txt opened: Thu May 22 05:04:17 1997
Packet **Type** Counts: Thu May **22** 07: 10:11 1997
IP: 255
ICMP: 124
port_unreachable: 61
host–redirect: 63
TCP: 10
unknown: 10
UDP: 121
unknown:46
BOOTPC: 17
netb-dg: 3
route:55
ARP:2 17

##

Resumen de los resultados:

	Lunes	Martes	Miércoles	Jueves
No. Paquetes leídos	463	453	454	472

Estas lecturas demuestran que la red entre las 5:00 am y 7:00 am puede considerarse semi vacia o sin flujo variable. Por lo tanto, la red esta en condiciones para realizar pruebas de rendimiento de firewalls asumiendo que el servidor no atiende a ningun proceso que no sea FTP.

B.3. Resultados de las pruebas de Rendimiento

Los archivos en que se registraron los resultados de las pruebas de rendimiento contienen la informacion de cada sesion FTP, desde que se inicia la conexión hasta que transfiere un archivo "pq1" con la cantidad de tiempo que se demoro en hacerlo. De toda esta informacion, lo que nos interesa es obtener el tiempo que demoro la transferencia del archivo.

Las pruebas se realizaron primero sin firewall y luego con los siguientes firewalls:

- Sinus
- Ipfwadm
- FWTK
- Socks

Debido a extension de los archivos de resultados, tan solo se presentan algunos y luego en el resumen de datos se presentan todos.

B.3.1.Sin firewall

Los resultados de las pruebas sin utilizar firewalls para 5 clientes virtuales son:

```
##########################################################################################
Cliente Virtual 1
Connected to 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srv1 .telconet.net FTP server (Version2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version2.1WU(1)) ready.
```

```
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl.telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmauari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmauari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmauari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmauari.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 1.23 secs (2.8e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.03 secs (1.7e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
230-Please read the file README
230 User gmazzari logged in.
357920 bytes received in 2.16 secs (1.6e+02 Kbytes/sec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.95 secs (1.8e+02 Kbytes/sec)
221 Goodbye.
```

226 Transfer complete.
357920 bytes received in 1.38 secs (2.5e+02 Kbytes/sec)
221 Goodbye.

##

Con 10 clientes virtuales:

##

Cliente Virtual 1
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl .telconet.net)
220-
220 srv1 .telconet.net FTP server (Version 2.1WU(1)) ready. .
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl .telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected lo 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected lo 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
220 srvl .lelconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl .telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode lo transfer files.
331 Password required for gmazzari.

```
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl.telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful,
230-Please read the file README
230 User gmazzari logged in.
230-Please read the file README
230 User gmazzari logged in.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 1.24 secs (2.8e+02 Kbytes/sec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
226 Transfer complete.
357920 bytes received in 1.32 secs (2.6e+02 Kbytes/sec)
221 Goodbye.
250 CWD command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pq1 (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.06 secs (1.6e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 1.24 secs (2.8e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
230-Please read the file README
230 User gmazzari logged in.
230-Please read the file README
230 User gmazzari logged in.
```

```
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmauari logged in.
250 CWD command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
local: pql remote: pql
200 PORT command successful.
250 CWD command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
150 Opening BINARY mode data connection for pql (357920 bytes).
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
230-Please read the file README
230 User gmazzari logged in.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.20 secs (2.9e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 1.16 secs (3.0e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
226 Transfer complete.
357920 bytes received in 1.20 secs (2.9e+02 Kbyteslsec)
221 Goodbye.
357920 bytes received in 1.26 secs (2.7e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 1.16 secs (3.0e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.06 secs (1.6e+02 Kbytes/sec)
221 Goodbye.
```

B.3.2. Firewall SINUS

Los resultados de las pruebas utilizando el firewall SINUS para 5 clientes virtuales son:

```
##############################################################################################
```

```
Cliente Virtual 1
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pq1 (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 1.80 secs (1.9e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
```

```
Using binary mode to transfer files.
331 Password required for gmauari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmauari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmauari.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
226 Transfer complete.
357920 bytes received in 1.52 secs (2.3e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
local: pql remote: pq1
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
Remote syslem type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 1.32 secs (2.6e+02 Kbytes/sec)
221 Goodbye.
```

```
226 Transfer complete.
357920 bytes received in 1.55 secs (2.2e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmauari.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.24 secs (2.8e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
226 Transfer complete.
357920 bytes received in 2.18 secs (1.6e+02 Kbyteslsec)
221 Goodbye.
250 CWD command successful.
230-Please read the file README
230 User yrnazzari logged in.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.24 secs (2.8e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
226 Transfer complete.
357920 bytes received in 1.35 secs (2.6e+02 Kbyteslsec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pq1 (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.52 secs (2.3e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
250 CWD command successful.
230-Please read the file README
230 User ymazzari logged in.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pq1
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
```

```
226 Transfer complete.
357920 bytes received in 2.06 secs (1.7e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 2.16 secs (1.6e+02 Kbytes/sec)
221 Goodbye.

##############################################################################################
```

B.3.3. Firewall IPFWADM

Los resultados de las pruebas utilizando el firewall IPFWADM para 5 clientes virtuales son:

```
##############################################################################################
Cliente Virtual I
Connected to 206.72.133.69.
220-Bienvenido Welcome (srv1.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pq1 remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
```

```
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 1.62 secs (2.1e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.05 secs (1.7e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
230-Please read the file README
230 User gmazzari logged in.
357920 bytes received in 1.35 secs (2.5e+02 Kbyteslsec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.08 secs (1.6e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 1.72 secs (2.0e+02 Kbytes/sec)
221 Goodbye.
```

```
##############################################################################################
```

Con 10 clientes virtuales:

```
##############################################################################################
Cliente Virtual 1
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-BienvenidoWelcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
```

```
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready. .
Remote system type is UNIX.
Using binary mode lo transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl ,telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode lo transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconel.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes),
Remote system type is UNIX.
Using binary mode lo transfer files.
331 Password required for gmazzari.
226 Transfer complete.
357920 bytes received in 1.34 secs (2.6e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
```

```
230-Please read the file README
230 User gmauari logged in.
250 CWD command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmauari logged in.
226 Transfer complete.
357920 bytes received in 1.38 secs (2.6e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 1.62 secs (2.1e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.82 secs (1.9e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
226 Transfer complete.
357920 bytes received in 1.68 secs (2.0e+02 Kbytes/sec)
221 Goodbye.
250 CWD command successful.
230-Please read the file README
230 User gmazzari logged in.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.45 secs (2.4e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
226 Transfer complete.
357920 bytes received in 1.76 secs (1.9e+02 Kbytes/sec)
221 Goodbye.
250 CWD command successful.
```

```
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.69 secs (2.0e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
230-Please read the file README
230 User gmazzari logged in.
local: pql remote: pq1
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pq1
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.63 secs (2.1e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 1.55 secs (2.2e+02 Kbytes/sec)
221 Goodbye.
```

B.3.4. Firewall F W K (TIS)

Los resultados de las pruebas utilizando el firewall FWTK **(TIS)** para 5 clientes virtuales son:

```
##########################################################################################################
Cliente Virtual 1
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
```

Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 2.29 secs (1.5e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
250 CWD command successful.
local. pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 **bytes).**
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.54 secs (1.3e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
230-Please read the file README
230 User gmazzari logged in.
357920 bytes received in 3.01 secs (1.1e+02 Kbyteslsec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes)
226 Transfer complete.
357920 bytes received in 2.85 secs (1.2e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 2.41 secs (1.4e+02 Kbytes/sec)
221 Goodbye.

Con 10 clientes virtuales :

##
Cliente Virtual 1
Connected to 206.72.133.69.

```
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl lelconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl ,telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
```

Using binary mode to transfer files.
331 Password required for gmazzari.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pq1 (357920 bytes).
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
226 Transfer complete.
357920 bytes received in 2.25 secs (1.5e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
local: pq1 remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmauari logged in.
226 Transfer complete.
357920 bytes received in 2.19 secs (1.5e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 2.25 secs (1.5e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmauari logged in.
250 CWD command successful.
local: pq1 remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for grnazzari.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.10 secs (1.6e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 2.15 secs (1.6e+02 Kbytes/sec)
221 Goodbye.
250 CWD command successful.
230-Please read the file README
230 User gmazzari logged in.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).

```
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.08 secs (1.6e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 2.11 secs (1.6e+02 Kbyteslsec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.05 secs (1.7e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
230-Please read the file README
230 User gmazzari logged in.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.95 secs (1.7e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 1.85 secs (1.8e+02 Kbytes/sec)
221 Goodbye.
```

6.3.5. Firewall SOCKS

Los resultados de las pruebas utilizando el firewall SOCKS para 5 clientes virtuales son:

```
##############################################################################################
Cliente Virtual 1
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
```

```
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for grnazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for grnazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 2.25 secs (1.5e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
150 Opening BINARY mode data connection for pql (357920 bytes).
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.68 secs (1.3e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
230-Please read the file README
230 User gmazzari logged in
357920 bytes received in 2.85 secs (1.2e+02 Kbytes/sec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
```

357920 bytes received in 2.45 secs (1.4e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 2.88 secs (1.2e+02 Kbytes/sec)
221 Goodbye.

Con 10 clientes virtuales:

```
##########################################################################################################
Cliente Virtual 1
Connectedto 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connectedto 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version2.1WU(1)) ready.
Connected to 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
Connectedto 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connectedto 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Connectedto 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for grnazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
33t Password required for gmazzari.
Connectedto 206.72.133.69.
220-Bienvenido Welcome  (srvl.telconet.net)
220-
220 srvl .telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for grnazzari.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for grnazzari.
Remote system type is UNIX
```

```
Using binary mode to transfer files.
331 Password required for gmazzari.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl.telconet.net FTP server (Version 2.1WU(1)) ready.
230-Please read the file README
230 User gmazzari logged in
250 CWD command successful.
Connected to 206.72.133.69.
220-Bienvenido Welcome (srvl.telconet.net)
220-
220 srvl.telconet.net FTP server (Version 2.1WU(1)) ready.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
local: pq1 remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
Remote system type is UNIX
Using binary mode to transfer files.
331 Password required for gmazzari.
226 Transfer complete.
357920 bytes received in 2.25 secs (1.5e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 2.27 secs (1.5e+02 Kbytes/sec)
221 Goodbye.
226 Transfer complete.
357920 bytes received in 2.08 secs (1.6e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
Remote system type is UNIX.
Using binary mode to transfer files.
331 Password required for gmazzari.
150 Opening BINARY mode data connection for pql (357920 bytes).
```

```
226 Transfer complete.
357920 bytes received in 2.05 secs (1.6e+02 Kbytes/sec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 3.07 secs (1.6e+02 Kbyteslsec)
221 Goodbye.
250 CWD command successful.
230-Please read the file README
230 User gmazzari logged in.
local: pql remote: pq1
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 2.08 secs (1.6e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
226 Transfer complete.
357920 bytes received in 1.68 secs (2.0e+02 Kbyteslsec)
221 Goodbye.
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.69 secs (2.0e+02 Kbyteslsec)
221 Goodbye.
230-Please read the file README
230 User gmazzari logged in.
250 CWD command successful.
230-Please read the file README
230 User gmazzari logged in.
local: pq1 remote: pq1
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
250 CWD command successful.
local: pql remote: pql
200 PORT command successful.
150 Opening BINARY mode data connection for pql (357920 bytes).
226 Transfer complete.
357920 bytes received in 1.68 secs (2.0e+02 Kbyteslsec)
221 Goodbye.
226 Transfer complete,
357920 bytes received in 1.68 secs (2.0e+02 Kbyteslsec)
221 Goodbye.
```

b.3.6. Resumen de los resultados

Aquí se detallan los resultados de cada evaluación:

a) Sin firewall

5 sesiones simultaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	1.23	1.36	1.24	1.41	1.19
2	2.03	1.75	1.25	1.97	1.73
3	2.16	1.27	2.07	2.05	1.37
4	1.95	1.18	2.1	1.29	1.23
5	1.38	1.26	1.26	1.28	1.25
suma	8.75	0.82	7.92	8.0	6.77

10 sesiones simulaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	1.24	1.32	1.32	1.30	2.01
2	1.32	2.06	1.35	1.35	2.16
3	2.00	2.16	1.35	1.21	1.20
4	1.24	1.20	1.32	1.32	1.24
5	1.20	1.26	1.90	1.24	1.32
6	1.16	1.32	2.16	1.32	1.35
7	1.20	1.16	1.32	2.16	1.74
8	1.26	2.18	1.20	1.85	1.20
9	1.16	1.24	1.24	1.35	1.35
10	2.06	1.55	1.40	1.32	1.30
suma	13.09	15.2	14.4	14.4	14.8

b) Sinus

5 sesiones simultaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	1,80	2.16	1.77	1.62	1.75
2	2.0	1.95	1.41	2.05	1,0X
3	2.0	7.05	1.64	1.93	2,09
4	1.95	2.10	2.02	2.09	1,83
5	2.08	1.93	1.72	1.82	1,09
suma	9.8	10.1	8.5	9.5	8,9

10 sesiones simulaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	1.52	1.20	1.48	2.13	**2.18**
2	1.32	1.26	2.08	2.15	1.45
3	1.55	1.32	1.35	1.92	1.52
4	1.24	1.83	1.90	1.52	2.01
5	2.18	1.07	1.72	1.46	1.55
6	1.24	1.22	1.54	1.24	1.45
7	1.35	1.94	2.01	1.52	2.00
8	1.52	2.54	1.48	1.32	1.42
9	2.06	2.59	1.92	2.06	1.76
10	2.to	1.91	1.04	1.63	**1.92**
suma	16.14	17.54	17.1	16.9	17.3

c) IPFWADM

5 sesiones simultaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	1.62	1.84	1.62	2.11	1.78
2	2.05	2.07	1.40	1.83	1.64
3	1.35	1.95	2.10	1.75	1.88
4	1.50	1.69	1.05	**1.08**	***2.02***
5	1.72	1.80	1.41	1.55	1.43
suma	8.5	9.3	8.2	8.9	***8.7***

10 sesiones simulaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	1.34	2.08	2.04	1.85	1.98
2	1.38	1.56	1.51	2.10	1.71
3	1.62	1.64	1.82	1.69	1.39
4	1.82	1.72	1.34	1.58	1.64
5	1.68	1.58	1.93	1.65	1.52
6	1.45	1.65	1.46	1.72	2.01
7	1.76	1.76	1.53	1.69	1.63
8	1.69	1.52	1.62	1.52	1.61
9	1.63	1.51	1.52	1.49	1.79
10	1.55	1.50	1.60	1.51	1.64
suma	15.9	16.5	16.5	16.8	16.9

d) FWTK

5 sesiones simultaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	2.29	2.65	2.42	3.09	2.03
2	2.54	2.54	2.56	2.58	2.59
3	3.01	2.51	2.60	2.03	2.56
4	2.85	2.69	3.02	2.48	2.99
5	2.41	2.56	2.61	2.05	2.85
suma	13.1	12.9	13.2	13.4	13.6

10 sesiones simultaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	1.34	2.08	2.04	1.85	1.98
2	1.38	1.56	1.51	**2.10**	**1.71**
3	1.62	1.64	1.82	1.69	1.39
4	1.82	1.72	1.34	1.58	1.64
5	1.0X	1.58	1.93	1.65	1.52
6	1.45	1.65	1.46	1.72	2.01
7	1.76	1.76	1.53	1.69	1.63
8	1.69	1.52	1.62	1.52	1.61
9	1.63	1.51	1.52	1.49	1.79
10	1.55	1.50	1.60	1.51	1.64
suma	15.9	16.5	16.5	16.8	16.9

e) SOCKS

5 sesiones simultaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	2.25	2.35	2.29	2.38	2.68
2	2.68	2.65	2.88	2.98	2.39
3	2.85	2.05	2.59	2.49	2.51
4	2.45	2.35	2.08	2.53	2.35
5	2.88	2.39	**2.43**	2.47	2.68
suma	13.1	12.7	12.9	12.8	12.6

10 sesiones simultaneas

	C. Virtual 1	C. Virtual 2	C. Virtual 3	C. Virtual 4	C. Virtual 5
1	2.25	1.98	2.14	2.18	2.20
2	2.27	1.78	2.28	2.30	2.34
3	2.0s	2.15	2.07	2.10	2.00
4	2.05	2.16	2.04	2.05	2.04
5	2.07	2.19	2.18	2.11	2.15
6	2.08	1.88	**1.98**	2.01	2.04
7	1.68	2.08	1.69	1.80	1.83
8	1.09	2.12	1.67	1.85	1.88
9	1.68	1.05	1.65	1.82	1.85
10	1.68	1.68	**1.84**	1.98	1.94
suma	19.5	19.6	19.5	20.2	20.3

BIBLIOGRAFÍA

1. [CHAP95] Chapman & Zwicky, Building Internet Firewalls, 1era. Edicion, O'Reilly, 1995.
2. [SIYA95] Siyan & Hare, Internet Firewalls and Network Security, 1era. Edicion, New Riders Publishers, 1995.
3. [GARF96] Garfinkel & Spafford, Practical Unix and Internet Security, 2da. Edicion, O´Reilly, 1996.
4. [CHES94] Cheswick & Bellovin, Firewalls and Internet Security, 1era. Edicion, AT&T, 1994.
5. [ZIMM87] Zimmerman, Fuzzy sets, decision making and expert system, 1era. Edicion, Kluwer Academic Publisher, 1987
6. [COME95] Comer D., Internetworking with TCP/IP, volumen I, 3era. Edicion, Prentice Hall, 1995
7. [PELA95] Peláez E. & Bowles J., Proceedings of IEEE, volumen 83, "Aplication of Fuzzy logic to reliability engineering", 1995
8. [NEWM97] Newman D. & Holzbaur H. & Bishop H., Data Communications, "Firewalls: Don't get burned", marzo 1997
9. [NEWM95] Newman D. & Melson B., Data Communications, "Can Firewalls take the heat?", noviembre 1995
10. [PLAN95] CESERCOMP, Plan de desarrollo Informático, ESPOL, 1995
11. [NORM96] CESERCOMP, Normas y Regulaciones para conectarse al backbone y servicios de Internet de la ESPOL, ESPOL, 1996