Diseño de una Plataforma de Seguridad Reconfigurable (PSR) sobre NetFPGA para Redes de Área Local

Francisco Javier Guerra Manchego[1], Raúl Ramiro Peralta Meza[2]
francisco.guerra@ucsp.edu.pe, rperalta@nnmc.edu
[1]Universidad Católica San Pablo, Perú
Campus Campiña Paisajista s/n Quinta Vivanco, Barrio de San Lázaro
Arequipa – Perú
[2]Nothern New Mexico College, Estados Unidos
921 N. Paseo de Oñate Española
New Mexico – Estados Unidos

Resumen: *En este paper, se presenta el diseño de una Plataforma de Seguridad Reconfigurable (PSR) que permite monitorear y controlar la información que ingresa a las Redes de Área Local (LAN). El diseño propone el uso de dos mecanismos que realicen esas funciones. En primer lugar, se encuentra una tarjeta NetFPGA, donde se realizará el procesado de paquetes a nivel de capa de Red. El otro mecanismo se halla en un Servidor Proxy que realizará el filtrado de paquetes a nivel de capa de Aplicación. Por tanto, el diseño de la PSR ofrece un control de flujo de paquetes que ingresa a las Redes ofreciendo un sistema robusto frente a posibles ataques que se puedan producir.*

Abstract: *This paper presents the design of a Reconfigurable Security Platform (RSP) which can monitor and control the information transmitted within a Local Area Network (LAN). The design proposes the use of two mechanisms to perform those functions. First, a NetFPGA card performs the packet processing at network layer. The other mechanism is a Proxy Server, which performs packet filtering at the application layer. Therefore, the design of the PSR provides a flow control for packet that entering to the network by offering a robust system against possible attacks that may occur.*

Palabras clave: Firewall, IPS, VPN SSL, Claves Públicas y Privadas.

1. Introducción

Los servicios y aplicaciones disponibles en Internet se han convertido en piezas fundamentales de nuestras vidas, lo cual ha llevado a un crecimiento exponencial no solo de la infraestructura de los proveedores de acceso a Internet sino también de usuarios que demandan una mejora constante en el ancho de banda. La convergencia digital demanda una velocidad de acceso cada vez mayor por ello nuevas interfaces como Gigabit Ethernet se están convirtiendo en la norma para la conectividad de redes debido a que aumentan la capacidad de conexión a la red. Más aún, el crecimiento experimentado por Internet no solo ha sido por parte de usuarios convencionales, sino también por parte de las empresas que ven en Internet la oportunidad de ofertar sus productos y servicios.

A esto hay que añadir que toda información que es transmitida entre redes es un bien valioso y protegerla ha sido una tarea que se ha desarrollado continuamente [Cifuentes+04]. En toda sociedad existen personas inescrupulosas que se infiltran en la red tratando de acceder a algún servidor para ganar privilegios de administrador y eventualmente provocar daños como: Robo de información, corrupción de sistemas, destrucción de recursos. Para muchas organizaciones estas pérdidas pueden significar cuantiosos gastos. El informe desarrollado por [Gordon+04] menciona que en los últimos años el número de ataques contra la seguridad en Estados Unidos se ha incrementado de manera exponencial, pasando de 10000 en 1999 a más de 300000 en el 2004 y los gastos de las empresas por este concepto han superado los cientos de millones de dólares. Es por ello de la aparición de los Firewalls, que según [Cheswick+03] son dispositivos o programas que controlan el flujo de tráfico entre redes empleando diferentes mecanismos de seguridad, los cuales, en los últimos años, han tenido un constante uso y desarrollo.

Por otro lado, no se debe olvidar que el procesamiento y manejo de paquetes debe tener un alto rendimiento con el objetivo de conseguir un mejor desempeño en las redes de acceso [Limari04]. Para cumplir tal meta, se han desarrollado procesadores de red, los cuales son circuitos programables que incluyen recursos hardware para el procesamiento de las funciones de comunicación de alto rendimiento. Un ejemplo de ello son los dispositivos FPGA (Field-Programmable Gate Array) [Bozich05], los cuales permiten reconfigurar o reprogramar una aplicación tantas veces como se desee y de forma sencilla con la consecuente mejora continua de diseños y productos. NetFPGA, que es una plataforma abierta basada en FPGA, que permite a investigadores y desarrolladores construir prototipos de trabajo para sistemas de redes de alta velocidad.

En este artículo, se presenta el diseño de una plataforma para la inspección de los paquetes, el cual será desarrollado posteriormente sobre una tarjeta NetFPGA. El diseño considera que la tarjeta NetFPGA estará conectada a un servidor Proxy, en el cual se complementa otro mecanismo de seguridad implementado en software de modo que la plataforma sea lo más robusta posible frente a ataques.

El resto del paper está organizado de la siguiente manera. En la sección 2, se presenta los trabajos previos relacionados a la seguridad, los Firewalls, su arquitectura, los mecanismos de seguridad, la tarjeta NetFPGA, Router de Referencia IPv4, seguido por el diseño de la plataforma en la sección 3. El artículo finaliza con la sección 4 que presenta las conclusiones y el trabajo futuro.

2. Trabajos previos

2.1. Seguridad

De acuerdo con los autores [Shirey00] y [Strand04], seguridad es aquello que se preocupa por la prevención y detección de acciones no autorizadas por usuarios de un sistema de computador.

Por otro lado, se debe diferenciar lo que seguridad en redes y seguridad en el host. Seguridad en el host consiste en ofrecer seguridad por separado a cada host de la red de computadoras, aplicando todos los esfuerzos para evitar problemas de seguridad, lo cual involucra desactivar servicios, procesos del sistema operativo, entre otros. Pero existe un problema en este esquema debido a que el ambiente de computadoras es abierto a diversas plataformas lo que hace que este modelo sea impracticable por lo complejo de su implementación. En tanto que en [Shirey00] se señala que seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el completo control del sistema.

Así mismo, toda acción destinada a ofrecer seguridad debe garantizar el cumplimiento de cuatro objetivos importantes: confidencialidad, integridad, disponibilidad y autentificación, todos ellos definidos por el estándar X.800 [ITU01].

2.2. Firewall

En [Limari04] se menciona que, un Firewall es un sistema que impone una política de seguridad entre la red privada e Internet, donde se determina los servicios de red que pueden ser accedidos de tal modo que la red se encuentre protegida contra accesos no autorizados.

2.2.1. Técnicas de Filtrado

En [Limari04], [Strand04] y [Díaz01] se menciona que existen tres diferentes técnicas de filtrado de tráfico que realizan los Firewalls, éstos son: Filtrado a nivel paquetes, Filtrado a nivel de aplicación, Filtrado a nivel de conexión.

La técnica de Filtrado a nivel de paquetes es la más usada hoy. Se basa en el análisis de la información contenida en las cabeceras de los paquetes IP con el fin de tomar una decisión que permita o niegue el paso de la trama que se recibe. Los campos que se analizan en esta cabecera corresponden a las direcciones IP fuente y destino, el número de puerto [Villalón02], [Chapman92].

Tal como se muestra en la Figura 1, un filtro a nivel de paquetes consiste de:

- El filtro de paquetes, quien se encarga de verificar los paquetes en base a un conjunto de reglas.
- El conjunto de reglas, que está basada en políticas de seguridad y definida por un administrador de sistema.
- Tabla de estado, la cual contiene el estado de los paquetes que llegan a la red.

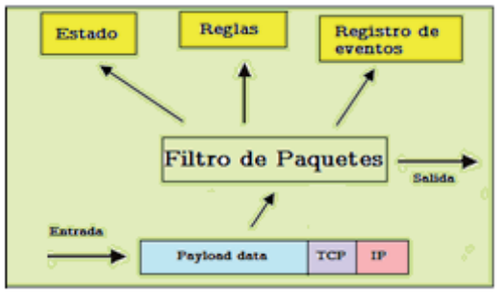

Figura 1. Esquema del Filtrado a nivel de paquetes.

En tanto que el Filtrado a nivel de Aplicación, es una técnica que funciona como un intermediario en la comunicación, previniendo que un servidor no confiable de Internet acceda a nuestra red. A diferencia de los Firewalls a nivel de paquetes, los Firewalls a nivel de aplicación ejecutan programas de proxy, como los servicios FTP ó Telnet, en donde examinan el contenido de los paquetes que filtran, estas aplicaciones analizan cada paquete y filtran diferentes tipos de comandos o información de los protocolos de aplicación [Mazzarani98].

2.2.2. Arquitectura de Firewalls

Existen diversas formas en la que se puede diseñar un Sistema de Firewall. Entre las arquitecturas más desarrolladas se tiene: Arquitectura Dual-Homed, Arquitectura Screened-Host y Arquitectura Screened-Subnet [Ranum93].

La Arquitectura Dual-Homed consiste de un computador intermediario, el cual tiene dos tarjetas de red, una de éstas va conectada hacia la red interna, en tanto que la otra tarjeta hacia la red externa. Este host Dual-Homed actúa como un router entre las dos redes a la que sus interfaces están conectadas. Por lo tanto, la red interna y externa no se comunican directamente, sino a través del host Dual-Homed, ello se muestra en la Figura 2. En esta arquitectura, el host Dual-Homed puede contener sistemas proxy, filtradores de paquetes (a través de programas de software) o ambos [Mazzarani98], [Ranum93].

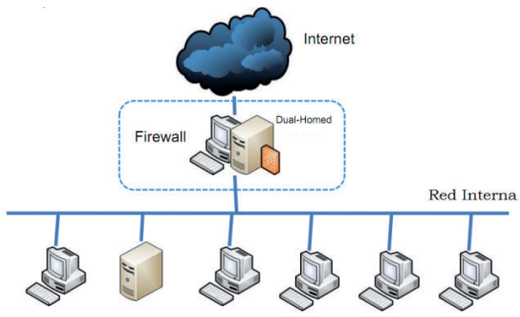

Figura 2. Arquitectura Dual-Homed.

Por otro lado, la Arquitectura Screened-Host es mostrada en la Figura 3, la cual consiste de un host bastión, el cual está conectado a la red interna y un router conectado a la red externa. La seguridad primaria es provista por un filtraje de paquetes y la secundaria a través del sistema proxy instalado en el host bastión, esto significa que combina las técnicas de sistemas proxy y filtradores de

paquetes. Se pueden planear diferentes métodos para los diferentes servicios, algunos pueden ser habilitados por el router, mientras otros pueden ser permitidos a través de servicios proxy ubicados en el host bastión [Ranum93].

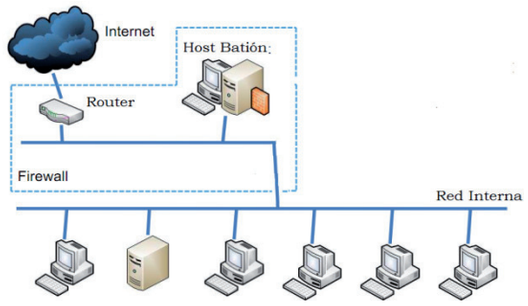

Figura 3. Arquitectura Screened-Host.

Finalmente, la arquitectura Screened-Subnet añade una capa extra de seguridad a la arquitectura anterior, ello lo hace a través de lo que se denomina red perímetro, la cual tiene como fin aislar la red interna de Internet. En esta arquitectura, el host bastión se conecta a la red perímetro y no a la red interna, de modo que se reduzca el impacto de un posible ataque a la red interna.

En la Figura 4, se presentan los elementos con los que cuenta esta arquitectura: Dos screening routers, cada uno se conecta a la red perímetro. Uno se coloca entre la red interna y la red perímetro al que se denomina router interno y el otro entre la red externa y la red perímetro llamado router externo, además de un host bastión que ejecuta un sistema de proxy ofreciendo un sistema con mayor seguridad [Mazzarani98].

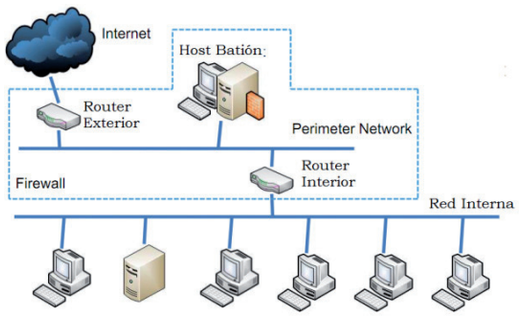

Figura 4. Arquitectura Screened-Subnet.

2.3. NetFPGA

Actualmente, la infraestructura de Internet está siendo dominada por los fabricantes de tecnologías propietarias, es por ello que existe un impulso a la democratización del hardware, para permitir a los investigadores a revisar algunos protocolos referidos a la capa 2 y 3 (Enlace de datos y Red, respectivamente) del modelo de referencia OSI, los cuales no han evolucionado en más de una década. Por lo tanto, los FPGA son una posible solución para cumplir con esta necesidad, ya que permiten desarrollar rápidamente aplicaciones de bajo nivel en el procesamiento de paquetes.

Éste es el caso de la plataforma de desarrollo NetFPGA, la cual ha sido desarrollada por investigadores de la Universidad de Standford, con el fin de que se puedan crear diseños personalizados de hardware, para poner a prueba las nuevas teorías, algoritmos y aplicaciones mucho más cercanas a la realidad sobre el procesamiento y envío de paquetes en la red [Lockwood+07], [NetFPGA12].

2.4. Router de Referencia IPv4

Este proyecto es desarrollado sobre la tarjeta NetFPGA en el cual se implementa los diferentes bloques a nivel de hardware haciendo uso de un lenguaje de descripción como Verilog, para la construcción de un router IPv4.

De acuerdo con los autores en [Lockwood+07], el Router de Referencia IPv4 consta de cinco etapas, tal como se muestra en la Figura 5. La primera etapa, son las colas de recepción (Rx Queues), las cuales reciben cada paquete provenientes de las interfaces de entrada de la tarjeta (puertos Gigabit Ethernet), éstas añaden una cabecera que contiene la longitud del paquete y el puerto de entrada, para que luego ello pase hacia la ruta de datos (User DataPath).

Esta ruta de datos consta de tres etapas que llevan a cabo el procesamiento de paquetes. La primera etapa en la trayectoria de la ruta de datos es el árbitro de entrada (Input Arbiter), el cual utiliza el mecanismo round-robin como forma de arbitraje para seleccionar a una de las colas de entrada para proporcionarle servicio y luego colocar ese paquete hacia el puerto de salida (Output Port Lookup). En la segunda etapa, el puerto de salida (Output Port Lookup) se encarga del procesamiento de paquetes, tales como, el decremento del TTL (TimeToLive), la revisión y actualización del CRC, decidir si va a enviar el paquete al CPU como un paquete de excepción o lo envía hacia uno de los puertos Ethernet.

A continuación, el paquete queda en manos de la tercera etapa de la ruta de datos Output Queues, que se encargará de enviar el paquete hacia alguno de los puertos físicos de salida y pueda ser transmitido Finalmente, los paquetes llegan hacia el quinto estado, llamado colas de transmisión (Tx Queues), las cuales se encargan de transmitir los paquetes por una de las interfaces del NetFPGA.

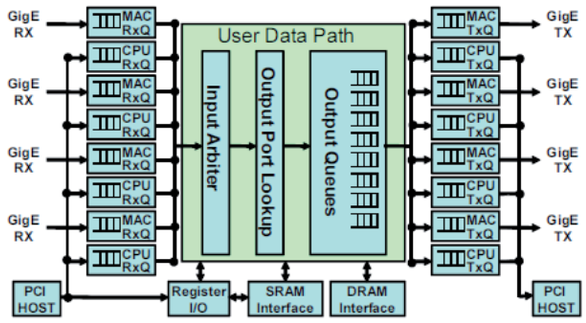

Figura 5. Diagrama de bloques del Router de Referencia IPv4.

2.5. Sistema de seguridad basado en la integración NIDS y Firewall de Filtrado de Paquetes

En [Innella01], se menciona que el objetivo del NIDS (Network Intrusion Detection System) es supervisar

activos de la red con el fin de detectar comportamientos anómalos. Por otro lado, existen herramientas más dinámicas que han sido necesarias para proteger los nuevos y complejos ataques, el resultado fue el IPS (Intrusion Prevention System), el cual abarca una serie de aspectos como antivirus, software de detección de intrusos y firewalls, lo que permite que esta herramienta determine el tipo de ataque y tome medidas pertinentes para contrarrestar el ataque. Esta política requiere hardware caro, además de cambios apropiados en el diseño de la red y sus políticas, por lo que el coste puede no ser tan razonable para las empresas medianas y pequeñas.

En [Salehi+09], se desarrolla un sistema que integra NIDS y un Firewall de Filtrado de paquetes, tal como se muestra en la Figura 6, el cual ofrece un coste menor en comparación con los actuales IPS. El Firewall de Filtrado de paquetes se realiza a través de comandos IPTABLES de Linux, en tanto que el NIDS es desarrollado modificando un software open-source, de modo que pueda comunicarse con el Firewall. Así mismo, las reglas de protección entre el NIDS y los demás servidores de la red se transmiten usando el formato XML, esto debido a que este formato es independiente de la plataforma que se use.

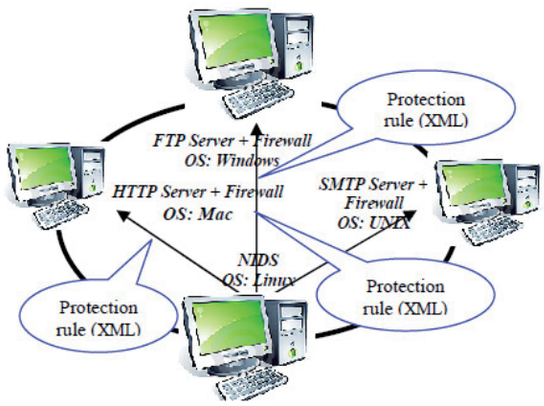

Figura 6. Sistema de seguridad basado en la integración de NIDS y Firewall de Filtrado de Paquetes.

3. Diseño

El diseño de la PSR se muestra en la Figura 7, la cual sigue la arquitectura Screened Host, y consta de dos componentes principales: Firewall en hardware, implementado sobre la tarjeta NetFPGA, y el Firewall en software, que es un servidor Proxy, el cual es configurado en el host bastión.

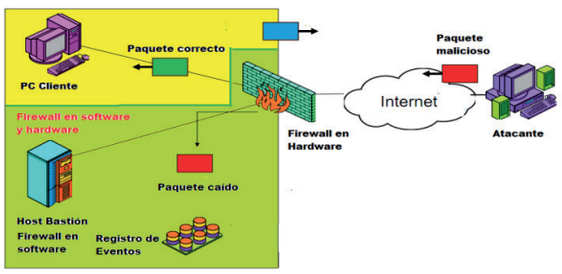

Figura 7. Diagrama de bloques del diseño de la plataforma de seguridad.

3.1. Firewall en hardware

El diseño del Firewall en hardware toma como base el desarrollado en el Router de Referencia IPv4 al cual se le añade ciertas funcionalidades. En la arquitectura interna del bloque Output Port Lookup del Router de Referencia, se le inserta un bloque llamado *packet_filter*, tal como se muestra en la Figura 8, que se encargará de analizar tanto la dirección IP como el puerto de cada paquete que llega. El bloque *packet_filter* se encarga de aceptar o desechar los paquetes que ingresan basado una tabla de direcciones IP y puertos, los cuales se almacenarán en la memoria del NetFPGA.

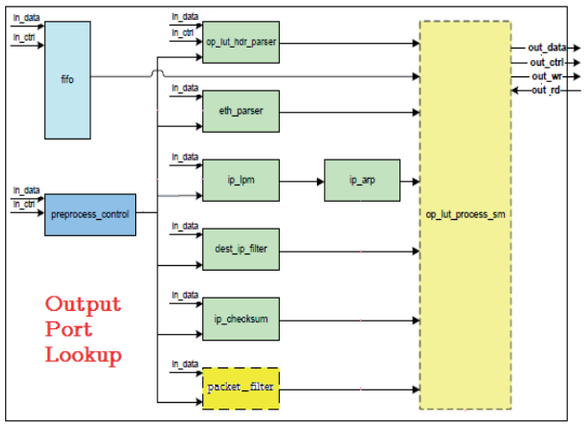

Figura 8. Diagrama de bloques del Firewall en Hardware.

Así mismo, es importante que la tarjeta intercambie información con el CPU del host bastión. Para ello se utiliza la interfaz PCI que presenta la tarjeta. En la figura 9, se presenta el diagrama de bloques del intercambio de información entre el programa desarrollado en Verilog y el host bastión, así como el contenido de la memoria de la tarjeta. Los bloques Eth MAC corresponden a las interfaces Gigabit Ethernet que tiene la tarjeta NetFPGA que permite transmitir y recibir información de los nodos que conforman la red local. Por otro lado, la presencia del bloque Programa Verilog representa el programa que se implementará sobre la tarjeta haciendo uso de Verilog, el cual consiste en desempaquetar la trama y analizar las direcciones IP destino y fuente que serán comparadas con direcciones IP habilitadas por el administrador de red, estas direcciones estarán almacenadas en las memorias SRAM de la tarjeta, de tal modo que en el programa diseñado se compare y se analice si la dirección proveniente tiene acceso la red interna, si eso sucede el paquete será enrutado hacia el CPU del host que realizará otra medida de seguridad para que en ese momento el paquete sea enviado hacia su destino final, caso contrario si el paquete que llega no tiene los permisos necesarios, el programa en Verilog tiene que eliminar el paquete, el resultado de este proceso es informado al CPU de modo que se conozca sobre un posible ataque.

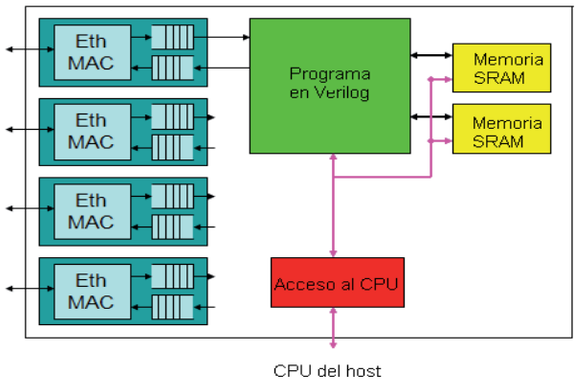

Figura 9. Intercambio de información entre el host bastión, la memoria y el programa en Verilog.

3.2. Firewall en software

La implementación del Firewall en software consiste de un software que será instalado en la computadora denominada Host Bastión que se encargará de permitir/denegar los paquetes que ingresen a la red por medio de un sistema proxy. Este software se ejecutará sobre el Sistema Operativo (SO) Fedora, esto debido a que los programas que se desarrollan en la tarjeta NetFPGA utilizan tal SO. La idea consiste en deshabilitar/habilitar los servicios no requeridos en la red de modo que sólo se pueda acceder a lo que los usuarios en la red interna necesiten. Por otro lado, es importante mencionar que también es necesario conocer los eventos que se producen cuando el Firewall esté siendo atacado, es por ello de la creación de un registro en donde se almacene los ataques provenientes de Internet y que ello se muestre sobre la pantalla del computador

4. Conclusiones y trabajos futuros

A partir del diseño de la plataforma presentada, se desprenden las siguientes conclusiones:

Es posible combinar interfaces, protocolos y algunos conceptos que se emplean en el desarrollo de los Firewalls para diseñar y posteriormente implementar soluciones que ayuden a controlar y monitorear el flujo de información que se recibe/transmite sobre las LAN.

El uso de la tarjeta NetFPGA como herramienta para el filtrado de paquetes, ofrece ventajas no sólo de procesamiento sino también por ser una plataforma libre donde se desarrollan y se prueban nuevos protocolos que sirvan para el desarrollo de Internet.

Como trabajo futuro se propone lo siguiente:

Construcción del diseño desarrollado, utilizando cada una de las tecnologías planteadas. Más aún, una vez terminada la implementación integrarla a un algoritmo de procesado de paquetes eficiente que reduzca el tiempo de filtrado de paquetes.

Modificación de la ruta de datos para que la Plataforma de Seguridad sea compatible con redes IPv6.

Referencias bibliográficas

[Bozich05] Bozich, E. Introducción a los Dispositivos FPGA. Análisis y ejemplos de diseño. http://www.ing.unlp.edu.ar/islyd/Trabajo%20Final.pdf

[Chapman92] Chapman, D. Network (In)Security through IP packet filtering.

http://cs.unc.edu/~fabian/course_papers/filtering.pdf

[Cheswick+03] Cheswick, W., Bellovin, S. & Rubin, A.. Firewalls and Internet Security: Repelling the Wily Hacker. AddisonWesley, 2nd ed.

[Cifuentes+04] Cifuentes, J. & Narvaez, C. Detección de Vulnerabilidades de Sistemas Operativos Linux y Unix en Redes TCP/IP.

http://www.univalle.edu.co/~telecomunicaciones/trabajos_de_grado/informes/tg_JesusCifuentes_CesarNarvaez.pdf

[Díaz01] Díaz, D. Sistemas de control de accesos entre redes por medio de Firewalls, Universidad Francisco Marroquin, Ciudad de Guatemala.

[Gordon+04] Gordon, L., Loeb, M., Lucyshyn, W & Richardson, R. CSI/FBI Computer Crime and Security Survey. http: //i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[Innella01] Innella, P. The Evolution of Intrusion Detection Systems, Tetrad Digital Integrity. 2001 http://www.securityfocus.com/infocus/1514

[ITU01] International Telecommunication Union. Security Architecture for Open Systems Interconnection. X.800 Standard.

[Limari04] Limari, V. Protocolos de Seguridad para Redes Privadas Virtuales (VPN). Universidad Austral de Chile.

[Lockwood+07] Lockwood J. et al. NetFPGA–an open platform for gigabit-rate network switching and routing. http://yuba.stanford.edu/~jnaous/papers/NetFPGA-MSE-2007.pdf

[Mazzarani98] Mazzarani, G. Seguridad de redes de computadoras frente a Internet: Estudio, diagnóstico e implementación de firewalls. Escuela Superior Politécnica del Litoral, Guayaquil.

[NetFPGA12] NetFPGA, 2012. http://www.netfpga.org/

[Ranum93] Ranum, M. 93. Thinking about Firewalls. http://www.vtcif.telstra.com.au/pub/docs/security/ThinkingFirewalls/ThinkingFirewalls.html

[Salehi+09] Salehi, H. Shirazi, H. Reza Moghadam, A. Increasing overall network security by integrating Signature-Based NIDS with Packet Filtering Firewall. International Joint Conference on Artificial Intelligence, 2009

[Shirey00] Shirey, R. Request For Coments 2828. http://www.ietf.org/rfc/rfc2828.txt.

[Strand04] Strand, L. Adaptive distributed Firewall using intrusion detection, University of Oslo.

[Villalón02] Villalón, A. Seguridad en Unix y Redes. Universidad Politécnica de Valencia, España.