EVALUACIÓN DE FIREWALLS BASADOS EN SOFTWARE LIBRE

FIREWALL EVALUATION BASED ON OPEN SOURCE SOFTWARE

Adalberto Iriarte Solís
Universidad Autónoma de Nayarit
adalberto.iriarte@uan.edu.mx

Pablo Velarde Alvarado
Universidad Autónoma de Nayarit
pvelarde@uan.edu.mx

Arturo Aguirre Villaseñor
Universidad Autónoma de Nayarit
arturo.aguirre@uan.edu.mx

Luis Javier Mena Camaré
Universidad Politécnica de Sinaloa
lmena@upsin.edu.mx

Rafael Martínez Peláez
Universidad de la Salle Bajío
rmartinezp@delasalle.edu.mx

Alberto Manuel Ochoa Brust
Universidad de Colima
aochoa@ucol.mx

Resumen

En este trabajo se propone la evaluación de firewalls basado en software libre GNU/LINUX con las características que les permitan integrarse a una cama de pruebas en la cual se estudiaron, evaluaron y analizaron diversos entornos de red y escenarios de ataque. Los firewalls de software libre son una buena alternativa cuando se trata de brindar seguridad en una red, en este trabajo fueron evaluados cuatro distribuciones Linux que han sido especialmente diseñadas para brindar este servicio. Las herramientas de software libre empleadas demostraron ser las adecuadas para las pruebas realizadas a los diferentes firewalls, de este modo se logró obtener resultados que muestran la factibilidad de ClearOS para ser implementado en la cama de pruebas. También se probó su efectividad al mostrar

una buena respuesta en la defensa de los ataques, con y sin la inyección del tráfico de fondo generado por la herramienta iperf.

Palabras Claves: Cama de pruebas, firewall, linux, software libre.

Abstract

In this work we propose the evaluation of firewalls based on free software GNU / LINUX with the characteristics that allow them to be integrated into a test bed in which various network environments and attack scenarios were studied, evaluated and analyzed. Free software firewalls are a good alternative when it comes to providing security in a network, in this work were evaluated four Linux distributions that have been specially designed to provide this service. The free software tools used, proved to be adequate for the tests carried out on the different firewalls, in this way it was possible to obtain results that show the feasibility of ClearOS to be implemented in the test bed. Its effectiveness was also proven by showing a good response in the defense of attacks, with and without the injection of background traffic generated by the iperf tool.

Keywords: Firewall, linux, open software, testbed*.*

1. Introducción

Con la explosión del Internet, la proliferación de aplicaciones de software y el ingenio de los hackers, la seguridad se ha convertido en un problema complejo que requiere de una solución de seguridad bien pensada para tratar con él. La solución de seguridad debe ser capaz de hacer frente a las amenazas de seguridad de estos nuevos escenarios, así como ser lo suficientemente flexible para adaptarse a los cambios tecnológicos, [Richard, 2004].

Para proporcionar un mayor grado de protección a los recursos de la red es necesario utilizar Redes Virtuales Privadas (VPNs), Sistemas de Detección de Intrusiones de Red (NIDSs), firewalls perimetrales, entre otros. Este último, el firewall perimetral es un sistema diseñado para evitar los accesos no autorizados a una red privada. La idea fundamental de funcionamiento se basa en construir una barrera de seguridad entre redes privadas y la Internet, [Kadhim, 2006].

El firewall es un elemento fundamental en una solución de seguridad perimetral, por lo cual este dispositivo debe poseer las características siguientes, [Zwiky, 2000]:

- Capacidad de monitoreo y notificación.
- Inmunidad a la penetración o subversión.
- Ser robusto en la identificación de ataques de red.
- Capacidad de realizar traducción de direcciones de red (NAT).

Un problema persistente en la investigación en redes de cómputo es la validación. Cuando se desea evaluar una nueva característica o corregir un fallo, un investigador u operador debe hacer uso de algún tipo de escenario, virtualizado, emulado, simulado o real. La simulación y la emulación proporcionan ambientes controlados para ejecutar experimentos repetibles, [White, 2002].

Las desventajas de estos escenarios son la carencia de escala y de realismo, no consideran todo el trayecto hasta el usuario final, tampoco manejan tráfico real generado por los usuarios.

Por otro lado, una cama de pruebas especializada permite realizar pruebas en escala y manejar tráfico real de usuarios. Sin embargo, usualmente están dedicadas a un tipo particular de experimento y pueden requerir una fuerte inversión económica para su implantación. La virtualización puede contribuir a minimizar estos costos y aumentar en gran medida la eficiencia de las pruebas a la vez que se reproduce con mayor exactitud los entornos físicos, [Richmond, 2005].

Sin la infraestructura adecuada para evaluar alguna nueva propuesta es relativamente difícil lograr la transferencia de tecnología desde el laboratorio de investigación a las redes del mundo real.

En este trabajo se consideran escenarios híbridos los cuales incorporan elementos de infraestructura física como servidores Linux, estaciones, dispositivos de capa 2 y 3. Así mismo, se considerarán elementos de virtualización mediante el uso de máquinas virtuales para representar el atacante, por ejemplo usando BackTrack o Kali.

Las máquinas virtuales también se utilizarán para representar servidores vulnerables, para ello se utilizará Metasploitable 2. Bajo este planteamiento, el firewall propuesto en este trabajo podrá ser evaluado adecuadamente a través de pruebas de stress y ataques para confirmar las características que debe de poseer un firewall y que se mencionaron en el punto anterior.

2. Métodos

Existen en la actualidad diversas distribuciones de Linux que han sido creadas especialmente para proteger las redes de cómputo, brindando grandes capacidades de seguridad para administrar una red de la mejor forma y con todos los servicios que se pudieran requerir. Entre estas distribuciones se revisaron, IPCop, Endian Firewall (EFW), ClearOS y Fedora 21; esta última no fue pensada desde su creación para ser exclusivamente firewall, sin embargo, cuenta en su kernel con *iptables*, que permite manejar el firewall a nivel de línea de comandos en Linux. Los firewalls pueden ser evaluados en función de sus actividades y procesos a través de distintas métricas que proporcionan información dentro de un periodo de tiempo. Las unidades de medición pueden incluir conteos, frecuencia, porcentajes o valores físicos.

Diversos estudios muestran la evaluación de firewalls basados en software libre. Ejemplo de esto son los trabajos realizados por Schuettinger, Sampaio y Bernardino. Schuettinger selecciono las distribuciones de IPfire, IPCop y ClearOS; mientras que Sampaio y Bernardino compararon a IPCop, PFSense, Zentyal, [Schuettinger, 2017]; [Sampaio, 2017].

Algunas de las métricas de evaluación a considerar en un firewall son el *throughput* y el *goodput*, que describen tasas de transferencia de datos entre redes; así como la latencia, que describe el tiempo en que un paquete tarda en pasar por el firewall desde el momento que ingresa en él hasta el momento en el que sale.

Métricas de evaluación

Una métrica es una medida tomada en un periodo de tiempo y que proporciona información vital sobre un proceso o actividad. Las unidades de medición pueden

incluir conteos, frecuencia, porcentajes o valores físicos, [Cambra, 2004]. En un trabajo realizado en la Universiti Teknologi Malaysia [Kean, 2002], los autores proponen una metodología de evaluación comparativa para evaluar el desempeño del firewall tomando en cuenta tres distintas métricas: throughput, latencia (*latency*) y goodput, se representan gráficamente en la figura 1:

- ***Throughput*:** Es la tasa máxima en la capa de red en la cual ninguno de los paquetes recibidos es descartado (dropped) por el firewall sin la activación de las reglas de filtrado. El tamaño del thoughput es determinado principalmente por las tarjetas de red y la eficiencia de los algoritmos programados dentro del firewall. La unidad de medición es paquetes entrantes por segundo, [Wenhui, 2013].
- **Latencia (*latency*):** Es el intervalo de tiempo que comienza cuando un paquete ingresa al firewall y finaliza cuando el mismo paquete sale de este. Se mide en segundos.
- ***Goodput*:** Es la tasa en la cual los paquetes son reenviados a las interfaces de destino del firewall sin tomar en cuenta aquellos que fueron descartados debido a las reglas de filtrado; en otras palabras se puede definir como la tasa efectiva de paquetes transmitidos [Clement, 2011].

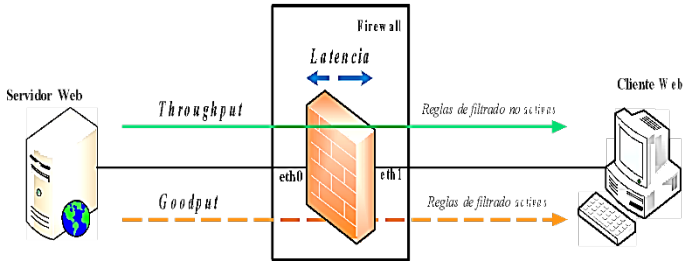

Figura 1 Métricas de evaluación de firewalls.

El throughput y a la latencia se destacan como métricas críticas para evaluar el desempeño del firewall, y se introducen cuatro nuevas métricas de evaluación para satisfacer las necesidades de su evaluación: tasa de establecimiento de conexión, capacidad de conexión concurrente, tasa de transferencia HTTP y tasa de derribe de conexión (Connection Teardown rate), [Snyder, 2010], tabla 1.

Tabla 1 Métricas adicionales para firewalls.

Métricas	Descripción	Importancia
Tasa de establecimiento de conexión	Velocidad a la cual, los firewalls pueden entablar conexiones y el Full Three- way handshake para establecer una sesión TCP/IP. Son multitudes de conexiones que intentan establecer conexión a una red a través de un firewall.	Pueden ser provocadas por un simple clic de aplicaciones web. Si son demasiadas conexiones, el servidor podría saturarse y causar la reducción de velocidad de las aplicaciones.
Tasa de transferencia HTTP	Velocidad a la cual un objeto HTTP solicitado cruza a través del firewall.	Radica en el impacto que tiene el tráfico HTTP en un firewall debido a que es el tipo de tráfico más común que cruza por él.
Tasa de derribe (*teardown*) de conexión	Velocidad a la cual los firewalls pueden derribar las conexiones y liberar recursos de la red para ser usados posteriormente por tráfico entrante o saliente.	Puesto que cada conexión que se estableció debe ser derribada cuando haya sido filtrada por el firewall, éste último debe mantenerse disponible en ambas direcciones.
Manejo de tráfico ilegal	Comportamiento del firewall cuando se le presenta una combinación de tráfico legal e ilegal.	El firewall tiene la capacidad de filtrar (permitir y descartar) el tráfico bajo la presión de grandes entradas y salidas de paquetes.

Se configuraron cuatro equipos, cada uno con diferente sistema operativo mencionados anteriormente, para realizar pruebas con ellos. Para cada uno se requirieron tres tarjetas de red; para el atacante, la víctima y la de Internet, respectivamente. Por practicidad se manejan direcciones IP comunes entre las interfaces de cada sistema operativo, tanto para la de la víctima como para la del atacante, tal como se expresa a continuación:

- Interfaz del atacante: 192.168.20.1.
- Interfaz de la víctima: 192.168.10.1.
- Interfaz de Internet: 192.168.0.x (Proporcionada por el DHCP)

Para su configuración, en la tabla 2 se muestran los nombres de las interfaces de los diferentes sistemas operativos (firewalls) con los que se trabajaron así como las zonas que se emplearon tanto en Endian como en IPCop.

Tabla 2 Nombres de interfaces en firewalls.

Sistema Operativo (Firewall Linux)	Interfaz de Atacante (192.168.20.1)	Interfaz de Víctima (192.168.10.1)	Interfaz de Internet (192.168.0.x)
Endian Firewall Community 3.0	br2	br0	eth0
IPCop 2.1.5	wan-1	lan-1	wlan-1
ClearOS Community 6.5.0	eth1	eth0	eth2
Fedora 21 (iptables)	enp3s0	enp2s0	enp2s4

Para evaluar los diferentes firewalls que se han manejado, se montó el siguiente escenario con la finalidad de inyectar tráfico sintético a la víctima, a la máxima tasa de transferencia que soporta la red local (1 Gbit Ethernet). Esto permitió comprobar qué tan capaces son los firewalls de soportar grandes tasas de información, así como su viabilidad para ser seleccionados por encima de los demás y comenzar a operarlo en un escenario de tráfico real con la certeza de que proporcionará el máximo rendimiento y confiabilidad. También se agregan a este escenario las herramientas ntop y nload las cuales permiten monitorizar el tráfico de una red en tiempo real; gracias a ntop se pudo obtener resultados gráficos del comportamiento de la red al emplear cada firewall. Cabe mencionar que se utilizó la herramienta hping3 (corriendo desde Backtrack 5 r3) para perpetrar ataques DDoS en el tiempo en que se esté introduciendo a la red la máxima tasa de datos.

Para finalizar, con el fin de evaluar los diferentes firewalls, se les realizaron tres pruebas diferentes de inyección de tráfico a la máxima tasa, con duración cada una de ocho minutos; estas son:

- ***Prueba 1:*** Solo tráfico de fondo (sin ataque DDoS).
- ***Prueba 2:*** Con ataque DDoS y con la regla desactivada en el firewall para mitigarlo.
- ***Prueba 3:*** Con ataque DDoS y con la regla activada en el firewall para mitigarlo.

3. Resultados

En la tabla 3 se muestran los resultados obtenidos de la prueba 1 (solo con tráfico de fondo), realizada a los cuatro diferentes firewalls. En las cuatro columnas

de los resultados obtenidos se puede observar una clara superioridad de ClearOS y Fedora 21 sobre IPCop y EFW. Esto puede notarse en que el máximo throughput generado en ClearOS y Fedora 21 estuvo por encima de los 900 Mbit/s, siendo estos de 924.7 y 939 Mbit/s respectivamente, mientras que en los otros dos, por debajo apenas de los 600. De igual manera, las pérdidas de datos en IPCop y Endian rebasaron los 240 Mbit/s, mientras que ClearOS y Fedora 21 tan solo fueron de 0.3 y 16.02 Mbit/s, respectivamente. En cuanto al consumo de memoria, IPCop presentó mejores resultados, seguido por Fedora 21, ClearOS y en último lugar EFW.

Tabla 3 Resultados de firewalls (prueba 1).

Firewall (Prueba 1)	Throughput máximo generado (Mbit/s)	Throughput recibido (Mbit/s)	Pérdida (Mbit/s)	Consumo de memoria (%)
ClearOS	924.7	924.4	0.3	3.963
Fedora 21	939.7	923.68	16.02	3.5
Endian Firewall	594	353.28	240.72	7.296
IPCop	587.3	310.61	276.69	1.83

En la tabla 4 se muestran los resultados obtenidos de la prueba 2, (con ataque DDoS sin regla de mitigación) realizada a los firewalls. Al igual que en la tabla 1 se muestra la superioridad de tanto de ClearOS como de Fedora 21.

Tabla 4 Resultados de firewalls (prueba 2).

Firewall (Prueba 2)	Throughput máximo generado (Mbit/s)	Throughput recibido (Mbit/s)	Pérdida (Mbit/s)	Consumo de memoria (%)
ClearOS	751.7	420.68	331.02	4.210
Fedora 21	749.7	415.33	334.37	3.8
Endian Firewall	594	45.80	548.2	8.521
IPCop	603.6	95.46	508.14	2.512

Por causa del ataque, en los cuatro firewalls se observó un decremento de valores, proporcionales al rendimiento de los equipos en la red y en este caso ClearOS mostró mayor estabilidad y capacidad de transferencia con una tasa de 751.7 Mbit/s (ligeramente por encima de Fedora 21 con 749.7), lo mismo que en la

pérdida de datos, debido a que fueron menores las cifras de ClearOS en comparación con las de Fedora 21; mientras que en los otros dos las pérdidas de datos rebasaron los 500 Mbit/s, lo cual representa en promedio el 88.2% del total de su tráfico máximo generado. Cabe señalar que en esta prueba IPCop demostró su incapacidad para procesar tales cantidades de paquetes, debido a que aproximadamente en el minuto cinco, su sistema colapsó y se reinició automáticamente.

En la tabla 5 se muestran los resultados obtenidos de la prueba 3 (con ataque DDoS con regla de mitigación) realizada a los firewalls. Se puede observar que debido a la activación de la regla, se presentó un aumento en el throughput en ClearOS y en Fedora 21 con respecto a la tabla anterior, asimismo, ocurrió una disminución considerable en la pérdida de datos en ambos firewalls; mientras que los valores de IPCop y EFW en las cuatro columnas de datos se mantuvieron prácticamente iguales con respecto a la prueba 2, solamente en IPCop se obtuvo una reducción del 29.2% en la pérdida de datos y cabe señalar que en esta prueba IPCop presentó estabilidad en su sistema, al igual que los demás.

Tabla 5 Resultados de firewalls (prueba 3).

Firewall (Prueba 3)	Throughput máximo generado (Mbit/s)	Througput recibido (Mbit/s)	Pérdida (Mbit/s)	Consumo de memoria (%)
ClearOS	836.7	672.21	164.49	4.157
Fedora 21	860.7	709.32	151.38	3.7
Endian Firewall	594.5	45.56	548.94	6.878
IPCop	597.8	238.41	359.39	1.77

4. Discusión

Las herramientas de software libre empleadas demostraron ser las adecuadas para las pruebas realizadas a los diferentes firewalls, de este modo se logró obtener resultados que muestran la factibilidad de ClearOS para ser implementado en la cama de pruebas. Sin la generación de tráfico sintético se perpetraron ataques DDoS (tipo SYN flood) con hping3, los cuales tuvieron gran efecto de saturación de recursos en el equipo víctima; posteriormente dichos ataques fueron

correctamente mitigados mediante las reglas añadidas a los cuatro diferentes firewalls.

Una vez que se comprobó que tanto los ataques, como la defensa de los mismos funcionaban correctamente, se prosiguió con la evaluación de los firewalls con el apoyo de herramientas de generación de tráfico y de monitoreo de la red. Para ello se efectuaron tres pruebas distintas a cada firewall.

La primera consistió en la generación de tráfico sintético a la máxima tasa de transferencia posible (1 Gbit) desde tres equipos mediante la herramienta iperf en un lapso de tiempo de ocho minutos totales con el fin de comprobar si los firewalls son capaces de entregar a la víctima la misma tasa que fue generada.

La segunda consistió en repetir la primera, pero efectuando un ataque DDoS desde el atacante durante un lapso de tres minutos, tiempo en el que se mide la pérdida de datos que se tiene con respecto a la primera prueba.

La tercera y última prueba consistió en repetir la segunda, con la diferencia de que para esta estuvo activa la regla de mitigación del ataque para comprobar el throughput máximo recibido por la víctima y de este modo determinar la efectividad, estabilidad y rendimiento de cada firewall. Una vez realizadas las evaluaciones a los cuatro firewalls se determinó que la mejor opción fue ClearOS.

5. Conclusiones

Los firewalls de software libre son una buena alternativa cuando se trata de brindar seguridad en una red, es por ello que en este trabajo fueron evaluados cuatro distribuciones Linux que han sido especialmente diseñados para brindar este servicio.

Una ventaja muy grande es que son administrables mediante iptables, el cual permitió la manipulación de las reglas a nivel de línea de comandos, y esto fue útil en el establecimiento de las condiciones para la realización de las pruebas necesarias.

Dichas pruebas, junto con el estudio de las herramientas empleadas, arrojaron resultados que muestran la factibilidad de la elección de ClearOS por encima de las demás distribuciones Linux. Se reveló de este modo la incapacidad tanto de

IPCop como de Endian Firewall de procesar la máxima tasa de transferencia en la cama de pruebas con capacidad de 1 Gbit Ethernet. Aunado a esto, la efectividad de las reglas para contener los ataques perpetrados del atacante a la víctima en estas dos distribuciones (junto con el máximo tráfico de fondo), presentó anomalías en la defensa de los mismos causadas por la sobresaturación del ancho de banda. Esto también debido a que solo son soportados por arquitecturas de 32 bits y están limitadas a ser instaladas solo en equipos de bajas prestaciones. Por otro lado, tanto Fedora 21 como ClearOS, mostraron que son capaces de alcanzar la máxima tasa de transferencia de datos, esto sin tener un consumo de recursos importante que afecte su rendimiento. También se probó su efectividad al mostrar una buena respuesta en la defensa de los ataques con las reglas del firewall, con y sin la inyección del tráfico de fondo generado por la herramienta iperf.

A pesar de que Fedora 21 arrojó resultados similares a los de ClearOS, no cuenta por sí mismo con las herramientas necesarias para la administración y protección de una red; no sucede así con ClearOS, que además de ofrecer iptables en su interfaz gráfica. Cuenta con una completa suite de aplicaciones de software libre con propósitos de seguridad, además de brindar soporte al alcance de todos dentro de una comunidad web dedicada a realizarle mejoras y actualizaciones constantemente; por tal motivo, fue ésta la opción seleccionada.

Este resultado es muy similar al obtenido por Schuettinger, al realizar una comparación de firewalls basados en software libre utilizando unas pruebas de comparación diferentes a los de este estudio, llegando a la conclusión de que Clear OS fue claramente superior a los otros, [Schuettinger, 2017].

Cabe mencionar que el sistema ClearOS es muy utilizado en pequeñas y medianas empresas, con alrededor de 100 a 150 usuarios o dispositivos, y que no están en la capacidad o no tienen como objetivo del negocio destinar muchos recursos a dispositivos de conectividad. Lo cual lo vuelve una buena elección al momento de elegir un firewall para una empresa, como fue el caso de las empresas INVELIGENT y TeamSourcing Cía. en Ecuador, [Erazo, 2015]; [Freire Bastidas, 2015].

6. Bibliografía y Referencias

[1] Cambra, R. Metrics for Operational Security Control, SAN Institute. 4, July 2004.

[2] Clement B. Evaluation of a Virtual Firewall in a Cloud Environment. Edinburgh Napier University. December, 2011.

[3] Erazo, P., & Rubén, E. Implementación de un sistema de seguridad perimetral para las empresas Teamsourcing Cia. Ltda. con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar ISO-27001. (Bachelor's thesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería Electrónica en Redes y Comunicación de Datos.). 2015.

[4] Freire Bastidas, D. M. Rediseño de la intranet para la empresa Soluciones Tecnológicas Solteflex sa (INVELIGENT) e implementación de un prototipo utilizando ClearOS (Bachelor's thesis, Quito: EPN). 2015.

[5] Hickman, B., Newman, D., Tadjudin, S. & Martin, T. Benchmarking. Methodology for Firewall Performance, IETF RFC 3511. April 2003.

[6] Kadhim D. J. & Hussain W. K. Design and Implementation of a Proposal Network Firewall. Al-Khwarizmi Engineering Journal, Vol. 2(1), 52-69, 2006.

[7] Kean, L. E. & Mohd N. S. A Benchmarking Methodology for NPU Based Statefull Firewall, Universiti Teknologi Malaysia. 2002.

[8] Richard A. Deal. Cisco Router Firewall Security. Cisco Press. 2004.

[9] Richmond M. ViSe: The Virtual Security Testbed. 2005.

[10] Sampaio, D., & Bernardino, J. Evaluation of Firewall Open Source Software. In Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST), 356-362. 2017. http://www.scitepress.org/Papers/2017/63612/63612.pdf.

[11] Snyder, J. Firewalls in the Data Center: Main Strategies and Metrics, Opus Network. 2010.

[12] Wenhui S. & Junjie X. Performance evaluations of Cisco ASA and Linux iptables firewall solutions. Master Thesis. Halmstad University, Sweden, 2013.

[13] Schuettinger, J. Comparing Linux Firewalls. Collections 2017 Student Project Showcase. SUNY Polytechnic Institute. 2017. https://dspace.suny connect.suny.edu/bitstream/handle/1951/69341/Schuettinger_2017StudentProjectShowcase_Final.pdf?sequence=1&isAllowed=y

[14] White B., et al. An integrated experimental environment for distributed systems and networks. ACM SIGOPS Operating Systems Review 36.SI (2002): 255-270

[15] Zwiky E., Copper S., & Chapman D. Building Internet Firewalls. Second Edition, O'relly & Association, 2000.