MODELO DE SELECCIÓN DE FIREWALL DE CÓDIGO ABIERTO MEDIANTE EL ANÁLISIS DE VULNERABILIDADES Y FORTALEZAS

Ricardo Pertuz De Las Salas, Edward Paul Guillen. Autores,
Universidad Militar Nueva Granada, Bogotá, Colombia, gissic.umng.edu.co

Resumen– Los firewalls son herramientas de seguridad implementados tanto en hardware como en software y su función es proteger las redes de datos por medio de varias técnicas, como el filtrado de paquetes permitiendo o bloqueando puertos, o por medio de la autorización o negación de paquetes, entre otras muchas estrategias [3] [7]. Este paper compara cuatro firewalls basados en software de código abierto teniendo en cuenta sus vulnerabilidades y fortalezas en seguridad, además desarrolla un modelo de elección de firewall teniendo en cuenta las políticas de seguridad y características de una red en particular. Los desarrollos aquí condensados obedecen a la necesidad de crear un marco de referencia para la escogencia de firewalls acorde a las políticas de seguridad de las compañías, en especial medianas y pequeñas, no por referencia de sus características sino por una evaluación de sus vulnerabilidades y fortalezas, con parámetros objetivos y claramente definidos

Palabras Claves – Análisis de Vulnerabilidades, Análisis de Fortalezas, Firewall, Política de Seguridad.

Índice

1. INTRODUCCIÓN

Si consideramos el crecimiento exponencial de ataques informáticos realizados a través de Internet a redes privadas junto con la falta de bases para que un administrador de red pueda escoger un firewall que se acople de la mejor forma posible a las necesidades de su red, resulta necesario hacer una comparación de algunos firewalls y crear un marco para decidir cual es la mejor opción para cada tipo de red; para efectos de esta investigación se escogieron cuatro firewalls, todos ellos de código abierto sobre diferentes plataformas de las mismas características. Como primer paso para llevar a cabo lo anteriormente mencionado se hace una elección de los firewalls a estudiar, luego se identifican sus vulnerabilidades y sus fortalezas mediante un modelo propuesto, para luego ser usado como criterio de comparación, dicha comparación se lleva a cabo mediante un método de calificación también propuesto en este paper y de esta forma se desarrolla el modelo de selección de firewall de código libre.

2. FIREWALLS A EVALUAR

Buscando en los diversos sistemas operativos de código abierto disponible, se encontraron los siguientes firewalls y sus respectivas plataformas:

NOMBRE	PLATAFORMAS
IPTABLES	LINUX
IPCHAINS	LINUX
IPWADM	LINUX
IPFILTER	FreeBSD, HP-UX, OpenBSD, DragonFlyBSD, NetBSD, otros
PACKET FILTER (PF)	NetBSD, OpenBSD, FreeBSD, DragonFlyBSD
IPFIREWALL (IPFW)	FreeBSD, DragonFlyBSD

Tabla 1. Firewalls seleccionados

Los firewalls escogidos son los encerrados con el círculo rojo que aparecen en la Tabla 1. Es claro que sobre Linux hay tres firewalls disponibles, sin embargo se escogió Iptables por ser este la evolución de Ipchains que a su vez es la evolución de Ipwadm. Otro punto importante a resaltar en la Tabla 1 es que mediante esta investigación se encontró que en el vasto mundo de los firewalls todos los encontrados actualmente sobre plataforma libre (Sistemas Operativos de código abierto) están montados sólo sobre 4 firewalls específicos: Iptables, Ipfilter, Packet Filter (PF) e Ipfirewall (Ipfw) (teniendo en cuenta de que Ipchains e Ipwadm están descontinuados), por lo tanto fueron estos los que se escogieron para efectos de comparación en esta investigación, a pesar de que existen otros firewalls de código abierto pero sobre plataforma cerrada, como por ejemplo Netdefender sobre Windows, lo que implica una desventaja.

3. MODELO DE IDENTIFICACIÓN DE VULNERABILIDADES

Actualmente existen diversos organismos dedicados al reporte de bugs de los software de mayor uso, dentro de estos se encuentran los firewalls escogidos para la comparación en esta investigación, estos bugs dentro de dichos firewalls resultan muchas veces en fallos de seguridad que permiten explotar el sistema privado supuestamente protegido. Sin embargo

para obtener una información útil de estos reportes publicados en Internet, es necesario tener en cuenta diversos criterios mediante unos pasos propuestos a continuación:

Paso 1: Revisar las vulnerabilidades reportadas para cada firewalls en las siguientes bases de datos.

Base de datos	Información sobre la vulnerabilidad
X-Force http://xforce.iss.net/	- Valor de riesgo (Alto, Medio y Bajo) - Breve descripción - La solución si existe - Forma de explotación, remota o local
Secunia http://secunia.com	- Valor de riesgo (1-5) - Breve descripción - La solución si existe - Forma de explotación, remota o local
National Vulnerability Database http://nvd.nist.gov/	- Valor de riesgo (1 - 10) - Breve descripción - Plataformas vulnerables - Tipo de vulnerabilidad - Consecuencias - La solución si existe - Forma de explotación, remota o local
Security Focus http://www.securityfocus.com/bugtraq/archive	- Valor de riesgo (1 - 1000) - Quien la descubrió - Código o herramienta de explotación - Descripción más detallada - Plataformas vulnerables - Tipo de vulnerabilidad - Consecuencias - La solución si existe - Forma de explotación, remota o local - Nomenclatura propia BID / Bugtraq ID

Tabla 2. Bases de datos consultadas

Paso 2: Una vez consultada las bases de datos, se revisa que ninguna este repetida, para no contar una vulnerabilidad en un firewall más de una vez, la forma más sencilla de revisar esto es mediante la consulta de la nomenclatura asignada a cada vulnerabilidad, la organización encargada de administrar esta nomenclatura se conoce como Common Vulnerabilities and Exposures, mejor conocidas por su siglas CVE, a continuación un ejemplo:

CVE-CAN-2004-0626 / CVE-2004-0626

En este ejemplo se muestra dos formas de nombrar una misma vulnerabilidad, la primera es *CVE-CAN-2004-0626*, donde *CVE* es el nombre de la organización, *CAN* proviene de la palabra candidate lo cual quiere decir que dicha vulnerabilidad ha sido reportada pero se encuentra en estudio por la mesa directiva para entrar a la lista CVE final, el *2004* indica el año en que fue reportada y el *0626* es un número secuencial para diferenciarla con las demás vulnerabilidades, una vez aprobada por la mesa directiva de la CVE, dicha vulnerabilidad entra a pertenecer a la lista CVE final bajo la nomenclatura *CVE-2004-0626* donde desaparece la palabra CAN.

Sin embargo en caso tal de que CVE no reporte alguna vulnerabilidad existente, otra organización como Security Focus aporta una nomenclatura propia conocida como Bugtraq ID ó simplemente BID, donde también se usa un número secuencial, como por ejemplo BID 7895, esta nomenclatura también se usa para evitar repeticiones de vulnerabilidades en firewalls en la consulta de las diferentes bases de datos.

Paso 3: Sin embargo los resultados obtenidos aún necesitan pasar por ciertos filtros para ser considerados como vulnerabilidades válidas en esta investigación, estos filtros o criterios de selección de vulnerabilidades son:

- Que de verdad dicha vulnerabilidad se refiera a la herramienta que estamos buscando.
- Que dicha vulnerabilidad si pertenezca a alguna función de un firewall como tal, y no por ejemplo que la vulnerabilidad sea del módulo NAT que tiene IPTABLES el cual no corresponde a una función firewall por definición.
- Que la vulnerabilidad provenga de la herramienta como tal afectando su normal funcionamiento o que el firewall junto con otro módulo del sistema provoquen fallos en las funciones del firewall debido a su incompatibilidad y no lo contrario es decir que el error provocado por dicha incompatibilidad produzca un error en el otro módulo y no en el firewall.

Cada uno de estos pasos se realiza para cada uno de los cuatro firewalls. La figura 1 resume el modelo propuesto para la identificación de vulnerabilidades en firewalls.

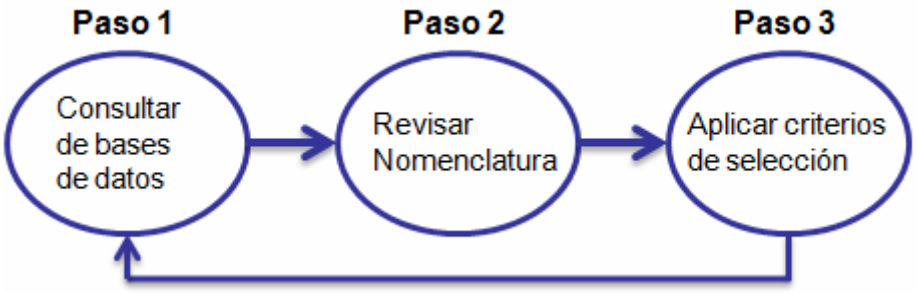

Figura 1. Diagrama de identificación de fortalezas

4. MODELO DE IDENTIFICACIÓN DE FORTALEZAS

A diferencia de la sección anterior en donde se identificaron las vulnerabilidades de los firewalls, las fortalezas no se buscaron de la misma forma debido a la ausencia de bases de datos especializadas en este tipo de información, por lo tanto dichas vulnerabilidades fueron encontradas directamente de la documentación de cada firewall, teniendo como criterio de elección aquellas características especiales que usa los firewalls de esta investigación para mejorar la función del filtrado de paquetes. La documentación es la encontrada para las últimas versiones disponibles de los firewalls hasta el 31 de Agosto del 2007, las cuales son:

IPTABLES

Versión: 1.3.8 para la última versión del kernel de Linux 2.6.22.1 a la fecha 10 de julio de 2007.
Lanzamiento: Julio del 2007

PF

Versión: Para OpenBSD 4.1
Lanzamiento: Mayo 1 del 2007

IPFW

Versión: IPFW2 para FreeBSD 4.7
Lanzamiento: 10 Octubre del 2002 con varias actualizaciones hasta FreeBSD 6.2 en Enero del 2007.

IPFILTER

Versión: 4.1.23
Lanzamiento: 31 de Mayo del 2007

5. MÉTODO DE CALIFICACIÓN DE FIREWALLS

Uno de los alcances de esta investigación es el entregar un método de calificación de los firewalls que permita evaluar la confiabilidad de cada uno de ellos, y con esta información más las de las características de una red en particular generar finalmente el modelo de selección de firewall. Para efectos de dicha evaluación consideramos las siguientes variables:

- **Número de fortalezas y vulnerabilidades**

  Cantidad total de vulnerabilidades y fortalezas encontradas para cada firewall.

FIREWALL	No. Vulnerabilidades	No Fortalezas
Firewall IP	X	Y

Tabla 3. Ejemplo de Número de vulnerabilidades y fortalezas

- **Valor de Riesgo**

  Representa el daño potencial que tiene cada vulnerabilidad, para esta investigación se maneja una escala de 1 a 5.

  - Bajo Riesgo = 1
  - Riesgo Potencial = 2
  - Riesgo Moderado = 3
  - Riesgo Significante = 4
  - Alto Riesgo = 5

  Para evaluar las fortalezas se tomó de la definición de firewall tres variables con diferente ponderación, tal y como se ve en la Tabla 4.

Capacidad para evitar ataques 60%	Nivel de innovación de la tecnología 30%	Facilidad de uso 10%

Tabla 4. Tres variables para evaluar las fortalezas

Estas tres variables sumadas representan el 100% el cual significa el nivel de eficacia para cada fortaleza, la cual también se evalúa con una escala de 1 a 5.

- Poco Eficaz (1)
- Potencialmente Eficaz (2)
- Regularmente Eficaz (3)
- Significativamente Eficaz (4)
- Muy Eficaz (5)

- **Variable de Cercanía**

Mide que porcentaje se acerca un punto del otro con respecto a un valor total

Ejemplo:

Que tanto se acerca o qué porcentaje es 75,8 con respecto al total de 87,4

X = (75,8 * 100) / 87,4 = 86,72 %

- **Nivel de Impacto**

Mide que tanto afecta de forma positiva las fortalezas o negativa las vulnerabilidades comparando las posiciones alcanzadas con la variable de cercanía.

Por ejemplo, debido a que son 4 firewalls se tienen 4 posibles posiciones, cada una es obtenida según la comparación de la variable de cercanía, la primera posición obtiene un valor de 4 puntos disminuyendo en un punto a medida que aumente la posición.

Empezando el procedimiento de identificación de vulnerabilidades para los cuatro firewalls encontramos los valores para las dos primeras variables descritas: Número de vulnerabilidades y valor de riesgo, obteniendo los resultados de la Tabla 5.

Firewall	No. Vulnerabilidades	Valor total de riesgo
Iptables	11	45,35
PF	5	22,6
Ipfilter	8	34,5
Ipfw	5	14,9

Tabla 5. Vulnerabilidades encontradas y valor total de riesgo

Como se observa en la Tabla 5, la tercera columna muestra el valor total de riesgo, este valor es el resultado de sumar todos los valores de riesgos de cada vulnerabilidad para cada firewall encontrada en cada base de datos consultada. Todas las vulnerabilidades encontradas para cada firewall se encuentran en la página http://gissic.umng.edu.co/firewalls, de nuestro grupo de investigación en seguridad y sistemas de comunicación de la Universidad Militar Nueva Granada.

Graficando el riesgo total para cada firewall, obtenemos la Figura 2.

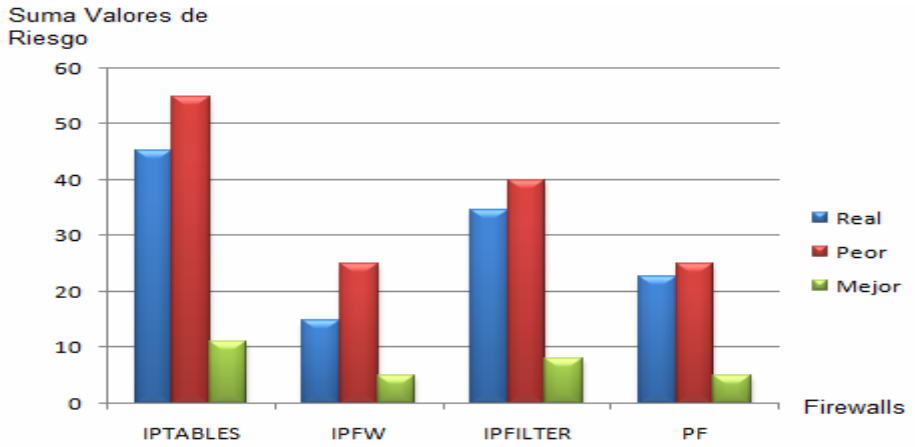

Figura 2. Valor de riesgo total, peor y mejor caso

Observando la Figura 2, el valor total de riesgo es el representado en la barra azul, adicional a esta barra se gráfica dos barras más, una roja y una verde, la roja indica el peor de los casos, es decir si cada vulnerabilidad para un firewall en particular tuviera un valor de riesgo de 5, y la barra verde representa el mejor de los casos, si cada vulnerabilidad para un firewall en particular tuviera un valor de riesgo de 1. Ingresando estos resultados en tablas, aplicando la formula de variable de cercanía, comparando los resultados de cada firewall y aplicando el concepto de nivel impacto obtenemos las Tablas 6 y 7.

Puesto	Firewall	Real	Peor	Valor % (Peor)	Puntos por Posición
1	Ipfw	14,9	25	59,60%	4
2	Iptables	45,35	55	82,45%	3
3	Ipfilter	34,5	40	86,25%	2
4	PF	22,6	25	90,40%	1

Tabla 6. Valores de cercanía vulnerabilidades, peor caso

Puesto	Firewall	Real	Mejor	Valor % (Mejor)	Puntos por Posición
1	Ipfw	14,9	5	33,55%	4
2	Iptables	45,35	11	24,25%	3
3	Ipfilter	34,5	8	23,18%	2

4	PF	22,6	5	22,12%	1

Tabla 7. Valores de cercanía vulnerabilidades, mejor caso

Las Tablas 6 y 7 muestran que Ipfw obtuvo la primera posición ya que este firewall es el que más se aleja de su peor caso con un 59,6%, lo que simétricamente muestra que es el que más se acerca a su mejor caso con un 33,55%, por lo tanto obtiene 4 puntos, dicho valor significa que este firewall es el que menos se ve afectado por sus vulnerabilidades. Lo contrario ocurre con PF, el cual es el firewall más afectado por sus vulnerabilidades, obteniendo un solo punto aplicando el concepto de la variable nivel de impacto, ya que este es un 90,4% de su peor caso y solo un 22,12% de su mejor.

Continuando con las fortalezas de cada firewall las cuales no se encuentran en ninguna base de datos, fue necesario recurrir a la documentación de cada uno para encontrar aquellas características especiales obteniendo la Tabla 8.

Firewall	No. Fortaleza	Valor total de eficacia
Iptables	10	34,2
PF	7	24
Ipfilter	4	10,4
Ipfw	10	36,3

Tabla 8. Fortalezas encontradas y valor total de eficacia

En la tercera columna de la tabla 8, se muestra el valor total de eficacia, este valor se obtiene primero sacando el valor de eficacia de cada fortaleza que es la suma del resultado de la calificación de las tres variables para evaluar una fortaleza (Capacidad para evitar ataques (60%) + Nivel de innovación de la tecnología (30%) + Facilidad de uso (10%)), luego de tener este valor para cada fortaleza lo sumamos con las demás fortalezas para cada firewall y así damos con el resultado obtenido en la tabla.

Graficando la eficacia total para cada firewall, obtenemos:

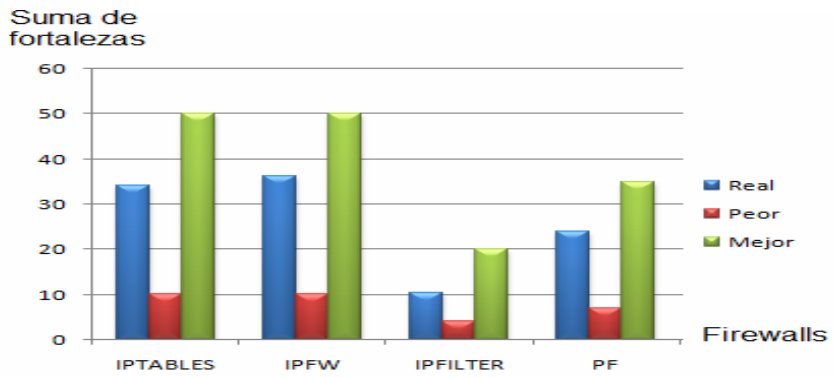

Figura 3. Valor de eficacia total, peor y mejor caso

Haciendo el análisis análogo suponemos que el peor de los casos es cuando cada fortaleza para cada firewall tiene un valor de 1 y el mejor de los casos es cuando cada fortaleza para cada firewall tiene un valor de 5, de esta forma ingresamos dichos resultados en las Tablas 9 y 10:

Puesto	Firewall	Real	Peor	Valor % (Peor)	Puntos por Posición
1	Ipfw	36,3	10	27,54%	4
2	PF	24	7	29,16%	3
3	Iptables	34,2	10	29,24%	2
4	Ipfilter	10,4	4	38.46%	1

Tabla 9. Valores de variable de cercanía fortalezas, peor caso

Puesto	Firewall	Real	Mejor	Valor % (Mejor)	Puntos por Posición
1	Ipfw	36,3	0	72,60%	4
2	PF	24	0	68,57%	3
3	Iptables	34,2	9	68,40%	2
4	Ipfilter	10,4	3	52,00%	1

Tabla 10. Valores de variable de cercanía fortalezas, mejor caso

Como resultado a las Tablas 9 y 10, Ipfw mantiene la primera posición, pero ahora PF sale de la última para pasar a la segunda y Ipfilter ocupa la última.

- **Análisis vectorial**

Ya habiendo obtenido los puntos por posición para cada firewall tanto para sus vulnerabilidades como para sus fortalezas debemos relacionarnos de alguna forma, sin embargo a pesar que las vulnerabilidades y fortalezas son propias de cada firewall son independientes las unas de las otras, por lo que dichos puntos por posición se pueden considerar como ortogonales de manera que merecen un análisis vectorial.

Firewall	Puntos vulns	Puntos fortalezas	Vector	Magnitud	α
Ipfw	4	4	4V+4F	5,65	45°
Iptables	3	2	3V+2F	3,60	33,7°
Pf	1	3	1V+3F	3,16	71,56°
Ipfilter	1	1	1V+1F	1,41	45°

Tabla 11. Valores de puntos por posición y vectores

Como se observa en la Tabla 11 a cada firewall se le asigna un vector en el que su dirección y su ángulo dependen de los puntos obtenidos de sus vulnerabilidades y sus fortalezas. La magnitud de cada vector indica la confiabilidad del firewall y el ángulo indica de donde obtiene la mayoría de sus puntos, entonces si el vector tiene un ángulo menor a 45° es porque dicho firewall obtiene la mayoría de los puntos gracias a la vulnerabilidades, en cambio si es mayor a 45° es porque dicho firewall obtiene la mayoría de los puntos gracias a la vulnerabilidades y finalmente si el ángulo es exactamente 45° el firewall es estable con respecto a ambas. Gráficamente obtenemos la Figura 4.

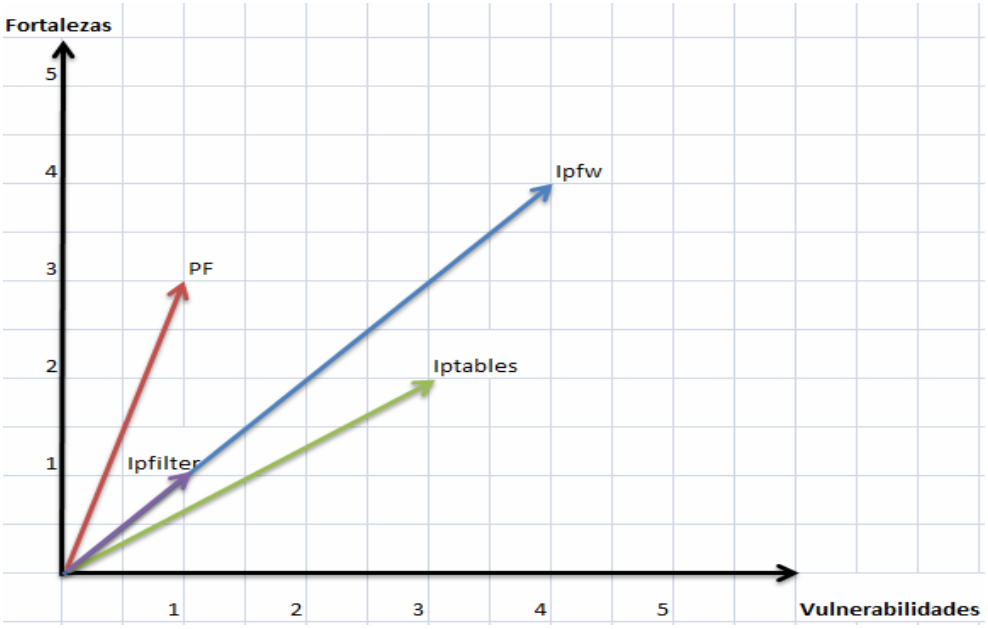

Figura 4. Vectores de confiablidad

Entonces como vemos en la Figura 4 el firewall más confiable es Ipfw y el menos es Ipfilter, sin embargo ambos son estables con respecto a ambas coordenadas, por otro lado PF tiende hacia el eje de la fortalezas al igual que Iptables tiende hacia el eje de las vulnerabilidades.

6. MODELO DE ELECCIÓN

Por último para poder sacar un modelo de elección de firewalls teniendo en cuenta sus políticas de seguridad y características de una red en particular debemos tener en cuenta lo siguiente:

- Política de seguridad: Una política de seguridad es un conjunto de reglas que indican que está permitido y que no está dentro de una organización. Estas políticas de seguridad son realizadas a nivel de gestión dentro de una empresa sin tener en cuenta la técnica ni la tecnología, para poder realizar el modelo se decidió analizar los puntos claves para definir una política seguridad y de esta forma obtener los criterios generales de elección, además de considerar que actualmente la mayoría de la empresas cuentan con un acceso a Internet lo que obliga a definir también políticas de acceso a Internet [17] [8] [6].

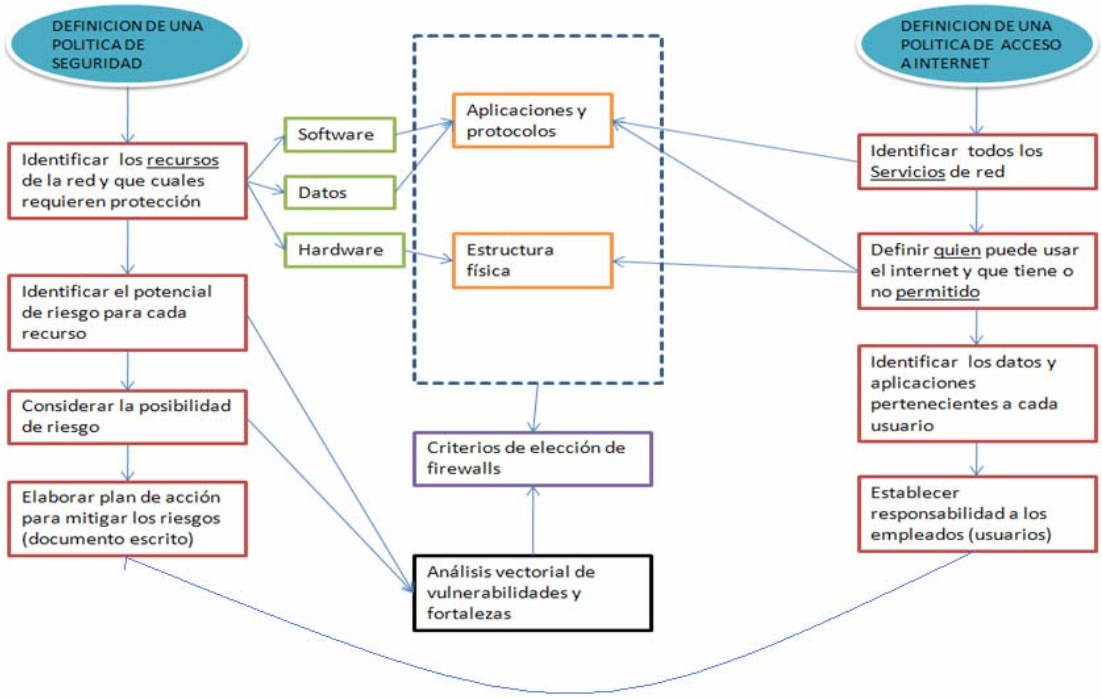

Figura 5. Definición de políticas de seguridad y política de acceso a Internet

Como se observa en la Figura 5 de los recursos se desprende el software y datos que implican a su vez las aplicaciones y protocolos de una red en particular lo que para las políticas de acceso a Internet son los servicios y lo que esta y no permitido dentro de dicha red. Por su lado el hardware implica la estructura física de la red al tener en cuenta esto se crean criterios de elección de los firewalls, sin embargo para efectos de esta investigación también se tuvo en cuenta el análisis vectorial de la sección anterior que como se ve en la Figura 5 se desprende para una política de seguridad de la identificación de riesgo y la posibilidad de ocurrencia.

- Tipo de empresa: Para efectos de esta investigación se tuvo en cuenta el tipo de empresa según su tamaño:

  - SOHO y pequeña Empresa: Máximo 50 empleados
  - Mediana Empresa: Máximo 200 empleados
  - Gran Empresa: Más de 200 empleados

Habiendo hecho el análisis para definir una política de seguridad encontramos los siguientes criterios:

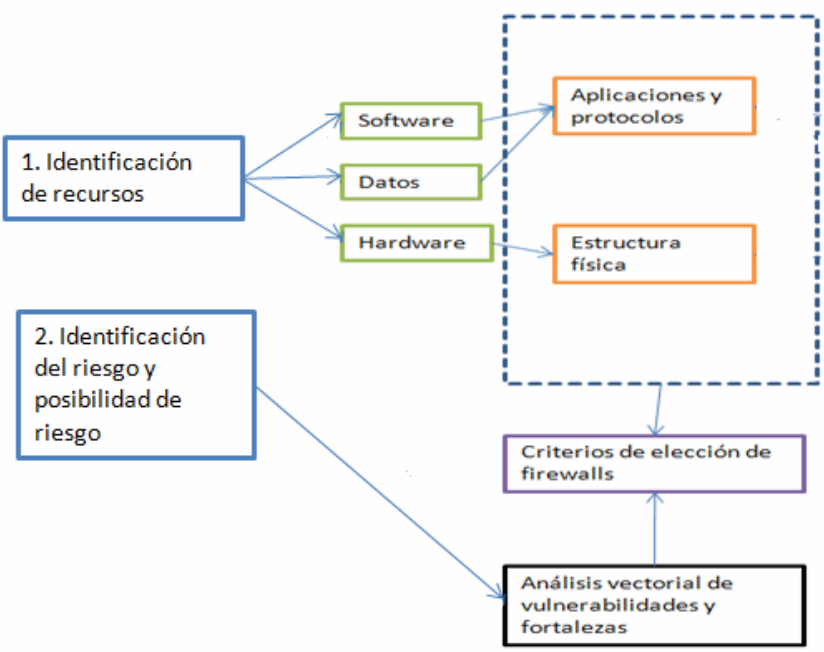

Figura 6. Criterios de elección de firewall

De la Figura 6, se usará el análisis vectorial de la sección anterior como criterio de desempate entre firewalls, ya que este me muestra la confiabilidad de cada uno.

Ahora teniendo el tipo de empresa junto con los anteriores criterios de elección sacamos las necesidades de cada empresa y de esta determinar que firewall se suple mejor esas necesidades:

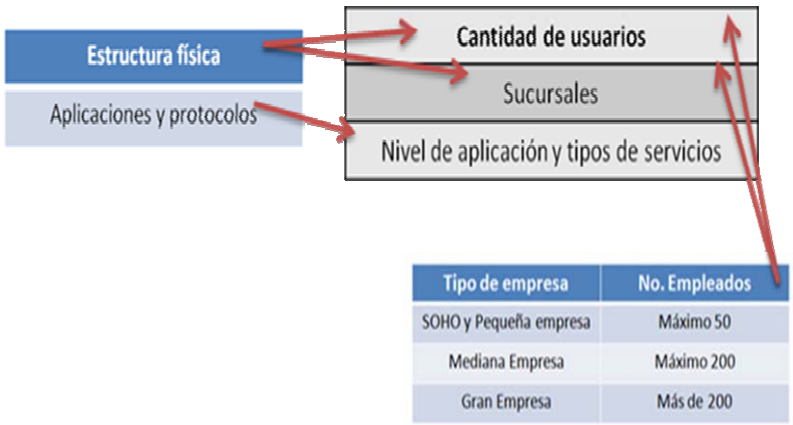

Figura 7. Necesidades de firewall según las empresas

En este orden de ideas ya podemos saber que característica (fortaleza) de cada firewall necesita cada tipo de empresa, entonces por ejemplo:

SOHO necesita de ipfw las técnicas: Keep State y Limit.

Mediana Empresa de Iptables: Keep State, Jump, Owner, rttl, Hashlimit, Filtrado tipo de paquete, Filtrado de otros parámetros de las cabeceras TCP e IP.

SOHO de PF: Keep State, Modulate State, Limite de estados por regla, Overload support.

Gran empresa de Ipfilter: Keep state, Ipstat, Iptest.

SOHO de Netdefender: Ninguna

Completando la información y sabiendo que cada fortaleza tiene un valor de eficacia diferente, mostramos en la Tabla 12 el número de fortalezas que necesita cada empresa de cada firewall seguido de un valor total que resulta de sumar todos los valores de eficacia correspondientes a las coincidencias que tuvo cada empresa con cada firewall y así sacar las mejores alternativas. El valor de eficacia de cada fortaleza junto con todas las asignaciones de fortalezas y el porqué de dichas asignaciones se encuentra en el anexo "Asignación de fortalezas" disponible en nuestro sitio http:gissic.umng.edu.co/firewalls.

Tipo de empresas/ Firewall	**SOHO**	**Mediana Empresa**	**Gran Empresa**
Ipfw	2 / 7,5	8 / **27,8**	10 / **36,3**
Iptables	2 / 7,5	7 / 24,1	10 / 34,2
Pf	4 / **14,1**	7 / 24	7 / 24
Ipfilter	3 / 8,4	3 / 7,8	3 / 7,8
Netdefender	0 / 0	1 / 1,4	1 / 1,4

Tabla 12. Coincidencias/Suma total Alternativas

Teniendo el valor total según las coincidencias entre cada firewall y cada tipo de empresa podemos sacar las mejores alternativas:

SOHO:

1era. Alternativa: Pf (4 coincidencias) = 3,8 (Keep State) + 3 (Modulate State) + 3,6 (Limite de estados por regla) + 3,7 (Overload support) = 14.1

Resolviendo para los demás firewalls y empresas obtenemos:

2da: Ipfilter (3 coincidencias): Suma total = 8.4

3ra: Ipfw (2 coincidencias): Suma total = 7.5

4ta: Iptables (2 coincidencias): Suma total = 7.5

5ta: Netdefender (0 coincidencias): 0

Mediana Empresa:

1era: IPFW (8 coincidencias): Suma total = 27.8

2da: Iptables (7 coincidencias): Suma total = 24,1

3ra: Pf (7 coincidencias): Suma total = 24

4ta: Ipfilter (3 coincidencias): Suma total = 7.8

5ta: Netdefender (1 coincidencias): Suma total = 1.4

Gran Empresa:

1era: Ipfw (10 coincidencias): Suma total = 36.3

2da: Iptables (10 coincidencias): Suma total = 34.2

3da: Pf (7 coincidencias): Suma total = 24

4da: Ipfilter (3 coincidencias): Suma total = 7.8

5da: Netdefender (1 coincidencias): Suma total = 1.4

De estos resultados vemos que para SOHO Ipfw e Iptables aparecen con el mismo valor sin embargo Ipfw aparece como una mejor alternativa ya que se uso como criterio de desempate el análisis vectorial que indicaba que Ipfw era más confiable que Iptables. Con esto damos por terminado el modelo de elección de un firewall según las políticas de seguridad y características de una red en particular. En caso de que un administrador sienta que su empresa no se identifica con ninguna de los diferentes tipos de empresas aquí mencionados, es necesario hacer el análisis de:

- El contexto empresarial
- Identificación recursos y cuales requieren protección
- Identificación riesgos y posibilidad de riesgo
- Tamaño de la empresa

Una vez hecho este análisis se determinan que necesidades de filtrado de paquetes necesita dicha empresa y aplicar las tablas aquí propuestas para obtener la mejor alternativa.

7. CONCLUSIONES

- Aunque existen muchos firewalls de código abierto sobre sistemas operativos libres, su core está basado únicamente sobre 4 específicos: Iptables, Ipfw, PF, Ipfilter y sobre ellos se basó la investigación del modelo de calificación, sin embargo es posible calificar otros firewalls aunque debido a lo repetitivo del core, los resultados deben ser los mismos.

- El método de calificación de firewall uso valores positivos únicamente tanto para vulnerabilidades como para fortalezas, ya que un 4 en vulnerabilidades indica que dicho firewall es poco afectado por las que este posee, y un 4 en fortalezas significa que dicho firewall es altamente beneficiado por las que este posee

- Establecer políticas de seguridad es un proceso más administrativo y de gestión que técnico y tecnológico, por lo tanto en esta investigación se partió de la definición de una política de seguridad y sus pasos para establecerlas, y de esta forma encontrar las diferencias técnicas de cada empresa en cuanto al filtrado de paquetes de las cuales surgen las necesidades que los firewalls deben suplir.

- Para una empresa específica se pueden tener varias alternativas según el modelo de elección, o ajustar la tabla de asignación y seguir el procedimiento para obtener la mejor alternativa.

8. REFERENCIAS

[1] Vassilis Prevelakis, “The Virtual Firewall”, Drexel University, 2005.

[2] Stephen P. Cooper, “Firewall Products Today”, Publicacion de Computer Security Technology Center, 2003.

[3] Seny Kamara, “Analysis of Vulnerabilities in Internet Firewalls”, Pardue University, 2003.

[4] Shawn Grimes, “Firewalling for free”, 2001

[5] Nitesh Dhanjani, “Claves Hackers en Linux y Unix”, pp. 23-38, McGrawHill primera edición, 2003

[6] Brian Komar, Ronald Beekelaar y Joern Wettern, “Firewalls for dummies”, pp. 71-160, Wiley Publishing Segunda edición, 2003.

[7] Robert Shimonsky, Debra Littlejohn y Thomas Shinder, “The best damn firewall book period”, pp. 56-57, Syngress, primera edición, 2003.

[8] ISO 17799, “Seguridad de la información”, pp 8 y 14-15

[9] Samuel Patton, David Doss,William Yurcik, Open Source Versus Commercial Firewalls: Functional Comparison, Illinois State University, 2000.

[10] “Cisco Systems”, Academia de Networking de Cisco Systems, página 65, ISBN: 84-205-4079-2.

[11] Doug Lowe, “Networking for dummies”, pp. 321 – 345, Wiley Publishing Séptima edición, 2005.

[12] “Vulnerability databases from the Common Vulnerabilities and Exposures (CVE) and Candidates” (CAN), http://cve.mitre.org/cve/, 2007

[13] “X-Force,” http://xforce.iss.net/, 2007.

[14] “Bugtraq”, http://www.securityfocus.com/bugtraq/archive, 2007.

[15] “Secunia”, secunia.com

[16] “National Security Vulnerabilities”, http://nvd.nist.gov