Implementación de un Cortafuegos Transparente con Monitoreo y Administración de Ancho de Banda Basado en Código Abierto.

Marco Aravena Vivar , Andrés Ramos, Mitchell Ferrand

Departamento de Computación
Universidad de Valparaíso
Gran Bretaña #1091, Valparaíso, Chile
marco.aravena@uv.cl,andres.ramos@uv.cl,mitchell.ferrand@uv.cl

Abstract. Este artículo presenta la implementación de un cortafuegos transparente con monitoreo y administración de ancho de banda basado en código abierto. El objetivo es otorgar seguridad a una red interna a través del filtraje de paquetes y la administración y monitoreo del ancho de banda. El sistema consiste en un servidor, donde se instala un sistema operativo y aplicaciones de código abierto, que interconecta las redes interna y externa de un departamento. A diferencia de los productos presentes en el mercado, el sistema propuesto se instala en forma transparente (no requiere de la modificación de ningún parámetro de red), permite el monitoreo y administración en tiempo real del ancho de banda, es de alto rendimiento, y su desarrollo e implementación es de bajo costo, debido a que se utilizan herramientas de código abierto. Para validar el sistema se realizan pruebas de usuario y se analiza su funcionamiento en producción por 2 meses. Los resultados obtenidos son excelentes comprobando la eficacia y eficiencia del cortafuegos transparente en incrementar la seguridad de la red.

Key words: seguridad, cortafuegos, ancho de banda, puente de red.

1 Introducción.

Las Tecnologías de la información en Chile han dado un gran salto en los últimos años, dejando a este país, entre los 30 más competitivos dentro de esta área [1]. Tal como la competitividad en Chile ha crecido, en su conjunto lo han hecho las necesidades de los usuarios, quienes utilizan Internet para realizar actividades transaccionales, lúdicas, comunicacionales e informativas. El usuario promedio realiza algunas de estas actividades en un promedio de 16 horas semanales según los resultados de la encuesta [2].

De la misma forma que han aumentado las conexiones y transacciones en Internet, lo han hecho también los ataques a organizaciones corporativas y académicas o institucionales. Según Gastón Tanoira, gerente de Sistemas y Soluciones de Seguridad de Cisco Systems en Latinoamérica "la seguridad de las redes debe encararse en una forma integral. No es solo un producto sino el diseño, los

procesos y sistemas integrales que hacen que una red sea segura. No se trata sólo de la instalación de un antivirus o un cortafuegos (firewall)". Ya antes de 1993 los ataques comenzaron a utilizar métodos de captura de paquetes (sniffer [3]) para detectar contraseñas, y spoofing para utilizar computadores con identificadores falsos en la transmisión de sus propios paquetes.

Dentro de una red institucional o corporativa se maneja un alto flujo de información, en el que destaca primordialmente el correo electrónico. La importancia de esta herramienta tecnológica radica en que es unos de los medios de comunicación mas importantes [4], considerando que una institución académica puede recibir seis millones de correos en un mes [5], es vital brindar seguridad a dicha información.

Por otro lado la existencia de las aplicaciones peer-to-peer (P2P [6]), dentro de una red institucional compromete su estabilidad, debido al sobreconsumo de ancho de banda que puede producir. Este problema es común en instituciones de educación, por ejemplo, en [7] se realiza un proyecto para atacarlo. Por lo que se hace necesario mantener un monitoreo y un control de ancho de banda, que permita la detección simple de un abuso en el consumo de los recursos y al mismo tiempo proteja al resto de los segmentos de red.

En este artículo se presenta un cortafuegos transparente con un sistema de monitoreo con administración de ancho de banda el cual permite brindar seguridad del tráfico entrante y saliente de una red además de un control de ancho de banda para un eficiente uso de los recursos.

2 Cortafuegos y Uso de la Red de Computadores.

Los ataques típicos que son realizados a una red de área local, pueden ser: ataque al protocolo ARP (ARP poisoning, man-in-the-middle), ataque al protocolo ICMP (ICMP flood, smurf, redirecciones), ataques al protocolo IP (Spoofing), y ataques al protocolo TCP/UDP (escaneo de puertos, SYN flood, UDP flood, DoS y DDoS) [8,9].

Para brindar seguridad a una red o a los host pertenecientes a una red se puede describir 3 tipos de cortafuegos [11]:

- Cortafuegos de capa de red o de filtrado de paquetes: funciona a en la capa 3 del modelo OSI (red), o en la capa 2 del stack de TCP/IP, como filtro de paquetes IP. Los filtros se realizan según puertos y direcciones IP de origen y destino.
- Cortafuegos de capa de aplicación: funciona a en la capa 7 del modelo OSI (aplicación).Los filtros se pueden adaptar a características propias de las aplicaciones y protocolos de esta capa.
- Cortafuegos personal: Es este caso, el cortafuegos no es instalado en el perímetro de la red, si no que corresponde a una aplicación en el computador del cliente. Filtrando solo las comunicaciones entre dicho computador y el resto de la red.

Un cortafuegos resulta útil para proteger una red interna de una externa, pero los riesgos también provienen desde la red interna como lo señala el estudio realizado por Kaagan Research & Associates (NY) a un universo de 203 directores de tecnología y jefes de seguridad de empresas latinoamericana el cual indica que el 39% son ataques internos. En muchos casos estos ataques corresponden a un abuso del ancho de banda, debido principalmente a los usuarios que utilizan aplicaciones del tipo P2P. Tal y como indica la Universidad de Chile en [7], no es muy útil utilizar cortafuegos o router que filtren este tipo de tráfico debido a que las aplicaciones se mudan a otros puertos de conexión, bajo el protocolo de comunicación de Internet TCP/IP. Según [2], dentro de los distintos usos que realizan los usuarios de internet, un 50% corresponde escuchar música online y descarga de archivos (ver fig. 1) lo que en general se realiza con algún tipo de aplicación p2p.

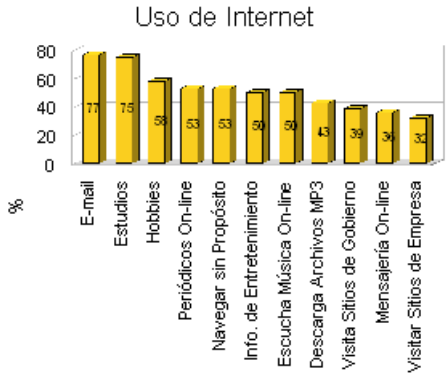

Fig. 1: Uso de Internet

La necesidad de prohibición de estos programas radica en evitar el abuso del recurso de ancho de banda. Esta problemática se ha detectado en distintas universidades como es la Universidad de Valparaíso y la Universidad de Chile, donde se han visto afectadas en la disponibilidad de la red producto del abuso de la aplicaciones P2P. En base a estas problemáticas los administradores recomiendan la prohibición del uso de este tipo de aplicaciones, pero para lograr que estas políticas se cumplan es necesario mantener un monitoreo constante de la red, identificando por este medio a los usuarios que causan el problema de disponibilidad.

3 Caso de Estudio: un Departamento al Interior de una Institución de Educación Superior.

El caso de estudio corresponde a la conectividad de un departamento (red interna), perteneciente a una institución (red externa) que cuenta con facultades (compuestas por escuelas y departamentos). En la Fig. 2 se aprecia un esquema

jerárquico donde muestra la ubicación del departamento (denominado Departamento 3).

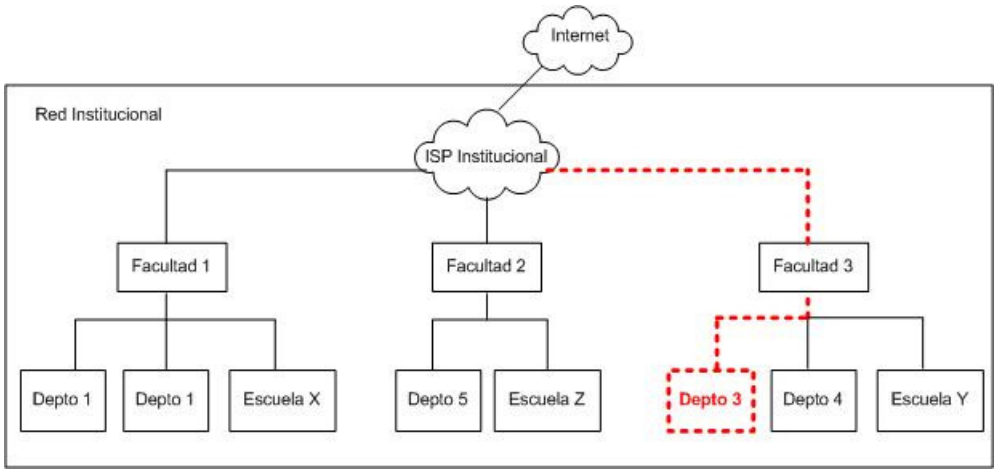

Fig. 2 : Diagrama de la red institucional

La red institucional, que engloba a toda la universidad, esta administrada por lo que se podría denominar ISP institucional. El cual asigna a todos los departamentos y escuelas de la universidad los parámetros de conectividad a internet (IP, máscara, DNS, puerta de enlace) , sin que puedan ser modificados.

La red del departamento (red interna) no cuenta con un cortafuegos, por lo que se encuentra vulnerable a ataques, y se divide en :

- **Red de Docentes**: su dirección es 10.100.6.0/24 y en ella se encuentran la mayoría de los servidores, así como también las estaciones de trabajo de los docentes. Actualmente esta red se encuentra en una etapa de aumento en sus servicios, por lo cual requiere mayor seguridad.
- **Red de Alumnos**: su dirección es 192.168.1.0/24 creada mediante NAT en un servidor perteneciente a la red 10.100.6.0. En esta red se encuentra un servidor de correos y de archivos de los alumnos el cual da soporte a 450 usuarios aproximadamente.

Los servicios de la red perteneciente al departamento se encuentran en funcionamiento en régimen 24X7, lo que implica un problema de disponibilidad a la hora de intervenir un servidor en producción en caso de ataques.

El problema de seguridad dentro de la red mencionada se puede visualizar y dividir en dos bloques:

- **Problemas desde red externa**: en la actualidad la topología, dada por el ISP institucional de la universidad, corresponde a una red "plana" físicamente (no hay segmentación física por departamento o escuela). Esto se puede apreciar en la digura 3.1. donde se observa a todos los departamentos conectados a mismo switch.

- Ejemplos de problemas de seguridad:
  - Cualquier computador puede acceder a otro sin ningún tipo de restricción (independiente del departamento al cual pertenezca) , ver Fig. 3 círculo 1.
  - Un computador perteneciente a la red de la Escuela Y puede tener asignada una ip perteneciente a la red del Departamento 3 para realizar ataques (posible problema de suplantación de IP y desorden administrativo), ver Fig. 3 círculo 2.

– **Problemas desde red interna**: uno de los problemas en la red interna es la asignación de ip de manera no autorizada, dado que no existen restricciones para que un usuario pueda asignarse arbitrariamente parámetros de red.
  - Ejemplos de problemas de seguridad:
    - Descargas tipo P2P realizadas por un supuesto usuario válido, ver Fig. 3 círculo 3.
    - Captura de paquetes y suplantación de identidad, ver Fig. 3 círculo 4.

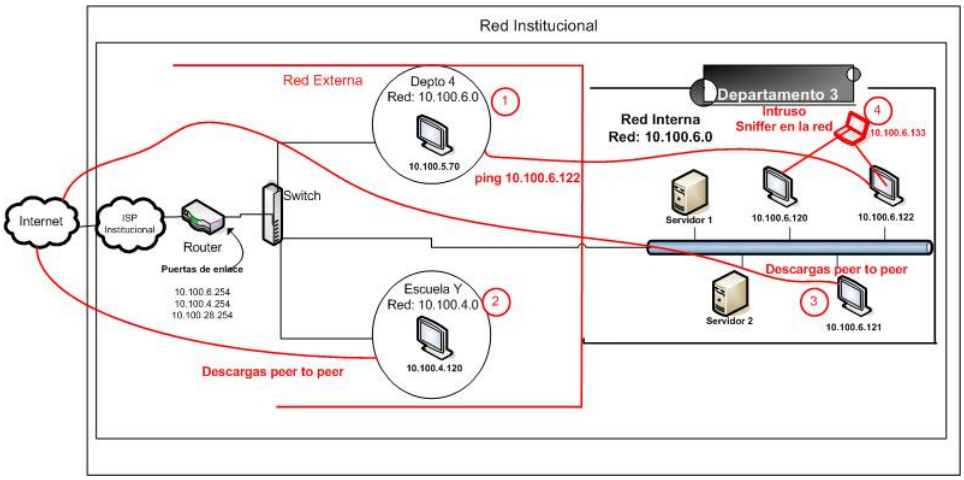

Fig. 3: Vulnerabilidades red externa e interna.

4 Soluciones Existentes.

Debido a la estructura de la red descrita anteriormente, se hacen necesaria la instalación de un sistema que permita incrementar el nivel de seguridad bajo las siguiente condiciones:

– Administración y monitoreo en tiempo real del ancho de banda. De tal manera que problemas de descargas tipo P2P no afecten al resto de los departamentos o facultades y sea rápido identificar el origen de un abuso de consumo de ancho de banda.

- Incorporar filtrado de paquetes desde y hacia el departamento (cortafuegos). Para limitar el acceso indebido desde y hacia la red externa.
- No modificar parámetros asignados por el isp institucional (no se puede usar NAT) .
- No intervenir en la conectividad de los distintos servidores en producción del departamento.

En el mercado existen aplicaciones y sistemas orientados a este tipo problema (ver tabla 1), pero lamentablemente ninguna de ellas cumple con los requisitos anteriormente expuestos.

Tabla 1: Características de sistema o aplicaciones

Sistema o aplicación	Licencia	Complejidad de configuración	Cantidad de equipos	Admin. Ancho de banda	Monitoreo	Cortafuegos	Adaptación
BandwidthD's	GNU/GPL	media	muchos	no	si	no	no
Bmon	GNU/GPL	alta	uno	no	si	no	no
Cacti	GNU/GPL	medio	muchos	no	si	no	no
Cbm	GNU/GPL	alta	sin info	no	si	no	No complejo de visualizar
Iptraf	GNU/GPL	media	muchos	no	si	no	no
MRTG	GNU/GPL	alta	muchos	no	si	no	complejo
Iptables	GNU/GPL	alta	muchos	no	no	si	no
NetFlow	US$12,99	media	muchos	no	si	no	no
PRTG Traffic Grapher	US$99,95	alta	muchos	no	si	no	no
3Com OfficeConnect VPN cortafuegos	US$485	alta	sin info	no	no	si	no
FortiGate-50A	US$799	alta	muchos	no	no	si	no
Cisco PIX 501	US$669	alta	muchos	no	no	si	no
Trendnet TW100BRV204	US$699	alta	media	no	no	si	no

5 Propuesta: Cortafuegos Transparente con Administración y Monitoreo de Ancho de Banda.

La solución propuesta consiste en la instalación de un servidor que conecta la red interna con la externa (ver Fig. 4) configurado con las siguiente características:

- **Filtrado de paquetes transparente**: basado en ipfw [12](implementado en el kernel del sistema operativo FreeBSD [13]) e instalado como puente de red (bridge[14])
- **Administración de ancho de banda**: basado en DUMMYNET [15](implementado en el kernel del sistema operativo FreeBSD).
- **Monitoreo de ancho de banda**: medición de tráfico en las interfaces de red y visualización mediante un servidor web instalado en el mismo servidor.

Las ventajas de este sistema son:

- **Bajo costo**: todas las aplicaciones, así como también el sistema operativo tienen licencia de software libre o código abierto.
- **Alto rendimiento**: como ejemplo se puede mencionar la instalación de un servidor configurado con las características mencionadas y un uso de menos del 5% de CPU para una red interna con mas de 500 computadores (el servidor tiene 2GB en RAM, tarjetas de red operando a 1Gbps y CPU dual core 1.8GHz)
- **Instalación en forma transparente**: la gran ventaja de esta propuesta es que el servidor es instalado sin la modificación de ningún parámetro de red, tanto en la red interna como en la externa.

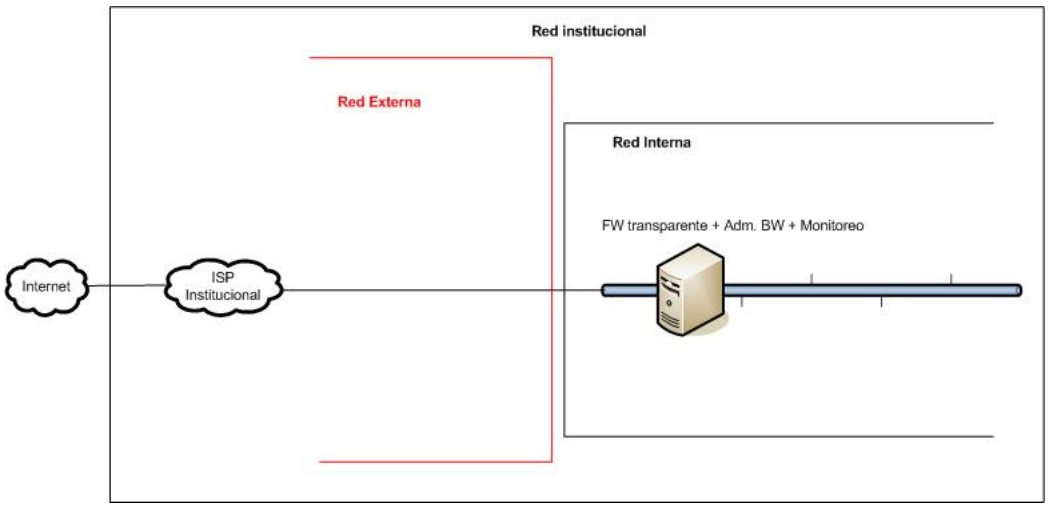

Fig. 4: Implementación del Sistema

6 Validaciones y Resultados.

Las pruebas realizadas al sistema son de dos tipos: pre-instalación y post-instalación(puesta en marcha del sistema) .

Las pruebas de pre-instalacióncorresponden a la verificación de los requisitos para el sistema. Los resultados obtenidos se muestran la tabla 2.

Tabla 2: Pruebas realizadas

Prueba	Resultado Esperado	Resultado Obtenido	Mantención
Conectividad con ip válida a través del cortafuegos transparente desde la red interna.	Conectividad OK.	Conectividad OK.	Sin mantención.
Conectividad con ip no autorizada a través del cortafuegos transparente desde la red interna.	Sin conectividad.	Sin conectividad.	Sin mantención.
Conectividad no autorizada con ip válida, desde una red externa hacia la red interna	No hay respuesta.	Hay respuesta.	Se reestructuran las reglas del cortafuegos. Y se reintenta la prueba obteniéndose los resultados esperados.
Consumo de ancho de banda por un equipo de la red.	Ok en comparación con el programa de descarga de mozilla.	Ok en comparación con el programa de descarga de mozilla.	Sin cambios
Consumo de ancho de banda sobre el máximo configurado.	No se excede del límite configurado.	No se excede del límite configurado.	Sin cambios

Estas pruebas han permitido obtener y detectar la eficacia y eficiencia de la red, determinado la seguridad existente es la esperada y que la administración y el monitoreo del trafico existente es correcto, limitando el ancho de banda a niveles que no afectan al resto de la universidad.

Para las pruebas de post- instalación, se realizó una aplicación web que permite visualizar el tráfico de los distintos equipos que componen el departamento. Además se implementa un procedimiento de restauración, en caso de que el servidor que se encuentra como cortafuegos fronterizo y monitoreo no soporte las necesidades que el departamento requiere para su tráfico.

Los resultados obtenidos son los esperados, donde el sistema soporta la carga esperada para el departamento para una red con 90 computadores y 4 servidores. Lo anterior fue corroborado en un periodo de 2 meses de funcionamiento en producción. Un ejemplo de ataque ocurrido en ese período de tiempo se puede

ver en la Fig. 5. En este caso, no se sobrepasa el límite de 10Mbps configurado en el servidor.

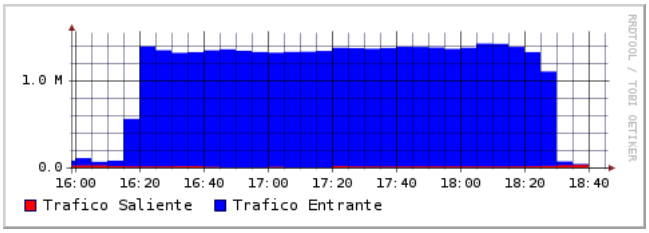

Fig. 5: Utilización de aplicación P2P con el uso de todo el ancho de banda (medido en bytes).

7 Conclusiones.

Se ha presentado la implementación de un cortafuegos transparente con administración y monitoreo de ancho de banda basado en herramientas de código abierto. El sistema propuesto responde a las necesidades actuales de seguridad, (filtraje) y administración de ancho de banda en forma transparente, que no son cubiertas por las soluciones de mercado. Por lo cual, presenta ventajas en cuanto a funcionalidad (alto rendimiento, funcionamiento en modo transparente, monitoreo y administración en tiempo real del ancho de banda) y costos, debido a que es implementado con herramientas de código abierto. Para su validación se realizan pruebas de usuario con excelente resultados. Además, el sistema es puesto en producción por 2 meses en un escenario real, comprobánse su eficacia y eficiencia en otorgar seguridad y administrar el ancho de banda.

References

1. World Economic Forum, Reporte mundial sobre Tecnología de la Información 2005-2006, http://www.chilecompra.cl
2. World Internet Project Chile (WIP chile), http://www.wipchile.cl
3. Tipos de Sniffer, http://es.wikipedia.org
4. Mejorando la competitividad mediante el uso del correo electrónico, http://www.microsoft.com
5. Estadísticas Tráfico Correo Electrónico UACh Junio 2007, http://www.uach.cl
6. P2P, http://es.wikipedia.org/
7. Postulación a proyecto para delimitación de ancho de banda, http://www.sti.uchile.cl
8. Ataques de Red, http://www.linuxfocus.org
9. Richard Stevens, W. : TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley Professional (1994)
10. Kaspersky Lab virus analyst, http://www.viruslist.com
11. Network Working Group, http://tools.ietf.org
12. ipfw, http://www.freebsd.org
13. FreeBSD, http://www.freebsd.org
14. Puente de Red, http://es.wikipedia.org
15. DUMMYNET, http://info.iet.unipi.it