Arquitecturas para bastiones (firewalls)

Jesús Oliva García

Departamento de Automática
Universidad de Alcalá
joliva@arrakis.es

Juan Antonio Rodrigo Yanes

Departamento de Automática
Universidad de Alcalá
jrodrigo@aut.uah.es

José Antonio Gutiérrez de Mesa

Departamento de Ciencias de la Computación
Universidad de Alcalá
jgutierrez@uah.es

Jordán Arribas Aranda

Departamento de Automática
Universidad de Alcalá
jordan.arribas@eresmas.net

ABSTRACT

This work shows the valuable results of some firewall architectures. The architectures are building with firewall applications running in PC or specific hardware, and routers. There is the risk of inadequate implementation of the firewall architecture. This risk is related with user security. The user not fully understanding the firewall architectures and installing theirs in such a way as not to give the desired level of protection. The set of architectures studied in this paper address some major impediments to effective mapping user security and user resources.
Key-word: Firewalls, firewall architecture.

1. INTRODUCCIÓN

La seguridad de las redes de ordenadores ha pasado de ser algo desconocido para la mayoría de los profesionales a ser uno de las temas más activos. Cualquier usuario de un PC tiene el ordenador repleto de programas recomendados por individuos que avisan de la cantidad de gente peligrosa que hay en las redes. Sin duda, la culpa de la extensión de toda esta avalancha armamentística (tanto a nivel de defensa como de protección) es de Internet. Además, la proliferación de la "banda ancha", ADSL, y las posibilidades de conexión que para "otros" supone contratarla, ha convertido la seguridad de las redes/ordenadores en un tema de máxima actualidad.

En este artículo se hace un análisis de la situación desde el punto de vista de la defensa de la red. Se analizan varias arquitecturas para cortafuegos desde el punto de vista de la seguridad y del coste, en pérdida de velocidad de la red.

Este trabajo ha sido financiado como parte del Proyecto de Investigación CICYT Ter-98-0544.

2. BASTIONES

Para proteger una red se dispone de diversas herramientas entre las que elegir las más adecuadas para la red concreta a proteger: medidas a nivel del sistema operativo, bastiones/cortafuegos, sistemas de detección de intrusos, de auditoría, etc. Sin duda alguna, uno de los más utilizados son los bastiones.

Sin embargo, los bastiones no tienen una arquitectura y tecnología concreta. Dependiendo del sistema sobre el que se vaya a instalar, los servicios que se quieren prestar, del presupuesto disponible y de otros factores, convendrá más una arquitectura u otra. El rango de posibilidades va desde equipos diseñados específicamente para realizar esta función, como los PIX de cisco [1], hasta los programas de libre distribución para Linux o Windows. La arquitectura del cortafuegos es la suma, la topología, de los distintos elementos que lo forman [2]. Dentro de las tecnologías para bastiones podemos distinguir los bastiones basados en filtrado de paquetes, los basados en *proxies* y los basados en la tecnología "stateful inspection".

Hay que tener en cuenta que los bastinones son una herramienta para la seguridad, pero que no dan seguridad en sí mismos

3. SOBRE EL ANÁLISIS DE UN BASTIÓN

A la hora de elegir un cortafuegos hay que sopesar varios factores. En este trabajo básicamente se van a tener en cuenta los siguientes:

-Nivel de seguridad: Seguridad que se requiere para el sistema; vendrá determinado por la política de seguridad de la red. Una arquitectura no es más segura que otra por sí sola, aunque bajo ciertas circunstancias y con una configuración adecuada sí que puede serlo.

-Presupuesto: Se refiere al coste total del bastión, tanto de instalación como de mantenimiento. Suele ser el factor determinante, la mayoría de las veces, en la elección de una u otra arquitectura.

-Complejidad: Dificultad en el montaje y mantenimiento del sistema. A mayor complejidad mayor probabilidad de cometer errores en la instalación.

-Rendimiento: El rendimiento a nivel de red del sistema es fundamental, por ejemplo, para servidores que atienden grandes cantidades de clientes diariamente, como pudiera ser el servidor de un sitio web muy frecuentado. Para estas medidas se han utilizado tanto aplicaciones comerciales (NetDoppler®) como aplicaciones construidas específicamente para el estudio. Se han seguido las recomendaciones de las RFCs 2544 [3] y 2647 [4] redactadas como "patrón" para realizar estas medidas, además de otras fuentes [5]. El problema aquí es la falta de patrones reales que utilizar como referencia, las RFC son muy genéricas.

Se han realizado pruebas tanto con carga artificial, pruebas a "nivel de laboratorio" con paquetes Icmp, como pruebas con tráfico real (protocolos http y ftp). Además, se han realizado pruebas para medir la velocidad de conexión, muy importantes para evaluar el rendimiento de un bastión.

Los resultados y medidas que se van a presentar en este artículo se deben considerar como medidas relativas. Es decir, no disponemos de parámetros que evalúen lo segura o insegura que es una arquitectura en forma absoluta, siempre se debe entender como lo segura que es en comparación con otra. Este comentario sobre la seguridad se puede extender al resto de los factores.

Al considerar los elementos que formarán parte de la arquitectura se presentan varias opciones básicas: PCs ejecutando aplicaciones de cortafuegos, encaminadores (routers), aplicaciones cortafuegos y, en definitiva, cualquier elemento que se pueda colocar entre dos redes y que sirva para controlar todo el tráfico que circula entre ellas.

Sin duda, la elección de uno u otro elemento afectará al resultado del análisis, aunque a nivel comparativo los resultados serán correctos. Para estas pruebas se han utilizado el paquete Firewall-1 v4.0 de CheckPoint® [6] y encaminadores de la casa CISCO®. Se han utilizado estos elementos porque son de los más extendidos en la construcción de cortafuegos.

En cuanto a la presentación de las pruebas, primero se empezará analizando la arquitectura más simple de todas, en la que no existe cortafuegos, para ir aumentando la complejidad y el número de los elementos, paso a paso. Se presentan los resultados de 4 arquitecturas: conexión directa a la red exterior, conexión a través de un bastión, conexión a través de un bastión de tres vías, arquitectura con encaminador y bastión.

4. RED SIN BASTIÓN

Esta arquitectura se analiza para disponer de un conjunto de valores de los parámetros que podamos utilizar como referencia, sobre todo para evaluar la pérdida de rendimiento que se produce al incluir el bastión. A pesar de ello no deja de ser una "arquitectura" muy utilizada. Es típica en lugares donde sólo se construye la seguridad a nivel de nodo y se olvida un poco la seguridad a nivel de red.

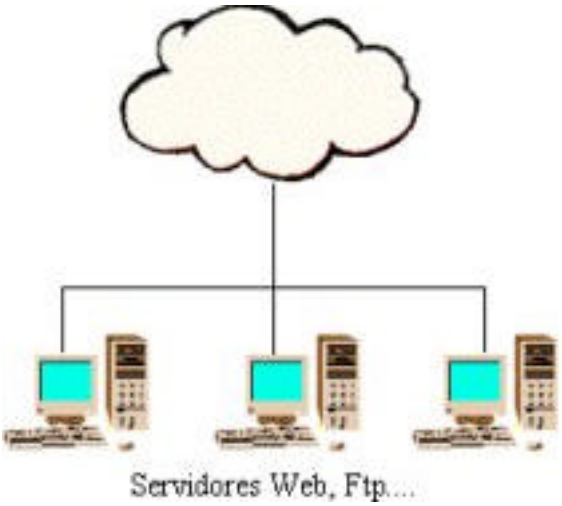

Figura 1. *Red sin bastión*.

Esta arquitectura tiene sus ventajas, es la más barata y la menos compleja de todas ya que no hay cortafuegos y, por tanto, no hay que configurarlo. Además, es la de más alto rendimiento. Sin embargo, es también la menos segura. Hay que advertir que el no tener bastión no quiere decir que el sistema sea inseguro, sino que debe ser menos seguro que si lo tuviera (siempre que esté configurado correctamente). Como la seguridad es a nivel de nodo, se debe construir en cada uno de los equipos de la red. Sin embargo, la inclusión del cortafuegos protegería toda la red a nivel global, además de proporcionar un mecanismo centralizado de registro de las entradas.

El resultado de las pruebas de rendimiento puede verse en la siguiente tabla (tabla 1):

Número de conexiones/sg	685,4
Latencia ICMP (msg)	0,580
Velocidad ICMP (Kb/sg)	842’160
Páginas web/sg (100kb/pag)	10,05
Velocidad tráfico real (Kb/sg)	1.032’886

Tabla 1.Rendimiento de la primera arquitectura.

5. BASTIÓN SIMPLE

Ésta es la arquitectura más sencilla que ya contiene un cortafuegos. Consiste en situar un ordenador como bastión, con la aplicación Firewall-1® instalada, entre la red exterior y la red a proteger.

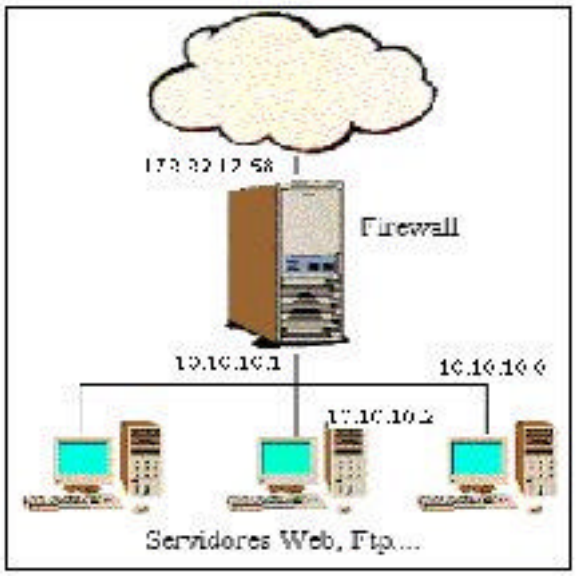

Figura 2. *Sistema con un único bastión.*

Este sistema dispone de un único punto desde el que controlar toda la seguridad de la red y en el que realizar el registro. Esto es posible porque todo el tráfico que entra y sale de la red es inspeccionado por el cortafuegos. Otra ventaja que tiene el que todo el tráfico pase por un único punto, es que se puede utilizar NAT (traducción de direcciones) [6] ahorrando direcciones públicas. Sin embargo, como se verá en las pruebas, el uso de NAT produce una pequeña pérdida de rendimiento.

Desde luego, el precio aumenta con respecto a la arquitectura anterior. Además, este elemento añadido y el hecho de tener todo el tráfico y las funciones de control centralizadas en un único punto hace que se pierda rendimiento. La complejidad aumenta al tener que instalar, configurar y mantener la aplicación cortafuegos, la máquina sobre la que trabaja y realizar una redistribución topológica de la red.

Centralizar la seguridad en un punto, tiene el inconveniente de que si se "cae" el bastión se queda toda la red sin conexión con el exterior.

En este caso, las medidas de rendimiento se han realizado con dos variantes: utilizando y sin utilizar NAT.

	Sin NAT	Con NAT
Número de conexiones/sg	373,69	346,62
Latencia ICMP (msg)	1,458	1,617
Velocidad ICMP (Kb/sg)	348,48	349,39
Páginas web/sg (100kb/pag)	8,66	8,5
Velocidad tráfico real (Kb/sg)	894,621	878,25

Tabla 2.*Rendimiento de un bastión simple.*

6. BASTIÓN CON DMZ Y ENCAMINADOR

En una red es normal que los equipos se puedan dividir en dos grupos desde el punto de vista de la seguridad. Uno de los grupos lo forman los equipos, normalmente servidores, que dan acceso a Internet. Estos equipos se deben proteger, pero en ellos no se sitúa información sensible.

En el segundo grupo lo forman los equipos con información sensible que se tratan de proteger de forma especial frente a accesos no autorizados.

Para disponer de dos grupos de máquinas con restricciones de acceso muy diferentes se recurre a una arquitectura con dos redes. A la primera de las redes, la que tiene restricciones de acceso menos fuertes, se la denomina DMZ (zona desmilitarizada).

Al dividir las máquinas en dos redes se puede conseguir que el tráfico de la red interna no sea visible en la DMZ, con lo que se consigue que un *sniffer*, introducido en esta red, no acceda a la información sensible de la organización [7]. Además, los nodos que ofrecen servicios son siempre más vulnerables a los ataques, por lo que resulta aconsejable separarlos [8].

Para aumentar la seguridad del conjunto se puede utilizar un encaminador. El encaminador se puede instalar entre la red externa y el bastión, a modo de primera barrera defensiva. Con estos elementos se configura la tercera arquitectura que se presenta (ver figura 3).

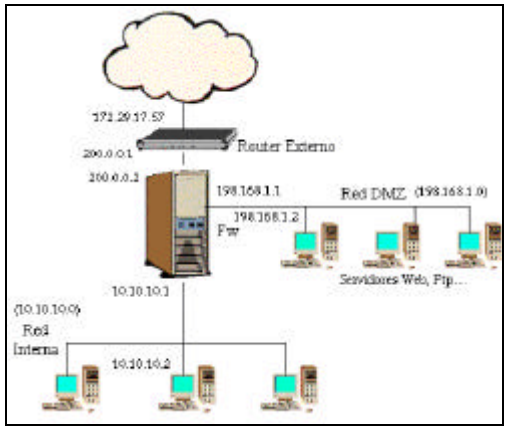

Fig. 3. *Bastión, DMZ y encaminador.*

Si se configura el filtrado de paquetes en el encaminador, se puede, además, proteger el primer nodo (con fw-1), el bastión, de modo que el *router* sólo reencamine hacia esta defensa la información que va para la red, y, de ésta, sólo la que esté permitida. Por ejemplo, si alguien lanzara un ataque *Syn flood* [9] sobre la red, desde el bastión hacia abajo todo funcionará correctamente sin verse siquiera influidos. Será el encaminador el que se encargue de proteger la red del ataque. Esto descarga de trabajo al bastión lo que influye en el rendimiento.

La política de seguridad se puede hacer más selectiva al discriminar entre las dos redes, con la complejidad añadida de la configuración del encaminador y sus reglas de filtrado.

El presupuesto se incrementa con el precio del encaminador, que en algunos casos puede llegar a ser bastante alto en relación con el resto de componentes.

El rendimiento es lógico que caiga un poco debido a que ahora hay un elemento más por el que tiene que pasar el tráfico antes de llegar a su posible destino. Los resultados obtenidos para los paquetes que van desde el exterior hasta la red DMZ son los siguientes:

Número de conexiones/sg	160,18
Latencia ICMP (msg)	5,852
Velocidad ICMP (Kb/sg)	239,392
Páginas web/sg (100kb/pag)	4,82
Velocidad tráfico real (Kb/sg)	498,373

Tabla 3. *Rendimiento del acceso a la DMZ*

En el caso de los paquetes que van desde el exterior hacia la red interna:

Número de conexiones/sg	153,18
Latencia ICMP (msg)	6,402
Velocidad ICMP (Kb/sg)	239,432
Páginas web/sg (100kb/pag)	4,83
Velocidad tráfico real (Kb/sg)	498,377

Tabla 4. *Rendimiento del acceso a la red interna.*

Las diferencias entre los resultados de las dos tablas se deben al orden de las reglas de filtrado. Este punto sirve para advertir de la importancia que tiene, en cuanto al rendimiento se refiere, tanto el número como el orden en que se colocan las reglas de filtrado de un cortafuegos [10].

Es por eso recomendable colocar antes las reglas de filtrado que se refieren al tráfico al que se quiere dar prioridad (en este caso el correspondiente a los servicios públicos) ya que supone un aumento del rendimiento.

En relación con las arquitecturas anteriores, esta arquitectura pierde bastante rendimiento. La perdida de rendimiento debida al encaminador es aproximadamente del 50% (cisco 2600). Para comprobar este resultado se hizo una traza desde el exterior hasta el interior obteniéndose el siguiente resultado (figura 4).

En la gráfica se ve claramente que la pendiente mayor corresponde a la recta del tramo medio, que es la latencia de paso de los paquetes por el encaminador. Queda confirmado entonces que la diferencia en el rendimiento se debe a este equipo.

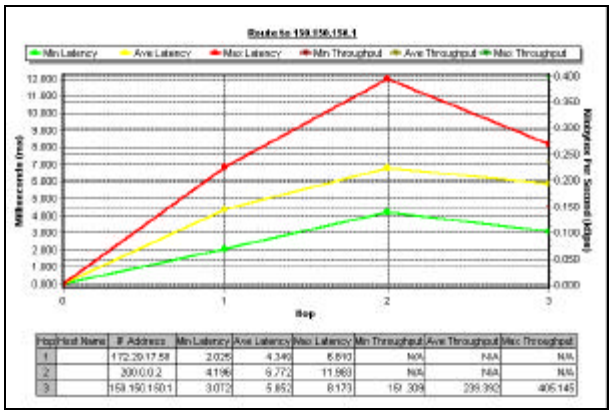

Fig. 4. *Traza del tráfico con encaminador.*

Para obtener un rendimiento mayor cabría sustituir el encaminador utilizado por otro más rápido para, de este modo, eliminar el *cuello de botella*.

7. CONCLUSIONES

Se ve claramente que las arquitecturas más simples tienen un mejor rendimiento, que se sacrifica para mejorar las características de otros parámetros.

El salto más brusco se corresponde con la introducción del encaminador.

8. REFERENCIAS

[1] Cea, Francisco "Nokia y Check Point: Positioned to Win", Seminario Wireless, Madrid, 2002.

[2] Chapman, D.B. and Zwicky, E., "Building Internet Firewalls", O'Reilly, 1995.

[3] RFC 2544 "Benchmarking Methodology for Network Interconnect Devices *001"*

[4] RFC 2647, Benchmarking Terminology for Firewall Performance.

[5] Firewall Performance bench,

"http://www.keylabs.com/services/benchmark.html"

[6] Firewall-1®.User´s Guide. CheckPoint 1998.

[7] Anónimo, "Máxima Seguridad en Internet", Ed. Anaya, 1998.

[8] W.R. Cheswick and S.M. Bellovin. "Firewalls and Internet Security", Ed. Addison Wesley, 1994.

[9] S. Northcutt and J. Novak. "Detección de intrusos", Ed. Prentice Hall, 2001.

[10] Mason, A.G. and Newcomb, M.J., " Cisco Secure Internet Security Solutions", Ed. Cisco Press, 2001.