Firewalls de aplicación

Alfonso Franco Gómez — *Responsable de Preventa y Tecnología*

Pablo García Pérez — *Ingeniero de proyecto. División de Seguridad Lógica de Germinus*

Introducción

Desde la aparición de los primeros cortafuegos, las medidas de seguridad han ido evolucionando de la misma forma que lo han hecho las aplicaciones y servicios desplegados en Internet. Desde las primeras páginas http estáticas, pasando por los primeros CGI's, hasta los servidores de aplicación actuales se han producido numerosos cambios, todos ellos han motivado un cambio de estrategia a la hora de defender y proteger las infraestructuras conectadas a Internet frente a nuevas formas de ataque y nuevas amenazas que afectaban a estos nuevos servicios.

En primer lugar conviene hacer un poco de historia que ayudará a entender la necesidad y el auge actual de estos sistemas, de forma que no se confundan conceptos puesto que un firewall http no es lo mismo que un firewall de nivel de aplicación, aunque ambas cosas suenen "parecidas".

A continuación se muestra un esquema de la evolución de los sistemas cortafuegos, desde los primeros filtros de paquetes hasta los cortafuegos a nivel de aplicación.

- Filtrado de paquetes: Únicamente protegen permitiendo o bloqueando determinados puertos UDP o TCP. No establecen ningún control sobre la sesión una vez que está establecida.
- Inspección de estados: Establecen un nivel de seguridad adicional al mantener un control de la sesión desde su establecimiento hasta su finalización.
- FW a nivel de aplicación: Constituyen sin duda un paso más en la evolución de los sistemas cortafuegos, ya que en este caso analizan todo el paquete a nivel de aplicación o, lo que es lo mismo, controlan no solo los puertos o las sesiones, sino el protocolo que se utiliza para la comunicación, evitando que puedan falsearse servicios. Por ejemplo, sería posible prohibir el acceso http independientemente de que el servicio http estuviera levantado en el puerto 80 o en el puerto 145, ya que el firewall analizará el protocolo de los paquetes y al ver http bloqueará la conexión.

¿Y ahora qué? Llegados a este punto ¿cómo nos protegemos de los nuevos ataques?, o mejor aún, ¿cuáles son los nuevos ataques?

Problemática actual

La proliferación de intrusiones a través de los aplicativos y la concienciación de las empresas por la necesidad de realizar auditorías de seguridad comenzaron a revelar que la mayor parte de los ataques que se sufrían venían derivados precisamente de fallos o vulnerabilidades en los aplicativos propios de las empresas. Estos aplicativos representaban, y hoy en día siguen representando, la mayor amenaza para las empresas.

Contra estos problemas poco, o mas bien nada, puede hacer un firewall (del nivel que sea), por lo que se hace necesario recurrir a nuevas soluciones que actúen como complemento a los sistemas de seguridad perimetral y que permitan de alguna manera paliar estos problemas que, en la mayor parte de los casos, se deben a deficiencias en la programación de las aplicaciones.

Tecnología de los Firewalls HTTP

Los firewalls http son cortafuegos a nivel de aplicación que ofrecen protección para servidores Web,

tratando de prevenir y controlar todos los posibles ataques y vulnerabilidades que se produzcan a nivel de aplicación. Algunos pueden ofrecer además servicios de Proxy (ó Proxy inverso) de http.

Es decir, dentro de la evolución de los sistemas de firewall, los cortafuegos http se centran en la protección de las aplicaciones situadas en servidores Web y, por tanto, deben ocuparse de todo lo asociado con el protocolo http.

Nivel TCP/IP	Tipo de firewall utilizado
Aplicación	FIREWALL HTTP
Transporte	Firewall de filtrado de paquetes e inspección
Red	Firewall de filtrado de paquetes
Enlace	Conmutadores, filtrado de direcciones MAC,...

Figura 1: Niveles de la torre TCP/IP donde aplican los distintos tipos de firewall

Existen actualmente diversos ejemplos de firewalls http disponibles en el mercado:

- ✗ Hive, de s21sec.
- ✗ AppShield™ 4.5 Web Application Firewall, de Sanctum.
- ✗ Zorp, cortafuegos tipo proxy muy modular.

Pueden implementar distintos mecanismos de filtrado, como son:

- ✗ En función del método HTTP utilizado y la información de cabeceras.
- ✗ En función de la URL solicitada y sus contenidos.
- ✗ En función del contenido http.
- ✗ En función del origen o destino.

Se pueden definir dos estrategias generales distintas a la hora de implementar estos firewall:

1. La primera estrategia se basa en dos aproximaciones complementarias:

Por un lado, se implementan reglas de filtrado basadas en añadir ataques conocidos a servidores Web. Esta información de ataques (firma) puede ser obtenida tanto de herramientas de prueba de vulnerabilidades, que simulan ataques a servidores Web, como de la información de vulnerabilidades conocidas asociadas a estos servicios Web.

En segundo lugar, el mecanismo de filtrado se basa en el tráfico http habitual del servicio actualmente desplegado. El análisis de este tráfico permite definir una serie de generalidades asociadas al servicio (URLs y métodos permitidos, contenido en la llamada de aplicaciones, etc.) que permiten implementar una política "todo lo que no está expresamente permitido está prohibido"; que puede denegar, de forma directa, los ataques ya sean conocidos o no. Sin embargo, hay que recalcar que esto puede ser difícil de definir para ciertos ámbitos y entornos.

2. La segunda estrategia consiste en implementar el protocolo HTTP tal y como está definido en los estándares de Internet, prohibiendo a cualquiera que trate de romper la seguridad de las aplicaciones protegidas usando peticiones deformadas o modificando peticiones legítimas.

Ambas estrategias son compatibles y/o complementarias entre sí.

Son muchos los ataques que pueden bloquear estos sistemas, a continuación se citan los más importantes y relevantes de ellos:

- ✔ Filtrado de URLs: Un grupo de ataques habituales a servidores web, realizados por herramientas automáticas y gusanos, se realizan a través de URLs que aprovechan vulnerabilidades específicas de los servidores web. Por tanto deben ser capaces de filtrar URLs, tanto definidas de forma completa, como a través de expresiones regulares. Esta información se recoge en firmas y las solicitudes web que incorporen estas firmas deben ser bloqueadas por el firewall.
- ✔ Control de protocolo http: Ofrecen una alta granularidad en el control de la funcionalidad ofrecida en el protocolo http. Así, se pueden controlar tanto las operaciones (GET, POST, PUT, DELETE, TRACE...) como los parámetros que se incluyan en dichas operaciones. Se exige conformidad completa con el protocolo, y se pueden filtrar solicitudes de un tipo concreto (User-Agent de sólo unos tipos concretos,...).
- ✔ Resistencia y mitigación a ataques de denegación de servicio
- ✔ Ataques a aplicaciones vulnerables: La mayoría de servidores Web, al ser instalados por defecto, incluyen páginas de ejemplo y aplicaciones que pretenden mostrar las capacidades del servidor a los nuevos usuarios; suelen ser vulnerables a ataques y por tanto activamente explotadas por crackers. Estos firewalls detienen el acceso a estas páginas que no están directamente referenciadas en el sitio web.
- ✔ Problemas de implementación de servidor: Se trata de eliminar los problemas generados por los errores en la implementación de los servidores Web, como el error de programación en Unicode encontrado en IIS, o el desbordamiento de memoria shtml en Iplanet.
- ✔ Manipulación de campos ocultos: Existen unos campos de formularios no visualizables por el usuario final, donde las aplicaciones almacenan la información de sesión. Se puede acceder a ellos a través del código fuente de

la página HTML o de la barra de direcciones del navegador, y por tanto son susceptibles de ser modificados por cualquier atacante. Lo que se hace es proteger los campos con firmas digitales para que no sean modificados, o bloquear los ataques y registrarlos.

- ✔ Desbordamiento de memoria (buffer overflow): Solucionan los problemas de desbordamiento de memoria, que presentan las aplicaciones que confían en los límites de la longitud del campo de los formularios, ya que esta limitación es fácilmente superable.
- ✔ Deterioro de cookies: A través de, por ejemplo, la firma digital del contenido, se evitan los problemas de seguridad generados por la información transitoria almacenada en las cookies.
- ✔ Cross-site scripting: Este problema es cada vez más frecuente, y consiste en hacer creer a una persona que está accediendo a un sitio web cuando en realidad lo está haciendo al otro, con el fin de conseguir información como el login del usuario, o los datos de su tarjeta de crédito.
- ✔ Puertas traseras: Este tipo de ataque consiste en que a través de parámetros específicos a la hora de acceder a una aplicación, se puede llegar a una puerta trasera en el servidor, o alcanzar una función de depuración que visualiza información prohibida, lo cual permitiría a un cliente remoto entrar en el servidor.

Arquitecturas tipo

En este punto se describen las arquitecturas habituales para el despliegue de este tipo de soluciones. La elección de una solución u otra dependerá de las funcionalidades que ofrezca el producto escogido y de la configuración de la red del cliente.

En primer lugar y como ya se ha mencionado anteriormente, estas soluciones no sustituyen en ningún caso a los firewalls tradicionales, sino que suponen un complemento a la seguridad que estos ofrecen. Por lo tanto en todas las soluciones mostradas a continuación aparecerán tanto los firewalls corporativos, como los firewalls http.

Una de las soluciones habituales para el despliegue de este tipo de cortafuegos consiste en su instalación en modo bridge transparente situado en la DMZ, donde se ubican los servidores web, de forma que todo el tráfico pase por este equipo antes de llegar a los servidores finales.

De esta forma, el firewall http puede analizar el tráfico destinado a los servidores, aplicando la política establecida sin interferir ni en la configuración de los firewalls corporativos ni en la de los servidores web. El principal inconveniente de este tipo de implantaciones radica en que todo el tráfico destinado a los servidores web, ya sea http, ftp, smtp o cualquier otro tráfico permitido por la política de los firewalls corporativos, atravesará el firewall http aunque no tenga nada que hacer con dicho tráfico. Por el contrario la ventaja fundamental es la sencillez de instalación, puesto que no interfiere con la arquitectura actual y no se precisan cambios en la misma.

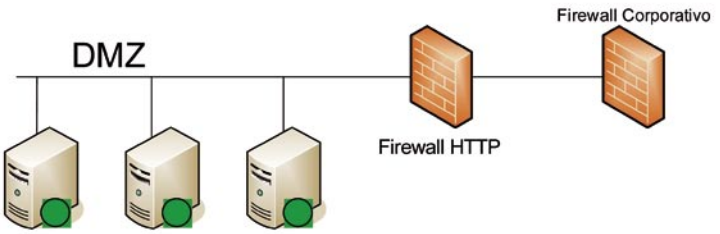

Ilustración 1: Configuración en modo bridge

Otra opción a la hora de implantar estas soluciones consiste en la definición del firewall http como un servicio "Proxy inverso", que responde a las peticiones que llegan desde Internet como si se tratase de los propios servidores web y luego encamina esas peticiones a los servidores destino, filtrando todo aquel contenido que pudiera vulnerar la política establecida en el firewall o suponer un peligro para los servidores web. ❑

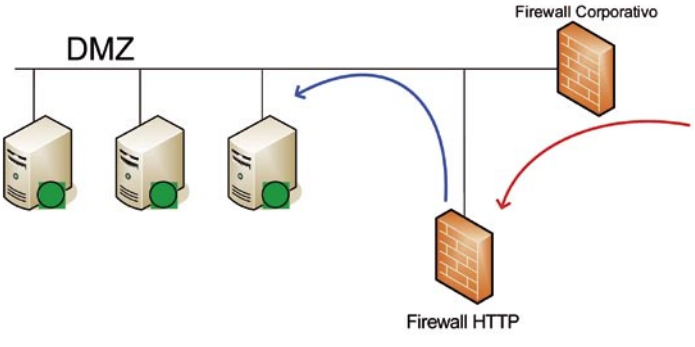

Ilustración 2: Configuración en modo proxy inverso.