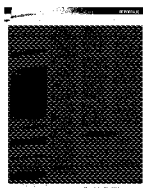




Aplicaciones web seguras

**FIREWALL PARA APLICACIONES WEB. UN MERCADO EN RAPIDO
CRECIMIENTO QUE EN BREVE TENDRA TAMBIÉN A LA PYME COMO OBJETIVO**





Los firewalls para aplicaciones web están erigiéndose como elementos básicos de las políticas de seguridad corporativas. Y es que, las empresas comienzan a sensibilizarse ante la idea de que este tipo de aplicaciones representan una interesante solución a desafíos expansivos, caracterizados por operaciones con un creciente número de usuarios distribuidos, ya sean colaboradores externos, empleados, partners, clientes, etc. Además, la explosión de servicios de comunicación gratuitos, como Skype o MSN Messenger, y sitios web donde descargar todo tipo de archivos sin coste y en tiempo real han traído consigo la necesidad de optimizar la seguridad en el mundo de los aplicativos web. En este sentido, y en un contexto en el que el mercado demanda soluciones que garanticen un uso eficiente de estas herramientas, los cortafuegos de aplicaciones web empiezan a incluirse cada vez más en casi todas las propuestas de seguridad lógica de los principales fabricantes de software. No hay duda de que el control de puertos y protocolos es preciso en todo el entorno empresarial, pero aún más cuando se trata de combatir posibles ataques contra la banda ancha y la integridad corporativa.

Las compañías encuestadas para la elaboración de este artículo coinciden en apuntar que si bien las pymes no han llegado aún al nivel de implantación de firewalls de aplicaciones de las grandes cuentas, se trata sólo de una cuestión de tiempo, puesto que el problema existe en ambos casos.

Con todo, y parafraseando a Emilio Román, director general de Fortinet, "hoy en día, las aplicaciones web son

el punto más vulnerable de la infraestructura de una empresa. Este mercado se encuentra en una situación de rápido crecimiento, pero muy pocos son los fabricantes que pueden ofrecer un rendimiento tal a nivel de aplicación como para no introducir retardo en las redes".

Donde otros no llegan

Tal y como hemos expuesto, los cortafuegos para aplicaciones web funcionan allí donde otros tipos de protección convencional no consiguen llegar. Los sistemas habituales de seguridad no logran prevenir ataques relacionados con los códigos de las aplicaciones, servidores web, o herramientas de negocio como ERPs, CRMs..., o aquellas dirigidas al usuario final –banca on-line o comercio electrónico–. Por tanto, para proteger este tipo de servicios es necesario contar con un eficiente firewall, puesto que es capaz de tener en cuenta el código, la lógica de utilidad, y las herramientas corporativas... Además, este tipo de productos no sólo responden al peligro que esconde una seguridad inadecuada en las aplica-

ciones, sino que también tienen que ver con los requisitos complementarios referidos a la disponibilidad y optimización de las mismas.

Menores costes

Tal y como apuntan algunos de los actores del mercado, los cortafuegos para aplicaciones web suponen, para los responsables de los departamentos de RRHH de las empresas, la posibilidad de contar con herramientas esenciales en la protección de tales aplicativos, ya que inciden en un uso más responsable de Internet en el entorno laboral, y, en consecuencia, en un aumento de la productividad. Para los responsables de sistemas, estas soluciones ayudan a controlar el uso y los costes de la banda ancha, y garantizan un bloqueo de los agujeros de seguridad, que son el blanco perfecto para quienes quieren introducirse en la red corporativa y robar –o perjudicar– información privilegiada.

Por otro lado, y según Ana Puente, responsable de ventas de Allnet, "los cortafuegos de aplicaciones web garantizan la calidad del servicio, y permiten reducir los costes de gestión de las infraestructuras, ya que protegen

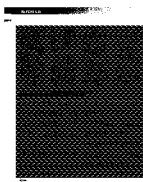
MÁS DE UN 50%

■ En el periodo comprendido entre el primer trimestre de 2004 y el primer trimestre de 2005, el número de vulnerabilidades identificadas que afectaron específicamente a las aplicaciones creció un 20% (Fuente: SANS Institute).

■ Más del 50% de las nuevas vulnerabilidades detectadas tienen que ver con las aplica-

ciones web (SANS @RISK, "The Consensus Security Vulnerability Alert").

■ Según distintas fuentes, más del 80% de todo el malware aparecido durante el pasado año ha tenido como objetivo aprovecharse de las vulnerabilidades de las aplicaciones.



➤ al sistema de cualquier amenaza, sobre todo desde que los niveles de intrusismo han crecido de manera importante, y los ataques ya logran sobrepasar las soluciones tradicionales de seguridad”.

En opinión de **Natalia Gómez del Pozuelo, directora de marketing y distribución de Optenet**, “los firewall de aplicaciones web intentan luchar contra las problemáticas registradas en los distintos segmentos de usuarios. Así, por ejemplo, en el escenario residencial se habla de piratería, de adicción a Internet, o de formas de contactar con desconocidos, con el peligro que eso entraña. En el ámbito educativo se menciona la necesidad de un uso

didáctico de los PCs y de Internet. Y, finalmente, en el segmento corporativo y de las Administraciones Públicas se habla de agujeros de seguridad, de protección de información confidencial, de falta de productividad, y de saturación de la banda ancha”.

Soluciones parciales

Entre las razones que los fabricantes han apuntado como responsables de la creciente necesidad de contar con firewalls de aplicaciones web en las empresas, destaca el hecho de haber respondido masivamente al cada vez mayor número de amenazas desarrollando soluciones parciales, que se han ocupado

básicamente de ataques centrados en la conexión, tales como cortafuegos, VPN e IDSs. “Estos sistemas trabajan generalmente examinando las cabeceras de los paquetes –esto es, direcciones y protocolos–, pero no analizan el contenido de los mismos. Aunque son efectivos proporcionando protección a nivel de red, lo cierto es que firewalls, VPNs e IDSs no cubren las necesidades de protección actuales en los ámbitos telemáticos. Y es que, se fijan solamente en las cabeceras del paquete, no en su interior. Por eso, no pueden comprobar el contenido de éste en tiempo real, ni procesarlo después para

identificar virus, gusanos u otras amenazas. Consecuentemente, virus, gusanos y troyanos transmitidos mediante correo electrónico y tráfico http se cuelan fácilmente a través de cortafuegos y VPNs, pasando a menudo desapercibidos por los sistemas de detección de intrusiones. La defensa contra ataques combinados va más allá de la capacidad de las soluciones convencionales de seguridad de red. Además, estos productos no pueden ayudar contra el uso indebido de los recursos de la red, negando los paquetes que contienen material inapropiado, como pornografía o sitios web inadecuados”, apostilla Román. ●

EN BOCA DE TODOS

“En un futuro inmediato, las prestaciones de cortafuegos se van a mover dentro de la infraestructura de los ISPs (Proveedores de Servicios de Internet), justamente para evitar problemas de compatibilidad y de instalación. De esta forma, pymes y grandes empresas podrán darse de alta a través de su ISP de forma sencilla y segura. Los servicios de firewall en red tienen un nivel de eficacia igual o mejor que las versiones de servidor o PC, por lo que los ISPs podrían llegar a convertirse en grandes distribuidores. Otra opción es que los mismos fabricantes provean servicios de firewall en red a partir de sus propios servidores. De hecho, Optenet ya lo hace con sus servicios web filter y antispam”

Natalia Gómez del Pozuelo, directora de marketing y distribución de Optenet

“En 2006, como continuación a la tendencia ya claramente marcada en 2005, cada vez serán más las organizaciones que opten por una cobertura completa y no sólo a nivel de conexión de la seguridad de sus redes”

Emilio Román, director general de Fortinet

“Los fabricantes del sector deben apostar por soluciones que no sólo permitan garantizar la seguridad de las redes, sino que también ayuden a acelerar las aplicaciones web. En el futuro,

estas soluciones serán productos multifuncionales, como por ejemplo un firewall con gateway de correo y servidor VPN integrado. Es decir, soluciones que permitan proteger la red eficazmente contra cualquier ataque externo (detección de intrusos, inspección de contenidos, protección contra amenazas), que incluyan un sistema antivirus y antispam actualizable a través de la Red, y que, además, permitan filtrar los contenidos y virus del e-mail antes de enviarlo (gateway)”

Ana Puente, responsable de ventas de Allnet

“Las principales tendencias tecnológicas tienen que ver con productos cada vez más integrados que estén basados en políticas estándar para permitir una mayor integración de soluciones y programas. La tendencia en la empresa es la de convertirse en una organización extendida y abierta que intercambie información en muchos frentes: clientes, proveedores, partners... Esta apertura corporativa también se manifiesta en la existencia de cada vez más trabajadores móviles que tienen que acceder a la información de la compañía. Se crea así una situación para las redes empresariales donde se mezcla apertura y movilidad, a la que deben enfrentarse las compañías de seguridad”

Diego Arrabal, director general de F5 en España