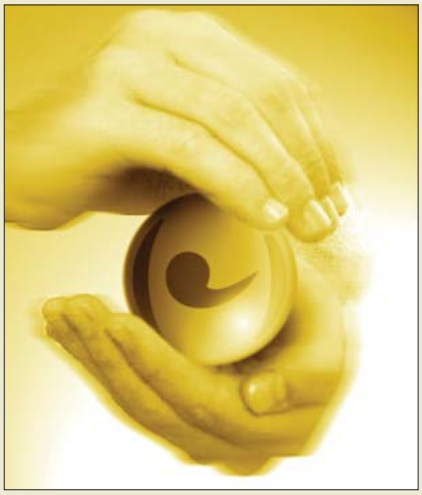
Comenzamos con este artículo una serie de textos orientados a introducir en el mundo de la seguridad informática, habitualmente denominada Seguridad Lógica, a los no iniciados. No pretenden ser un análisis de alto nivel técnico, sino que su objetivo consiste en plasmar de forma clara y sencilla los conceptos y términos básicos, que habitualmente se manejan en este área de conocimiento.

Sistemas Cortafuegos (Firewalls)

Por Pedro Domingo Pérez

Jefe de Proyecto de la División de Seguridad de Germinus Solutions

Quizás una de las primeras cosas de las que uno oye hablar, junto con los sistemas de antivirus, cuando se acerca al mundo de la seguridad lógica sea del término Firewall o Cortafuegos. Podríamos definir un cortafuegos como aquel sistema de red expresamente encargado de separar redes de comunicación de datos, efectuando un control del tráfico existente entre ellas. Este control consiste, en última instancia, en permitir o denegar el paso de la comunicación de una red a otra.



El concepto que subyace detrás de un sistema cortafuegos es el de Seguridad Perimetral Centralizada, es decir, la creación de perímetros de separación implantados mediante puntos donde se centraliza el control de las comunicaciones. El caso más básico involucra a dos redes, una red a proteger (normalmente una red corporativa) y una red externa (normalmente Internet).

Otras configuraciones habituales cuentan con la división de la red corporativa en distintas subredes con el fin de aplicarles distintas reglas de control y lograr un control más detallado, un control de grano fino. Para la distinción de las distintas redes que separa el cortafuegos se utilizan denominaciones particulares e incluso código de colores. Así dentro de las redes intermedias entre la interna y la externa nos podemos encontrar con la o las redes de servicio, también conocidas como desmilitarizadas o DMZ (DeMilitarized Zone), en la que se suelen ubicar los sistemas que ofrecen servicios públicos (como el servidor web de la compañía) y que habitualmente se caracteriza con el color naranja.

También nos podemos encontrar con una red de autorización, en donde se suelen ubicar perfiles de permisos de acceso de usuarios particulares (logrando autorizaciones mucho más detalladas, por identidad del usuario y no por la red en la que se encuentre), y que habitualmente se

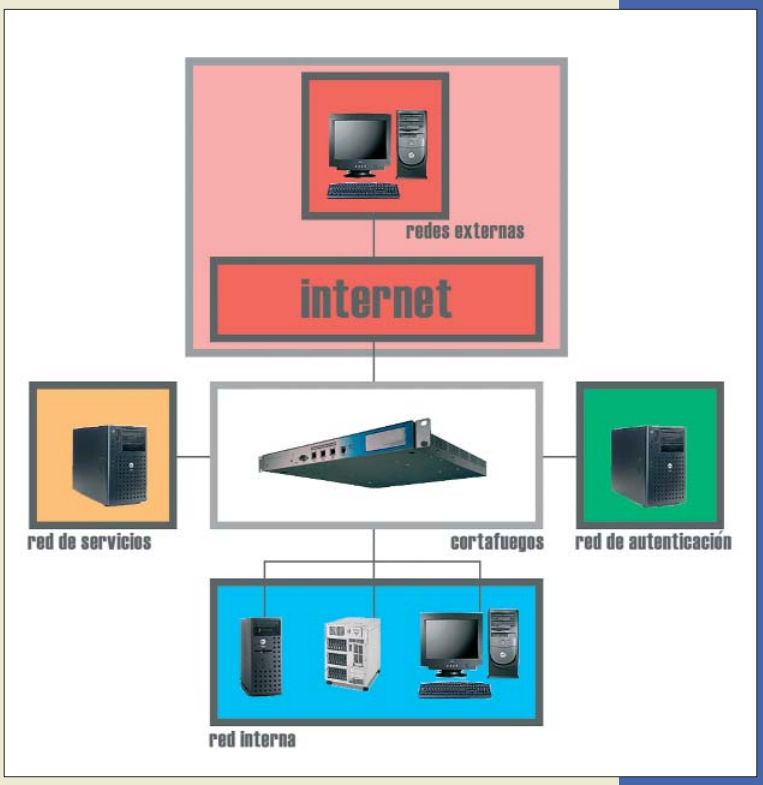
caracteriza con el color verde, o la red interna, la red corporativa de trabajo de la organización, caracterizada por el color azul.

En cuanto a las redes no pertenecientes a la corporación, suelen considerarse como una única red externa denominada red roja, que evidentemente se caracteriza con ese mismo color.

El control del tráfico se realiza autorizando o denegando las comunicaciones mediante el cumplimiento de una serie de reglas. Los parámetros de definición de estas reglas varían en contenido y complejidad según el sistema utilizado pero, básicamente, se podría decir que las reglas deberían de poder definirse en función de al menos tres parámetros: origen de la comunicación, destino y tipo de servicio a utilizar. Los cortafuegos permiten normalmente la definición de reglas más complejas basadas en los protocolos que rigen las comunicaciones entre los equipos, las horas del día, los usuarios o incluso el tamaño de la comunicación o su contenido.

Al hacer coincidir los puntos de salida y entrada del tráfico de datos de una corporación con sistemas cortafuegos, normalmente estos sistemas ofrecen otro tipo de servicios adicionales a la autorización de las comunicaciones, como pueden ser el análisis del tráfico conforme a la aplicación que lo genera (por ejemplo inspección del tráfico web), o la traducción de direcciones de red, con el fin de permitir la utilización de direccionamiento privado en las redes internas. Otros ejemplos son el establecimiento de canales cifrados con equipos externos y la integración con otros sistemas, con el fin de realizar tareas tales como análisis antivirus o control de contenidos.

En la práctica, los sistemas cortafuegos se pueden implementar mediante plataformas multipropósito, en donde se instala un software específico que realiza las funciones de cortafuegos aunque, últimamente, es cada vez más habitual encontrarnos con plataformas dedicadas denominadas appliances, optimizadas para obtener el máximo rendimiento de las funciones descritas con mínimas necesidades de administración. Estas plataformas no deben verse con la visión máquina + sistema operativo + software de cortafuegos, sino como una caja cerrada y autónoma. La administración de estos sistemas es más sencilla, tanto de forma individual como en configuraciones en grupo, con el fin de obtener alta disponibilidad del servicio y reparto del tráfico en varios sistemas de control. ❑



Más información:

http://www.checkpoint.com	Fabricante de software de cortafuegos
http://www.stonesoft.com	Fabricante de software de cortafuegos
http://www.securecomputing.com	Fabricante de software de cortafuegos
http://www.netfilter.org/ipchains/	IP chains, software de cortafuegos para Linux
http://www.watchguard.com	Fabricante de appliances cortafuegos
http://www.netscreen.com	Fabricante de appliances cortafuego
http://www.sonicwall.com/	Fabricante de appliances cortafuegos
http://www.nokia.com/	Fabricante de plataformas hardware de seguridad