INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES &SEGURIDAD

9

SEGURIDAD EN REDES CABLEADAS E INALÁMBRICAS

En este fascículo veremos aspectos de seguridad en la implementación de redes, revisaremos el funcionamiento del firewall y entregaremos consejos útiles.

- FIREWALL POR HARDWARE
- FIREWALL POR SOFTWARE
- INSTALACIÓN DE UN FIREWALL
- DETECCIÓN DE INTRUSOS
- HONEYPOTS Y HONEYNETS
- DNS Y SEGURIDAD

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez

Curso visual y práctico **Técnico en redes y seguridad** es una publicación de Fox Andina en coedición con Dálaga S.A. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Distribuidores en Argentina: Capital: Vaccaro Sánchez y Cía. S.C., Moreno 794 piso 9 (1091), Ciudad de Buenos Aires, Tel. 5411-4342-4031/4032; Interior: Distribuidora Interplazas S.A. (DISA) Pte. Luis Sáenz Peña 1832 (C1135ABN), Buenos Aires, Tel. 5411-4305-0114. Bolivia: Agencia Moderna, General Acha E-0132, Casilla de correo 462, Cochabamba, Tel. 5914-422-1414. Chile: META S.A., Williams Rebolledo 1717 - Ñuñoa - Santiago, Tel. 562-620-1700. Colombia: Distribuidoras Unidas S.A., Carrera 71 Nro. 21 - 73, Bogotá D.C., Tel. 571-486-8000. Ecuador: Disandes (Distribuidora de los Andes) Calle 7° y Av. Agustín Freire, Guayaquil, Tel. 59342-271651. México: Distribuidora Intermex, S.A. de C.V., Lucio Blanco #435, Col. San Juan Tlihuaca, México D.F. (02400), Tel. 5255 52 30 95 43. Perú: Distribuidora Bolivariana S.A., Av. República de Panamá 3635 piso 2 San Isidro, Lima, Tel. 511 4412948 anexo 21. Uruguay: Espert S.R.L., Paraguay 1924, Montevideo, Tel. 5982-924-0766. Venezuela: Distribuidora Continental Bloque de Armas, Edificio Bloque de Armas Piso 9no., Av. San Martín, cruce con final Av. La Paz, Caracas, Tel. 58212-406-4250.

Impreso en Sevagraf S.A. Impreso en Argentina.

Copyright © Fox Andina S.A. I, MMXIII.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Características y opciones de seguridad en redes cableadas e inalámbricas así como también las opciones de un firewall por software y por hardware.

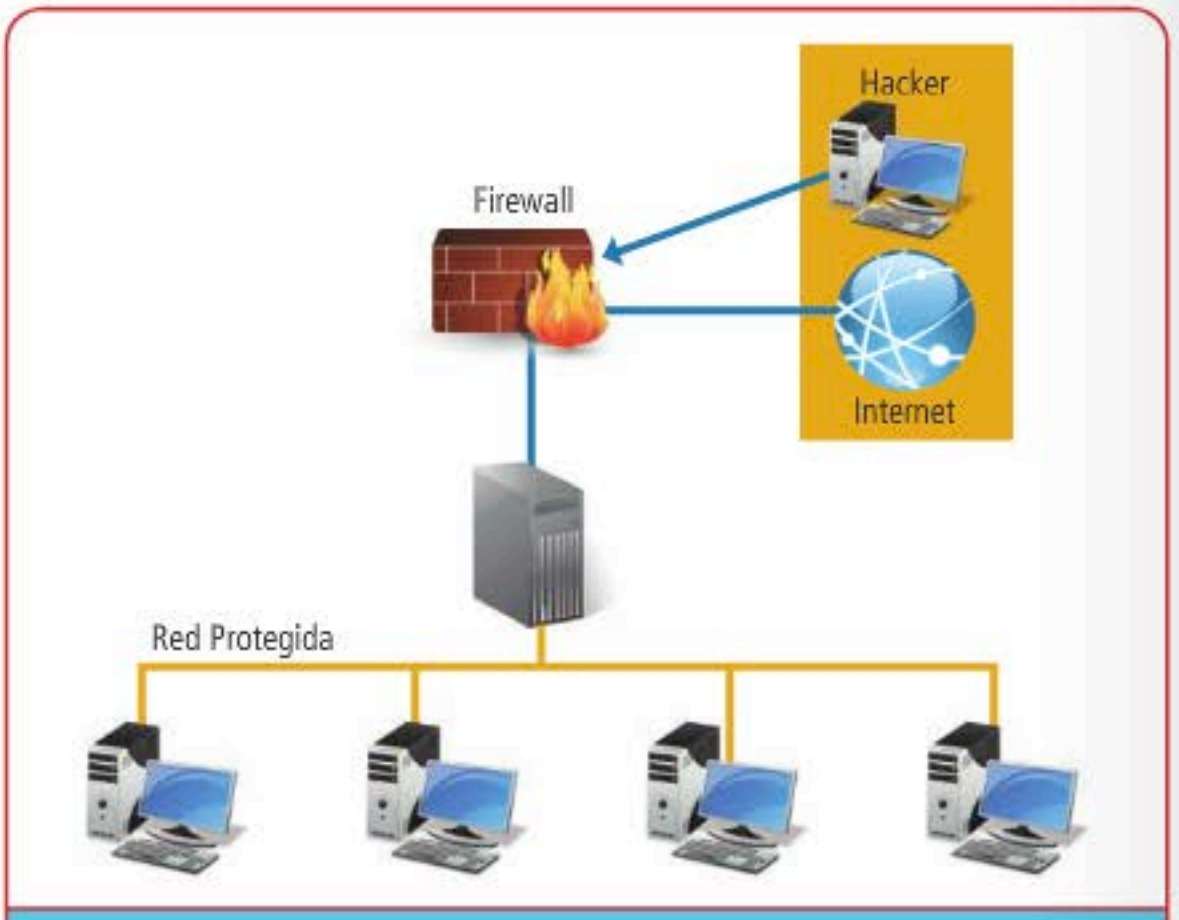
En la clase anterior, vimos en profundidad las tareas de configuración de una red inalámbrica. Analizamos las topologías Wi-Fi y configuramos un access point en forma avanzada. Conocimos los alcances del wardriving y los tipos de antenas y repetidores existentes. Por otra parte, también revisamos algunos conceptos sobre autenticación con servidores AAA, TKIP y MIC. Finalmente, aprendimos a ocultar el SSID para aumentar el nivel de seguridad de una red.

En esta clase, revisaremos en detalle la seguridad en redes cableadas e inalámbricas. Conoceremos qué es un firewall y cuáles son sus características y funciones. Revisaremos los alcances del firewall que acompaña a los sistemas operativos Windows y caracterizaremos a los firewalls por software y hardware. Detallaremos los pasos que debemos efectuar para instalar una aplicación de firewall y conoceremos los sistemas de detección de instrusos. Para terminar, conoceremos los honeypots, los honeynets y veremos la seguridad relacionada con los DNS.

Qué es un firewall

Un firewall nos ayuda a proteger nuestra red informática de potenciales amenazas. En estas páginas podremos conocer sus características, así como también todas sus ventajas.

El **firewall**, conocido como **cortafuegos**, tiene su origen en la seguridad industrial, donde se utilizaban gruesas paredes con cámara de aire en los lugares con peligro de incendio; así, se los podía aislar rápidamente, y su potencial daño sería mucho menor. Estas paredes de seguridad pueden ser con fines internos o externos. Por ejemplo, en ambos casos, si queremos aislar un determinado sector, porque por la actividad que se realiza en él existe un factor de riesgo alto de incendio, lo que trataremos de hacer es que ese fuego no se propague al resto del lugar, con lo cual los muros de firewall servirían de contención. También puede ocurrir que, por razones de seguridad, aunque el riesgo de incendio no sea alto, se decida utilizar paredes firewalls en un determinado sector por la información crítica que contiene; pueden ser desde servidores hasta un conjunto de archivos,donde hay circulación de personas constantemente; en este caso, los muros de protección funcionarían como aislante ya que, si se produjera un incendio general, se protegería este sector.
Un ejemplo sería la caja negra de los aviones: está construida de forma que, aunque el avión sufra daños totales, la caja pueda estar segura, de esta manera, posteriormente se podrá realizar el análisis del problema que sufrió el avión, para determinar sus causas.



La función principal del firewall es proteger y defender la red local de posibles ataques provenientes de la red externa.

Firewall informático

Aplicado a la informática, el término **firewall** hace referencia a un nivel de seguridad, usado para limitar el acceso interno o externo de contenidos en la

Actualizaciones periódicas

Debemos aplicar las actualizaciones lo más rápido posible, en especial en aquellos equipos cuya confidencialidad queremos proteger. Si contamos con un firewall por hardware, las actualizaciones no son tan regulares como las que pueden salir para nuestro sistema operativo. Mantener actualizado el software de seguridad, y un mantenimiento al hardware aumentan el nivel de seguridad ante la aparición de alguna nueva modalidad de intrusión. Si algo logra esquivar al firewall, puede ser detenido o anulado desde el mismo equipo.

Los firewalls por hardware tienen costos muy elevados, además, su configuración debe estar a cargo de personal capacitado.

red, por personal no autorizado, o evitar que este pueda descargar algún software dañino para el equipo o la red.
El firewall es una herramienta para proteger nuestro equipo de potenciales daños desde la red, como el producido por la infección de un virus, o que algún atacante intente acceder a nuestra red. Se puede implementar por hardware o por software; además, existe hardware especial, como los IDS e IPS, que complementan la función del firewall para evitar ingresos no autorizados a nuestra red. La función principal que persigue la implementación de un firewall es proteger a los equipos y sus datos de accesos no autorizados externos a la red.

ES POSIBLE UTILIZAR EL PUERTO DMZ (DE ZONA DESMILITARIZADA) PARA SEPARAR LAS REDES.

Hardware y software

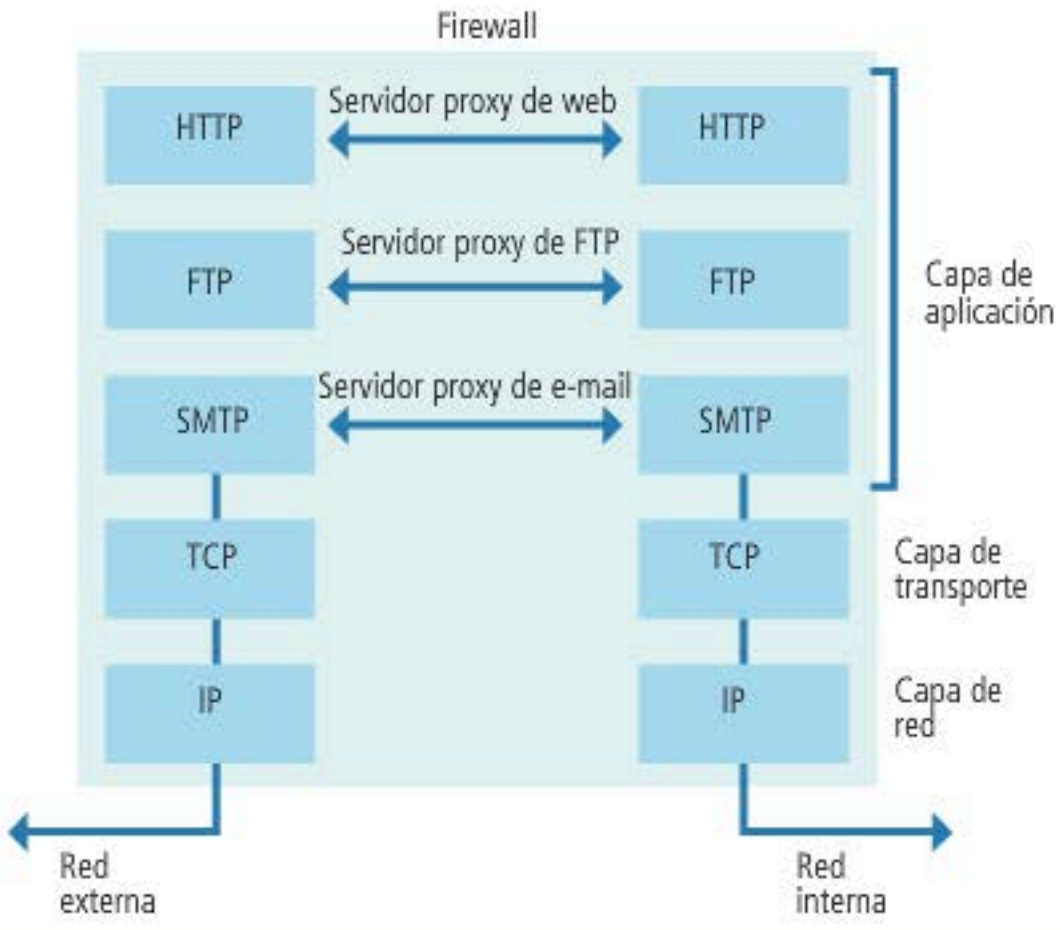
Se puede utilizar firewall por hardware o por software, dependiendo de la necesidad que tengamos. El costo de hardware diseñado para firewall, además de ser más elevado que el costo de un firewall por software, puede ofrecer varias herramientas. Si nuestra red cuenta con muy pocos equipos activos constantemente en Internet, adquirir un firewall por software es la mejor opción, ya que no se justificaría instalar un firewall por hardware. En cambio, cuando el volumen de la red y de los equipos activos es mayor, y también lo es su actividad, podemos encontrarnos con tres equipos que realizan varias operaciones de transferencia monetaria por día, y por lo tanto, su seguridad es muy importante. En casos como este, se justifica por completo realizar la adquisición de un firewall por hardware.

Funcionamiento

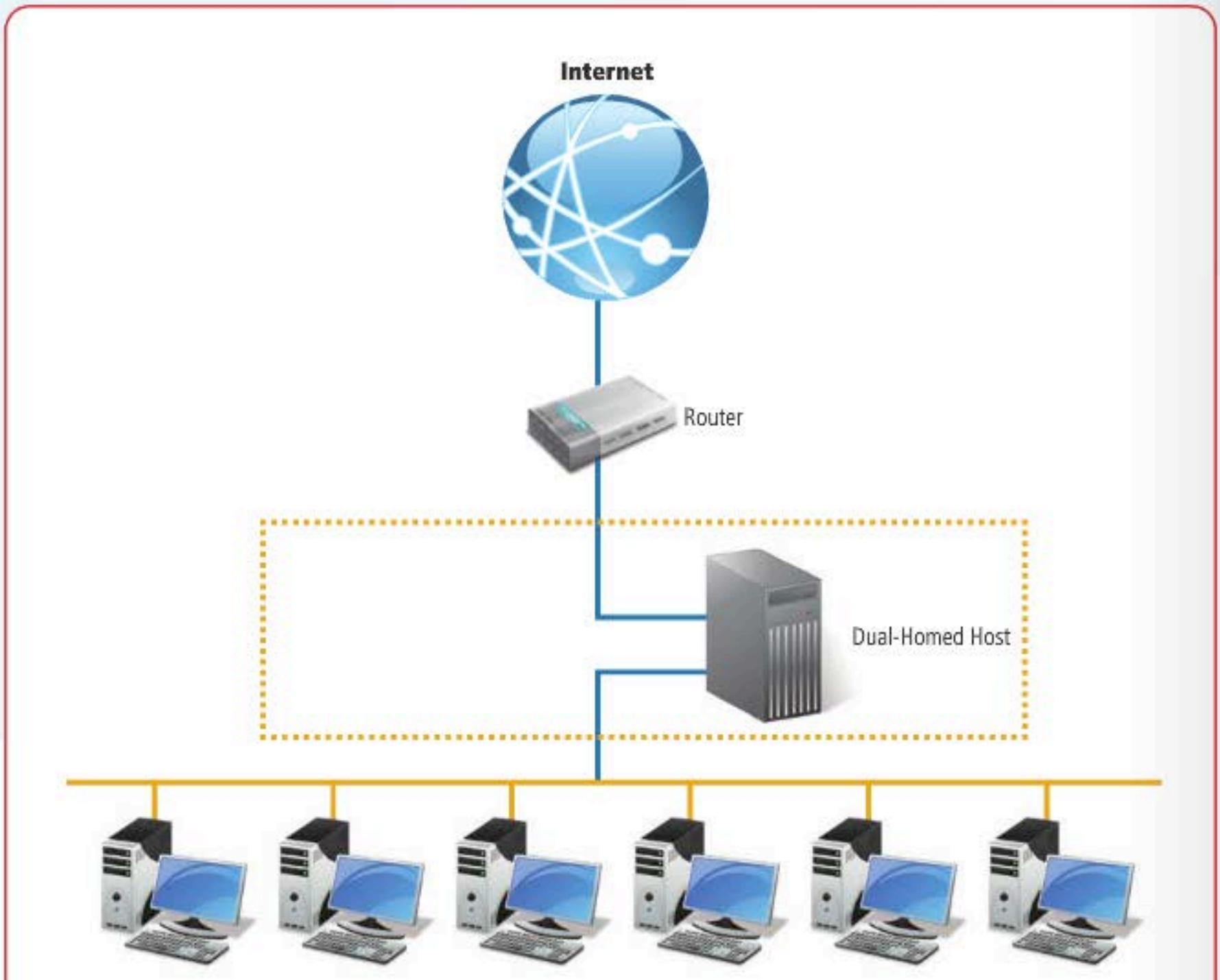
El fin de un firewall es evitar que paquetes IP no deseados lleguen a nuestra red; actúan como las zanjas profundas que rodeaban a los castillos de la Edad Media, y todo lo que ingresaba (o salía) de ellos podía ser inspeccionado por los guardias. Según su modo de actuar, el firewall puede configurarse como:

- Filtrado de paquetes.
- Inspección de paquetes de estado.
- Firewall del proxy.

Para el filtrado de paquetes, debemos configurar determinadas reglas, con las cuales el firewall permitirá o denegará el ingreso del paquete inspeccionado.
La primera generación de firewalls, filtraba los paquetes leyendo sus encabezados, donde se almacenan las direcciones IP de origen y destino (capa 3 del modelo OSI). Luego, los filtros se aplicaron al encabezado de los paquetes TCP o UDP (capa 4). En esta capa, los paquetes utilizan números de puertos para direccionar los paquetes de datos, configurando las listas de acceso en



Para cada servicio que deseemos utilizar, será necesario que realicemos la configuración de su respectivo proxy.



Dual-Homed Host. El router no forma parte de la seguridad, ya que toda ella recae en el host bastión.

el firewall (Acces List, o **ACL**), utilizando los puertos de origen y destino para permitir o denegar el paquete, o se puede establecer que todo el tráfico destinado a un puerto específico sea direccionado a una IP específica.

Configuración

Algunos firewalls pueden configurarse para examinar los bits de código que forman parte del encabezado TCP. Estos bits de control son para sincronizar los paquetes TCP entre los equipos que mantienen una conexión; al ser analizados por el firewall, este puede saber si se tratan de paquetes esperados o no.

Como UDP junto con IP son protocolos no orientados a conexión, el firewall debe tomar decisiones para dejar pasar el tráfico sin conexión esperado, y denegar el resto. Para hacer eso, el firewall monitorea qué tipo de tráfico sin conexión se origina en la red LAN, sobre esa base crea una tabla que almacena los puertos UDP de origen y destino. En otra tabla, también se almacenan las direcciones IP de origen y destino. Este tipo de filtrado se llama inspección de paquetes por estado, ya que analiza el tráfico, las conversaciones entre los equipos para determinar qué paquetes UDP dejar pasar, analizándolo y comparándolo con las tablas internas que se generaron al revisar la red interna.

Por lo general, la ubicación del firewall por hardware se encuentra al inicio de la red interna.

Firewall por hardware y por software

	Firewall por hardware	Firewall por software
Costo	Costo elevado	Diversos costos: depende de las funciones prestadas.
Alcance	Protege toda la red	Software individual, aunque pueden adquirirse versiones para servidores.
Mantenimiento	Personal capacitado	Personal capacitado. Según la licencia, soporte directo por la empresa desarrolladora.
Actualización	Costo elevado, ya que puede requerir el reemplazo del equipo	Costos leves. Puede requerir actualización de hardware del equipo (ampliación de memoria RAM).
Rendimiento de los equipos	Pequeño o nulo efecto sobre el rendimiento general de los equipos	Mayor impacto en el rendimiento del equipo, ya que utiliza sus mismos recursos (hardware y SO) para funcionar.

Arquitecturas del firewall

Se pueden diferenciar varios modos de trabajo del firewall:

▶ **Dual-Homed Host**: en este modo, se utiliza un equipo con dos placas de red (o una placa con dos interfaces). Una conexión se deja para la red interna, y la otra, para la red externa.

▶ **Screened Host**: en esta configuración, se utiliza un router para el filtrado de paquetes, que recibe el nombre de **screening router**, y un equipo denominado **host bastión**, que recibe ese nombre por tener instalada una aplicación, para ofrecer seguridad a la red interna, de manera que sea el mismo quien reciba los ataques desde fuera de la red.

▶ **ScreenedSubnet**: también conocida como red perimétrica. Esta configuración es la más compleja, ya que se emplean dos routers y el host bastión. El host bastión quedará limitado por los routers, mientras que los routers cumplirán la función de router exterior, conecta al host bastión con la red, y de router interior, que conecta al host bastión con la red interna.

Elección y ubicación del firewall

La ubicación del firewall estará determinada luego de que hayamos decidido qué equipos queremos proteger, y las prestaciones del firewall en sí. Si utilizaremos Firewall por software en todos los equipos, entonces debemos definir una política de seguridad y mantenimiento para aplicar sus actualizaciones. Podemos optar por instalar un firewall por hardware, o tener ambos, un firewall por hardware para un sector específico, como finanzas por ejemplo, y para el resto de la red, firewall por software.

Por ubicación del firewall, nos referimos a su ubicación lógica, ya que es muy probable que todos los equipos de redes (routers, switches, patcheras) se encuentren centralizados en un lugar físico especialmente adecuado para estos equipos.

En el caso del firewall por hardware, debemos prestar mucha atención a sus características, que son la cantidad de conexiones activas que puede permitir, y la carga de tráfico (*throughput*).

LA FUNCIÓN PRINCIPAL DEL FIREWALL ES PROTEGER LOS EQUIPOS, DE ACCESOS NO AUTORIZADOS DESDE LA RED.

Esto es importante ya que utilizar un firewall con características básicas no es conveniente para proteger la red completa.

También es posible utilizar el puerto **DMZ** para separar las redes. Supongamos un router con tres conexiones, un puerto WAN, un puerto LAN y un puerto DMZ. El puerto WAN es para la conexión con nuestro prestador del servicio de Internet (ISP). El puerto DMZ lo utilizaremos para la red pública interna, es decir, podemos conectar un access point al DMZ, para ofrecer Internet libre a nuestros clientes que están esperando ser atendidos, mientras que en el puerto LAN conectaremos mediante un switch los equipos de nuestra red de datos. ■

El Firewall de Windows

En estas páginas, conoceremos las características y la funcionalidad del firewall de software incorporado en los sistemas Windows.

Cuando Windows XP fue lanzado originalmente en octubre de 2001, incluyó un firewall limitado llamado **Firewall de conexión a Internet**; este venía deshabilitado por defecto debido a preocupaciones por compatibilidad, y las pantallas de configuración fueron ubicadas en las pantallas de configuración de red que muchos usuarios nunca vieron. Como resultado de ello, se lo utilizaba raramente.
A mediados de 2003, debido al ataque de diferentes malware que afectaron a un gran número de máquinas Windows, Microsoft decidió mejorar significativamente la funcionalidad y la interfaz de Firewall Integrado de Windows XP y es activado por defecto con el Service Pack 2.
A partir del SP2 en Windows XP, y SP1 en Windows Server 2003, comenzamos a disponer de una protección de firewall nativa en los productos Microsoft.

En esta imagen podemos ver el panel de administración del Firewall de Windows 7; en él se indica el perfil activo.

Recomendación de seguridad

Es recomendable tener el firewall con las opciones bloqueadas para todas las conexiones entrantes, es decir, que no haya excepciones; de esta manera, abriremos y habilitaremos el acceso a nuestro equipo a aquellas conexiones que consideremos seguras, y evitaremos que software malintencionado pueda ingresar al sistema. Lo mismo debemos realizar para la salida, aunque es una tarea más engorrosa, ya que cada aplicación que abra un puerto de comunicación hacia un equipo externo no podrá funcionar a menos que lo habilitemos en forma específica.

Perfiles

El Firewall de Windows dispone de tres perfiles que se activan automáticamente:

- **Público**: supone que la red se comparte con el mundo y es el perfil más restrictivo.
- **Privado**: asume que la red está aislada de Internet y permite conexiones entrantes. Una red no se supone que es privada a menos que sea designada como tal por el administrador local.
- **Perfil de dominio**: es el menos restrictivo. Admite más conexiones

entrantes para permitir el uso compartido de archivos, etc.; se selecciona automáticamente cuando se conecta a una red con un dominio de confianza para el equipo local.

Características

Una de las funcionalidades del Firewall de Windows es el **Registro de seguridad**, permite registrar las direcciones IP y otros datos relativos a las conexiones procedentes de la red. Es posible grabar tanto los paquetes perdidos como las conexiones correctas; esto se puede utilizar, por ejemplo, para seguir cada vez que un equipo de la red se conecta a un determinado equipo. Este registro de seguridad no está habilitado de forma predeterminada, el administrador debe habilitarlo a demanda.

EL FIREWALL DE WINDOWS ES UNA MEDIDA DE PROTECCIÓN QUE NO DEBEMOS OBVIAR EN NUESTRO EQUIPO.

¿Cómo funciona?

Cuando alguien en Internet o en una red intenta conectarse a un equipo, ese intento se conoce como **solicitud no autorizada**. Cuando el equipo recibe una solicitud no autorizada, el Firewall de Windows bloquea la conexión.
Si utiliza un programa, por ejemplo, de mensajería instantánea o un juego de red con varios participantes, que tiene que recibir información desde Internet o de una red, el servidor de seguridad le pregunta si desea bloquear o desbloquear (permitir) la conexión.
Con la llegada de Windows Vista y Windows Server 2008 (y sus versiones posteriores), viene de forma nativa el Firewall de Windows con Seguridad Avanzada, que dispone de muchas funcionalidades básicas de las que carecía su predecesor, como por ejemplo el bloqueo a las conexiones salientes, permitiendo de esta manera tener un mayor control de las conexiones de red del equipo. En Windows Vista y Windows Server 2008, solo un perfil de firewall puede estar activo a la vez. Si el equipo está conectado a más de una red, el perfil que tiene las normas más restrictivas se aplica a todas las conexiones en el equipo. El perfil público es el más restrictivo, seguido por el perfil privado y, luego, por el perfil de dominio.

Windows 7

En Windows 7 y Windows Server 2008 R2, a cada adaptador de red se le asigna el perfil adecuado (dominio, privada o pública), independientemente de los otros adaptadores de red en el equipo. El tráfico de red *enviado a* o *procedente de* cada red es procesado por las reglas que son apropiadas para ese tipo de red.
La administración del firewall se puede realizar por medio de comandos a través del símbolo del sistema, ejecutando `netsh firewall` o por medio de la consola, yendo a `Inicio/Ejecutar/Firewall.cpl` o consola MMC a partir del **Firewall con Seguridad Avanzada**. Cuando comencemos a configurar el firewall, debemos tener la precaución de habilitar las notificaciones para cuando el Firewall de Windows bloquee un programa.

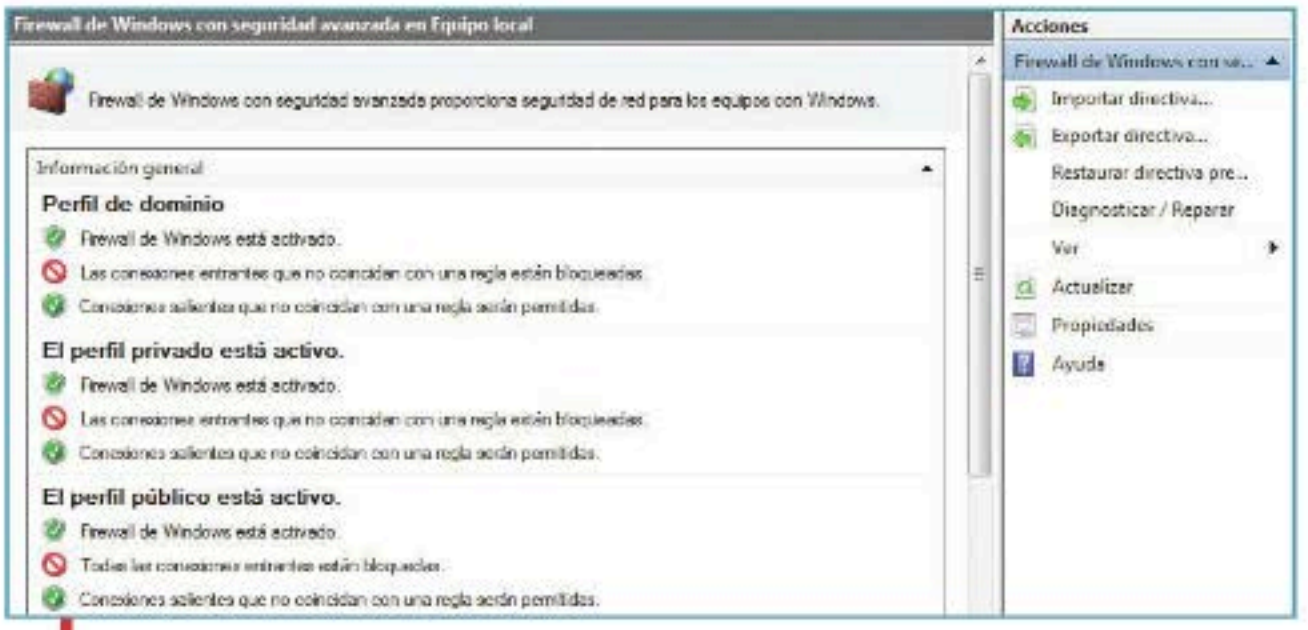
Reglas

El firewall ya dispone de reglas predeterminadas para habilitar, por ejemplo, la posibilidad de compartir

archivos e impresoras y el escritorio remoto, entre otras. En la creación de reglas de excepciones, debemos tener en cuenta qué tipo de protocolo usa –ICMP, TCP o UDP– y el puerto por utilizar; además, podemos especificar el ámbito de red: si es para toda la red, una subred o para determinadas direcciones IP.

Desventajas

Una desventaja que trae el Firewall de Windows es que no permite la selección de rangos de puertos; para esto, lo más conveniente es utilizar un script en `netsh` y abrir una determinada cantidad de puertos, para no hacerlo en forma manual.
Al momento de configurar el Firewall de Windows, debemos tener en cuenta y abrir solo los puertos que sean necesarios; no es una práctica conveniente deshabilitar el firewall porque una aplicación o un software no funciona; aunque parezca algo muy obvio, ya que podemos exponer la integridad del sistema operativo a cualquier posible atacante. ■



Así luce la interfaz de administración del firewall con seguridad avanzada.

Firewall por software

En estas páginas revisaremos las características principales para tener en cuenta al elegir el firewall que proteja nuestra red de datos.

Para proteger nuestros equipos, o si contamos con una pequeña red en una empresa, la mejor solución será implementar un firewall por software en cada uno de los equipos. También es posible adquirir un firewall por software para proteger toda la red. En ambos casos, el firewall se instala como una aplicación más; si nos encontramos en una red corporativa, se nos pedirá la contraseña de Administrador para su instalación y configuración.
Un firewall por software que se configura en un equipo con sistema Linux es **iptables**. Se trata de una potente herramienta, y su configuración se realiza por comandos desde la terminal, lo que implica que su configuración se limita a usuarios que estén sumamente familiarizados con el entorno Linux.

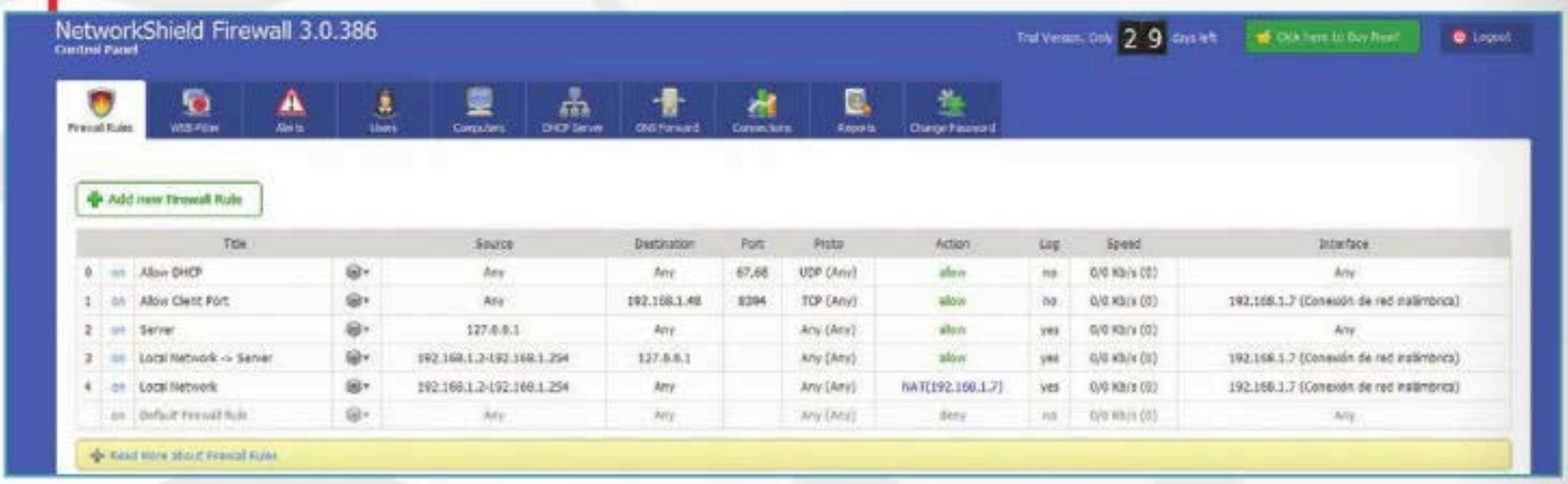
Pantalla principal de **BitDefender**. Desde el menú, podemos acceder a la configuración de cada módulo.

Alternativas disponibles

Para decidir qué firewall adquirir, debemos tener presente nuestras necesidades, ver qué tipo de firewall se ajusta a nuestros requerimientos, leer las descripciones ofrecidas por la empresa desarrolladora y, además, si es posible, leer los comentarios de otros usuarios que hayan utilizado o estén utilizando dicho software. También debemos tener presente el soporte ofrecido por la empresa desarrolladora del firewall: ¿ofrece soporte remoto?, ¿en qué idioma? Todas las dudas que nos surjan debemos dejarlas en claro antes de realizar una implementación que afectará a la seguridad de los equipos y de la red.

Además, al momento de elegir un software de firewall, en lo posible, debemos tratar de utilizar el mismo producto para el resto de los equipos, y no utilizar distintos software para cada uno, por una cuestión de precio o licencias. Si bien la función de todos los firewalls es la de defender el equipo, cada producto utiliza sus propias técnicas para llevar a cabo su fin. Todos los equipos y sus software pueden tener alguna vulnerabilidad y, por esa razón, las empresas desarrolladoras sacan actualizaciones para contrarrestar los potenciales riesgos. Utilizar distintos software de firewall para una misma red incrementa ese riesgo, ya que una vulnerabilidad puede estar contemplada en un firewall pero no en otro, y la seguridad de toda la red queda comprometida.

La configuración de NSF la realizamos desde el navegador. Su interfaz nos ayudará a realizar la configuración total.



En **WebRootSecureAnywhere**, podemos configurar qué advertencias queremos recibir cuando las aplicaciones intenten conectarse.

Para ayudarnos a elegir y comparar productos de firewall, analizaremos algunos de ellos, para luego evaluar cuál se ajusta a nuestras necesidades específicas.

NetworkShield Firewall

Es un potente firewall diseñado para ejecutarse en un equipo servidor. Una vez instalado, al abrir el programa, se nos abrirá nuestro navegador por defecto, y se nos pedirá que creemos un usuario. Como se trata de una versión para servidores, buscará las placas de red instaladas en nuestro equipo y nos preguntará cuál placa es para la conexión WAN y cuál, para la LAN.

Además de prestar funciones de firewall, también desde el mismo firewall podemos configurarlo como servidor DHCP y elegir el rango de direcciones IP; al configurarlo, podemos decidir si proteger toda la red o solo un sector de ella.

Una característica importante es que contiene un filtro de navegación que nos permite bloquear una gran cantidad de sitios de Internet seleccionando la temática de los sitios por bloquear (redes sociales, compra y venta, cultura y arte).

Este bloqueo puede ser para toda la red, o podemos definir una IP específica, a qué sitios no puede ingresar. Los registros tienen una interfaz muy simple que nos ayudará rápidamente a buscar algún dato en particular, ya que podemos filtrar para que solo nos muestre información sobre navegación, mensajería instantánea o los servidores de correo. Ofrecen soporte en inglés, también soporte remoto a través de TeamViewer, por teléfono o e-mail. Su sitio oficial es **www.networkshield.com**.

WinGate 7

WinGate es otro firewall que tiene funciones para servidor. Luego de instalarlo, tendremos que configurar las placas de red; podremos elegir si se trata de placas de red interna, externa, o DMZ. Luego de configurar las placas de red, podemos instalar los servicios para red, como DHCP, DNS. Varias de las opciones no estarán disponibles si utilizamos la licencia de prueba.

Podemos configurar los filtros a sitios por categoría o escribiendo el nombre del sitio web que deseamos bloquear. Además, es posible configurarlo para que esté bloqueado todo el tiempo, o elegir días y horarios específicos. Con esto podemos configurar el acceso a redes sociales en un determinado horario, y que permanezca bloqueado el resto del tiempo. Lo encontramos en su sitio web oficial: **www.wingate.com**.

ZoneAlarm Firewall

El **ZoneAlarm** ha sido una de las aplicaciones más utilizadas por años. Entre sus productos ofrece antivirus, firewall, o ambos. También dispone de una versión gratuita del firewall. Luego de la instalación, ingresamos a los detalles del firewall. En ellos, veremos las configuraciones, nos habrá detectado nuestras placas de red, y estarán marcadas como zonas seguras.

UN FIREWALL MAL CONFIGURADO PROVOCARÁ DIVERSOS PROBLEMAS DE SEGURIAD EN LA RED.

Para bloquear un sitio web, haremos clic en **View Zones**, luego en **Add**, y seleccionamos **Host/Site**. Aparecerá una nueva ventana que debemos completar, en **Zone** seleccionamos **Blocked**, luego ingresamos la dirección web del sitio que deseamos bloquear, y abajo pondremos una descripción que nos ayude a nosotros a identificar rápidamente por qué decidimos bloquear el acceso a ese sitio. Este proceso lo debemos realizar para cada sitio que deseemos bloquear o permitir su acceso total.

Es posible tener el control de las aplicaciones que quieran acceder a la red, y por medio de la configuración, podemos catalogarlas en

Optimización de la red

Al tener instalado un firewall como filtro de la red editando adecuadamente los bloqueos a sitios de Internet, se notará una disminución en el tráfico, que por lo general es tráfico ocioso. Si nos encontramos en una red empresarial, al limitar los accesos a redes sociales, sitios de adultos, salas de chat, no solo lograremos proteger la red, sino también evitar que los empleados puedan utilizarla para fines personales que pueden comprometer la seguridad del equipo o de la red.

En Web Filter, al tildar EnableCategoryFiltering, podemos ir destilando por categorías que deseamos filtrar en la navegación de Internet.

los niveles de confianza que nos ofrece ZoneAlarm. Podemos agregar a esta lista aplicaciones para que no tengan problemas, o editar su configuración, como para juegos multiplayer online. Entre otras funciones, nos provee de 5 GB de espacio online para guardar datos e incluye servicios de protección de identidad para protegerlos.
Además de cumplir con los requisitos de un firewall, su versión gratuita es una gran opción para aquellos padres que dejan solos a sus hijos pequeños con los equipos. Su configuración podemos protegerla mediante una contraseña, asegurándonos de que únicamente nosotros podremos realizar cambios.
La gran desventaja de ZoneAlarm consiste en que, si activamos la barra de herramientas, hay muchas funciones que no pertenecen a ella misma, y seremos redirigidos a otros sitios.
Encontramos su sitio web oficial en la dirección **www.zonealarm.com**.

BitDefender Internet Security

BitDefender ofrece sus tres clases de productos: Antivirus Plus, Internet Security y Total Security. Los dos últimos incluyen la función de firewall.
Durante la instalación, BD realizará un escaneo en búsqueda de virus; este proceso puede tomar varios minutos. Luego descargará los archivos necesarios y comenzará la instalación.
La versión trial es poco personalizable; en la configuración del firewall solo existe la opción de permitir o bloquear la navegación web, sin permitirnos editar qué sitios queremos bloquear.
Una característica importante es que mantiene la navegación en modo seguro de las páginas que utilicemos para realizar transacciones electrónicas.
Incluye el análisis de redes sociales, encriptando las conversaciones y analizando todos los links que podamos recibir. También, podemos utilizarlo como un eficiente antispam.
Es importante tener en cuenta que, en forma predeterminada, encontraremos que vienen cargados diversos perfiles, los cuales podemos seleccionar según la actividad que estemos realizando. En particular, ofrece configuraciones para el modo Gaming y tiene un apartado en la configuración del firewall, donde podemos agregar las aplicaciones de juegos que no estén reconocidas o sean nuevas. Esto evita que, cuando estemos en otra aplicación a pantalla completa, se nos cierre la ventana por mensajes de alerta. Podemos encontrarlo visitando su sitio web oficial, en la dirección **www.bitdefender.es**.

En esta imagen, vemos la pantalla principal de **WinGate 7**.

WebRootSecureAnywhere

WebRoot es otra combinación de antivirus y firewall. Incluye funciones de protección de identidad. Ofrece varias características de seguridad que se encuentran separadas por las categorías Escudo y Cortafuegos. También ofrece protección a dispositivos móviles, sean smarthphones o tabletas.
En esta aplicación, no podemos editar la configuración de firewall. Toda su configuración ya está preconfigurada y no es posible agregar configuraciones personalizables. Como la protección de antivirus que ofrece es muy buena, buscando amenazas en nuestras unidades removibles y bloqueando sitios de phishing, se convierte en una opción complementaria a un firewall dedicado en la red. Su sitio web es **www.webroot.com**.

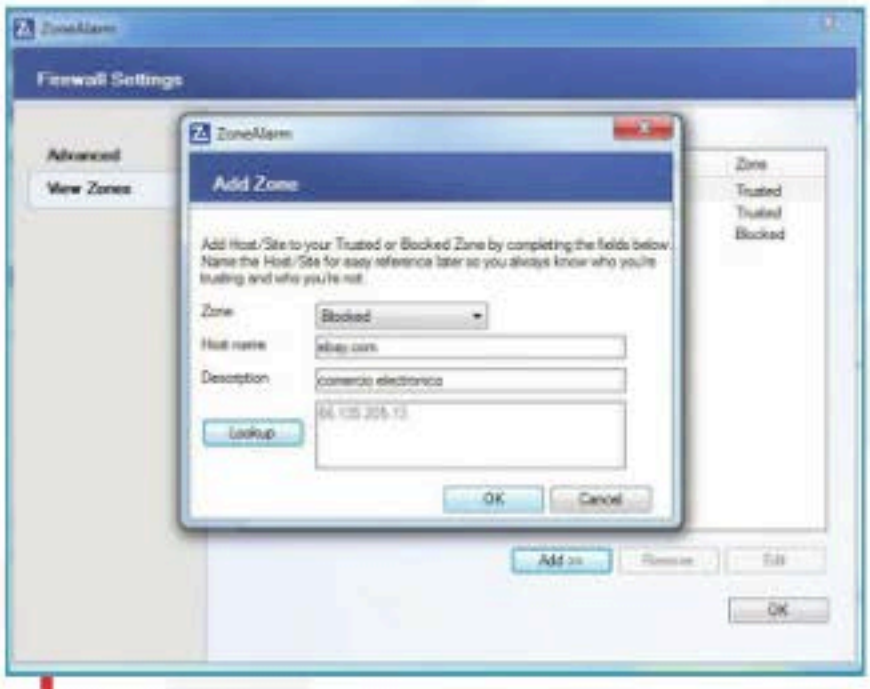
UN FIREWALL NO REEMPLAZA AL ANTIVIRUS. SON DISTINTOS, Y AMBOS SE COMPLEMENTAN PARA AUMENTAR LA SEGURIDAD.

COMODO Firewall

Antes de comenzar la instalación, tendremos que seleccionar unas configuraciones previas: si deseamos utilizar los servidores DNS de **Comodo** para toda nuestra navegación en la Web, enviar información sobre nuestra actividad, enviar a Comodo los programas no reconocidos (que pueden ser una amenaza). Además incluye el navegador ComodoDragon, que es una versión modificada del Google Chrome.
Podemos configurar el firewall de modo general, aplicar reglas para permitir o denegar el tráfico según el protocolo (TCP, UDP), y en qué sentido, tráfico entrante o saliente. No podemos editar para bloquear el acceso a determinados sitios.

Desde la configuración del firewall en COMODO, es posible seleccionar las aplicaciones a las cuales se les permitirá o denegará la conexión.

Recordemos que se pueden configurar las aplicaciones que deseemos que tengan comunicación externa, como también, bloquearlas, y en caso de que una aplicación se quiera conectar a Internet, nos avise mediante una ventana de alerta. Por otra parte, se puede activar el modo denominado **Gaming**. En la parte superior, se incluye un icono para que podamos iniciar una conversación directa con un técnico de Comodo ante alguna duda o ayuda en su configuración. Lo podemos encontrar visitando su sitio web oficial, en la siguiente dirección: **www.comodo.com**. ■



ZoneAlarm nos permite incluir sitios bloqueados. Deberemos ingresar uno por uno todos los sitios a los que queramos negar acceso.

Firewall dedicado

Instalar un firewall por software para cada equipo de la red no tendría que afectar significativamente al rendimiento general de cada equipo, los cuales podremos seguir utilizando para realizar las actividad cotidianas. Debemos tener en cuenta que un caso muy distinto es si realizamos la instalación de un firewall para proteger toda la red, además de al equipo en sí mismo, no conviene utilizar el equipo para realizar nuestro trabajo diario, ya que ante cualquier problema menor que se presente, estaríamos comprometiendo la seguridad de toda la red de datos.

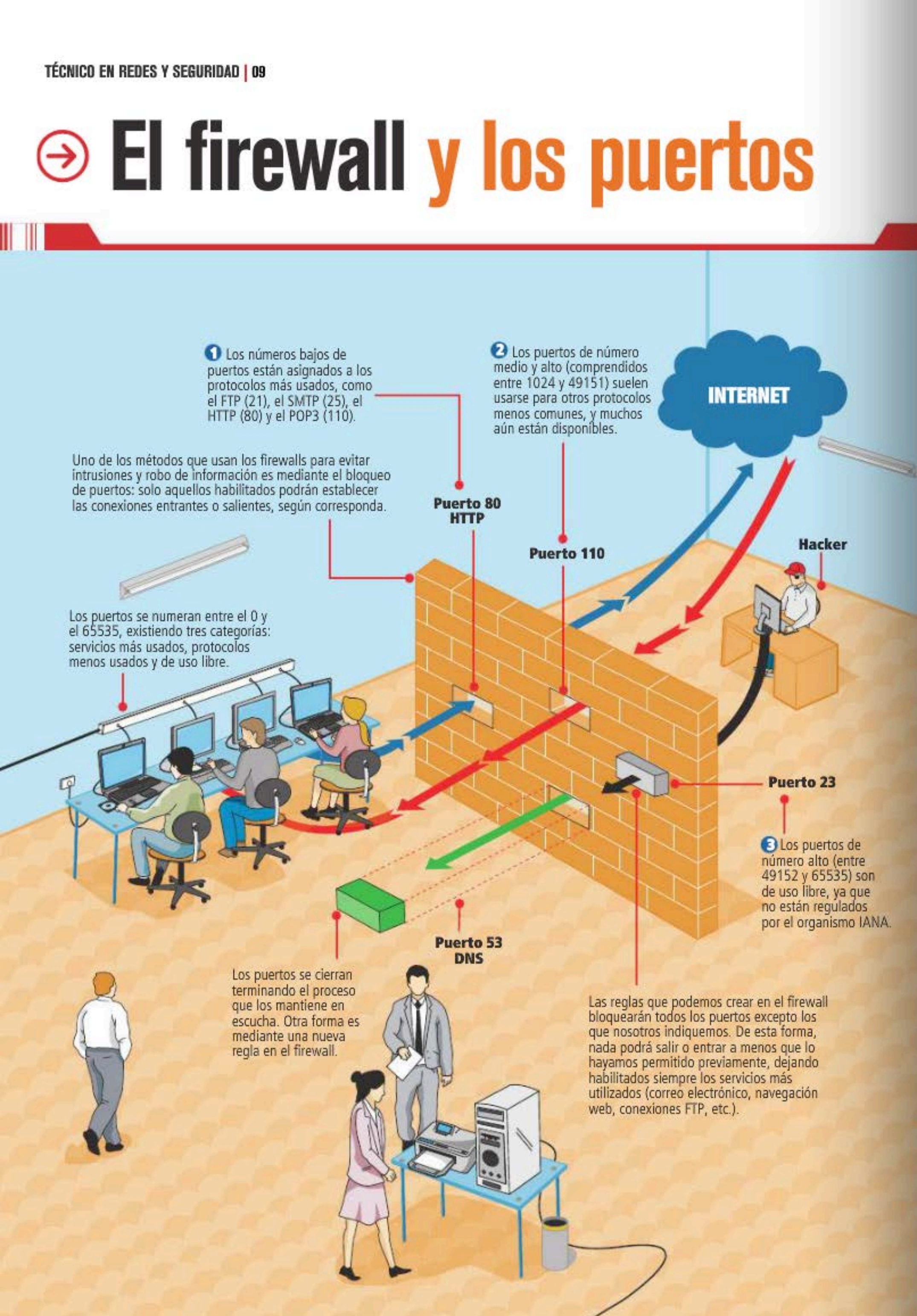
El firewall y los puertos

1 Los números bajos de puertos están asignados a los protocolos más usados, como el FTP (21), el SMTP (25), el HTTP (80) y el POP3 (110).

2 Los puertos de número medio y alto (comprendidos entre 1024 y 49151) suelen usarse para otros protocolos menos comunes, y muchos aún están disponibles.

Uno de los métodos que usan los firewalls para evitar intrusiones y robo de información es mediante el bloqueo de puertos: solo aquellos habilitados podrán establecer las conexiones entrantes o salientes, según corresponda.

Los puertos se numeran entre el 0 y el 65535, existiendo tres categorías: servicios más usados, protocolos menos usados y de uso libre.

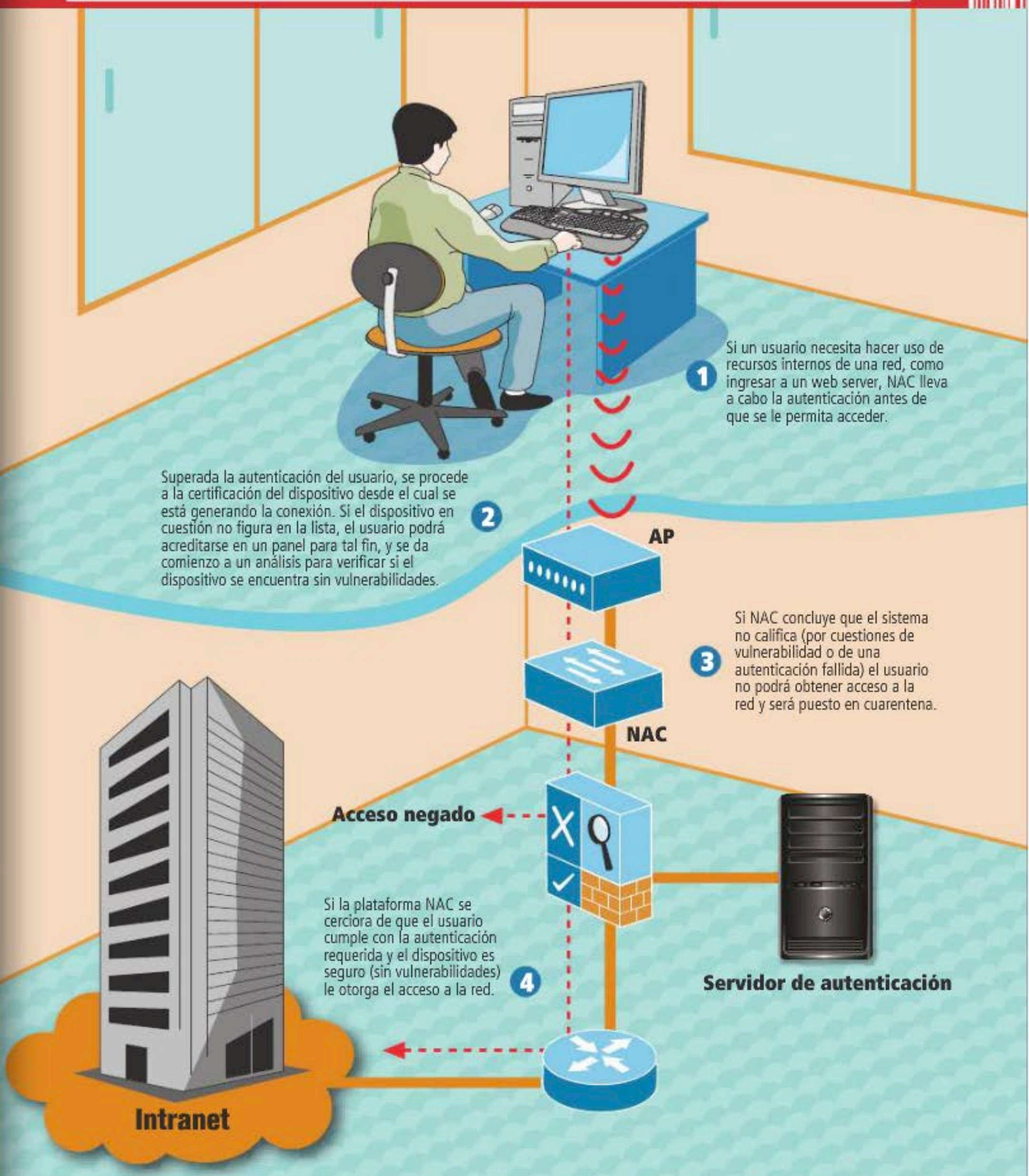


3 Los puertos de número alto (entre 49152 y 65535) son de uso libre, ya que no están regulados por el organismo IANA.

Los puertos se cierran terminando el proceso que los mantiene en escucha. Otra forma es mediante una nueva regla en el firewall.

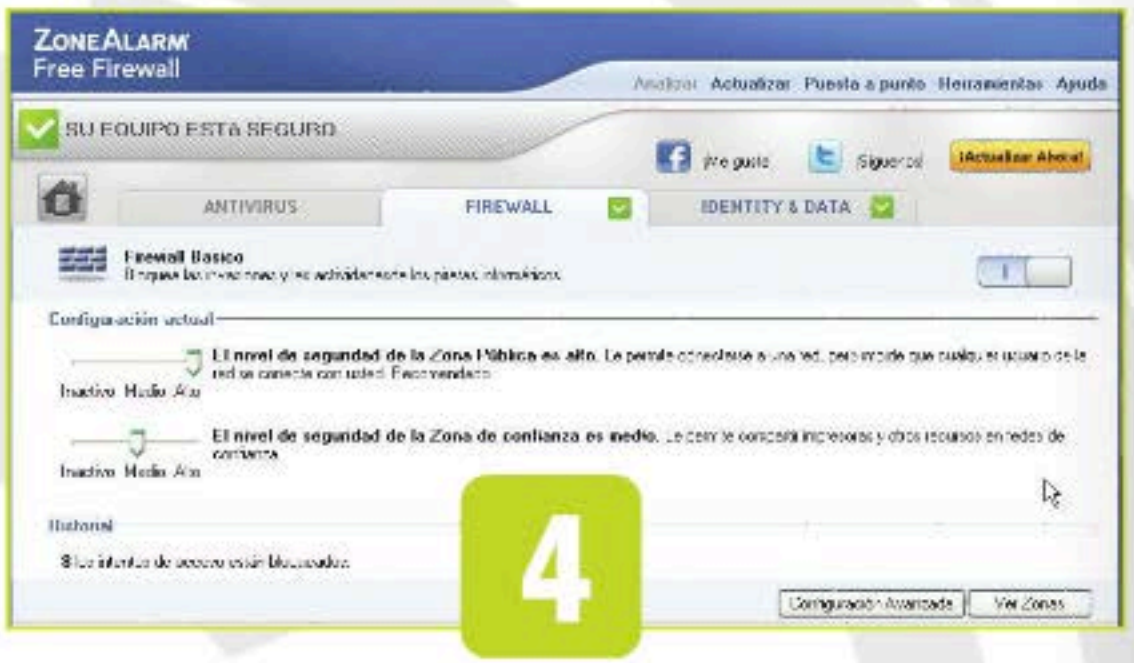
Las reglas que podemos crear en el firewall bloquearán todos los puertos excepto los que nosotros indiquemos. De esta forma, nada podrá salir o entrar a menos que lo hayamos permitido previamente, dejando habilitados siempre los servicios más utilizados (correo electrónico, navegación web, conexiones FTP, etc.).

Funcionamiento de NAC



Instalación de una aplicación firewall

En estas páginas, conoceremos en detalle la instalación de un firewall de software para un sistema Windows.

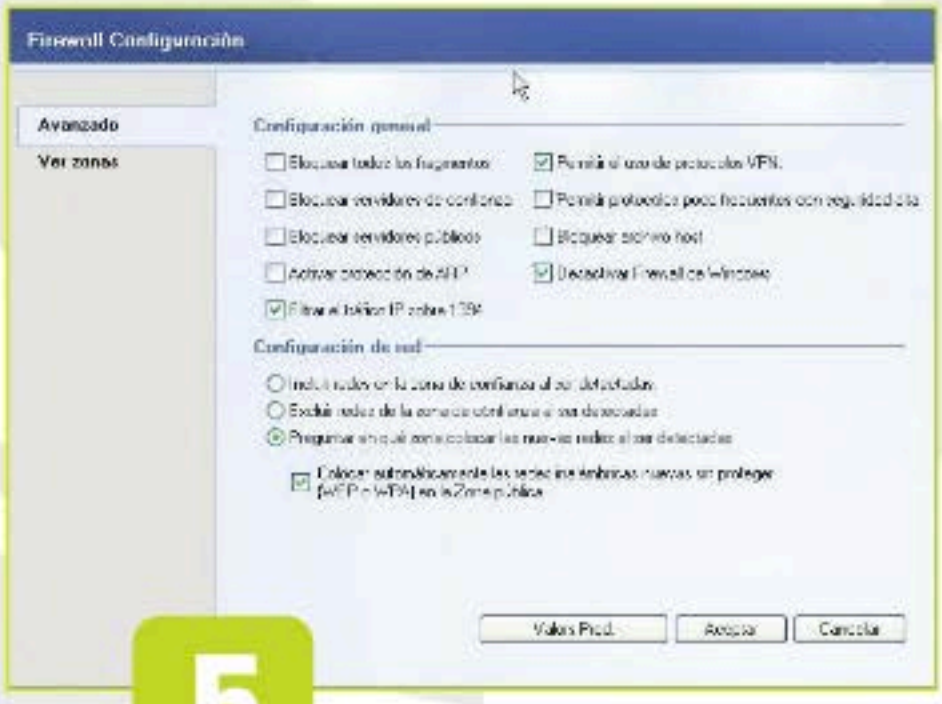


1 Al ejecutar el instalador que obtenemos en **www.zonealarm.com**, podremos realizar una instalación rápida o personalizada. Esta última opción, nos permitirá seleccionar unos ítems particulares.
La instalación rápida suele utilizar las configuraciones más estándares.

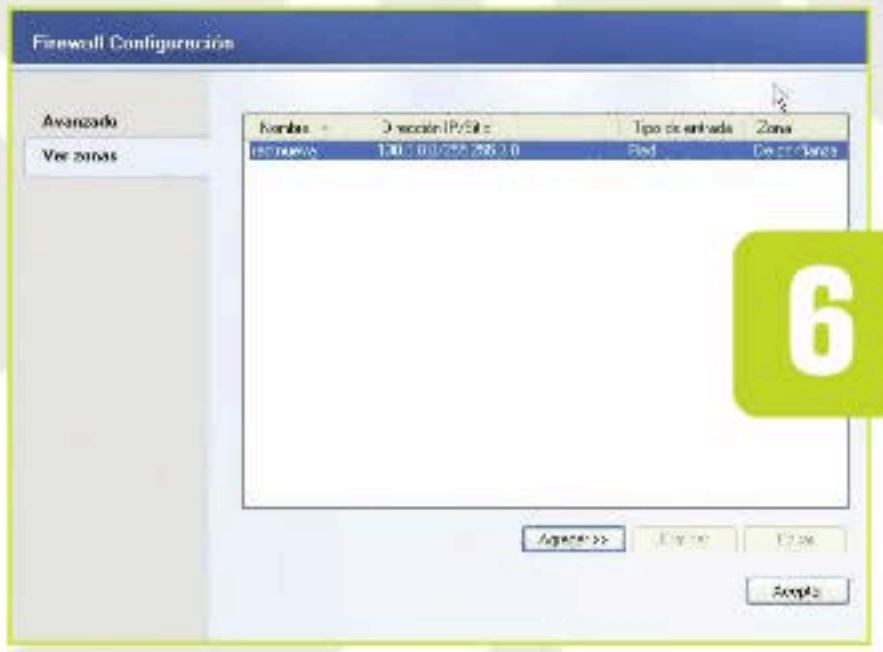
2 Durante la instalación, podremos deshabilitar la instalación de las barras de navegador, seleccionar la descarga de firmas y también la forma de configuración inicial del firewall: **Por aprendizaje** o **Seguro**; el primero permitirá aprender de las aplicaciones instaladas, y el segundo bloqueará todo, a menos que se lo habilite.

3 Al terminar la instalación, se nos pedirá reiniciar el equipo. Al iniciar nuevamente, detectará la red, para que identifiquemos la conexión en la que estamos conectados, utilizando las categorías **Pública** (más restrictiva) o **De confianza**.

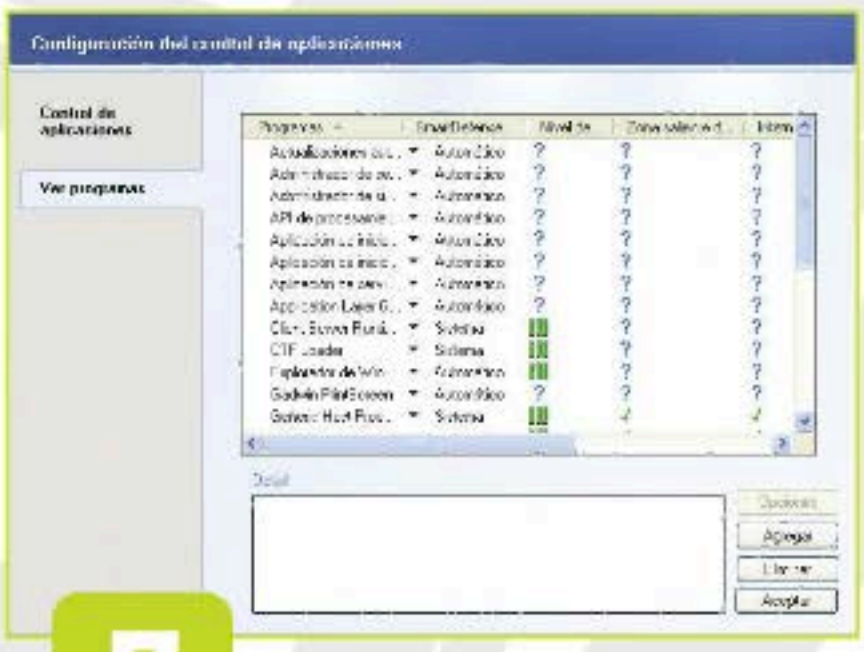
4 En la consola de administración, podemos ver la configuración actual del firewall, el nivel de seguridad que corresponde a cada zona, el historial de intentos de accesos bloqueados, y realizar las configuraciones de acceso y bloqueo.



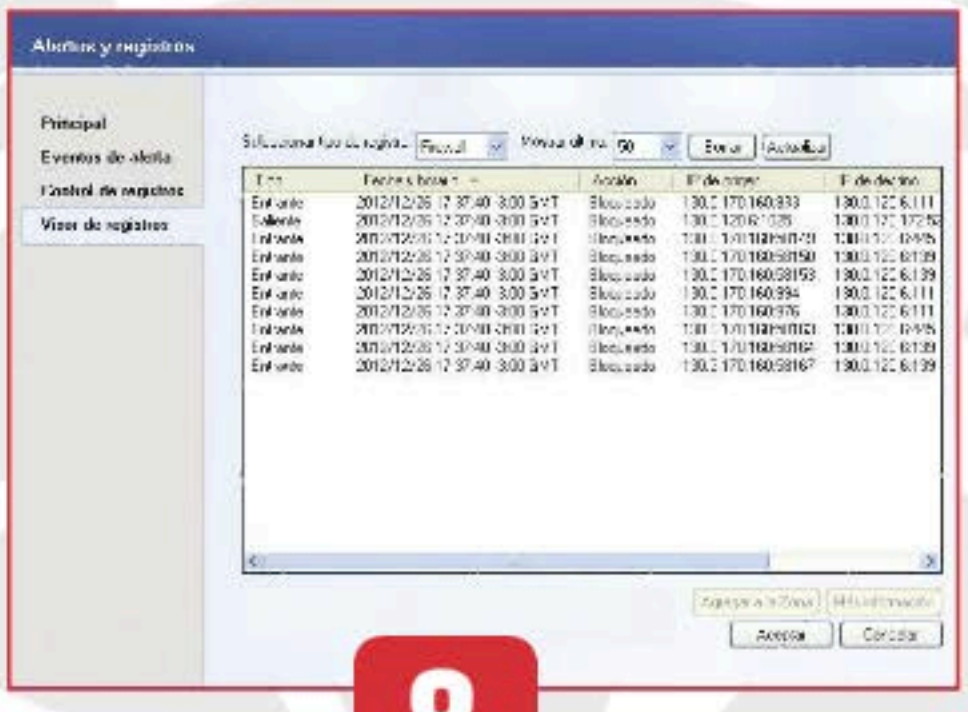
5



6



7



8

5 Para continuar, nos dirigimos a la configuración avanzada; en ella, para que no se generen incompatibilidades, deshabilitamos el Firewall de Windows, además nos permite definir los tipos de bloqueos y la configuración de red para las zonas.

6 En el apartado **Zonas**, podemos ver la designación de cada red que hemos catalogado en nuestro firewall; es posible modificarlas si consideramos que es necesario y, en la misma pantalla, agregar nuevas zonas.

7 En el panel de administración, ingresamos a **Ver programas**, y se abrirá una opción mostrándonos los programas habilitados para cada zona de red. Aquí podemos modificar, denegar el acceso y agregar nuevos programas.

8 Debemos revisar frecuentemente el **Visor de registros** y no olvidamos de realizar esta tarea, ya que quizás pueda haber algún software malintencionado que esté intentado establecer una conexión y no sepamos lo que sucede, o que un software que utilicemos no funcione porque está siendo bloqueado por el firewall.

Firewall por hardware

La solución más robusta que podemos encontrar para nuestra red en términos de seguridad es un firewall por hardware dedicado a protegernos.

Los **firewalls físicos**, al igual que los firewalls por software proporcionan una barrera que evita que intrusos tengan acceso a información confidencial en nuestros servidores o computadoras de nuestra red. El firewall hace su trabajo mediante la inspección de los paquetes de datos de la red y la toma de decisiones sobre la conveniencia de dejar pasar ciertos paquetes, o bloquearlos e impedir su acceso. Con este equipamiento podremos definir, imponer y auditar políticas de uso aceptables y de seguridad, lo que aumentará la productividad y disminuirá el riesgo de la propiedad intelectual o información crítica de nuestros clientes.

Aquí podemos ver una advertencia de un posible malware sobre el sitio al que estamos intentando acceder.

Métodos de intrusión

Los **métodos de intrusión** son numerosos, por nombrar solo algunos: inyecciones de SQL (infiltración de código intruso que se vale de una vulnerabilidad informática), **cross-site scripting** (típico de las aplicaciones web, permite a una tercera parte inyectar en páginas web código JavaScript malicioso), desbordamientos de buffer (si nuestro servidor no controla adecuadamente la cantidad de datos que se copian sobre el buffer, se podría llegar a conseguir cierto nivel de control saltándose las limitaciones de seguridad básicas), denegación de servicio (DoS, **Denial of Service**, es un ataque que causa la pérdida de la conectividad de la red por el consumo del ancho de banda en nuestra red), entre otros.

La versión de firewall con wireless nos permite brindarles acceso a la web a nuestros invitados sin comprometer la seguridad de la empresa.

Software

Un **software** instalado en un servidor puede causar un retraso en la red ya que hay más software involucrado, como el sistema operativo, servicios de seguridad, proxy, VPN, filtrado de contenido, etc. Un software instalado en la computadora personal también ve afectada su performance por las mismas razones; sin embargo, el retraso es leve y, en la mayoría de las PyMEs, no es considerado de mayor importancia, pero a medida que aumenta el tráfico por cantidad de usuarios, el impacto en el rendimiento aumenta, y debemos pensar en una solución más robusta. Una pieza de hardware que tiene todo el software instalado es el firmware del dispositivo.

Firewall por hardware

Los **firewalls por hardware** miden su capacidad de rendimiento según su velocidad. En la actualidad, podemos encontrar equipos con una velocidad de firewall de hasta 20 Gbps, velocidad de VPN de hasta 2 Gbps y más de

2 millones de sesiones de usuarios concurrentes. La **consola de administración** centraliza las funciones de seguridad que suelen incluir: bloqueo de spyware, ataques DoS, paquetes fragmentados y malformados, amenazas combinadas, protección de proxy en distintos protocolos: **HTTP**, **HTTPS**, **FTP**, **SMTP**, **POP3**, **DNS**, **TCP/UDP**.

La VPN también suele ser el punto fuerte de esta clase de equipos con múltiples formatos de cifrado, como ejemplo, podemos mencionar los siguientes: DES, 3DES, AES 128-, 192-, 256-bit), IPsec (*Internet Protocol Security*), PPTP (*Point to Point Tunneling Protocol*), y además ofrece un completo soporte para diversos dispositivos móviles, entre otras características.

Los **administradores IT** pueden imponer una política de uso aceptable para usuarios y grupos de usuarios: por categoría, por aplicación y por subfunciones. Esto se da especialmente en la mensajería instantánea (IM) y peer-to-peer (P2P), donde son particularmente notorias la apertura de puertas traseras en la red y la difusión de contenido malicioso. Un ejemplo sería la definición de una política que permite al departamento de marketing acceder a Facebook pero no a los juegos.

EL CONCEPTO DE LOS NGFW ESTÁ BASADO EN UN MODELO EN EL CUAL SOLO LO AUTORIZADO ES PERMITIDO, LO DEMÁS ES BLOQUEADO.

Las suscripciones de seguridad actualizan las bases de datos del firewall para estar siempre al día. Nos permiten cargar filtros de direcciones URL que, de otra manera, sería imposible que el administrador de la red los cargara a mano. No solo hablamos a nivel de seguridad; también podemos inhabilitar sitios que consideremos inapropiados e incrementar la productividad de los empleados. La función básica de un **router** es encaminar la información hacia su destino. Para hacerlo, necesita información acerca de las rutas existentes para alcanzar los distintos destinos en nuestra red. El firewall tiene, también, la capacidad de enrutamiento (dinámico y estático), lo cual agilizará nuestra red.

Un dato interesante a la hora de elegir un firewall se refiere a la certificación. Hay equipos que cuentan con la aprobación de **ICSA Labs** (*International Computer Security Association*). Una división independiente de Verizon, que se encarga del testeo intensivo de este tipo de hardware; allí se someten a rigurosas pruebas que reproducen el mundo real de las redes corporativas. Algunos equipos incluyen Wi-Fi, lo que nos permitiría proveer acceso a Internet a nuestros invitados sin comprometer la seguridad.

Próxima generación

Los llamados firewalls de próxima generación (**NGFW** - *Next Generation Firewall*) describen un firewall/VPN corporativo que puede hacer barridos de prevención de intrusiones de tráfico, como así también tener **conciencia** sobre las aplicaciones que se mueven a través de él (como **VoIP**) o integrarse con el AD (*Active Directory*) de nuestro servidor. Si hablamos de marcas, **WatchGuard** y **Fortinet** quizás sean las más reconocida del mercado. Las alternativas de igual calidad son: **SonicWALL** (de Dell), **Palo Alto Networks**, **Juniper**, **Cisco** y **Barracuda**. Este último también cuenta con versiones virtuales para montarlo en servidores dedicados con **Hiper-V** en **VMware**. Con este mismo concepto, también existe la posibilidad de montar nuestro propio servidor (olvidándonos de la principal filosofía y ventaja de los firewalls por hardware) e instalar alguna distribución Linux que esté optimizada para trabajar con iptables, como es la distribución IPCop entre otras. ■

Los equipos más completos están diseñados para soportar un alto desempeño, en bancos o ISP.

Las múltiples salidas nos facilitarán el enrutamiento (dinámico y estático) agilizando nuestra red.

Estadísticas

Según una estadística publicada en el Google Online Security Blog, **aproximadamente entre 12 y 14 millones de consultas de búsqueda en Google por día muestran una advertencia a los usuarios sobre sitios que se encuentran comprometidos (podemos efectuar un test en:** http://malware.testing.google.test/testing/malware**). Recordemos que 9.500 sitios web maliciosos nuevos surgen cada día, y se registran cerca de 300 mil avisos de malware de descargas por día.**

Sistemas de detección: prevención de intrusos

Un sistema que monitorea y registra toda la actividad de nuestro servidor, o incluso de toda la red, en busca de posibles ataques o anomalías.

Un **IDS** (*Intrusion Detection System*) es, como su nombre lo indica, un sistema de detección de intrusos. Se trata de un programa de seguridad que intenta monitorear y detectar eventos no autorizados. Este software se dedica a monitorear la PC o la red (sniffer de paquetes) en busca de anomalías y comportamientos sospechosos, como una petición sobre escaneo de puertos, paquetes malformados, que nos daría el indicio de la presencia de intrusos o de ataques.

IDS pasivo

Se llama IDS pasivo cuando el sistema almacena las anomalías detectadas en un registro para su posterior análisis offline. Tomemos un ejemplo: el simple acto de copiar un archivo es una actividad común en nuestro servidor o PC, pero no lo sería copiar la base de datos de nuestros clientes vía FTP. En un IDS pasivo, quedaría registrado en un log la anomalía, pero el daño ya estaría hecho. En algunos casos, nos puede ser útil esta información durante una auditoría. Si la copia de la DB se hizo en un pendrive USB, se deduce un problema de seguridad interno y se tomarán las medidas del caso.

IDS reactivo

Por suerte también existe el sistema reactivo, que interactúa para evitar el daño. En el mismo ejemplo, si la copia de datos se hace vía FTP, el IDS responde a la actividad sospechosa reprogramando el firewall para que bloquee el tráfico que proviene de la red del atacante. Este sistema reactivo se denomina **IPS** (*Intrusion Prevention System*).
Este mecanismo de detección está basado en la metodología heurística (como en un antivirus). En otras palabras, determina cuándo hay actividad normal en la PC según protocolos, puertos y dispositivos que, en condiciones normales, se interconectan. En la red, lo hace según el ancho de banda usado, y alerta al administrador IT cuando se detecta alguna anomalía, para tomar las precauciones del caso. Otro mecanismo de detección es el basado en patrones. Los datos del análisis los compara con patrones de ataques conocidos y preconfigurados. Así, los IDS disponen de una base de datos o firmas (seguimos con la comparación con el antivirus) y permiten al programa distinguir entre el uso normal de una PC y el comportamiento sospechoso en el tráfico de la red.

OSSEC

Existen muchos software HIDS, pero la mayoría son comerciales. OSSEC es quizá la única opción gratuita.

HIDS y NIDS

Existen dos tipos de IDS: HIDS y NIDS. A continuación, analizaremos las características del **HIDS** (*Host Intrusion Detection System*) y del **NIDS** (*Network Intrusion Detection System*):

- El HIDS fue el primer IDS en desarrollarse en la industria de la seguridad informática. Protege una única PC o servidor (host). Escanea archivos, logs, recursos del sistema, procesos, y estudia a los usuarios que se involucran en una determinada acción (copiar, modificar o borrar un archivo).

Solución completa

Una solución NIDS completa sería instalar un servidor Linux que se desempeñará como firewall en nuestra red, con el software **Arno'siptables Firewall**. Como motor de detección de ataques elegiremos a Snort. Las reglas que ofrece **Snort** gratuitamente son escasas, pero podemos descargar y utilizar las de Debian. Por último, a **BASE** (***Basic Analysis and Security Engine***), como aplicación web para la monitorización de Snort.

Según el fabricante, un puerto espejo puede tener distintos nombres: *portmirroring*, *SPAN* o *portmonitoring*.

El HIDS detecta las modificaciones del equipo afectado y hace un reporte con sus conclusiones.

- Los **NIDS** protegen la red; son sniffers de tráfico de red que analizan los paquetes capturados buscando patrones de ataque.

Instalación

La gran pregunta al momento de instalar un NIDS es en dónde se lo ubica. Antiguamente, con un hub (capa 1 del modelo OSI) no existía el problema de analizar todo el tráfico de la red, ya que se realizaba una conexión a cualquier puerto del equipo (un repetidor). Hoy, estos equipos son obsoletos y en un switch no podremos analizar toda la red. Solo lograremos analizar los datos dirigidos a ese puerto en particular. Algunos switches tienen la opción de configurar un **port mirror** (puerto espejo) o **SPAN** (*Switch Port Analyzer*), como lo denomina Cisco. Pero seguimos con la misma intriga, ¿dónde instalamos nuestro NIDS? Y la realidad es que no hay segmento de red por donde pase todo el tráfico. Si instalamos el NIDS antes del firewall, analizaremos todo el tráfico de entrada y salida de nuestra red, pero el equipo estará tan expuesto que las posibilidades de falsas alarmas es muy grande. Debemos tener en cuenta que la instalación detrás del firewall se encarga de monitorizar todo el tráfico que permita el firewall, y, aunque no analicemos el tráfico interno, priorizamos el análisis de un ataque realizado desde el exterior.

Snort

Snort (que podemos encontrar en el sitio web **www.snort.org**) es un IDS basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite alertarnos, almacenar un registro (pasivo) e interactuar (reactivo) ante cualquier anomalía previamente definida por patrones que corresponden a intentos de aprovechar alguna vulnerabilidad conocida. Está disponible bajo licencia GPL. Es OpenSource y no solo funciona bajo plataformas UNIX/Linux, también hay una versión en Windows. Es quizás el más usado y dispone de una gran variedad de patrones ya predefinidos.

Aspectos legales

Consideremos que los registros e informes generados por el IDS pueden ser requeridos en peritajes o investigaciones que ayuden a condenar a los responsables de los ataques o intromisiones. Lamentablemente, en muchos países, los sistemas legales no han avanzado a la misma velocidad que la tecnología, por esta razón difícilmente se condena a una persona basándose en un registro en formato txt aunque estemos frente al culpable de robar la vacuna del SIDA.

Snort es una herramienta de seguridad utilizada en Linux, pero también tiene un cliente Windows.

FLEXRESP

Cuando un IDS está configurado con la función de **Flexresp**, se encargará de bloquear la dirección del atacante en nuestro firewall. Se trata de una característica que nos permite responder automáticamente a un ataque si la opción correspondiente está especificada en la regla. Debemos tener en cuenta que, aunque mejoramos la seguridad de la red, la interrupción de sesión no debería de estar configurada para responder a todos ya que, de forma indirecta, estamos bloqueando nuestra propia red como con una denegación de servicio (**DoS**). Recordemos que Flexresp debe usarse con cuidado porque podría resultar contraproducente. ■

En el sitio web **www.snort.org** encontraremos información acerca de su instalación y funcionamiento, así como también del enlace de descarga apropiado.

Honeypots y honeynets

A veces, no basta solo con proteger nuestro sistema. También podemos interactuar con quienes nos ataquen, aquí revisaremos las opciones.

Honeypot significa **tarro de miel**; el término hace referencia a algo tentador que, en realidad, resulta ser una trampa. Honeypot es un software cuya intención es tentar a los mal llamados hackers, simulando sistemas vulnerables. Una herramienta de seguridad informática con la que podremos estudiar las técnicas de ataque para optimizar y reforzar las medidas de seguridad de nuestra infraestructura informática (sistemas informáticos y red de datos).

Interactividad

Tengamos en cuenta que existen dos clases de honeypots, según su nivel de participación. Por un lado encontramos los de baja interacción y por otro, los de alta interacción. La diferencia está en los distintos niveles a los que se le permite interactuar al atacante.

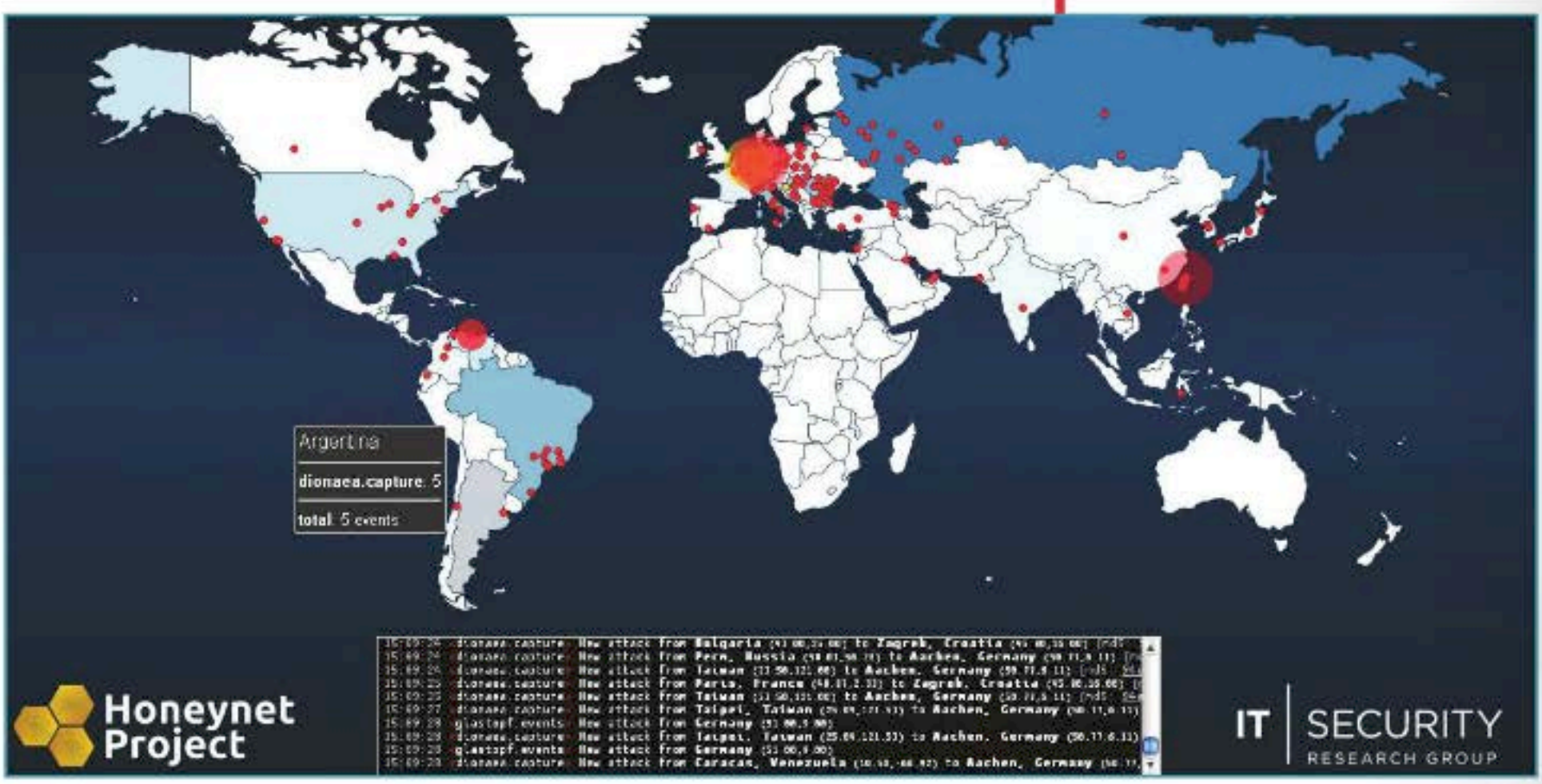
- **Baja interacción**: solo simulan una aplicación o servicio. Permiten a los atacantes interactuar con el sistema de forma muy limitada. Es más fácil la instalación y el mantenimiento, pero los datos recogidos son limitados.
- **Alta interacción**: la recopilación de información es mayor en cantidad y calidad, pero, si no está bien configurado, el atacante podría llegar a tener acceso real al sistema donde esté montado el Honeypot.

Despliegue

Podemos clasificar los honeypots según su papel o desempeño: los de producción y los de investigación. Aquí, la diferencia radica en cuál será su principal función.

- **Honeypots de producción**: son utilizados principalmente por empresas o corporaciones a modo de defensa. Se instalan dentro de la red, junto a los servidores de producción, a modo de "carnada" (seguimos con el concepto de trampa). Si el honeypot es atacado, nuestros servidores pueden estar comprometidos, pero, con la alerta generada y la información recopilada, podremos tomar las medidas necesarias para reforzar la seguridad de nuestros servidores reales. Un ejemplo sería instalar un honeypot en el puerto DMZ de nuestro router, y, al quedar expuesto nuestro pseudoserver fuera del firewall, el atacante que intente ingresar por nuestra IP pública, se entretendría con el honeypot.

HoneyMap es un proyecto donde se visualizan, en tiempo real, los ataques captados por honeypots del Honeynet Project.



▶ **Honeypots de investigación**: son sistemas montados para investigación. Por lo general, son instalados por empresas dedicadas a la seguridad informática, desarrolladores de antivirus, antispyware, y también por militares u organismos gubernamentales dedicados a la captura de ciberdelincuentes.

Software honeypot

▶ **Kippo** es un honeypot escrito en Python, que simula un servicio de SSH, registrando todas las combinaciones de usuarios y contraseñas e, incluso, simulando la interacción de la shell. Lo encontramos en **http://goo.gl/APQ0o**.

▶ **OpenVAS** (*Open Vulnerability Assessment System*) permite analizar un servidor en forma remota.

▶ **LaBrea** se toma literal la traducción de honeypot, ya que se autodefine como un software pegajoso. Crea servidores virtuales, atractivos para los hackers, e intenta respuestas de manera tal que la PC del atacante quede atrapada.

▶ **DeceptionToolkit**: fue el primer proyecto Open Source.

▶ **HoneyBOT**: para Windows, sencillo y gratuito.

Existen honeypots para todos los servicios. Los spammers aprovechan vulnerabilidades en servidores de correo y en proxy abiertos. Se han creado honeypots específicos de servidores SMTP (como el **Smtpot** o **Spamhole**, y el **Proxypot**) que imitan este tipo de recursos, para identificar a los presuntos spammers.

SI NUESTRO HONEYPOT NO ESTÁ BIEN CONFIGURADO, EL ATACANTE PODRÍA LLEGAR A TENER ACCESO REAL AL SISTEMA DONDE ESTÉ MONTADO.

Las bases de datos a menudo son atacadas por intrusos que utilizan **SQL Injection**. Debido a que estas actividades no son reconocidas por los servidores de seguridad básicos, algunos servidores permiten arquitecturas honeypot para permitir a un intruso ejecutar en una base de datos trampa, mientras que la aplicación web sigue funcionando normalmente.

Honeynets

Como acabamos de ver, algunos honeypots pueden apuntar específicamente a un servicio. De esta forma, consideremos que la instalación de dos o más honeypots en una misma red, para abarcar más cantidad de servicios, se denomina **HoneyNet**. Son honeypots de alta interacción que simulan una red de producción, configurada de tal manera que toda la actividad se controla y registra en forma discreta. Un concepto que se originó en 1999; en principio se utilizaban equipos reales con sistemas operativos reales y corriendo aplicaciones reales. Hoy, gracias a la virtualización, con el hardware adecuado, cualquiera de nosotros podría instalarse su propia HoneyFarm (como una gran granja de honeypots).

The Honeynet Project

The Honeynet Project **es una comunidad internacional, sin fines de lucro, dedicada a la investigación de los ataques más recientes y el desarrollo de herramientas de seguridad de código abierto para mejorar la seguridad en Internet. Son voluntarios que han contribuido a la lucha contra el malware (como** Confickr**), el descubrimiento de nuevos ataques y la creación de herramientas de seguridad. Debemos considerar que, lamentablemente, salvo en Brasil**

Más trampas

El concepto honeypot es tan amplio que se implementan trampas en todas las ramas de la informática. Algunos ejemplos:

▶ **HoneyMonkey** es un programa automatizado, que trata de imitar la acción de un usuario al navegar por Internet, en varios niveles de parches (algunos al día, y otros completamente vulnerables). Se visita un sitio web, y el registro se analiza para determinar si algún malware se ha cargado.

▶ **HoneyAP** crea acces point con conexiones Wi-Fi falsas para investigar a los wardrivers que quieran irrumpir vía wireless en nuestra red.

▶ **VoIPHoney** emula un entorno de comunicaciones VoIP como Asterisk PBX u OpenSER (*Open Source SIP Server*) con conexiones totalmente configurables. Hasta la creación de un sitio web o sala de chat trampa, para atrapar pedófilos. ■

Algunos routers cuentan con un puerto físico DMZ, en otros (aun en los routers hogareños) es posible configurarlo.

Seguridad relacionada con los DNS

En estas páginas analizaremos de qué forma los nombres de dominio pueden ser vulnerables y cómo prevenir posibles ataques.

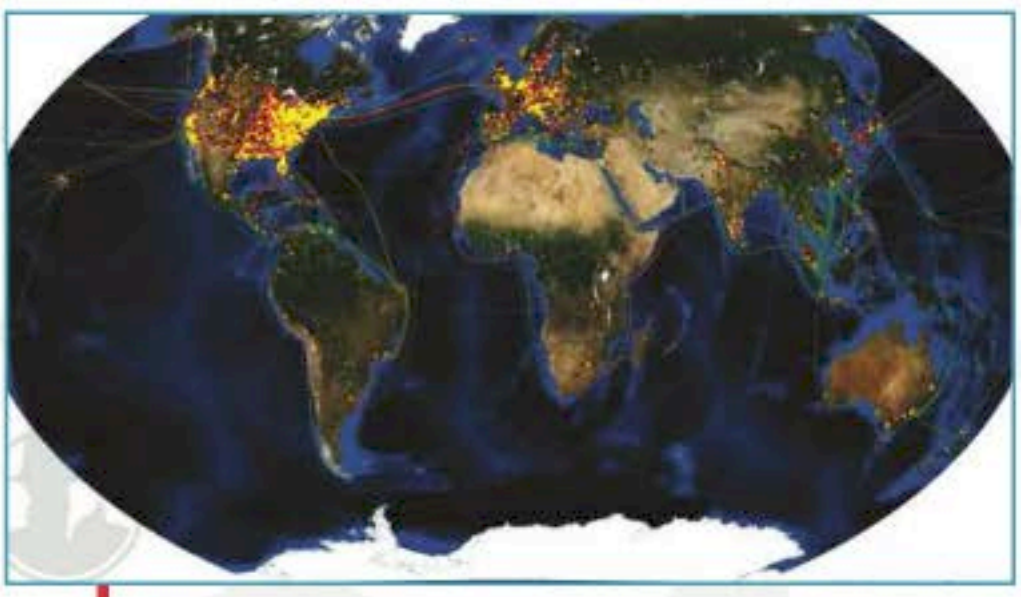
DNS (*Domain Name Server*) es un sistema de nombres de dominio. Su función más común es la asignación de nombres de dominio a direcciones IP, la localización de los servidores de correo electrónico de cada dominio y la resolución inversa de direcciones IP. Por tratarse de un sistema muy flexible, es utilizado también para otras funciones, pero, por ahora, vamos a centrarnos solo en estas tres. El DNS nació gracias a la necesidad de recordar con facilidad los nombres de los servidores conectados a Internet. El nombre de dominio RedUsers.com es claramente más fácil de recordar que su dirección IP, y además, la dirección numérica podría cambiar debido a muchas razones.

Componentes

Debemos tener en cuenta que un DNS se compone de un cliente DNS, un servidor DNS y las Zonas de Autoridad.

- **Cliente DNS**: nuestro web browser favorito, o nuestro cliente de correo son clientes DNS. O sea, es quien genera la petición al servidor DNS, preguntando por el nombre de dominio en Internet.
- **Servidor DNS**: según su clase, el servidor es el encargado de responder a las peticiones hechas por un cliente DNS o de otro servidor de DNS, con los registros de dominio almacenados.
- **Zonas de autoridad**: el sistema está estructurado en forma de árbol, en el que cada nodo del árbol está compuesto por un grupo de servidores que se encargan de resolver un conjunto de dominios. A este grupo, se lo denomina **zona de autoridad**.

SE ESTIMA QUE ALREDEDOR DE UN 60% DE LOS SERVIDORES DNS EN INTERNET SON VULNERABLES.



Aquí vemos un mapa interactivo del **DNS Changer Working Group (DCWG)** creado por el FBI para remover el **Rove Digital'smalicious DNS servers.**

Servidores DNS

En los clientes DNS, se pueden especificar varios servidores redundantes. Si el primero no responde en tiempo y forma, la consulta salta al segundo. Estos servidores son intercambiables, ya que deberían de tener la misma información, pero sería más eficiente poner como primario al DNS con caché más grande y topológicamente más cercano a nuestra PC

Caché DNS

Cuando se realiza una consulta, la respuesta se almacena en la base de datos del servidor para agilizar la repetición de estas peticiones en el futuro. Como ejemplo, veamos qué ocurre cuando escribimos **www.redusers.com** por primera vez en nuestra PC:

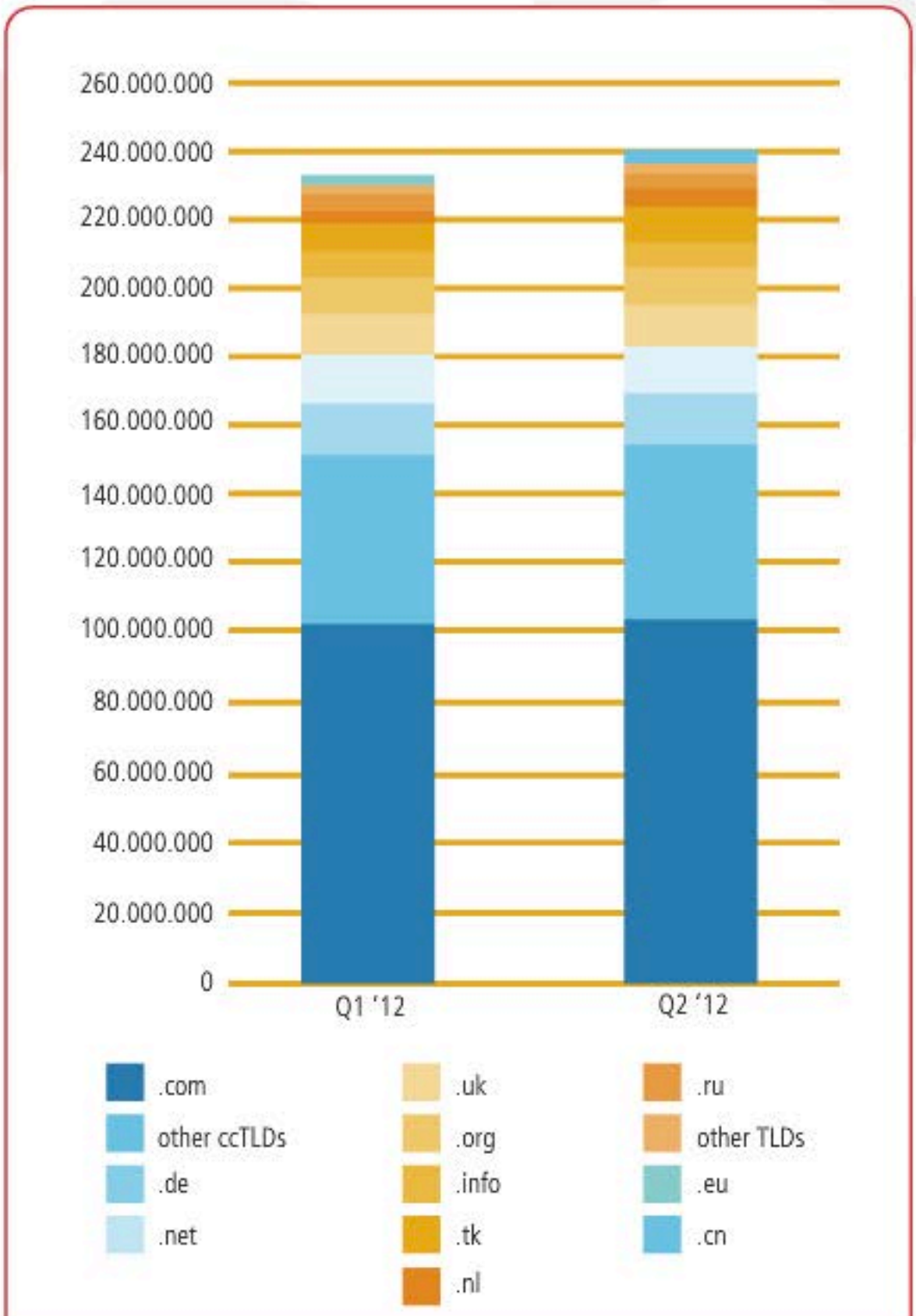
1. Nuestro navegador (cliente DNS) primero verifica en su minicaché si el dominio no fue resuelto con anterioridad y ya conoce la dirección IP de destino.
2. Si no tenemos suerte, la petición se envía al servidor DNS local del sistema operativo en nuestra PC.
3. El SO comprueba si la respuesta se encuentra en la memoria caché, y, en el caso contrario, se establecerá una comunicación externa, y la petición se enviará a uno o más servidores DNS.
4. En un ambiente corporativo, si nuestra PC es parte de un dominio en red, la petición viajará hasta nuestro servidor, donde se realizará la misma consulta en la memoria caché. Con algo de suerte, nuestro compañero de escritorio ya estuvo navegando

por nuestro sitio favorito, y el servidor podrá resolver la dirección IP correspondiente.

5. Ahora, si nuestra consulta viaja por la red, la mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el ISP (Internet ServiceProvider) y, con seguridad, nuestro proveedor nos resolverá la petición por tratarse de un sitio popular y regional, para finalmente poder visitar el sitio de la comunidad RedUsers.

6. ¿Qué ocurriría si quisiéramos visitar el blog personal de un amigo, en otro idioma, y en otro país? Las caché DNS son una gran solución, pero es imposible resolver los casi 240 millones de dominios registrados de primer nivel (*Top Level Domain*), de acuerdo con el último *Domain Name Industry Brief*. Nuestro ISP difícilmente pueda resolver una petición tan poco común, y la consulta seguirá subiendo en jerarquías viajando de servidor a servidor.

7. Siguiendo con nuestro viaje, podríamos terminar en el Root Server. El servidor raíz nos proporcionará, al menos, el nombre y la dirección del servidor autorizado de la zona de más alto nivel para el dominio que buscamos. Así, el servidor del dominio nos dará una lista de los servidores autorizados para la zona de segundo nivel, hasta obtener una respuesta en algún servidor donde esté registrada la web que buscamos.



El Resumen de la Industria de Nombres de Dominio en Internet, es una manera de conocer el incremento diario de la red.

Una forma de explotar estas consultas permanentes sobre la caché podría hacerse realizando una consulta no recursiva, en la que el servidor DNS no intentará escalar la consulta, así sabremos si ya se ha solicitado la misma consulta anteriormente. Entonces, realizando consultas sobre dominios de malware conocidos, sabremos si tenemos máquinas infectadas en nuestra red.

DNS information gathering

El registro SOA (*Start of Authority*) es el registro que señaliza el inicio de autoridad e indica que este servidor DNS es la mejor fuente de información para los datos del dominio. Si un servidor DNS está mal configurado, podremos, mediante un software como **Fierce**, forzar un volcado de los registros SOA y hacer una transferencia de zona. De esta forma podríamos obtener toda la información relativa a la navegación de una empresa, cuál es su home banking, sus proveedores y registros de correos, entre otros datos relevantes.

Otra herramienta es **Dnsenum** con la que podríamos obtener mucha información relativa al dominio. La dirección del host, el nameservers (*threaded*), el registro MX, realizar consultas sobre AXFR, etc.

AXFR

AXFR o DNS zone transfer es, en simples palabras, el mecanismo que se usa para replicar lo que hay desde los DNS maestros a los DNS esclavos.

1. El servidor DNS primario manda una notificación al servidor secundario.
2. Este responde con un SOA request.
3. El servidor DNS primario responde al SOA (SOA response).
4. El secundario devuelve un AXFR request.
5. Culmina.

En la dirección web **http://root-servers.org** podemos consultar un mapa con la ubicación de los servidores raíz correspondientes.

DNS spoofing

Spoofing, en términos generales, hace referencia al uso de técnicas de suplantación de identidad. Entonces, DNS Spoofing es la suplantación de identidad por nombre de dominio. Veamos el detalle:

1. Nuestro cliente DNS (navegador) hace una petición a un servidor DNS comprometido, consultando el dominio de nuestros home bankings.

2. Este, en lugar de devolvernos la dirección IP real del dominio consultado, nos devolverá otra dirección IP.

3. En esta dirección, se alojará un sitio web que será igual al real, donde se registrará el usuario y la contraseña.

DNS Poisoning

La suplantación de identidad por nombre de dominio solo es posible por el ataque de envenenamiento de caché.

La forma más simple de mitigar o prevenir este tipo de ataque es el uso de HTTPS: así forzamos el uso de certificados digitales y, si estos no son válidos, el navegador nos alertará.

DNS alternativos

El **Google Public DNS** nació a fines de 2009, como una alternativa a los DNS que nos configura nuestro ISP, y a la fecha responde a 70 mil millones de peticiones por día. Para utilizar este servicio, debemos cambiar, en la configuración de red, las direcciones IP de los servidores DNS por **8.8.8.8** y **8.8.4.4**.

A principio de 2011, el gobierno en conflicto de Egipto tomó la drástica determinación de apagar Internet.

Al principio se observó que lo que estaba bloqueado no era la navegación, sino los DNS. Usar un servidor DNS extranjero era la solución. El de Google (**8.8.8.8**) es el más fácil de recordar y se volvió muy popular entre los usuarios.

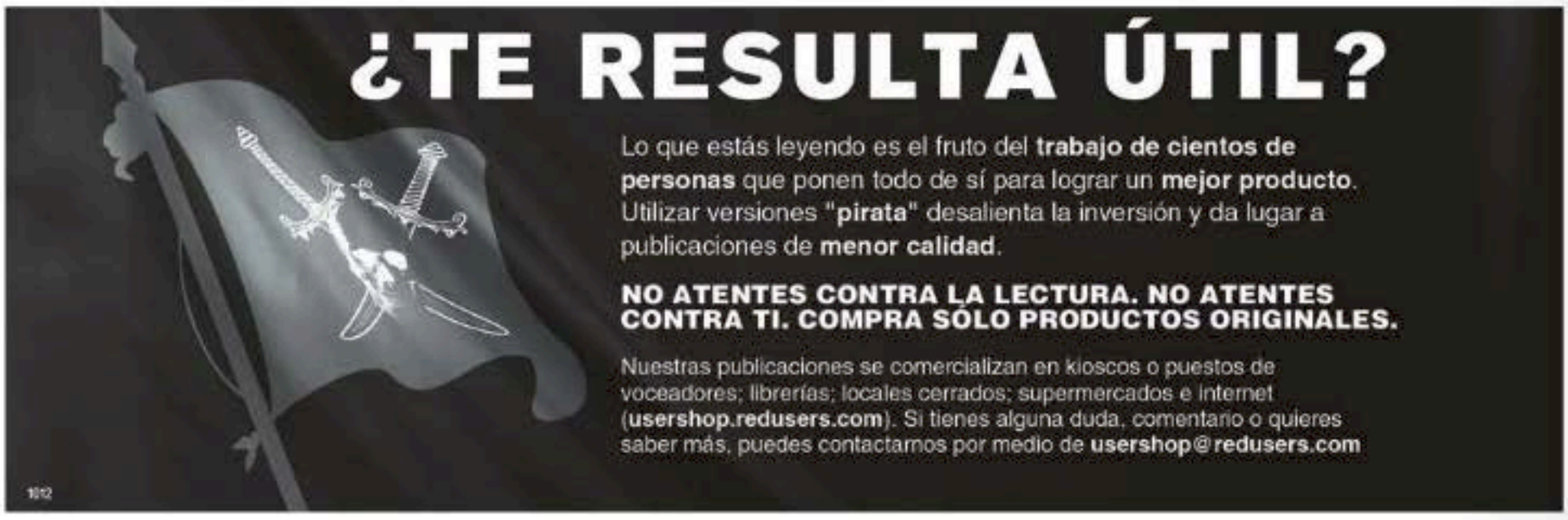
DNS Changer

DNS Changer fue descubierto en 2007. Este malware cambiaba los registros DNS locales de la PC infectada. El virus llegó a infectar a casi 900.000 computadoras y alertó al FBI, ya que peligraba la integridad de todo Internet. Se temía un apagado total. Como el código malicioso controlaba tanto tráfico de Internet, las autoridades obtuvieron una orden judicial que permitía al FBI reemplazar a los servidores donde se redirigía el tráfico, para permitir que el tráfico fluyera con normalidad, incluso desde las computadoras infectadas.

Pero ese mandato judicial expiró a mediados de 2012, y el *Federal Bureau of Investigation* dejaría de tener influencia sobre los servidores infectados.

Aun después de tantos años, se temía por las 300.000 computadoras que se estimaba todavía estaban infectadas.

El **DNS Changer Working Group** (**DCWG**) fue creado por el FBI para ayudar a los usuarios a remover por completo y de forma sencilla el **Rove Digital's malicious DNS servers**. ■



PRÓXIMA ENTREGA

10

CONFIGURACIÓN AVANZADA DE ROUTERS

En el próximo fascículo aprenderemos a establecer el correcto funcionamiento de un router. Conoceremos también conceptos tales como NAT y Port Forwarding.

Técnico en
REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00009
9 789871 857784

CONTENIDO DE LA OBRA