

La Vida tras el Cortafuegos y la "de-perimeterization"

# SIN FRONTERAS

Las empresas y las organizaciones solían sentirse a salvo detrás de los cortafuegos, pero con la llegada de las VPNs, el comercio electrónico, los servicios web y la Web 2.0, esta seguridad ha terminado. El perímetro de la red está perdiendo su significado y ha llegado el momento de adoptar una nueva solución con respecto a la seguridad. **POR JÖRG FRITSCH**

Dilezas, photocase.com

Los cortafuegos solían ser el orgullo de los departamentos de seguridad. Un cortafuegos bien diseñado protegía la red interna y debía tener diversos puertos abiertos en él. Los servidores anunciaban sus servicios a todos los integrantes de la LAN.

Esta visión en blanco y negro de la segura red interna y de la malvada red externa nunca fue tan simple como parece, ya que los ladrones de identidad y los empleados resentidos siempre han formado parte de este escenario. A pesar de ello, el sistema parecía funcionar. Sin el cortafuegos, la concepción actual de Internet, con las tiendas en línea, el banco en casa y las VPNs, sería totalmente impensable.

En las redes de hoy, los especialistas en seguridad tienen que enfrentarse al difícil problema de distinguir entre lo que se considera "dentro" y "fuera". Las nuevas fronteras están totalmente abiertas. Los accesos remotos por medio de las tecnologías VPNs, teléfonos móviles, PDAs, ordenadores portátiles, servicios web y la Web 2.0 están dejando lentamente a los cortafuegos obsoletos. En el pasado, cada aplicación del servidor poseía un puerto claramente definido y era fácilmente controla-

ble desde el cortafuegos, sin embargo, casi todos los servicios en el modelo de la web actual utilizan http/https y los puertos 80 ó 443. Este énfasis en http dificulta la tarea de identificar los servicios en el perímetro de la red.

Aunque este problema suena como una amenaza seria, algunos expertos creen que este cambio en el paradigma es una oportunidad. En vez de repetir los errores del pasado redefiniendo y extendiendo el concepto ya caducado de los cortafuegos, por qué no elaborar una solución completamente nueva de seguridad que se ajuste lo mejor posible a la realidad de las redes actuales.

El Foro de Jericho [1] es una organización internacional de seguridad dedicada a anticipar una nueva visión de la seguridad en las redes. En el centro de esta visión se encuentra el concepto que denominan de *de-perimeterization*, que echa por tierra la visión tradicional de las redes como un espacio finito con un interior, un exterior y un perímetro. De acuerdo con el foro de Jericho, las amenazas a las que se enfrentan las redes de hoy son tan extensas y variadas que "... La única estrategia de seguridad fiable consiste en proteger la información por sí misma, en

vez de la red y el resto de la infraestructura TI".

El foro de Jericho es un grupo de expertos en ISM (Gestión de la Seguridad de la Información) afiliados al Open Group [2], una organización formada por la unión de la Open Software Foundation [3] y la X/Open Limited. Open Group es famoso por sus especificaciones sobre UNIX y otras iniciativas.

Open Group registró el término "Boundary-less Information Flow" como marca para referirse al hecho de que las redes modernas no deberían depender de los límites de su perímetro para su protección. (De acuerdo con fuentes no oficiales, era necesario registrar este término como una marca para evitar que los fabricantes la utilizaran de forma indebida con propósitos comerciales o publicitarios sin cumplir realmente los principios que engloba).

Esta visión de una red segura sin fronteras se encuentra comprendida en los "Mandamientos" del foro de Jericho, disponible en PDF en la página web del foro de Jericho (véase el cuadro titulado "Mandamientos").

Los mandamientos son una colección de principios sobre seguridad, algunos de los cuales podrían considerarse consejos

de “buenas prácticas”, mientras que otros son bastante radicales y nuevos. El trabajo del foro hace especial énfasis en cuatro

áreas: cifrado; protocolos seguros, sobre todo SSL/TLS; sistemas seguros y autenticación y autorización a nivel de datos.

El concepto de protección de datos por sí mismo, en vez de simplemente restringir el acceso a la máquina que contiene los

## Mandamientos

La visión del Foro de Jericho de la “de-perimeterization” está recogida en un documento conocido como “Los mandamientos del foro de Jericho”, que se encuentra disponible en la página del foro de Jericho (Figura 2) del sitio web del Open Group [1]. Los once mandamientos del foro de Jericho son:

### Fundamentales

1. *El alcance y el nivel de protección debería estar especificado y ser el apropiado ante el riesgo.*

- Las empresas demandan que la seguridad sea ágil y no obstruya sus operaciones además y que, sea eficiente con respecto al coste.
- Mientras que los cortafuegos perimetrales podrían continuar proporcionando protección básica en la red, los sistemas individuales y los datos necesitarán ser capaces de protegerse a sí mismos.
- En general, es más sencillo proteger un recurso cuanto más cerca se encuentre la protección proporcionada.

2. *Los mecanismos de seguridad deben ser genéricos, simples, escalables y fáciles de gestionar.*

- La complejidad innecesaria es una amenaza para la buena seguridad.
- Mientras se expanden todas las capas de la arquitectura se necesitan principios de seguridad coherentes.
- Los mecanismos de seguridad deben escalarse; desde los objetos pequeños a los grandes.
- Para ser tanto simples como escalables, los “bloques de construcción” de la seguridad tienen que ser capaces de combinarse para proporcionar los mecanismos de seguridad requeridos.

3. *Mantener el contexto según el peligro.*

- Las soluciones de seguridad diseñadas para un entorno no deberían ser transferibles para que funcionen en otro. Por ello es importante comprender las limitaciones de cualquier solución de seguridad.
- Los problemas, las limitaciones y los fallos pueden venir desde distintas fuentes, incluyendo las geográficas, las legales, las técnicas, la aceptabilidad del riesgo, etc.

### Sobreviviendo en un Mundo Hostil

4. *Los dispositivos y las aplicaciones deben comunicarse utilizando protocolos seguros y abiertos.*

- La seguridad por medio de la ocultación es una mala práctica; los protocolos seguros demandan revisiones abiertas que proporcionen análisis robustos y por ello una amplia aceptación y uso.
- Los requisitos de seguridad de la confidencialidad, integridad y disponibilidad (fiabilidad) deberían evaluarse y construirse dentro de los protocolos apropiados, no ser un añadido.
- La encapsulación cifrada debería usarse solamente cuando se considere apropiado.

5. *Todos los dispositivos deben ser capaces de mantener su política de seguridad en una red que no sea de confianza.*

- Una “política de seguridad” define las reglas con respecto a la protección de los recursos.
- Las reglas deben ser completas con respecto a un contexto arbitrario.
- Cualquier implementación debe ser capaz de sobrevivir en Internet; por ejemplo, no debería fallar ante una entrada de datos.

### La Necesidad de Confianza

6. *Todos los usuarios, los procesos y la tecnología deben estar declarados, así como los niveles transparentes de confianza para cualquier transacción que tenga lugar.*

- La confianza en este contexto establece un entendimiento entre las distintas partes para dirigir una transacción y definir las obligaciones de cada parte.
- Los modelos de confianza deben comprender a las personas/organizaciones y a los dispositivos/infraestructuras.
- Los niveles de confianza podrían variar según la localización, el tipo de transacción, el rol del usuario y el riesgo de la transacción.

7. *Los niveles de garantía de la confianza mutua deben ser determinables.*

- Los dispositivos y los usuarios deben ser capaces de asignar niveles de autenticación “mutua” para acceder a los sistemas y a los datos.
- Los marcos de trabajo de autenticación y autorización deben soportar el modelo de confianza.

### Identidad, Gestión y Federación

8. *La autenticación, autorización y responsabilidad deben funcionar fuera del área de control.*

- La gente y los sistemas han de gestionar los permisos de los recursos y derechos de los usuarios que no controlan.
- Debe existir la capacidad de confiar en una organización que pueda autenticar los individuos o grupos, por ello se elimina la necesidad de crear identidades separadas.
- En principio, sólo debe existir una instancia de una persona/sistema/identidad, pero la privacidad necesita el soporte de múltiples instancias o de una instancia con múltiples facetas.
- Los sistemas deben transmitir las credenciales de seguridad.
- Deben soportarse múltiples zonas de control.

### Acceso a Datos

9. *El acceso a los datos debería estar controlado por atributos de seguridad de los propios datos.*

- Los atributos pueden encontrarse en el interior de los propios datos (DRM/Metadata) o en un sistema separado.
- El acceso y la seguridad podrían implementarse por medio del cifrado.
- Algunos datos podrían tener atributos “públicos, no confidenciales”.
- Los accesos y los derechos de acceso poseen una componente temporal.

10. *La privacidad de los datos (y la seguridad de cualquier recurso de gran valor) requiere una segregación de las funciones y de los privilegios.*

- Los permisos, las claves, los privilegios, etc, deben controlarse de forma independiente o siempre habrá una debilidad en la cima de la cadena de confianza.
- Los accesos de los administradores deben también estar sujetos a estos controles.

11. *Por defecto, cuando se almacenan los datos, se transmiten o se utilizan deben tener la protección apropiada.*

- Eliminar las opciones por defecto debe ser un acto consciente.
- La alta seguridad no debería estar forzada: la “apropiación” implica la variación de los niveles con algunos datos potencialmente no seguros.

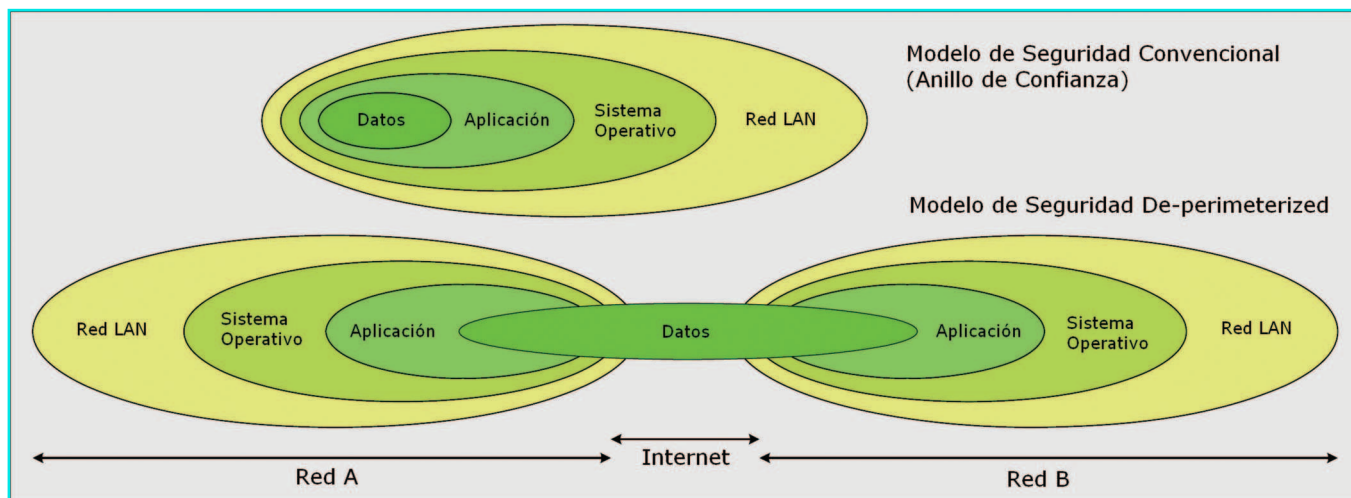


Figura 1: Los modelos de seguridad convencionales intentan salvaguardar los distintos componentes entre sí. El modelo tradicional denominado "Anillo de Confianza" (arriba) asegura cada anillo con respecto a los demás. El modelo "de-perimeterization" (abajo), supone que los datos son independientes del contexto y no deben depender de las aplicaciones, el sistema operativo o la protección de la red.

datos, es una característica fundamental de esta nueva solución. Otro principio de esta realidad "de-perimeterized" es que no hay *ninguna* red que sea de confianza. Cada dispositivo debe ser capaz de defenderse a sí mismo, incluso cuando se encuentre en Internet.

La Figura 1 muestra un esquema de esta nueva visión de red independiente de los datos. En la parte superior pueden verse los datos y la información del modelo clásico con un perímetro claramente definido. El modelo del Anillo de Confianza está diseñado para soportar la comunicación desde el lado seguro (por ejemplo, el lado más cercano al núcleo) al lado inseguro. En la parte inferior de la imagen se encuentra en nuevo modelo. Los datos existen independientemente de los límites de la red y no deben depender de la seguridad de ninguna aplicación, ordenador o red.

En un mundo perfecto, la información poseería atributos para asegurarse de que la visión y la modificación de los datos está restringida sólo a las personas autorizadas. Estos no tendrían ninguna utilidad si caen en manos equivocadas. Esta solución, a menudo conocida como IRM [4], Gestión de Derechos de la Información, consiste en algo más que el mero cifrado de los datos.

Actualmente muchos fabricantes están trabajando en marcos de trabajo que soportan directamente autenticación y autorización a nivel de datos: Oracle, EMC/RSA y Microsoft DRM por nombrar algunos. Determinadas soluciones ya están disponibles en parte, aunque frecuentemente se encuentran demasiado ligadas al modelo DRM. Por ello, es difícil decir qué tecnología se impondrá por ella misma. Las soluciones independientes no tienen

que se basa la "de-perimeterization" no deberían ser vulnerables a los ataques de secuestro de cuentas que se deben a un error mínimo de programación. Hay todavía mucho que hacer en el frente de las aplicaciones. En particular, los navegadores de Internet están constantemente saliendo en las noticias debido a sus agujeros de seguridad. Si trabaja habitualmente fuera de la oficina y se conecta con su portátil desde las habitaciones de los hoteles, o desde los establecimientos de sus clientes o desde sitios públicos como conferencias, hay que ser consciente de que la Internet actual no está muy lejos de la idea de la "de-perimeterization". Pero el peligro está al acecho en cada esquina, desde un ladrón que le robe el portátil hasta un ataque cuidadosamente premeditado contra un protocolo, aplicación o sistema. Esperemos que la "de-perimeterization" nos proporcione mejor protección que la que nos proporcionan los diversos cortafuegos, antivirus y VPNs actuales.



Figura 2: En el foro de Jericho abogan por una Internet "de-perimeterized" frente a las políticas, las prácticas, los servicios y los estándares.

sentido, ya que el objetivo de la "de-perimeterization" consiste en facilitar el flujo de la información.

Aún no se han encontrado algunos de los elementos críticos requeridos para implementar la idea de una red sin perímetro, como dispositivos terminales seguros. Aunque Linux posee una excelente reputación a este respecto, aún es demasiado vulnerable.

Los sistemas de seguridad inherentes en los

## RECURSOS

- [1] Foro Jericho: <http://www.jerichoforum.org>
- [2] Open Group: <http://www.opengroup.org>
- [3] Fundación Open Software: [http://en.wikipedia.org/wiki/Open\\_Software\\_Foundation](http://en.wikipedia.org/wiki/Open_Software_Foundation)
- [4] Gestión de Derechos de la Información de Oracle: <http://www.oracle.com/technology/products/content-management/irm/>