Análisis entorno a la tecnología de los cortafuegos para la seguridad de red perimetral

Prof. Dr. Javier Areitio Bertolín

Director del G. de I. Redes y Sistemas. Catedrático U.D.

En el presente artículo se identifica, clasifica y analiza una tecnología de seguridad de red denominada cortafuegos (ó "firewall") diseñada como protección de red perimétrica.

La utilización de los cortafuegos es clave con vistas a securizar redes corporativas que se deben conectar a Internet pero debe complementarse con algún tipo de sistema global de gestión (detección, reacción y prevención) de intrusiones para su correcta actualización y reconfiguración continuada. Así mismo puede combinarse con otras funcionalidades como anti-virus, gestión de contenidos web url, anti-spam, IPS-IDS (Sistemas de Prevención, Detección y Actuación contra Intrusiones) para formar una pasarela de seguridad ó "Security Appliance".

Definición de cortafuegos

Cuando se analiza la tecnología de los cortafuegos dentro del contexto de la seguridad de redes es necesario plantearse una serie de preguntas clave como por ejemplo las siguientes:

¿Qué es un cortafuegos?
¿Qué diferentes tipos de cortafuegos existen?
¿Para que sirven los cortafuegos?
¿Cómo se configuran los cortafuegos?
¿Qué problemas introducen los cortafuegos?
¿Qué no pueden hacer los cortafuegos?.
¿Cómo saltarse un cortafuegos?

Un cortafuegos es un dispositivo de seguridad de red diseñado para restringir el acceso a recursos (información, servicios) de acuerdo a una cierta política de seguridad basada en reglas.

Los cortafuegos no son una "solución definitiva" a todos los problemas de seguridad de red, no son una solución completa para los ataques remotos o el acceso no autorizado a los datos.

Un cortafuegos sirve para conectar dos partes de una red y controlar el tráfico (datos) que se permite que fluyan entre ellas. A menudo se instalan entre una red entera de la organización (red corporativa, intranet) e Internet. También pueden proteger departamentos mas pequeños dentro de una Intranet o también puede utilizarse entre socios corporativos o extranet.

Un cortafuegos siempre es el único camino de comunicación entre la red protegida y no protegida. A veces se pueden colocar varios cortafuegos de forma redundante en paralelo para crear tolerancia a fallos (alta disponibilidad) y balanceo de carga.

Un cortafuegos sólo puede filtrar el tráfico que pasa a través de él. Si el tráfico que puede obtener la red corporativa procede de otro conducto (por ejemplo un módem telefónico no autorizado utilizado por un empleado) el cortafuegos no puede bloquearlo.

La figura 1 muestra el esquema básico de colocación de un cortafuegos (ó "firewall") en la frontera entre una red corporativa protegida e Internet.

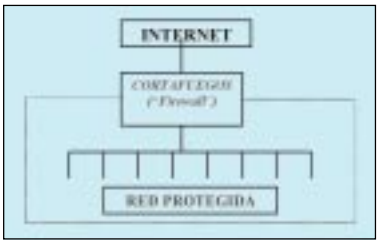

Figura 1. Esquema básico de colocación de un cortafuegos

Clasificación de los distintos tipos de cortafuegos

Existen cuatro tipos básicos de cortafuegos:

Cortafuegos de filtrado de paque-tes.- Es un router de filtrado de paquetes TCP/IP que reenvía paquetes.

Examina las cabeceras TCP / IP de cada paquete que circula a través del cortafuegos en cada dirección y filtra en función de las direcciones IP origen/destino y los números de puerto TCP / UDP origen y destino (Ej. Puerto 25 SMTP, envío de correo; 110 POP3, recogida de correo; 143 IMAP, recogida de correo; 80 http, páginas web; 443 https, páginas web seguras; 53 DNS, búsqueda de nombres; etc.

La mayor parte de los cortafuegos asume que el número de puerto define el servicio, aunque esto no siempre es cierto, ya que por ejemplo http puede tener asignado otro número de puerto distinto, por ejemplo el 8080. Utiliza reglas para especificar que paquetes se les permite atravesar el cortafuegos y cual se eliminan. Las reglas deben permitir circular los paquetes en ambas direcciones. Las reglas pueden especificar direcciones IP origen y destino y números de puerto origen y destino. Ciertos protocolos comunes, (como por ejemplo ftp) son muy difíciles de soportar de forma segura.Presentan un nivel de seguridad bajo.

Proxy de nivel de circuito.- Es un servidor proxy TCP/IP. Los paquetes se reciben y no se reenvían, el software proxy genera nuevos paquetes y estos van al destino. Es similar a un filtro de paquetes, salvo que los paquetes no se encaminan. Los paquetes TCP/IP que llegan los acepta el proxy.

Utiliza reglas que determinan que conexiones se permiten y cuales se bloquean. Las conexiones permitidas generan nuevas conexiones del cortafuegos al servidor. Presenta una especificación similar de reglas que el cortafuegos de filtrado de paquetes. El nivel de seguridad es bajo-medio.

Filtrado de paquetes "stateful".- Es un router de filtrado de paquetes TCP/IP. Es similar a un cortafuegos de filtrado de paquete, salvo que los paquetes iniciales en una dirección se

recuerdan y las respuestas se permiten automáticamente. Utiliza reglas que son mas simples que las de los filtros de paquetes.

Soporta mas protocolos del nivel 7 (smtp, http, ssh, ftp, etc) que un simple cortafuegos de filtrado de paquetes. Son filtros de paquete que entienden peticiones y respuestas como por ejemplo: TCP: SYN, SYN-ACK, ACK).

Utiliza reglas que sólo necesitan especificar paquetes en una dirección (desde el cliente al servidor - la dirección del primer paquete en una conexión). Las respuestas y paquetes adicionales de la comunicación se procesan automáticamente.

Soporta un mayor rango de protocolos que un cortafuegos de filtrado de paquetes simple (Ej. ftp, irc, H323, etc) y presenta un nivel de seguridad medio / alto.

Proxy de nivel de aplicación.- Es un servidor proxy de nivel 7. Tiene el servidor y cliente un una misma caja. Existe un proxy de nivel de aplicación para cada protocolo de aplicación soportado. (smtp, pop3, http, ssh, ftp, nntp, etc). Los paquetes se reciben y los procesa el servidor. Los nuevos paquetes los genera el cliente.

El proxy de nivel de aplicación posee una implementación completa cliente-servidor en una caja para cada protocolo que puede ser aceptado. El cliente conecta con el cortafuegos, este valida la petición y conecta con el servidor, la respuesta se devuelve a través del cortafuegos y también se procesa a través del cliente-servidor. Presenta una gran cantidad de procesado por conexión y un elevado nivel de seguridad.

En el nivel de aplicación existen: peticiones web, imágenes, ficheros ejecutables, virus, direcciones de correo electrónico, contenidos de correo, nombres de usuarios, contraseñas, etc..

Los cortafuegos de filtrado de paquetes simples y “stateful” y los proxies de nivel de circuito son como

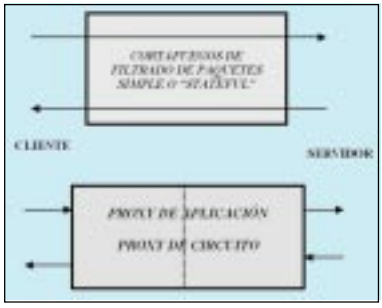

Figura 3. Esquema de los cuatro tipos básicos de cortafuegos: de filtrado de paquetes simple y “stateful”, proxy de nivel de aplicación y proxy de nivel de circuito.

barreras de llamada telefónicas por número: bloquean o permiten llamadas de móviles, llamadas internacionales, llamadas a teléfonos 806 (de “tasa premium”), llamadas procedentes de diferentes extensiones internas.

El proxy de nivel de aplicación es como un monitor de llamadas telefónicas que escucha las conversaciones las cuales pueden estar codificadas o en otra lengua.

La figura 2 muestra en dos diagramas de bloques los distintos tipos de cortafuegos agrupados en dos categorías los cortafuegos que permiten ó no el paso de paquetes y los proxy que establecen dos compartimentos para los paquetes que llegan y que salen.

Utilidad de los cortafuegos

Un cortafuegos sirve para llevar a cabo diferentes funciones:

- Controla el tráfico de red que entra y sale de la red protegida.
- Puede permitir / bloquear el acceso a servidores (tanto internos como externos).
- Puede hacer cumplir la autenticación antes de permitir el acceso a los servicios.
- Puede monitorizar el tráfico que entra / sale de la red.

Los cortafuegos normalmente defienden una red protegida contra un atacante, que intenta acceder a servicios vulnerables que no deberían estar disponibles desde el exterior de la red protegida. Por ejemplo, el servidor Microsoft Exchange que ejecuta smtp, puede ser accedido usando HTTP, FTP, SMB (Server Message Block, utilizado en la compartición de carpetas por red ente PCs). Un servidor Unix de correo electrónico o un servidor web pueden ser accedidos utilizando telnet o rlogin o ssh.

Los cortafuegos también se utilizan para restringir el acceso interno a servicios externos, por muchas diferentes razones:

- Por seguridad (no se quiere que usuarios bajen o instalen aplicaciones desconocidas)
- Por productividad (no se quiere que los usuarios malgasten el tiempo en web no relacionadas con el trabajo, etc.)
- Por coste (muchas conexiones a Internet, por ejemplo JANet se tarifican por datos transferidos, por lo tanto se debe asegurar que sean conexiones necesarias para la empresa.)

Los cortafuegos sirven para cumplir con las Leyes (Ej.: LOPD, Ley 15/1999-BOE 298 de 14/12/99 de protección de datos de carácter personal. Acta de Protección de Datos 1988 UK), el séptimo principio señala que deberían tomarse las medidas técnicas y organizativas apropiadas contra procesado no autorizado o fuera de la ley de datos personales y contra pérdida accidental o destrucción o daño a datos personales (téngase en cuenta que procesado incluye explícitamente acceso).

Configuracion de los cortafuegos

Existen dos enfoques básicos a la hora de realizar la configuración de un cortafuegos:

(1) Permitir todo el tráfico, pero bloquear protocolos TCP/IP específicos como: Irc, Telnet, snmp, etc.

El enfoque consistente en permitir por defecto y bloquear algún protocolo presenta las siguientes características:

• Fácil de cometer errores.
• Si te olvidas algo que deberías bloquear, estás permitiendo y no podrás darte cuenta por el momento.
• Si alguien halla un protocolo que se encuentra permitido, puede que no te lo diga y actúe a su favor.

(2) *Bloquear todo el tráfico, pero permitir protocolos específicos como: http, pop3, smtp, ssh, etc.*

El enfoque consistente en bloquear por defecto y permitir algún protocolo presenta las siguientes características:
• Es mucho mas seguro.
• Si se te olvida algo, alguien se quejará y podrás permitir el protocolo en cuestión.

En la configuración de un cortafuegos típico se especifica un conjunto de reglas, como por ejemplo:
• Permitir de la red interna para Internet: http, ftp, ssh, dns.
• Permitir los paquetes de respuesta.
• Permitir desde cualquier sitio al servidor de correo electrónico (sólo puerto TCP 25 smtp).
• Permitir desde cualquier sitio al servidor de correo electrónico (sólo puerto TCP 25 smtp).
• Permitir desde el servidor de correo a Internet: smtp, dns,
• Permitir desde dentro al servidor de correo: smtp y pop3.
• Bloquear todo lo demás.

El cortafuegos además de filtrar algunos paquetes es un dispositivo que puede incorporar:
• Tecnología VPN (Virtual Private Networking). Todo el tráfico pasa a través del cortafuegos. Lugar adecuado para encaminar tráfico vía VPN.
• Tecnología NAT (Network Address Translation). Las máquinas internas con direcciones privadas pueden estar ocultas detrás de una dirección pública IP. Las direcciones públicas pueden traducirse a direcciones privadas para los servidores internos. La dirección fuente siempre diferente con proxies.

Un cortafuegos sólo puede filtrar el tráfico que lo atraviesa. ¿Dónde colocar un servidor de correo electrónico?. Si requiere acceso externo para recibir correo de Internet, debería estar fuera del cortafuegos y si requiere acceso interno para poder recibir correo de la red interna, debería estar dentro. La solución es utilizar una red perimétrica (denominada DMZ, zona desmili-tarizada).

Una red perimétrica ó perimetral se utiliza para situar servidores que requieren acceso selectivo tanto de dentro como de fuera del cortafuegos. Por ejemplo: los servidores de correo, los servidores web, los servidores de nombre de dominio (DNS), los servidores ftp, etc.

Los cortafuegos pueden tener múltiples interfaces:
• Tantos como departamentos internos.
• A múltiples redes cliente, como pueden ser los ISP (Internet Service Provider).

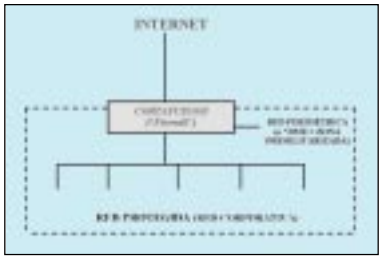

Figura 3. Esquema de una configuración de conexión de una red corporativa protegida a Internet utilizando cortafuegos y DMZ (Zona Desmilitarizada).

La figura 2 muestra la utilización de un cortafuegos y la creación de una DMZ

Problemas que plantean los cortafuegos

Los principales problemas que pueden aparecer por el hecho de utilizar cortafuegos son:
• Algunos servicios no trabajan debido a que están bloqueados. Se quejan las personas.
• Los diagnósticos de red pueden ser mas difíciles.
• La traducción NAT de direcciones de red IP puede causar confusión.
• Algunos protocolos son difíciles de soportar como: FTP, IRC, H.323.

Los cortafuegos presentan diferentes limitaciones:
• Los cortafuegos de filtrado de paquetes no proporcionan ningún filtrado basado en contenido.
• Si se permite un e-mail, entonces el correo que contiene virus se permite.
• Si se permite acceso a web, entonces se puede acceder a los sitios web pornográficos.
• Si se permite acceso a web a un navegador, entonces también se permite al código dañino Nimda.
• El tráfico cifrado no puede ser examinado ni filtrado, como por ejemplo: https, ssh.

Incluso los cortafuegos del tipo proxy de aplicación puede que no realicen verificaciones de contenido. Un número cada vez mayor de servicios que están siendo ofrecidos a través de Internet utilizan el puerto 80 TCP (http), no sólo el acceso a páginas web. Esto hace que aumente la dificultad a la hora de que los cortafuegos permitan o bloqueen acceso a diferentes servicios.

Se plantea un gran dilema: "Seguridad contra Conveniencia". Los datos cifrados son un gran problema para los cortafuegos. El cifrado se está extendiendo ampliamente para favorecer la Privacidad y aumentar la seguridad en las transacciones derivadas del Comercio Electrónico.

Protocolos como SSH, TLS, SSL, etc., son extremo a extremo, cliente a servidor. Cualquier sistema intermedio no puede decodificar los datos. Los usuarios pueden visitar sitios web desconocidos (consumiendo tiempo de negocios no productivo), se necesita control de contenidos y anti-spam para correo electrónico. Las descargas de software no pueden verificarse con antivirus.

Como saltarse a los cortafuegos

Los cortafuegos se pueden saltar de varias maneras:

- Mediante un módem u otro enlace externo. Si el tráfico no circula a través del cortafuegos, éste no puede bloquearlo.
- Mediante una mala configuración. Ej.: Permitir acceso a cualquier máquina interna o externa a través de los puertos TCP / UCP 53.
- Mediante filtrado entrante / saliente: El tráfico entrante se puede bloquear pero un enlace iniciado como saliente opera en ambas direcciones.
- Mediante túneles de protocolo (Ej. IPsec).

Supongamos que se desea enviar tráfico smtp a través de un corta-fuegos que bloquea smtp. Para ello se encuentra un número de puerto que lo permita y se ejecuta el servidor smtp externo para que escuche ese puerto. Otra alternativa es crear un VPN DIY, por ejemplo IPsec FreeS/WAN utilizando Linux. Otra posibi-lidad es crear un túnel ssh (muchos cortafuegos permiten ssh, ssh sopor-ta reenvío de puertos). Otra opción es con PPP sobre ssh (peligrosa pero efectiva).

Consideraciones sobre cortafuegos

Los cortafuegos protegen contra amenaza de red.

- No entienden de sistemas operativos ni de vulnerabilidades de aplicaciones.
- Los cortafuegos del tipo proxy de aplicación proporcionan control sobre el contenido de peticiones y respuestas.
- Presentan procesamiento complejo; el rendimiento es pobre, el coste elevado y son complicados de configurar.
- Presentan buena seguridad cuando la configuración es la apropiada.

Los cortafuegos de filtrado de paquetes y los proxy de nivel de circuito:

- Presentan alto rendimiento y bajo costo.
- Tienen un control mas tosco sobre el filtrado.
- Mas simples a la hora de especificar el tráfico aceptable.

Los cortafuegos deben estar entre los buenos y los malos. Pero qué pasa cuando la amenaza viene de dentro. Un cortafuegos es bueno para la seguridad de red, pero mucho mejor es un cortafuegos con:

- Un sistema de detección de intrusiones de red (con detectores-agentes internos y externos).
- Un sistema de detección de intrusiones de sistema de computación final (ó host) en las máquinas internas
- Aplicaciones seguras en los servidores y clientes internos.
- Contraseñas robustas en las cuentas de usuario.

Una característica importante de los cortafuegos es la seguridad balanceada. Un atacante tratará siempre de encontrar y atacar al elemento más débil del sistema de seguridad. Un cortafuegos débil proporciona seguridad pobre. Un cortafuegos fuerte necesita estar soportado por una seguridad robusta.

Ejemplos de cortafuegos y especificación de sus características

Firewall

El líder del mercado de cortafuegos es Firewall-1 de Check Point. Firewall es un cortafuegos de filtrado de paquetes "stateful". Posee algunas capacida-des de proxy y ciertas de autenticación. Es muy caro, alrededor de 10.000 Euros; Normalmente funciona bajo Windows (poco fiable, bajo rendimiento, seguridad cuestionable).

Raptor

El cortafuegos de Symantec es un proxy de aplicación. Posee algunas capacidades de filtrado de paquetes. Opera bajo Windows y es caro (10.000 Euros).

Corta-fuegos PIX

Este producto de la empresa Cisco, es un cortafuegos de filtrado de paquetes simple. De alto rendimiento y seguridad simple, es más barato que los anteriores.

Servidor SOCKS

El servidor SOCKS es un proxy de nivel de circuito. Que no se encuentra muy comúnmente. Difícil para establecer un propósito (en vez del cortafuegos de filtrado de paquetes). Tiene una seguridad muy general y no posee razones claras para servicio proxy. Presenta dificultades con algunos protocolos como por ejemplo el SSH.

Linux OS

Sistema Operativo *Linux*. Contiene filtrado de paquetes "stateful"; iptables (versión previa, ipchains no tiene "stateful"). Disponible gratuitamente.

Sistemas con interfaz GUI

Tienen un elevado rendimiento de red y un buen soporte de protocolo como por ejemplo FTP, IRC, H.323. No incorporan autenticación. No tienen balanceo de carga ni alta disponibilidad.

Aspectos finales

Una contramedida de seguridad (por ejemplo colocar un cortafuegos entre dos redes) puede tener uno o dos efectos en una amenaza:

- Puede reducir la probabilidad de que se manifieste dicha amenaza como un incidente y / o
- Puede reducir la severidad de las consecuencias que deberían ocurrir en el incidente.

Se pueden describir las contramedidas como preventivas si reducen la probabilidad y como curativas si reducen las consecuencias.

El ciclo de vida del riesgo es:
- Identificar los activos.
- Valorar los riesgos.
- Planificar y desarrollar contramedidas.
- Implementar un plan de continuidad de negocios.
- Monitorizar amenazas y gestionar vulnerabilidades.
- Detectar ataques.
- Responder a incidentes.

Uno de los decálogos de leyes (inmutables e invariantes) de la seguridad es:
- Si un atacante te persuade que ejecutes su programa en tu computadora, deja de ser tu computadora.
- Si un atacante puede alterar el SO de tu computadora, deja de ser tuya.
- Si un atacante consigue acceso físico no restringido a tu computadora, esta deja de ser tuya.
- Si tu permites que un atacante realice cargas de programas en tu sitio web, deja de ser tu sitio web.
- Las contraseñas débiles hacen fallar la seguridad fuerte.
- Una máquina de computación es sólo tan segura como lo digno de confianza que sea el administrador.
- Los datos cifrados sólo son tan seguros como la clave de descifrado (en algoritmos simétricos como IDEA/3DES/AES al menos 128 bits y en algoritmos asimétricos como RSA de 1024/2048 bits).
- Un anti-virus no actualizado es sólo ligeramente mejor que no tener anti-virus.
- El anonimato absoluto no es práctico, en la vida real ni en las web.
- La tecnología no es una panacea (ya que presenta riesgos que hay que gestionarlos). ❑

Bibliografía

(1) Areitio, J. et al. "Mecanismo de Administración y Control Remoto Transparente y de Bajo Costo para Seguridad-Auditoria Telemática". Simposio Español de Negocio Electrónico. SNE'01. Malaga. 2001.
(2) Harrington, J.L. "An Introduction to Network Security". Morgan Kaufmann. 2004.
(3) Ross, A.D., Feltman, K. and Morgan, D. M. "Network Security Essentials". John Wiley & Sons, 2003.