Identificación de la tecnología Firewall para la protección de la seguridad de red

Por: Prof. Dr. Javier Areitio Bertolín

El Dr. Javier Areitio Bertolín es Catedrático de la Facultad de Ingeniería. ESIDE. Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto.

En el presente artículo se analiza la tecnología firewall que puede ofrecer diversas funcionalidades como por ejemplo: definir las fronteras de seguridad para bloquear/permitir el acceso confiable/no confiable a los recursos internos, restringir el acceso externo, registrar las actividades de red, detectar y prevenir intrusiones y restringir que la información se transfiera a dentro o a fuera de la red o sistema protegido. Para ello inspecciona los paquetes IP, traduce direcciones IP y puertos e incluso cifra y descifra. Se trata de una de las medidas técnicas o contramedidas modernas esenciales para una defensa en profundidad en entornos de red. Esto significa desplegar varias medidas de seguridad, evitando que la seguridad sólo dependa de una única medida, por ejemplo las máquinas de computación protegidas por un firewall también deben tener los parches de seguridad actualizados, IPS, antivirus, antispam, etc. Los firewall deben colocarse no sólo en las fronteras de las redes sino también en los puntos finales como servidores, puestos de trabajo, PDAs, teléfonos móviles, etc.

Los atacantes de red suelen utilizar para realizar sus intrusiones un método formado por las siguientes fases:

- Recoger información. De sitios Web, de BDs de nombres registrados, de BDs de direcciones IP (RIPE en Europa e Internic en EEUU).
- Explorar los puertos de direcciones IP. El scanner intenta conectarse a todos los servicios deseados en todas las máquinas que pertenecen a un intervalo de direcciones concreto, el resultado es un listado de máquinas accesibles y puertos abiertos en estas máquinas. La tecnología firewall es una buena contramedida contra esta fase de los ataques.
- Enumeración de los servicios encontrados. Se trata de encontrar información acerca de los sistemas operativos, fabricantes del software y versión del software.
- Intrusión. Se buscan vulnerabilidades conocidas que no están parcheadas. Vulnerabilidades conocidas se pueden encontrar en sitios Web como securityfocus.com, secunia.com, etc. Las más recientes vulnerabilidades se publican en listas de correo como bugtraq y ntbugtraq. Los scanners de seguridad y analizadores de vulnerabilidades pueden ayudarnos en dicha tarea.
- Escalada de privilegios. Por ejemplo instalar un script que el administrador ejecute inadvertidamente, por ejemplo regedit.cmd.
- Saqueo. Robar los hashes de contraseñas, SAM bajo Windows y /etc/shadow bajo Unix. Buscar información interesante, documentos o correos electrónicos que contienen contraseñas.

POLÍTICA DEL CASO -1

- Permitir correo electrónico entrante (SMTP, puerto 25) pero sólo a nuestra máquina pasarela SIRIO. Bloquear el correo electrónico procedente del sitio Orion.

ACCIÓN	NUESTRO-HOST ORIGEN	PUERTO	SU-HOST DESTINO	PUERTO	COMENTARIO
Bloquear	*	*	Orion	*	No confiamos en esas personas
Permitir	Sirio	25	*	*	Conexión a nuestro puerto SMTP
Bloquear	*	*	*	*	Por defecto

POLÍTICA DEL CASO -2

- Permitir que cualquier computador de la red interna protegida pueda enviar correo electrónico al exterior.

ACCIÓN	NUESTRO-HOST ORIGEN	PUERTO	SU-HOST DESTINO	PUERTO	COMENTARIO
Permitir	*	*	*	25	Conexión a su puerto SMTP
Bloquear	*	*	*	*	Por defecto

CRÍTICA:

- Esta solución permite llamadas que vengan desde cualquier puerto de una máquina de dentro y se dirigen al puerto 25 en el exterior.
- La restricción definida sólo se basa en el número de puerto del *host* de fuera, que no tenemos forma de controlar.
- Un atacante puede acceder a cualquiera de las máquinas internas y puertos originando su llamada desde el puerto 25 de la máquina de fuera.

UNA SOLUCIÓN MEJOR:

ACCIÓN	NUESTRO-HOST ORIGEN	PUERTO	SU-HOST DESTINO	PUERTO	FLAG	COMENTARIO
Permitir	{nuestros hosts}	*	*	25	ACK=0	Nuestros paquetes a su puerto SMTP
Permitir	*	25	*	*	ACK=1	Sus respuestas
Bloquear	*	*	*	*		Por defecto

- El *ACK=1* significa que el paquete es parte de una conversación saliente.
- Los paquetes con *ACK=0* son mensajes de petición de conexión que sólo permitimos desde nuestros *hosts* internos.

Figura 1. Conjuntos de reglas de Firewall de filtrado de paquetes

•Eliminar posibles trazas. Modificar los logs con herramientas automatizadas. Disimular la intrusión con ayuda de rootkits (un rootkit es un paquete software que sustituye programas del sistema de modo que enmascara la presencia del atacante, similar a virus sigilosos).
•Creación e instalación de puertas traseras.

Caracterización de los Firewall

Un firewall o cortafuegos puede definirse como:
(1) Un punto de contención, de control y de monitorización para la seguridad de red. Permite la interconexión de dos o más redes con diferentes niveles de confianza (por ejemplo, una red corporativa-privada-intranet e Internet/Extranet o varias subredes con distinto nivel de protección dentro de una organización). El firewall impone restricciones en los servicios de red, de modo que sólo el tráfico autorizado es permitido. Así mismo, audita y controla el acceso, puede implantar alarmas en caso de detectar algún tipo de comportamiento anómalo. Trata de ser inmune a la penetración y proporciona una defensa perimetral. Los firewall de red se encargan de prevenir la propagación de un ataque permitiendo el tráfico autorizado.
(2) Un conjunto de programas que residen en un servidor-pasarela que se encargan de proteger los recursos de una red interna.
(3) Un dispositivo de red o un computador (host) que conecta dos o más redes.
(4) Un dispositivo capaz de monitorizar cada paquete IP para determinar si lo reenvía a su destino.
(5) Un dispositivo capaz de evaluar los paquetes con el objetivo de controlar, modificar y filtrar el tráfico de red.
(6) Cualquier sistema de seguridad que protege la frontera de una intranet contra Internet.
(7) Un componente o conjunto de componentes que restringen el acceso entre una red protegida e Internet o entre otros conjuntos de redes de modo que o bien permiten que pase el tráfico o bien bloquean el tráfico sin notificación alguna o bien rechazan el tráfico con notificación al origen. Para su cometido utilizan un conjunto pre-configurado de reglas y filtros.

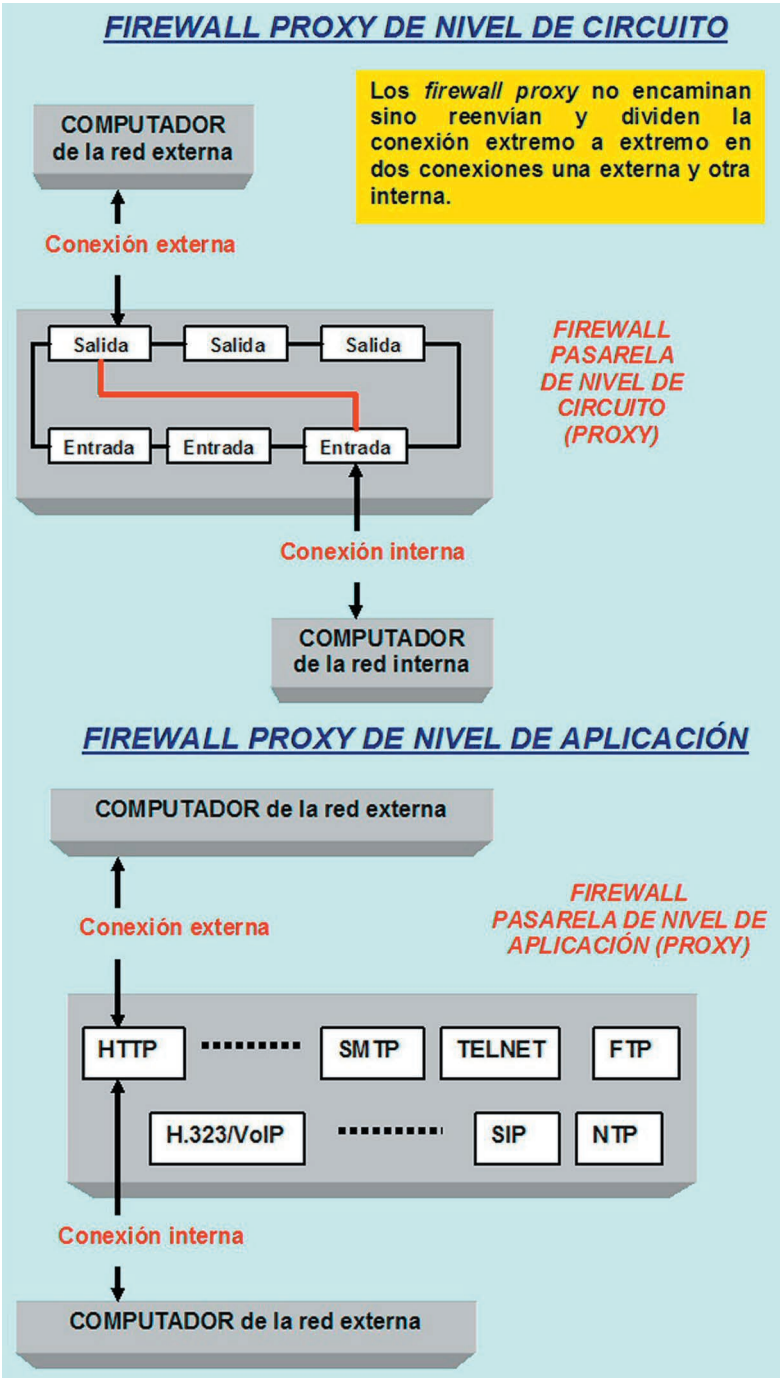

Figura 2. Funcionamiento de los Firewall proxy-gateway de nivel de circuito y de nivel de aplicación

Las principales tareas de un firewall son:

- Control de acceso basado en la dirección del emisor, del receptor o de los servicios direccionados (por ejemplo, protocolo de nivel de aplicación).
- Control de comportamiento, por ejemplo comprobar si existen virus en los ficheros entrantes.
- Control del usuario, por ejemplo autenticación basada en el origen del tráfico.
- Ocultar la red interna, por ejemplo su topología, direcciones, etc. con funcionalidades como NAT/PAT.
- Registrar en un log el tráfico que pasa.
- Hacer cumplir una política de seguridad, por ejemplo de control de acceso.
- Registrar en un log la actividad de red, permitiendo una auditoria con generación de estadísticas.

Clasificación de los Firewall. Arquitecturas con bastión y Multi Homed Proxy.

Los firewall se pueden clasificar en función de diferentes criterios, por ejemplo si los caracterizamos por el nivel de protocolo que controlan, se pueden identificar cuatro categorías:

(1) Firewall. Suelen soportarse en un router o dispositivo de encaminamiento L3. El filtrado ayuda a limitar el tráfico a los servicios útiles. Puede realizarse en base a diversos criterios: direcciones IP origen y destino, protocolos TCP, UDP, ICMP, IGMP y números de puertos, flags TCP (SYN, ACK, RST, FIN), opciones de IP y TCP, tipo de mensaje ICMP, etc. El filtrado de direcciones origen puede prevenir ataques del tipo IP spoofing. El filtrado de flags permite definir la dirección en la que puede establecerse la conexión de transporte, por ejemplo, si deseamos impedir que los clientes externos realicen conexiones TCP con clientes internos de una red corporativa pero nos interesa permitir a los clientes internos conectarse con el exterior se debería bloquear los segmentos TCP entrantes cuyo flan ACK = 0. Los firewall de filtrado de paquetes pueden clasificarse en dos categorías atendiendo a si tienen o no memoria:

- Stateless (sin memoria). No recuerdan los paquetes que ya han pasado.
- Stateful (con memoria). Mantienen una traza de los paquetes que han pasado, reconstruyen cada estado de la conexión o incluso ciertos protocolos. Observan las peticiones salientes para que sepa qué tráfico entrante permitir.

Los firewall stateful pueden analizar protocolos de aplicación como SMTP, prohibiendo ciertos comandos que puedan ocultan cierta información, como por ejemplo el comando: "220***2***200**22***0***00" También puede prohibir comandos de otros protocolos de aplicación como el put del FTP. Los firewall stateful que operan con conexiones TCP, saben para cada conexión, cual es el siguiente paquete que debería aparecer con sus flags y números de secuencia. Pueden eliminar los paquetes que no concuerdan con el contexto anterior, pueden reemplazar números de secuencia y pueden prevenir ataques DoS tipo syn-flooding.

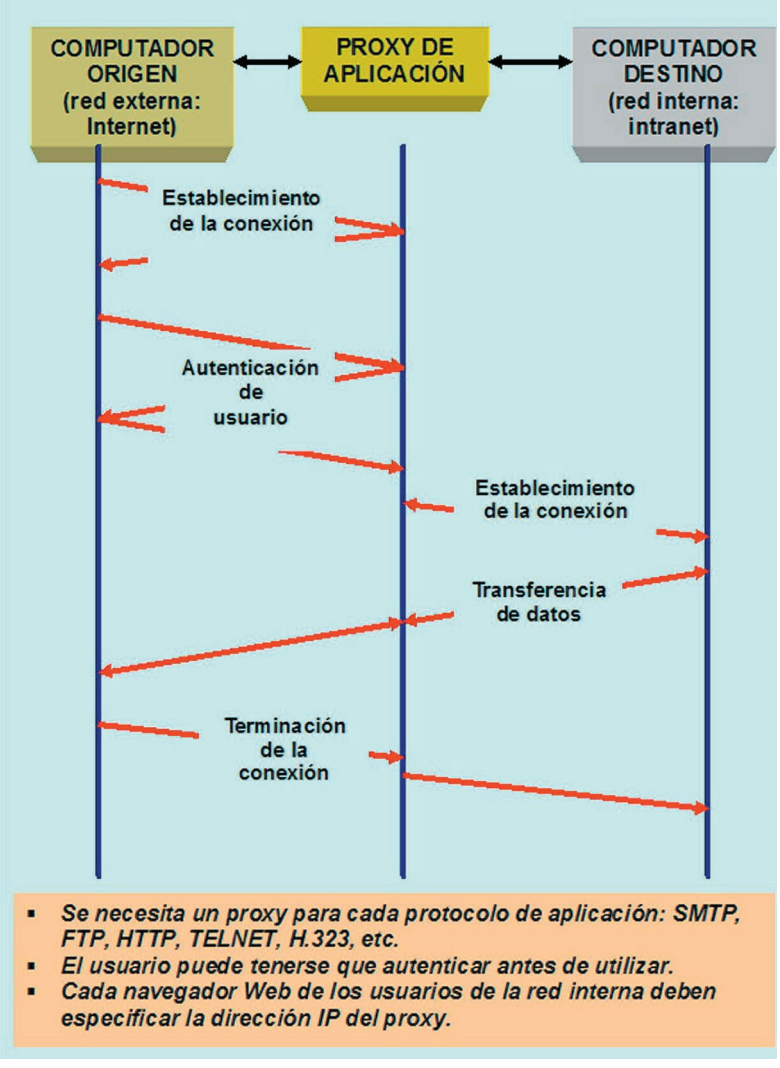

Figura 3. Funcionamiento de un Firewall tipo servidor proxy de aplicación

(2) Firewall tipo pasarelas o proxy de nivel de circuito o bastión.
(3) Firewall tipo pasarelas o proxy de nivel de aplicación o bastión o Dual Homed Host Proxy o Tri-homed gateway.
(4) Firewall del filtrado dinámico de paquetes o firewall de inspección con estados que son una combinación de las anteriores. Son los más comunes, proporcionan buena protección y una gran transparencia, posibilitan un gran control sobre el tráfico y capturan semánticas de una conexión.

Si el criterio utilizado es su naturaleza, podemos identificar:

•Firewalls basados en hardware de propósito especial, incluyen un núcleo de sistema operativo extremadamente recortado y resistente a ataques, por ejemplo PIX de Cisco con IOS, Juniper, WatchGuard, Sonicwall.

•Firewalls basados en hardware de propósito general, por ejemplo un PC con software firewall como Firewall-1 de Checkpoint, IP-tables de Linux, IPcop.

•Firewall personales, son de naturaleza software (se venden en CD) y se cargan sobre puestos de trabajo (desktop, PCs portátiles, PDAs, teléfonos móviles, etc.) así como también sobre servidores. La máquina sobre donde se ejecutan sólo dispone de un interfaz de red activo. Un firewall personal es una aplicación o módulo del sistema operativo que filtra paquetes a nivel de computador. Los firewall software filtran en base a llamadas a proceso: Firefox u Opera, pop-up de diálogo en intentos de conexiones. No son eficaces si el computador tiene comprometida su seguridad (esta infectado). Los firewall personales se caracterizan por controlar el acceso a un único dispositivo, no a una red confiable. Algunos ejemplos son Kerio, ZoneAlarm, Norton Internet Security de Symantec, ipchains, Firewall XP de Windows (este firewall no puede bloquear algunos tipos de paquetes ICMP), etc. Los firewall personales ponen obstáculos a que se puedan escanear los puertos de un computador con herramientas como Nmap (http://www.insecure.org/nmap) genérica para varias plataformas de sistema operativo, Superscan específico para Windows (http://www.webattack.com/get/superscan.shtml), así como NetCat y Cryptcat (http://www.farm9.com; http://www.securityportal.com).

•Firewall basados en hardware del tipo security appliance multi-funcional o UTM (Unified Threat Management), pueden soportar además de firewall, antivirus, IDS/IPS, VPN, DHCP, VPN, DNS, filtrado URL, antispam, etc. incorporan núcleos de sistema operativo exentos de servicios no necesarios.

Los firewall software que se ejecutan sobre sistemas operativos de propósito general, heredan todas las vulnerabilidades del sistema operativo sobre el que se ejecutan. Las arquitecturas firewall software son bien conocidas y es más fácil explotar sus vulnerabilidades, por ejemplo del tipo buffer overflow.

Un firewall de filtrado de paquetes puede desplegarse utilizando tres interfaces, uno para conectarse con la red interna a proteger, el segundo con la red externa no segura y el tercero con la DMZ (Zona Desmilitarizada) una red perimetral donde puede situarse un computador bastión, esta arquitectura se denomina basada en bastión de protección. Un computador bastión es una máquina de computación muy segura, potencialmente expuesta a elementos hostiles y securizada para resistirse posibles ataques. Tiene inhabilitados todos los servicios no necesitados, lo cual

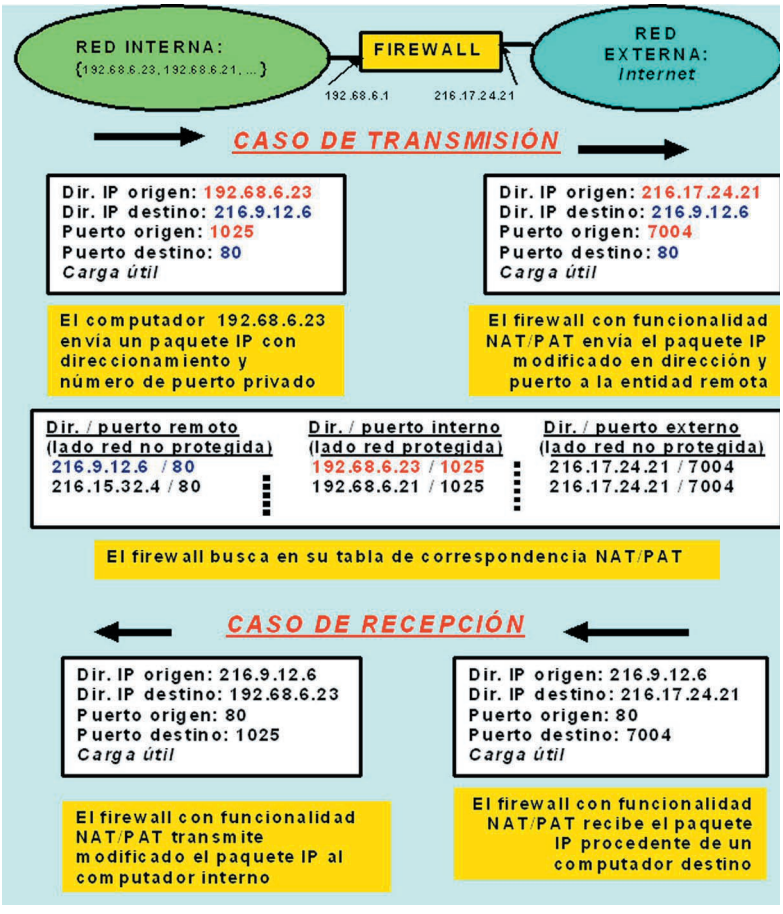

Figura 4. Funcionamiento de la funcionalidad NAT/PAT simétrica en un Firewall para ocultar la red interna

la hace simple y con pocas vulnerabilidades. Realiza la separación de conexiones de red, de modo que las conexiones entrantes que vienen de la red no segura pasan primero por el firewall y van a parar al computador bastión, el cual separa la conexión entrante y establece una conexión adicional con el dispositivo de la red protegida correspondiente; análogamente los dispositivos de la red protegida se conectan con el bastión para poder salir al exterior. El bastión ejecuta software de firewall de nivel de circuito y aplicación, instalando y modificando los servicios que se precise; también proporciona servicios accesibles externamente. Esta arquitectura puede modificarse utilizando dos firewall de filtrado de paquetes uno exterior conectado a Internet y otro interior en conexión con la red interna, entre ambos la red perimetral donde se sitúa el bastión que hace de intermediario en todas las comunicaciones entrantes y salientes. En la DMZ se deben situar el servidor ftp anónimos, el RAS (Servidor de Acceso Remoto, su función es dar servicio PPP dial-up a una batería de módems para PSTN), el servidor Web públicos, el servidor de correo electrónico público SMTP, el servidor DNS, el servidor VPN; pero sería una insensatez colocar el servidor de BD SQL de información privada de la empresa, el servidor de la impresora común de la intranet, el controlador principal de dominio o PDC, el servidor Web de la intranet, el servidor SMTP de correo electrónico de la intranet o los puestos de trabajo o desktop de la empresa. Entre dos redes, una protegida y otra insegura como Internet, se puede colocar una máquina proxy del tipo Dual Homed Proxy, el resultado es una arquitectura firewall basada en Dual Homed Host Proxy.

Firewall de filtrado de paquetes.

Un firewall de filtrado de paquetes es un dispositivo simple y muy rápido. Utiliza información del nivel de red y del nivel de transporte:
(i) Direcciones IP origen y destino.
(ii) Números de puerto TCP y UDP origen y destino. El puerto TCP 23 hace referencia a Telnet
(iii) Tipo de mensaje ICMP (como petición/respuesta de eco, destino no alcanzable, expiración del TTL, etc.) que se encapsula en los paquetes o datagramas IP.
(iv) Flags TCP (SYN, ACK, FIN, RST, PHS, etc.).

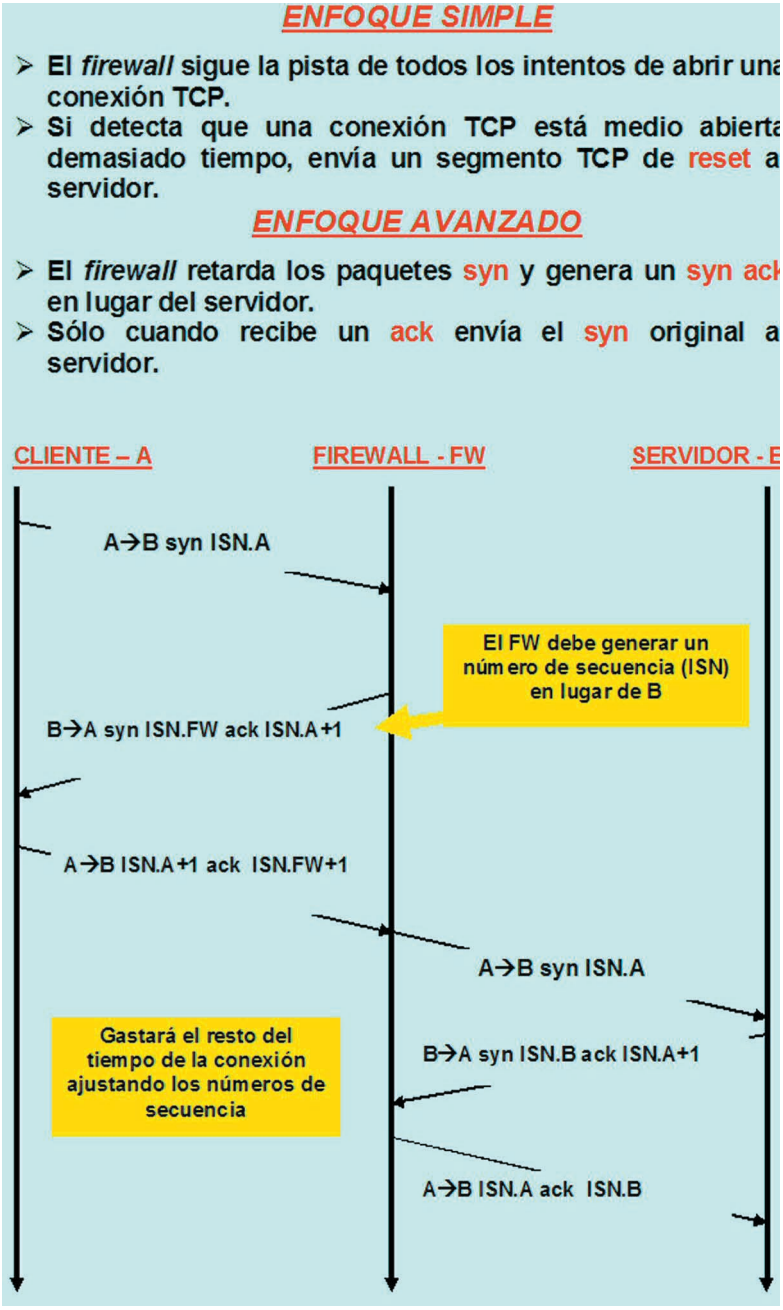

Figura 5. Dos enfoques de protección que proporcionan un firewall stateful contra ataques DoS tipo Syn-flooding contra un servidor B

(v) Protocolo encapsulado: TCP, UDP, RTP, ICMP, IGMP, etc. El valor 17 corresponde al protocolo transportado UDP. Por ejemplo, DNS utiliza el puerto 53; un firewall puede impedir paquetes entrantes al puerto 53 salvo los procedentes de servidores confiables conocidos. LDAP utiliza los puertos TCP 389 y 636.

Dos posibles usos de un firewall de filtrado de paquetes:

- Filtrar empleando los interfaces de entrada o de salida, por ejemplo, filtrado entrante de direcciones IP falsificadas o bien filtrado de tráfico saliente por ejemplo de un troyano.
- Permitir o denegar ciertos servicios, requiere un conocimiento de la utilización de puertos TCP o UDP en un conjunto de sistemas operativos desplegados.

Para configurar un firewall de filtrado de paquetes:
(i) Se comienza con una política de seguridad.
(ii) Se especifica los paquetes permitidos en términos de expresiones sobre los campos del paquete.
(iii) Se reescribe las expresiones en la sintaxis que soporte el fabricante.
(iv) Como regla general, utilizar el mínimo privilegio (todo lo no expresamente permitido esta prohibido), si no se necesita algo se elimina. Un firewall lo configura inicialmente un administrador de seguridad y puede ser reconfigurado bien por un administrador o bien por un IDS/IPS en caso de un ataque rápido.

Los firewall de filtrado de paquetes presentan como principales características en relación a su seguridad y rendimiento las siguientes:
(a) Posibilidad de falsificación de direcciones IP o spoofing IP. Se falsifica la dirección IP origen de un paquete para hacer creer que viene de un sitio confiable.
(b) Ataques basados en fragmentos pequeños. Se divide la información de la cabecera TCP en varios paquetes pequeños, se puede optar por descartarlos o reensamblarlos antes de comprobar.
(c) Degradación que depende del número de reglas aplicadas en un punto.
(d) Ordenar las reglas para que el tráfico más común sea tratado en primer lugar.
(e) La corrección es más importante que la velocidad.

Algunos criterios utilizados en la numeración de puertos es la siguiente:
(i) Conexiones TCP. El puerto servidor suele ser un número menor que 1024. El puerto cliente se numera por encima de 1024.
(ii) Los puertos menores de 1024 se asignan permanentemente, por ejemplo, el 20-21 para FTP, el 23 para telnet, el 25 para el servidor SMTP, el 80 o bien el 8080 para HTTP, el 123 para el servidor NTP, 22 para SSH, el 88 para Kerberos,

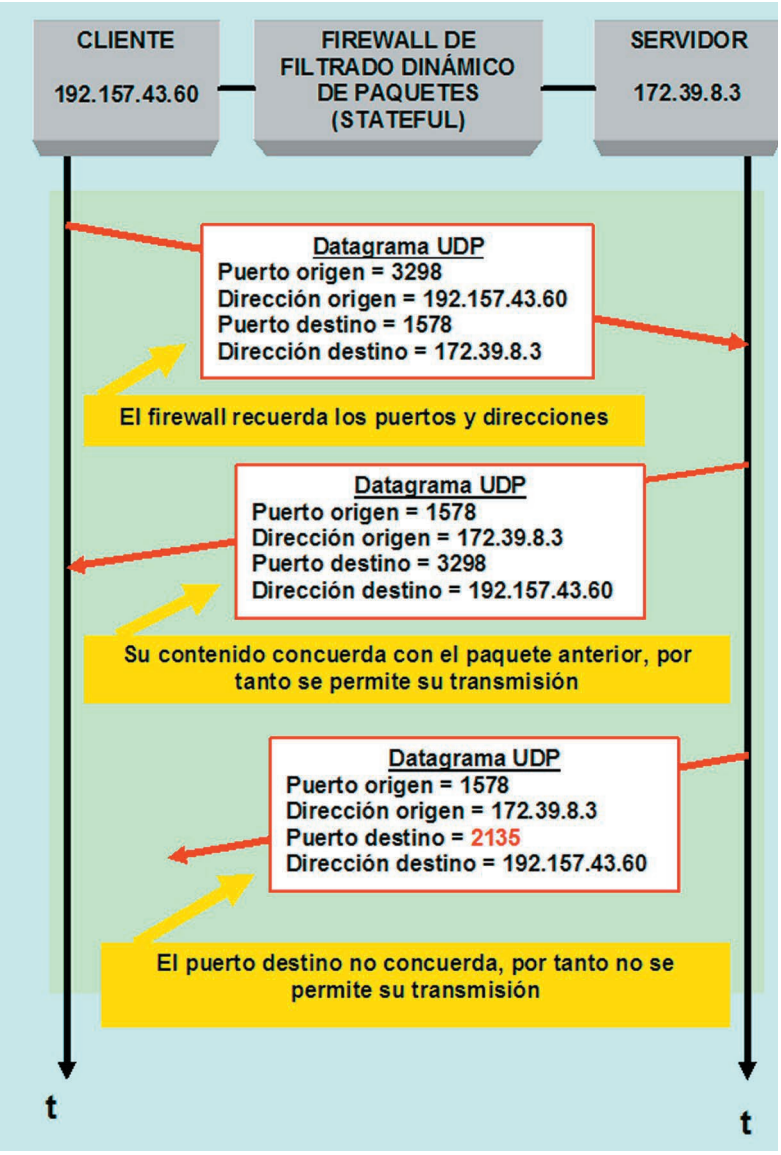

Figura 6. Funcionamiento de los firewall de filtrado dinámico de paquetes con memoria (stateful) actuando sobre un flujo de paquetes IP encapsulando datagramas UDP.

ORIGEN	DESTINO	PUERTO	PROTOCOLO	ACCIÓN	RAZÓN
*	*	53	UDP	Permitir	Petición DNS
Exterior	Interior	123	UDP	Permitir	Acceso NTP
*	*	69	UDP	Bloquear	No permitir TFTP
Exterior	*	513	TCP	Bloquear	No permitir RLOGIN desde el exterior

Figura 7. Reglas de un firewall de filtrado de paquetes.

el 110 para POP3, el 143 para IMAP (recuperación de correo electrónico), el 443 para HTTPS, el 139 para Netbios.

(iii) Uso variable. Los puertos mayores de 1024 deben estar disponibles para que el cliente pueda realizar sus conexiones. Esto presenta una limitación para los firewall de filtrado de paquetes stateless. Si el cliente desea utilizar el puerto 2048, el firewall debe permitir el tráfico entrante a este puerto. La mejor solución es utilizar firewall de filtrado de paquetes stateful que permite conocer las peticiones salientes. Por ejemplo, el puerto 3306 se utiliza para conectarse con un servidor MySQL, el servidor X11 escucha en el puerto 6000. Si necesitamos bloquear todos los flujos entrantes y salientes UDP y las conexiones telnet, deberemos establecer una regla firewall con el campo de protocolo igual a 17 (UDP) y como puertos origen y destino 23 (telnet).

Los firewall de filtrado de paquetes sin memoria o stateless no permiten un examen del contexto del nivel superior, es decir no comparan los paquetes de vuelta con el flujo saliente. Los firewall de filtrado de paquetes stateful examinan cada paquete IP en contexto, mantienen la pista de las sesiones cliente-servidor, comprueban cada paquete con legitimidad si pertenece a un contexto concreto. Por tanto, pueden detectar mejor los paquetes IP fraudulentos fuera de contexto.

Si el servidor de correo electrónico smtp de una intranet posee como dirección IP 137.123.19.43 sobre el puerto 25 se pueden definir reglas de firewall como:

(1) Denegar desde cualquier dirección IP y puerto a la dirección IP 137.123.19.43 y puerto 25.
(2) Permitir desde la dirección IP 137.123.19.43 y puerto 25 a cualquier dirección IP y puerto. Con estas reglas el servidor de correo electrónico puede enviar correos electrónicos a todos, pero a nadie se le permite enviar correos al servidor de correo electrónico.

Firewall tipo Pasarela-Proxy: de nivel de circuito y aplicación.

Firewall de filtrado de paquetes	<u>*VENTAJAS*</u>: • Cada paquete se inspecciona sin tener en cuenta los demás paquetes de la misma conexión (simplicidad). • El filtrado de paquetes se realiza en los niveles de red y transporte de la arquitectura TCP/IP, el tiempo que se requiere para procesar un paquete es mucho más rápido (velocidad). • No es necesario configurar a los clientes (transparentes al usuario). • Son menos caros. • El escalado es mejor que el de otro tipo de *firewalls*. El costo de procesamiento es menor. • Son independientes de la aplicación. <u>*INCONVENIENTES*</u>: • La definición de las reglas puede ser una tarea muy compleja. • No soportan autenticación de usuario. • No pueden prevenir ataques que utilicen vulnerabilidades específicas de las aplicaciones. No examinan los datos de la capa de aplicación. No pueden bloquear comandos específicos de la aplicación. • Son vulnerables a ataques de falsificación de direcciones IP. El intruso transmite paquetes desde el exterior con una dirección origen IP perteneciente a un computador interno. Como contramedida se puede descartar cualquier paquete con una dirección origen interna si el paquete viene de una interfaz externa. • Vulnerable a ataques de fragmentación de paquetes. Normalmente la decisión de filtrado se basa en el primer fragmento del paquete. El intruso utiliza la opción de fragmentación para crear pequeños fragmentos de modo que la cabecera TCP se encuentre en un fragmento separado.
Firewall de inspección con estados	<u>*VENTAJAS*</u>: • Muy poco impacto en el rendimiento de la red (muy rápidos). • Independientes de la aplicación y transparentes a los usuarios. • Más seguros que los *firewall* básicos de filtrado de paquetes. Determinan el estado de la conexión entre los puntos finales. • Tienen capacidades de registro en *log*. <u>*INCONVENIENTES*</u>: • Las reglas y filtros son más complejos de establecer, comprobar y gestionar. • Permite una conexión directa entre dos puntos finales (similar al *firewall* básico de filtrado de paquetes).
Firewall gateway de aplicación	<u>*VENTAJAS*</u>: ▪ No permite conexiones directas entre computadores internos y externos. ▪ Puede analizar comandos de aplicación de los paquetes de datos. ▪ No encamina entre las redes interna y externa. Oculta la topología de la red interna (similar a NAT/PAT). ▪ Soporta autenticación de nivel de usuario. ▪ Soporta registro en *log* en el nivel de aplicación. ▪ Quizás el *firewall* más seguro. <u>*INCONVENIENTES*</u>: ▪ Puede tener un impacto significativo en el rendimiento de red. ▪ Cada protocolo de aplicación requiere su propia aplicación proxy (HTTP, SMTP, FTP, H.323, ...). ▪ Vulnerable a algunos ataques *DoS* (*Denial of Service*) ▪ No escalan bien.

Figura 8. Ventajas e inconvenientes de los distintos tipos de firewall

Los firewall del tipo pasarela, gateway o proxy, ejecutan un conjunto de programas proxy. Los proxies filtran los paquetes entrantes y salientes, todo el tráfico entrante se dirige al firewall, así mismo, todo el tráfico saliente parece provenir del firewall. La política de control de acceso se encuentra embebida en los programas proxy. Se pueden identificar dos clases de firewall proxies:

(1) Firewall pasarela/proxy de nivel de aplicación. Se encuentran personalizados para los distintos servicios del nivel de aplicación como HTTP, FTP, SMTP (correo electrónico), DNS (Domain Name System), NTP, etc. Los firewall de filtrado nivel de aplicación como también se denominan, presentan un acceso completo al protocolo, el usuario solicita servicio al proxy, éste valida la petición como legal y luego tienen lugar las acciones de devolver resultados al usuario. Son necesarios proxies separados para cada servicio, por ejemplo SMTP (correo electrónico), NNTP (News Usenet: Network News Transfer Protocol), DNS (Domain Name System), NTP (Network Time Protocol), NFS (Network File System), finger (información sobre personas), SNMP, Messenger, etc. los servicios personalizados a medida generalmente no se soportan. Hace cumplir la política para protocolos específicos, por ejemplo explora virus en SMTP, necesita entender archivos comprimidos como zip, codificaciones como MIME, etc. Los proxies de aplicación pueden ejecutar políticas sobre protocolos de aplicación, como por ejemplo validar las cabeceras de correo electrónico smtp, pueden filtrar URLs, pueden inspeccionar malware. Existen dos tipos de proxy:

- Proxies clásicos. Los clientes tienen que conectarse primero al proxy.
- Proxies transparentes. Los proxies interceptan los paquetes IP del cliente y establecen una conexión con el servidor remoto. Siempre debe haber un proxy por aplicación. Un proxy general puede que no funcione adecuadamente (seguro) para aplicaciones específicas o no bien conocidas. El Toolkit de Firewall TIS puede utilizarse para construir proxies personalizados a medida.

(2) Firewall pasarela/proxy de nivel de circuito. Operan en el nivel TCP y dividen las comunicaciones extremo a extremo, haciendo que el proxy sea el intermediario que se encargue de retransmitir dos conexiones TCP. Impone seguridad limitando lo que se les permite a dichas conexiones. Una vez creadas normalmente retransmite sin examinar los contenidos. Normalmente se utilizan los firewall de nivel de circuito cuando los usuarios confiables de la red interna se les permiten conexiones salientes. Los proxy de nivel de circuito retransmiten los contenidos de dos conexiones TCP, una interna a la pasarela y otra de la pasarela al exterior. Puede filtrar dinámicamente paquetes, por ejemplo fragmentación IP (los flujos se reensamblan en el proxy). El filtrado dinámico permite a los paquetes de puertos del servidor a cualquier puerto del proxy. Normalmente registra las conexiones, puertos y número de bytes. Ejemplos de este tipo de firewall son SOCKS un "drop-in replacement" para la API TCP, reemplaza las llamadas al sistema con llamadas SOCKS equivalentes, WinSOCK es un proxy casi genérico para Microsoft.

Métodos para reconocer la existencia de un Firewall.

Los atacantes utilizan diversos métodos para reconocer la existencia de firewalls en una red:

(1) Traceroute. Lista los routers en el camino hasta el destino con lo cual se pueden monitorizar las posibles direcciones IP de algunos firewalls. El campo TTL se decrementa al pasar por cada dispositivo L3, cuando llega a cero se devuelve un mensaje ICMP de TTL expirado. Se puede enviar a un firewall petición de eco ICMP, paquetes UDP o TCP.

(2) Análisis del paquete de respuesta. Se trata de comparar las respuestas de puertos abiertos y cerrados. El paquete IP a un puerto cerrado, si da prohibido pone de manifiesto la existencia de un firewall.

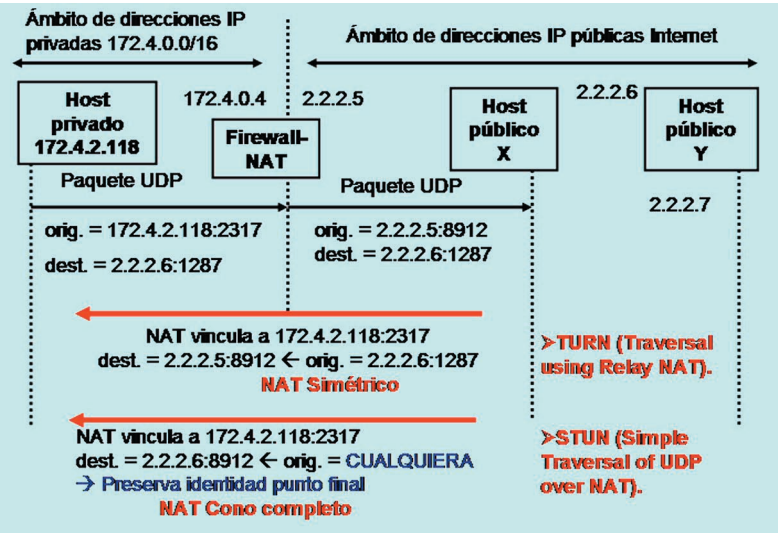

Figura 9. Comparativa entre firewall con funcionalidad NAT simétrico (TURN) frente a NAT cono completo (STUN)

(3) Exploración de puertos del firewall para intentar identificar el tipo de firewall, versión del sistema operativo, fabricante, etc.

Posibilidades y limitaciones de los Firewall.

Los firewall permiten bloquear muy diversos ataques por red como inundación ICMP, ataques DoS del tipo syn flood, ataques basados en opciones IP (por ejemplo encaminamiento desde el origen), ataques spoofing IP, ping of death, win nuke, tear drop, nestea, fragmentación igmp, smurf (utiliza la dirección IP de difusión de la subred. La mejor estrategia contra ataques smurf es bloquear en el firewall los pings entrantes a direcciones de difusión), land, puede bloquear un virus embebido en un correo entrante, puede prevenir un ataque online de diccionario de contraseñas desde una red externa en el puerto telnet de una máquina interna, puede prevenir que usuarios externos exploten un bug de seguridad en un script cgi sobre un servidor Web interno (el servidor Web sirve peticiones procedentes de Internet), puede prevenir que un usuario de una red externa abra una ventana en un X-server de la red interna (por defecto un X-server escucha las conexiones en el puerto 6000).

Entre las principales limitaciones de los firewall se pueden identificar:

(1) Rendimiento limitado. Se puede solucionar utilizando conexiones en paralelo que permite balanceo de carga y fail-over.

(2) No pueden prevenir todo tipo de ataques DoS.

(3) La administración puede ser complicada y puede ser difícil configurarlos adecuadamente.

(4) Son inútiles contra ataques de dentro de la red protegida. Los atacantes pueden existir dentro de una intranet corporativa, el código malicioso o malware puede ejecutarse en una máquina de computación interna.

(5) Las organizaciones con mayores amenazas de dentro, son los bancos e instalaciones del ejército.

(6) La protección debe existir en cada uno de los niveles, se debe valorar los riesgos de las amenazas en cada nivel.

(7) No se puede proteger contra la transferencia de todos los programas o ficheros infectados de virus debido al enorme conjunto de tipos de ficheros (.com, .exe, .bat, .sh, .elf, .pl, .prc, .doc, .xls, .bin, .mdb, .img, .ppt, .vbs, .msg, .vba, .ole, .htm, .ini, .smm, .xmi, . class, .hta, .php, .xml, .dat, .hqx, etc.) y de sistemas operativos.

La autenticación multi-factor incluye los siguientes métodos:

(1) Algo que uno sabe (PIN, contraseña, frase de paso).

(2) Algo que uno tiene (tarjeta inteligente, llave criptográfica USB).

(3) Algo que uno es (biometría estática: huella dactilar, iris/retina o biometría dinámica: como firma manuscrita o tecleas o hablas o caminas).

(4) Algo que uno puede hacer (CAPTCHA, teclear el valor mostrado en una imagen que se representa deformada).

(5) Donde se encuentra y cuando, especificando algún lugar y tiempo (control de acceso espacio-temporal; para ello se utilizan trazadores de coordenadas geográficas basados en GPS y de marcación de tiempos). Un IPS presenta FPR (False Positive Rate) = (Número de falsos positivos / Número de eventos normales) y FNR (False Negative Rate) = (Número de falsos negativos / Número de intrusiones), donde los falsos negativos son intrusiones que no generan alarma. Algunas direcciones IP como 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0 son declaradas por el IANA privadas y no pueden utilizarse para enviar paquetes a Internet. Un firewall de nivel de aplicación puede analizar el campo de datos buscando patrones (cadenas de caracteres) peligrosos, por ejemplo, un paquete IP puede contener su cabecera IP de 20 bytes sin opciones y en su carga útil, un segmento TCP con el puerto 80 y en su carga útil un patrón HTTP como el siguiente: GET/song.mp3 HTTP/1.1 User-Agent: Kazaa.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto LEFIS-APTICE (financiado por Socrates 2005-2007. European Commission.

Bibliografia

- Areitio, J. "Análisis en torno a la auditoria de seguridad en tecnologías de la información y las comunicaciones". Revista Española de Electrónica. Nº 625. Diciembre 2006.
- Areitio, J. "Tipificación de amenazas, identificación de contramedidas de seguridad en el ámbito de la gestión de redes y sistemas". Revista Española de Electrónica. Nº 613. Diciembre 2005.
- Areitio, J. "Identificación y análisis de la tecnología de detección y prevención de intrusiones". Revista Española de Electrónica. Nº 615. Febrero 2006.
- Areitio, J. "Identificación de la gestión de red y su implicación con la seguridad". Revista Española de Electrónica. Nº 620/621. Julio/Agosto 2006.
- Oppliger, R. "Internet and Intranet Security". Artech House. 2007.
- Buchanan, W.J. "The Handbook of Data and Networks Security". Springer. 2007.
- Reese, R. "Network Security". John Wiley & Sons, Inc. 2007.
- Forouzan, B.A. "Network Security". McGraw-Hill. 2007.
- Hurley, W. "Self-Defending Networks: Rules of Engagement for Active Network Security". O'Reilly Media. 2006.