Cortafuegos. Comparativa entre las Distintas Generaciones y Funcionalidades Adicionales

José María Morales Vázquez
Versión 1.1
Puedes recoger la última versión de este documento en:
http://jo.morales0002.eresmas.net/fencasa.html

Programa de Postgrado UNED – Curso 2001/2002
Departamento de Ingeniería Eléctrica, Electrónica y de Control E.T.S. de Ingenieros Industriales de la UNED
Curso de Experto Universitario en Seguridad y Comercio Electrónico
e-mail: josemaria.morales@hispalinux.es

Resumen: TCP/IP es, a pesar de sus orígenes seudo-militares, un protocolo inseguro. Hoy por hoy, la mejor forma de protección contra las vulnerabilidades derivadas de este protocolo es el uso de un dispositivo Cortafuegos. Además, un Cortafuegos ayuda a mitigar otros problemas asociados a sistemas inseguros y vulnerables proporcionando robustez y una forma ideal de implementar una férrea Política de Seguridad y de Auditoría que controle los accesos a nuestros sistemas. Existen diversos tipos de Cortafuegos y esquemas de protección derivados que son asociados a distintas generaciones que han ido apareciendo a medida que la tecnología de los mismos ha ido evolucionando. En este documento se pretende realizar una clasificación de los mismos atendiendo, fundamentalmente, a su forma de integrarse en el modelo OSI y, en particular, en la pila de protocolos TCP/IP.

0 Índice.

1 Introducción.

Los primeros dispositivos cortafuegos aparecieron en la mitad de la década de los 80. Desde esos primeros Cortafuegos que implementaban simples y rudimentarios filtros de paquetes hasta los actuales dispositivos capaces de analizar simultáneamente la actividad en múltiples capas de la red, la tecnología ha evolucionado mucho creando herramientas más sofisticadas y más seguras. La popularización de Internet ha originado múltiples problemas de seguridad hasta el punto en que, hoy por hoy, esta inseguridad inherente a la red es, según todos los expertos, el principal obstáculo para el éxito de las actividades de Comercio Electrónico. El Cortafuegos se ha convertido, de esta forma, en un dispositivo indispensable dentro de la arquitectura de cualquier red de ordenadores que tenga acceso a Internet.

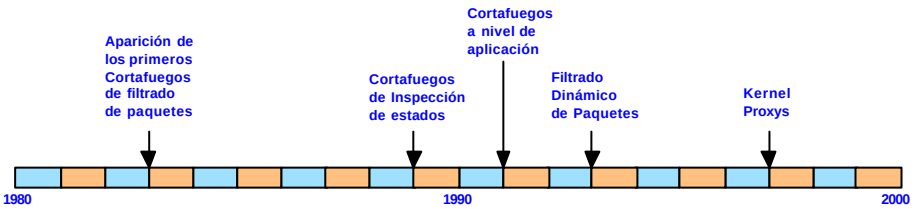

Fig. 1. Eje Cronológico de la Evolución de los Cortafuegos.

Este documento presenta información sobre los distintos esquemas usados por los dispositivos cortafuegos en la actualidad. Nos centramos en el, sobre todo, en la integración que realizan dentro del modelo OSI y la forma en que interactúan con los protocolos de la familia TCP/IP. Su propósito es informativo y la finalidad perseguida es tratar de aclarar la forma de actúar de los distintos modelos para que conozcamos en que pueden ayudarnos y cual es el Cortafuegos ideal de acuerdo a nuestras necesidades.

Aunque en algunas ocasiones es bastante difícil traducir términos que no son habituales, se ha tratado en todo momento de utilizar nominativos en castellano para los dispositivos y tecnologías comentados en este documento. No obstante, para evitar la dificultad que supone, en muchas ocasiones, identificar términos que estamos tan acostumbrados a ve en inglés, se cita siempre al menos una vez el término anglosajón más comúnmente usado. Las siglas se utilizan siempre en su terminología inglesa (VPN en lugar de RPV para referirnos a las Redes privadas Virtuales o IDS en lugar de SDI para los Sistemas de Detección de Intrusos).

La organización del documento es como sigue:

En el capítulo 2 se hace una breve semblanza para tomar conciencia de las debilidades inherentes a TCP/IP y de cuales de ellas puede defendernos un cortafuegos.

El capítulo 3, corazón de este documento, está dedicado a discutir las diferencias existentes entre los principales tipos de cortafuegos existentes en el mercado.

El capítulo 4 enumera y describe brevemente algunos de los servicios adicionales que incluyen los modernos cortafuegos y que nos pueden proporcionar evidentes ventajas en la protección y administración de nuestra red.

El capítulo 5 pretende mirar hacia el futuro de los cortafuegos: si su principal razón de ser es la debilidad de TCP/IP en su versión actúal ¿ desaparecerá su razón de ser cuando se generalice el uso de IPSec e IPv6 ?

Por último, el capítulo 6 recoge las conclusiones que hemos tratado de sumarizar en este documento y el capítulo 7 ofrece multitud de documentación, en su mayor parte disponible libre y gratuitamente en la red, para quien desee ampliar los temas aquí tratados.

2 Seguridad en la Familia de Protocolos TCP/IP.

A pesar de que la familia de protocolos TCP/IP fue desarrollada inicialmente para el Departamento de Defensa de los Estados Unidos, existen en ella un número considerable de graves problemas de seguridad que son inherentes al protocolo e independientes del nivel de corrección de cualquier implementación. El hecho de que un host confíe en algo tan vulnerable como la dirección IP que viene escrita en un paquete como única autenticación de la procedencia de dichos datos, los casi inexistentes mecanismos de autenticación asociados a los protocolos de rutado o la falta de mecanismos que garanticen la confidencialidad y la integridad de los datos que viajan a través de una red son claros ejemplos de ello.

Algunos de estos problemas pueden ser solventados mediante el uso de un cortafuegos. Los cortafuegos, junto con los antivirus, constituyen hoy en día la herramienta de seguridad más efectiva y ampliamente extendida a nivel corporativo (y crece poco a poco a nivel doméstico gracias a la proliferación de cortafuegos personales) y se revela como el único mecanismo de seguridad verdaderamente efectivo para protegernos de estas vulnerabilidades intrínsecas al protocolo TCP/IP.

Los principales riesgos de una organización con salida a Internet son los mismos que debemos tener en cuenta a la hora de proteger un sistema cualesquiera: confidencialidad, integridad, autenticidad y disponibilidad. Los siguientes son los ataque más frecuentes y populares que vulneran estos principios:

- Rastreadores o *Sniffers.*
- Suplantaciones de IP o *Spoofing*.
- Ataques de contraseñas
- Control de salida de ilegal información sensible desde una fuente interna.
- Ataques de Hombre en el medio (o *man-in-the-middle attacks*).
- Ataques de Denegación de Servicio, *Denial of Service* o ataques DoS.
- Ataques a nivel de aplicación para explotar vulnerabilidades conocidas.
- Caballos de Troya (*Trojan Horses*), Virus y otros códigos maliciosos.

2.1 ¿De que Puede Protegernos un Cortafuegos?

El nivel de protección que puede darnos un cortafuegos depende en gran medida, de nuestras necesidades. Imaginemos, por ejemplo, que nuestra única necesidad es recibir y entregar correos electrónicos. Un cortafuegos puede defendernos efectivamente de cualquier ataque que no vaya dirigido a este servicio.

Generalmente, los cortafuegos se configuran para protegernos contra cualquier intento de acceso desautorizado o no correctamente autenticado desde el exterior hacia el interior de nuestra red, o viceversa.

Pero, adicionalmente, uno de los puntos más importantes a tener en cuenta es que un cortafuegos nos proporciona un punto único e ineludible de acceso a nuestra red donde podemos centralizar las medidas de seguridad y auditoría sobre la misma.

2.2 ¿De que no Puede Protegernos un Cortafuegos?

Son tres las principales amenazas sobre las cuales un cortafuegos no puede protegernos. Las dos primeras son evidentes.

Un cortafuegos no puede protegernos contra amenazas que no pasan a través de el. Como decíamos en el punto anterior, el cortafuegos debe de ser el punto único e ineludible de acceso a nuestra red. Si esto no es así su efectividad es sólo parcial.

Tampoco pueden protegernos, generalmente, contra amenazas que proceden del interior de nuestra red. Un empleado malicioso, un troyano o algunos tipos de virus pueden usar mecanismos válidos 'desde dentro' para realizar acciones perniciosas.

Por último, los cortafuegos no pueden protegernos contra clientes o servicios que admitimos como válidos pero que son vulnerables. Tampoco puede protegernos contra mecanismos de *tunneling* sobre HTTP, SMTP u otros protocolos. No son muy efectivos, a pesar de que algunos fabricantes así lo anuncian, contra los virus. Los cortafuegos no pueden ni deben sustituir otros mecanismos de seguridad que reconozcan la naturaleza y efectos de los datos y aplicaciones que se estén manejando y actúen en consecuencia.

3 Cortafuegos. Generalidades, Tipos y Tecnologías Usadas por Estos.

Los cortafuegos (*firewalls* o *networtk firewalls* en la literatura anglosajona) son dispositivos o sistemas que controlan el flujo de tráfico entre dos o más redes empleando ciertas políticas de seguridad. Básicamente son dispositivos cuya funcionalidad se limita a permitir o bloquear el tráfico entre dos redes en base a una serie de reglas. Su complejidad reside en las reglas que admiten y en como realizan la toma de decisiones en base a dichas reglas.

La tecnología empleada en los cortafuegos ha ido madurando a medida que la industria especializada avanzaba y ahora tenemos una amplia variedad de dispositivos que realizan esta función de distintas formas. Una forma práctica y sencilla de comparar las bondades de cada plataforma es examinando las capas del modelo OSI (*Open System Interconnect*) donde el cortafuegos interactúa.

Fig. 2. Pila de Capas Definidas en el Modelo OSI.

La capa 1, o física, define la infraestructura tangible (medios, conectores, voltajes, etc.) necesaria para las comunicaciones.

La capa 2, o capa de enlace de datos es el nivel donde se desarrollan las comunicaciones en el interior de las LAN's (*Local Area Networks*) y es la primera en la que tenemos un espacio de direcciones a través del cual podemos identificar a una máquina determinada. Estas direcciones son asignadas a las tarjetas o interfaces de red y son llamadas direcciones MAC (*Media Access Control addresses*).

La Capa 3, o capa de red, es el nivel donde se interconectan las WAN's (*Wide Area Networks*) y en ella encontramos un segundo espacio de direcciones identificativo, conocido como direcciones IP (*Internet Protocol address*).

En la capa 4 o capa de transporte, introducimos dos nuevos conceptos útiles: sesiones y puertos. Un host puede tener abiertas cualquier número de sesiones de comunicación contra otro u otros hosts en la misma o distintas redes. Los puertos pueden verse como los puntos finales (y origen) de conexión de dichas sesiones.

Por último, las capas 5, 6 y 7 (sesión, presentación y aplicación) representan los niveles donde se desenvuelven las aplicaciones del usuario y los servicios finales de estas y para estas.

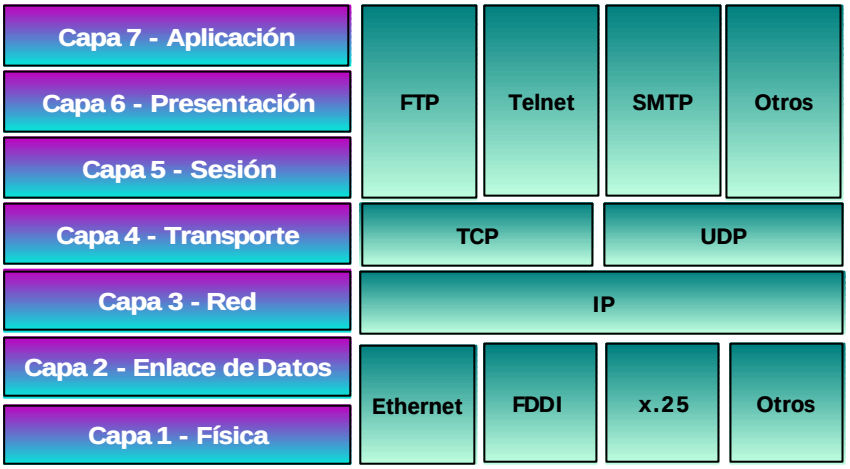

Fig. 3. Algunos de los servicios y protocolos más usados correlacionados sobre las capas del modelo OSI donde se desarrollan.

La clasificación conceptúal más simple divide los cortafuegos en sólo dos tipos:

- Cortafuegos a nivel de red (trabajan en las capas 2, 3 y/o 4).
- Cortafuegos a nivel de aplicación (trabajan en las capas 5,6 y/o 7).

Como regla general, podemos afirmar que cuanto más bajas sean las capas en las que el cortafuegos trabaja, su evaluación será más rápida y transparente pero su capacidad de acción ante ataques complejos es menor.

La industria, sin embargo, suele hacer una clasificación generacional más amplia: las dos primeras generaciones están formadas por cortafuegos de red con una diferencia fundamental entre ellas: que tengan en cuenta o no información del estado de la conexión a la hora de evaluar las reglas. La tercera generación está orientada a filtrados a nivel de aplicación y, por último, la cuarta generación vuelve al nivel de

red y está orientada al filtrado dinámico de paquetes. Incluimos un quinto apartado dedicado a los cortafuegos híbridos, última tendencia de la industria, los cuales pueden situarse simultáneamente en más de una de estas categorías.

Tenemos aún otra clasificación dependiendo del, por llamarlo de algún modo, 'acabado externo' del producto. Así, tenemos cortafuegos que son meros servicios que se ejecutan sobre sistemas operativos robustos (como IPFilter o IPTables en el mundo Linux o CISCO Centri Firewall para tecnología NT), complejas herramientas modulares que pueden instalarse en varias máquinas (como es el caso de Firewall-1 de Central Point que posee dos módulos separados: inspección y gestión), o puede tratarse de sistemas dedicados que incluyen dentro de una caja compacta el hardware, el sistema operativo y el software específico, todo ello completamente listo para trabajar (es el caso del CISCO PIX Firewall).

3.1 Cortafuegos de Filtrado de Paquetes.

El término en inglés por el que se los conoce es *Packet Filter Firewalls*. Se trata del tipo más básico de cortafuegos. Analizan el tráfico de la red fundamentalmente en la capa 3, teniendo en cuenta a veces algunas características del tráfico generado en las capas 2 y/o 4 y algunas características físicas propias de la capa 1. Los elementos de decisión con que cuentan a la hora de decidir si un paquete es válido o no son los siguientes:

- La dirección de origen desde donde, supuestamente, viene el paquete (capa 3).
- La dirección del host de destino del paquete (capa 3).
- El protocolo específico que está siendo usado para la comunicación, frecuentemente Ethernet o IP aunque existen cortafuegos capas de desenvolverse con otros protocolos como IPX, NetBios, etc (capas 2 y 3).
- El tipo de tráfico: TCP, UDP o ICMP (capas 3 y 4).
- Los puertos de origen y destino de la sesión (capa 4).
- El interface físico del cortafuegos a través del que el paquete llega y por el que habría que darle salida (capa 1), en dispositivos con 3 o más interfaces de red.

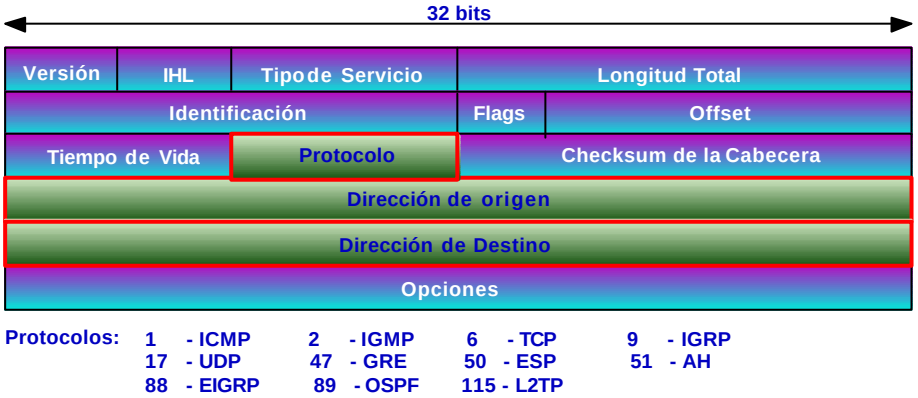

Fig. 4. Cabecera de un paquete en IPv4. En destacado los campos que habitualmente inspeccionan los Cortafuegos.

Con todas o algunas de esta características se forman dos listas de reglas: una de permitidas y otra de denegadas. La forma en que un paquete recibido se procesa en función de estas dos listas difiere según el modelo, el fabricante o el modo de actuación configurado y define en gran medida la permisividad del cortafuegos. Los más restrictivos exigen que el paquete pase con éxito por ambas listas, es decir, que no sea expresamente denegado en la una y sea expresamente autorizado en la

segunda. Otras veces existe una única lista de reglas y el paquete es procesado según la primera regla que encontramos en la tabla y define como tratarlo. Otros cortafuegos usan la última regla que encuentran como acción a efectuar. Por último, también encontramos diferencias en cuanto a que hacer cuando no se encuentra ninguna regla válida: algunos productos aceptan el paquete y otros lo rechazan. Es, pues, fundamental conocer perfectamente el modo de trabajo del equipo que nos ocupa en cada momento.

En la siguiente tabla tenemos un pequeño ejemplo de una de estas últimas listas de reglas en la que el cortafuegos posee la dirección IP 192.168.1.1:

	Dirección de origen	Puerto de origen	Dirección de destino	Puerto de destino	Acción	Descripción
1	Cualquiera	Cualquiera	192.168.1.0	>1023	Aceptar	Permite que pasen los paquetes de retorno de una conexión originada en la red interna.
2	192.168.1.1	Cualquiera	Cualquiera	Cualquiera	Rechazar	Previene conexiones directas del cortafuegos con otro host.
3	Cualquiera	Cualquiera	192.168.1.1	Cualquiera	Rechazar	Previene de accesos directos desde hosts externos al cortafuegos.
4	192.168.1.0	Cualquiera	Cualquiera	Cualquiera	Aceptar	Permite acceso al exterior sin restricciones a los usuarios internos.
5	Cualquiera	Cualquiera	192.168.1.2	SMTP	Aceptar	Permite a los usuarios externos enviar e-mail.
6	Cualquiera	Cualquiera	192.168.1.3	HTTP	Aceptar	Permite a los usuarios externos acceder al servidor web interno.
7	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Rechazar	Cualquier regla que no haya sido previamente definida es explícitamente denegada.

Tabla 1. Ejemplo de Lista de Reglas de un Cortafuegos por Filtrado de Paquetes.

Aparte de Aceptar (*Accept*) o Rechazar (*Deny o Drop*), la mayoría de los cortafuegos de este tipo poseen un tercer tipo de acción: Descartar (*Discard* o *Stealth*). Cuando un paquete es procesado por una regla que define esta acción, este se elimina 'silenciosamente' sin devolverse error alguno al originario del mismo creando un efecto de 'agujero negro' y evitando así el cortafuegos revelar su presencia.

Las principales bondades de este tipo de cortafuegos están en su rapidez, transparencia y flexibilidad. Proporcionan un alto rendimiento y escalabilidad y muy bajo coste, y son muy útiles para bloquear la mayoría de los ataques de Denegación

de Servicio, por ello se siguen implementando como servicios integrados en algunos routers y dispositivos hardware de balanceo de carga de gama media-alta.

Sus principales inconvenientes son su limitada funcionalidad y su dificultad a la hora de configurarlos y mantenerlos. Son fácilmente vulnerables mediante técnicas de *spoofing* y no pueden prevenir contra ataques que exploten vulnerabilidades específicas de determinadas aplicaciones, puesto que no examinan las capas altas del modelo OSI. La información almacenada en los logs de accesos es tan imprecisa como los parámetros usados en la configuración de su lista de reglas (direcciones de origen, de destino, puertos, protocolos, interfaces de red, etc.) y la complejidad en la construcción de reglas hace que deban de ser configurados por expertos conocedores del protocolo y que sean muy susceptibles a los errores.

No son, pues, efectivos como medida única de seguridad, pero si muy prácticos como primera barrera, en la que se bloquean ciertos ataques, se filtran protocolos no deseados y se pasan los paquetes restantes a otro cortafuegos que examine las capas más altas del protocolo.

3.2 Cortafuegos con Inspección de Estado.

Los cortafuegos de segunda generación, llamados con cortafuegos con inspección de estado, o *Stateful Inspection Firewalls* o *Circuit Level Firewalls*, son básicamente cortafuegos de filtrado de paquetes en los que, además, se valida a la hora de aceptar o rechazar un paquete el hecho de que este sea una petición de nueva conexión o pertenezca a un circuito virtual (o sesión) ya establecido entre un host externo y otro interno.

Cuando una aplicación crea una sesión TCP con un host remoto, se establece un puerto en el sistema 'originario' de la conexión con objeto de recibir allí los datos provenientes del sistema remoto. De acuerdo a las especificaciones de TCP, este puerto del host cliente estará comprendido entre el 1023 y el 16.384. En el sistema remoto se establecerá, asimismo, un puerto que será siempre menor al 1024.

Los cortafuegos por filtrado de paquetes deben de permitir tráfico entrante en todos los puertos superiores (1023 hasta 16.384) para permitir los datos de retorno de las conexiones salientes. Esto crea un gran riesgo de intrusiones. Los cortafuegos con inspección de estado resuelven eficazmente este problema construyendo una tabla con información correspondiente a todas las sesiones TCP abiertas y los puertos que utilizan para recibir los datos y no permitiendo el tráfico entrante a ningún paquete que no corresponda con ninguna de estas sesiones y puertos.

Para hacer esto, los cortafuegos de este tipo examinan rigurosamente el establecimiento de cada conexión (en la capa 4 del modelo OSI) para asegurarse de que esta es legítima y está permitida. Los paquetes no son remitidos a su destino hasta que el establecimiento de la conexión ha sido correctamente completado y verificado.

El cortafuegos mantiene una tabla de conexiones válidas (en la que se incluye información del estado de cada sesión) y deja pasar los paquetes que contienen información correspondiente a una entrada válida en dicha tabla de circuitos virtuales. Una vez que la conexión finaliza la entrada en la tabla es eliminada y el circuito virtual entre los dos hosts es cerrado.

Las tablas de estado de circuitos virtuales suelen contener, por cada conexión, la siguiente información:

- Un identificador de sesión único asignado por el cortafuegos a cada conexión establecida.
- El estado de la conexión: negociándose (*handshake*), establecida o cerrándose. (capa 4)
- El número de secuencia del último paquete (capa 4).
- La dirección IP origen de los datos (capa 3).
- La dirección IP destino de los datos (capa 3).
- La interfase física de red, si procede, a través de la que los paquetes llegan (capa 1).
- La interfase física de red, si procede, a través de la que los paquetes salen (capa 1).

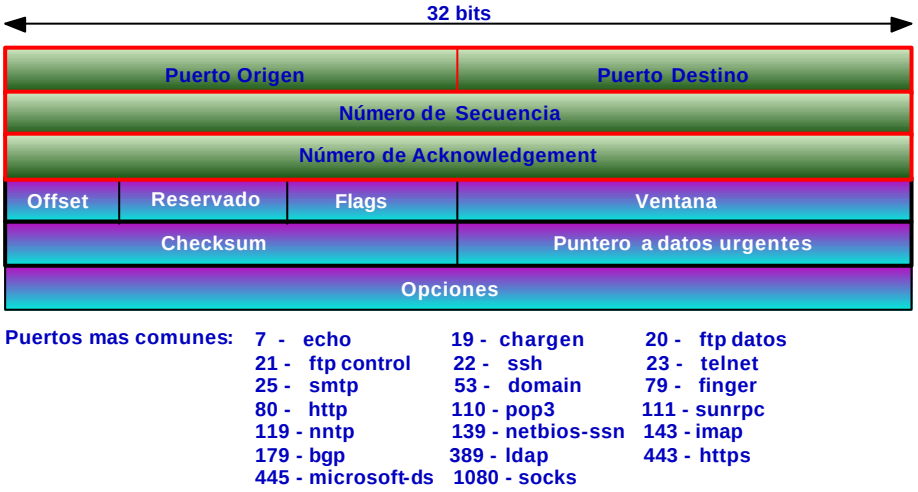

Fig. 5. Cabecera TCP. En destacado los campos que habitualmente inspeccionan los Cortafuegos.

Usando esta información y con un ligero escrutinio de las cabeceras de los paquetes, el cortafuegos es capaz de determinar cuando un paquete es válido y cuando no lo es. Una vez que la conexión es establecida, el resto de los paquetes asociados con ella son rutados sin mas comprobaciones. Esto los haría, de base, tremendamente vulnerables a ciertos tipos de ataques, pero muy pocos cortafuegos de este tipo son tan

rudimentarios. Sobre esta base, y aprovechando la gran velocidad y consistencia que supone la misma, se realizan otro tipo de verificaciones para, por ejemplo, asegurarnos que no ha habido suplantamiento (*spoofing*), que no existen paquetes malformados, etc. También son comunes en ellos la implantación de sistemas de translación de direcciones, NAT, que ocultan eficazmente el interior de nuestra red a intrusos externos.

Las principales ventajas de este esquema de salvaguardas son la velocidad de filtrado, la solidez de sus principios de cara a establecer una política de seguridad y, en conjunto con un esquema de traslación de direcciones, la sólida protección adicional a las direcciones IP internas.

Sus principales debilidades residen en su limitación estrictamente al escrutinio del protocolo TCP, la imposibilidad de chequear protocolos de niveles altos, las limitaciones inherentes a su mecánica de actuación a la hora de llevar un registro de sucesos y la imposibilidad de implementar algunos servicios de valor añadido, como realizar cacheado de objetos http o filtrado de URL's (puesto que no 'entienden' estos protocolos).

3.3 Cortafuegos a Nivel de Aplicación.

Como su nombre indica, esta generación de cortafuegos evalúa los paquetes realizando una validación en la capa de aplicación (capa 7) antes de permitir una conexión manteniendo, al igual que hacen los cortafuegos de inspección de estado, un riguroso control del estado de todas las conexiones y el número de secuencia de los paquetes. Adicionalmente, este tipo de cortafuegos suelen prestar, dado su emplazamiento en la capa 7, servicios de autenticación de usuarios.

La práctica totalidad de los cortafuegos de este tipo, suelen prestar servicios de Proxy. Tanto es así que a menudo se identifican biunívocamente unos con otros. Un Proxy es un servicio específico que controla el tráfico de un determinado protocolo (como HTTP, FTP, DNS, etc.), proporcionando un control de acceso adicional y un detallado registro de sucesos respecto al mismo. Los servicios o agentes típicos con que cuentan este tipo de dispositivos son: DNS, Finger, FTP, HTTP, HTTPS, LDAP, NMTP, SMTP y Telnet. Algunos fabricantes proporcionan agentes genéricos que, en teoría, son capaces de inspeccionar cualquier protocolo de la red, pero lógicamente, usarlos le resta robustez al esquema y facilita a un intruso la labor de establecer un túnel (*tunneling*) a través de el.

Los agentes o servicios Proxy están formados por dos componentes: un servidor y un cliente. Ambos suelen implementarse como dos procesos diferentes lanzados por un único ejecutable. El servidor actúa como destino de las conexiones solicitadas por un cliente de la red interna. El cliente del servicio proxy es el que realmente encamina la petición hacía el servidor externo y recibe la respuesta de este. Posteriormente, el servidor proxy remite dicha respuesta al cliente de la red interna. De esta forma estamos creando un aislamiento absoluto impidiendo una

comunicación directa entre la red interna y la externa. En el diálogo entre cliente y servidor proxy se evalúan las peticiones de los clientes de la red interna y se decide aceptarlas o rechazarlas en base a un conjunto de reglas, examinando meticulosamente que los paquetes de datos sean en todo momento correctos. Puesto que son servicios hechos a medida para el protocolo que inspeccionan, tenemos un control total y un registro de sucesos al más alto detalle.

En el siguiente gráfico podemos ver un ejemplo de cómo se desarrolla la comunicación antes descrita:

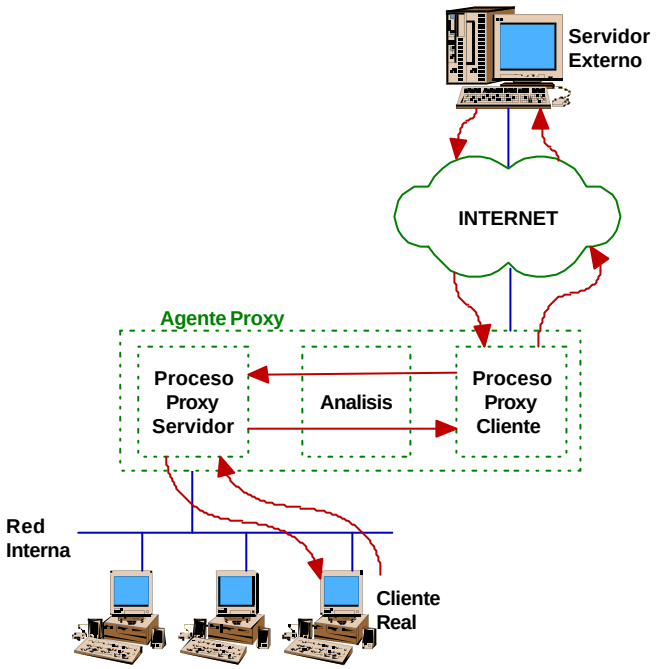

Fig. 6. Cómo trabaja un servicio Proxy.

Las principales ventajas de este tipo de cortafuegos son sus detallados registros de tráfico (ya que pueden examinar la totalidad del paquete de datos), el valor añadido que supone tener un servicio de autenticación de cara a securizar nuestra red, y la casi nula vulnerabilidad que presentan ante ataques de suplantación (*spoofing*), el aislamiento que realizan de nuestra red, la seguridad que proporciona la 'comprensión' a alto nivel de los protocolos que inspeccionan y los servicios añadidos, como caché y filtro de URL's, que prácticamente todos implementan.

Entre los inconvenientes están sus menores prestaciones (en cuanto a velocidad de inspección se refiere) frente a los otros modelos ya vistos, la necesidad de contar con servicios específicos para cada tipo distinto de tráfico, la imposibilidad de ejecutar muchos otros servicios en el (puesto que escucha en los mismos puertos), la imposibilidad de inspeccionar protocolos como UDP, RPC y otros servicios comunes, la necesidad de reemplazar la pila TCP nativa en el servidor donde se ejecutan y lo vulnerables que resultan ante ataques directos al sistema operativo sobre el que se suelen ejecutar.

3.4 Cortafuegos de Filtrado Dinámico de Paquetes.

Las técnicas de filtrado dinámico de paquetes surgen como necesidad de proporcionar mecanismos efectivos de seguridad sobre el tráfico UDP. Este tipo de cortafuegos asocian el tráfico UDP con conexiones virtual. Si un paquete de respuesta se genera y envía de vuelta al peticionario original, se establece una conexión virtual y se permite al futuro paquete de respuesta atravesar el cortafuegos. La información asociada a una conexión virtual se guarda durante un periodo de tiempo muy corto y si no se recibe dicho paquete de respuesta durante este, la conexión es invalidada. Algunos modelos de este tipo de cortafuegos pueden realizan controles similares a este sobre el protocolo ICMP.

Por lo demás, estos cortafuegos se comportan exactamente igual que los de filtrado simple de paquetes, con sus mismas ventajas e idénticos inconvenientes

3.5 Cortafuegos Híbridos.

En los últimos años las fronteras entre las distintas generaciones de cortafuegos aquí expuestas se han difuminado y, cada vez en mayor medida, aparecen en el mercado productos comerciales que combinan las mejores características de dos o más de estas plataformas. Así, por ejemplo, podemos encontrar con facilidad cortafuegos a nivel de aplicación con servicios de proxy que incluyen filtrado de paquetes para inspeccionar las tramas UDP que antes le estaban restringidas.

En definitiva, la hibridación de tecnologías y la amalgama de características de los actuales productos ha potenciado las ventajas de estos equipos pero también ha complicado en gran medida la tarea de elegir cual es el cortafuegos más adecuado a nuestras necesidades.

Quizás el mejor ejemplo de esto lo representa el que es, probablemente, el cortafuegos más ampliamente utilizado a nivel empresarial hoy en día: CheckPoint Firewall-1.

Aunque está catalogado como un cortafuegos de inspección de estados, el Firewall-1 en realidades un cortafuegos híbrido que intercepta los paquetes entre las capas 2 y 3 del modelo OSI, extrae aquí la información relativa al estado de la conexión y

mantiene dinámicamente unas tablas con información sobre el estado de las conexiones abiertas o en trámites de ser establecidas. El módulo de inspección del Firewall-1 se carga dinámicamente en el núcleo (*kernel*) del sistema operativo de la máquina que lo aloja inspeccionando todos los paquetes entrantes y salientes que pasan por las interfaces de red. Ningún paquete es procesado por las capas superiores hasta que el motor de inspección verifica que cumple con las políticas de seguridad establecidas.

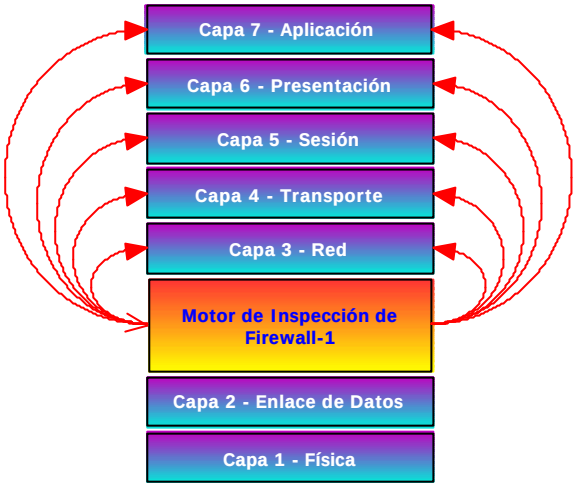

Fig. 7. Emplazamiento del Motor de Inspección del Firewall-1 dentro del modelo OSI.

Firewall-1 tiene acceso, dado su emplazamiento, a los mensajes 'en bruto' y, a diferencia de otros cortafuegos, no se limita a una somera inspección de algunos datos de las cabeceras correspondientes a su emplazamiento, sino que analiza, si así se lo indicamos, información específica referente a todas las capas situadas por encima suyo, así como la información contenida en los datos del paquete.

Para protocolos sin estado (como UDP y RPC) crea y almacena datos de contexto sobre una conexión virtual creada a tal efecto (tal y como se explica en el apartado 3,4 dedicado al filtrado dinámico de paquetes de este documento).

Otra importante funcionalidad es la de permitir ciertos comandos mientras que deshabilita otros para una determinada aplicación. Así, es posible permitir un ping ICMP mientras que se deniega un Redirect o permitir un get sobre SNMP mientras que deshabilitamos los comandos set sobre el mismo protocolo.

Posee, adicionalmente, módulos especificos para realizar inspecciones 'a medida' sobre cientos de aplicaciones, servicios y protocolos, tales como Oracle, MS SQL, RealAudio, etc.

4 Servicios Adicionales Proporcionados por los Cortafuegos.

Un valor añadido sobre los cortafuegos actuales son los servicios adicionales de que disponen y que facilitan las labores de protección y administración de la red. Se trata de servicios en algunos casos hechos a medida y en otros habituales de otros dispositivos pero que, en cualquier caso, representan un punto importante a la hora de decidirnos por una u otra implementación. En este apartado veremos brevemente algunos de ellos.

4.1. Translación de Direcciones de Red (NAT).

Los servicios de NAT (*Network Address Translation*) resuelven dos de los principales problemas de seguridad e infraestructura de las redes actuales. En primer lugar, constituyen una herramienta muy efectiva para esconder las direcciones de red reales de nuestra red interna. En segundo lugar, y debido a la reducción del espacio de direcciones IP disponibles, muchas organizaciones usan NAT para permitir la salida a Internet de sus equipos de la red interna con un mínimo de direcciones legalmente válidas (ver RFC 1918).

Existen tres estrategias diferentes a la hora de implementar NAT que veremos brevemente a continuación.

4.1.1 Translación de Direcciones de Red Estática.

En este esquema de NAT cada sistema interno de la red privada tiene su propia dirección IP exterior. Con este sistema se logra esconder el esquema interno de nuestra red, pero no la reducción de direcciones IP válidas de acceso al exterior. Los cortafuegos que incluyen esta característica usan para ello una simple tabla de correspondencia entre unas direcciones y otras.

4.1.2 Translación de Direcciones de Red Oculta.

Con este esquema todos los sistemas de la red interna comparten la misma dirección IP externa. Reviste dos importantes inconvenientes: es imposible poner a disposición de los usuarios externos ningún recurso de la red interna, y obliga al Cortafuegos a usar su propia dirección externa como sustituta de la dirección de todos los equipos que protege, con lo cual implícitamente estamos revelando la dirección del mismo y lo hacemos susceptible de ser atacado directamente, además de restarle flexibilidad al sistema.

4.1.3 Translación de Puertos.

El sistema de translación de puertos (PAT) resuelve los dos problemas vistos en el esquema anterior, convirtiéndolo en la mejor forma de implementar NAT. En primer lugar no es necesario usar la dirección externa del Cortafuegos, sino que podemos

crear otra dirección virtual para este propósito. En segundo lugar, es posible hacer accesibles recursos internos a los usuarios del exterior.

El cortafuegos usa el puerto del cliente para identificar cada conexión entrante y construye a tal efecto una tabla de translaciones como la mostrada a continuación:

Dirección IP interna	Puerto Cliente Interno	PAT
192.168.1.108	1028	3313
192.168.1.112	1039	3314
192.168.1.102	1400	3315
192.168.1.101	1515	3316
192.168.1.115	1027	3317
192.168.1.120	1026	3318

Tabla 2. Ejemplo de Translación de Puertos.

La translación de puertos se realiza de forma secuencial en algunos sistemas (como el de la tabla del ejemplo anterior) y aleatoria, dentro de un rango de puertos válidos, en otros.

Se trata, de los tres esquemas vistos, del más conveniente, flexible, seguro y por tanto el más ampliamente usado en la actualidad.

4.2 Protocolo de Configuración Dinámica de Hosts (DHCP).

DHCP, *Dynamic Host Configuration Protocol*, es un servicio de asignación automática de direcciones IP con importantes y evidentes ventajas administrativas a la hora de mantener redes de tamaño medio / amplio que muchos Cortafuegos (sobre todo los que trabajan en las capas 2, 3 y/o 4) incluyen como valor añadido.

4.3 Redes Privadas Virtuales (VPN).

Uno de los servicios adicionales más valorados de los Cortafuegos actúales es la posibilidad de construcción de Redes privadas Virtuales (VPN o *Virtual Private Networks*) que permiten extender a las comunicaciones externas la seguridad del interior de nuestra red.

Una VPN se construye en la cúspide de la pila de protocolos ya existentes en la red usando protocolos adicionales y fuertes cifrados y mecanismos de control de integridad, sustitución o repetición de la información transmitida.

Existen diferentes formas de construir una VPN. Quizás la forma más lógica y comúnmente usada es utilizar para ello el estándar IPSec., consistente en una porción de las características de seguridad de IPv6 separadas y portadas para ser usadas en IPv4. Otras opciones son el estandard propuesto por Microsoft llamado PPTP (*Point*

to Point Tunneling Protocol) o L2TP (*Layer 2 Tunneling Protocol*), propuesto por la IETF (*Internet Engineering Task Force*).

El motivo por el que se coloca el servidor de VPN en el cortafuegos es evidente: colocarlo detrás de el haría que el tráfico cifrado entrante y saliente generado por el servidor VPN no pudiese ser inspeccionado totalmente y hubiera que obviar funciones como las de autenticación, *logging*, escaneo de virus etc. sobre todo este tráfico. Colocando el servidor VPN detrás del cortafuegos lo hacemos vulnerable a ataques directos.

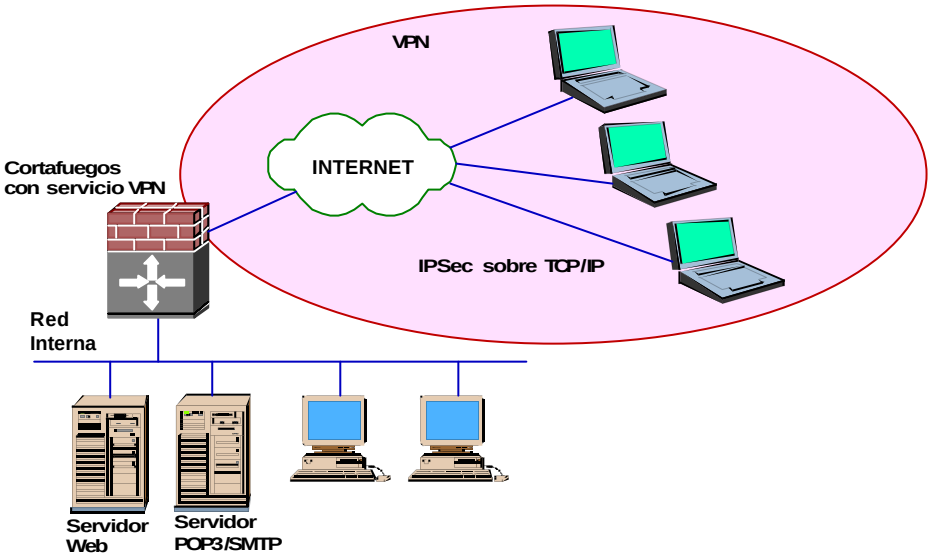

Fig. 8. Ejemplo de una Red Privada Virtual.

El principal problema de las VPN es el elevado coste de recursos que supone el cifrado completo de las comunicaciones lo cual reduce considerablemente el ancho de banda efectivo que somos capaces de tratar. Una solución para mitigar este problema es usar una tarjeta cifradora por hardware, las cuales suelen reducir en aproximadamente un 50% el tiempo necesario en realizar la encriptación.

4.4 Modeladores del Ancho de Banda o Reguladores.

Estos dispositivos, denominados *Bandwidth Shapers* o *Throttlers* en la literatura anglosajona, están adquiriendo un auge asombroso en los últimos tiempos y son ya muchas las formas en las que nos los encontramos: programas o elementos específicos o servicios de valor añadido en *routers* o cortafuegos.

Un modelador del ancho de banda se emplaza entre la red interna y la salida a Internet (el mismo lugar del cortafuegos, de ahí su inclusión en los mismos) y puede ser comparado con un 'guardia del tráfico'. Mediante reglas, se definen distintas colas, cada una de las cuales alberga un tipo distinto de tráfico: e-mails, transferencias de ficheros, tráfico http, archivos musicales o de video, etc. Cada una de las colas de tráfico posee una prioridad distinta, de forma que podemos poner en primer lugar aquellas que correspondan al tráfico más crítico para nuestra organización. El modelador realiza la distinción entre los distintos tipos de tráfico de formas muy diferentes: inspeccionando directamente las cabeceras en busca de identificar un determinado protocolo, en función de los puertos a los que son dirigidos los paquetes, etc. A veces esto no es suficiente. Un sistema bien conocido para intercambio de ficheros como edonkey usa el puerto 80 para asemejar tráfico web. Otros, como KaZaa, desobedece los estándares y usa más de un puerto simultáneamente. Para estos casos los *Shapers* usan métodos similares a los de los antivirus y buscan patrones (*signatures*) que identifican estos tráficos.

Aunque pueda parecer que estos métodos introducen más retardo que desahogo en el tráfico de la red no es así en absoluto: los *shapers* analizan, al igual que los cortafuegos con inspección de estado, sólo los primeros paquetes de una conexión y una vez que esta es identificada la asignan a una cola de tráfico en particular hasta que esta finaliza.

4.5 Inspección de Contenidos.

Es uno de los servicios adicionales más interesantes que ofrecen los Cortafuegos a Nivel de Aplicación: realizar una inspección de contenidos en el tráfico HTTP y SMTP incluyendo los siguientes elementos:

- Applets de Java
- Código ActiveX, JavaScript o CGI.
- Inspección de virus (binarios y de macro).
- Inspección del contenido de ciertos formatos ampliamente introducidos (.zip, .doc, .xls, .ppt, etc.)
- Bloqueo de contenidos en base a URL's, direcciones IP y/o palabras clave.
- Bloqueo de comandos específicos de determinadas aplicaciones.

4.6 Autenticación de Usuarios.

Otro servicio básico en los cortafuegos a nivel de aplicación es la autenticación de usuarios que en los dispositivos a nivel de red debe limitarse a la dirección IP de procedencia de la petición, con el consiguiente riesgo de suplantación, mientras que en estos pueden habilitarse servicios clásicos de combinación login / password.

4.7 Alta Disponibilidad y Balanceo de Carga.

Como hemos visto en las descripciones anteriores, uno de los principales inconvenientes de los cortafuegos es la disminución del rendimiento que provocan, efecto que se ve agravado en algunos esquemas más que en otros. Los cortafuegos empresariales de gama alta suelen ofrecer una solución para paliar este problema al mismo tiempo que ofrecen redundancia mediante el balanceo de carga entre dos o más dispositivos cortafuegos. Logramos, de esta forma, mejorar el problema del rendimiento y ofrecer alta disponibilidad y tolerancia a fallos en nuestra política de seguridad.

4.8 Integración con Sistemas de Detección de Intrusos (IDS's).

Los sistemas de detección de Intrusos son herramientas o dispositivos que nos permiten inspeccionar nuestro sistema y generar alertas que nos permitan conocer cuando alguien ha tratado de penetrar en nuestro sistema o lo ha conseguido. Se trata de una tecnología relativamente nueva y en un grado aún bajo de madurez, pero que va ganando cada vez más importancia y mejores resultados. Existen dos tipos de sistemas IDS los de hosts y los de redes. Los de redes se subdividen, a su vez, en distribuidos o no. Los IDS de hosts se basan en el análisis de las estadísticas de uso o el uso indebido de ciertos recursos (comandos, archivos, etc.) del sistema. Los IDS de red buscan patrones sospechosos en los paquetes TCP, malformaciones en la estructura de los mismos, etc. Se trata, pues, de *sniffers* que poseen tablas (actualizables) con los patrones característicos usados en los intentos de entrar en un sistema.

5 Un Vistazo al Futuro de los Cortafuegos.

IPSEC (*IP SECurity*) es un conjunto de estándares desarrollado por el IETF (*Internet Engineering Task Force*) destinado a solventar las deficiencias de seguridad de TCP/IP, proporcionando mecanismos fiables de autenticación, confidencialidad e integridad en las comunicaciones. ¿Quedaran obsoletos los Cortafuegos si llegamos a un escenario en el que exista una implantación generalizada de IPSEC? Para saberlo, lo primero que tenemos que analizar es lo que es capaz de hacer IPSEC.

IPSEC resuelve eficazmente dos de los principales problemas de la familia de protocolos TCP/IP a los que nos referimos al principio de este documento: la correcta y fiable autenticación entre dos hosts y la total confidencialidad de los datos intercambiados entre dichos hosts. Los cortafuegos no fueron creados para resolver ninguno de estos dos problemas aunque algunos de ellos proporcionen en la actualidad servicios adicionales que los solventan o mitigan, como las Redes Privadas Virtuales. El punto fuerte de los cortafuegos, la limitación en las clases o tipos de conectividad permitidos entre dos redes, no queda resuelto por IPSEC.

Por tanto, lejos de ser competencia, la combinación de la tecnología de los Cortafuegos e IPSEC nos hace vislumbrar un futuro de comunicaciones mucho más seguras, con Redes Privadas Virtuales independientes del fabricante, filtrado de paquetes en base a los campos adicionales de las cabeceras definidas en IPSEC, mejores y más eficientes cortafuegos en la capa de aplicación, y esperemos que una tecnología de detección de intrusos más madura y efectiva.

6 Conclusiones.

Todas las organizaciones o entidades que habiliten accesos de entrada y/o salida a través de Internet deberían, inexcusablemente, contar con un cortafuegos adecuado a sus necesidades y que cumpliera rigurosamente con una política de seguridad previamente estudiada. Los usuarios particulares, sobre todo los que cuentan con acceso permanente a Internet a través de ADSL, cable o cualquier otra conexión permanente, también deberían de considerar esta posibilidad.

Un Cortafuegos debería de ser, pues, la primera línea de defensa de cualquier organización con estas características, pero no la única: la seguridad interna y la continúa puesta al día de parches para corregir las vulnerabilidades emergentes no deben de olvidarse como objetivos prioritarios.

Es preciso un detallado examen previo a la hora de elegir que tipo de cortafuegos se adapta mejor a nuestras necesidades. Ayudarnos en esa elección ha sido el principal objetivo de este documento que puede ser complementado con la extensa documentación que se referencia en el siguiente y último capítulo.

A modo de resumen, estas son las principales necesidades que podemos encontrarnos y que debemos de tener en cuenta a la hora de elegir un cortafuegos:

- Filtrado de paquetes e inspección de determinados protocolos.
- Inspección del estado de las conexiones.
- Operaciones y servicios de Proxy para aplicaciones y protocolos específicos.
- Auditoría del tráfico, tanto del aceptado como del rechazado, por el cortafuegos.
- Proporcionar autenticación de usuarios en base a métodos que no requieren la reutilización de contraseñas que puedan ser 'escuchadas' por *sniffers*.

Usualmente requeriremos que nuestro cortafuegos esté especialmente diseñado para inspeccionar tráfico HTTP, SMTP, FTP y telnet.

No debemos de descartar la posible necesidad de usar más de un cortafuegos para cubrir todas nuestras necesidades si no encontramos un único producto que las cubra todas ellas.

Por último, no hemos de olvidar que seguridad y rendimiento son conceptos a menudo contrapuestos . Esto no es excusa para olvidar ninguna de ambas y llegar a un adecuado equilibrio entre ellas.

7 Bibliografía.

La bibliografía que aquí se cita es muy interesante para ampliar los contenidos del presente documento. Parte de ella ha sido de inestimable ayuda para la confección del mismo.

He querido dar una especial relevancia a la información accesible gratuitamente a través de Internet: cada vez hay más información disponible en la web y esto provoca que debamos de invertir más tiempo en encontrar información de calidad en ella, pero también que tengamos más probabilidades de ver recompensada nuestra búsqueda.

Quiero destacar como imprescindibles, dentro de este apartado de información libre, por supuesto el contenido de los RFC's tantas veces olvidados o desestimados, las recomendaciones hechas por Wack, Cutler y Pole desde la reciente guía publicada por el NIST, el libro *Securing Your Network with the Cisco Centri Firewall*, ofrecido gratuitamente por Cisco System y, por último pero no menos importante, las dos excelentes contribuciones de Bellowin: un breve *white-paper* sobre los problemas de seguridad inherentes a la familia de protocolos TCP/IP y un libro *"Firewalls and Internet Security: Repelling the Wily Hacker*", publicado por Addyson Wesley y que Alexandre Dulaunoy nos ofrece íntegramente en formato PDF (no se si legal o ilegalmente) desde su página personal.

7.1 RFC's.

1. R. Finlayson. *IP Multicast and firewalls*. RFC 2588. (1999). http://rfc.net/rfc2588.html
2. R. Thayer, N. Doraswamy, R. Glenn. *IP Security Document Roadmap*. RFC 2411. (1998). http://rfc.net/rfc2411.html
3. Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear. *Address allocation for private internets*. RFC 1918. (1996). http://rfc.net/rfc1918.html
4. M. Bellowin. *Firewall-friendly*. RFC 1579. (1994). http://rfc.net/rfc1579.html
5. J. Postel, J.K. Reynolds. *File Transfer Protocol*. RFC 0959. (1985). http://rfc.net/rfc0959.html
6. J. Postel, *Internet Protocol Handbook.* RFC 0774. (1980). http://rfc.net/rfc0774.html
7. J. Postel. *User Datagram Protocol*. RFC 0768. (1980). http://rfc.net/rfc0768.html
8. J. Postel, *Transmission Control Protocol*. RFC 0761. (1980). http://rfc.net/rfc0761.html

9. J. Postel. *Internet Protocol*. RFC 0760. (1980).
http://rfc.net/rfc0760.html
10. J. Postel. *Internet Message Protocol*. RFC 0759. (1980).
http://rfc.net/rfc0759.html

7.2 URL's.

1. J. Wack, K. Cutler, J. Pole. Guidelines on Firewalls and Firewall Policy, Recomendations of the National Institute of Standards and Technology. NIST Special Publication 800-41. MIS Training Institute, (2002).
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
2. C. Fulmer. *Firewall Product Overview*. (2002).
http://www.thegild.com/firewall/
3. M. Curtin, M.J. Ranum. Internet Firewalls: Frequently Asked Questions. (2000).
http://pubweb.nfr.net/~mjr/pubs/fwfaq/
4. Securing Your Network with the Cisco Centri Firewall, Cisco Systems Documentation, (1997).
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/index.htm
5. A. Villalón. *Seguridad en UNIX y Redes v2.0*. (2002)
http://www.kriptopolis.com/net/modules.php?op=modload&name=Downloads&file=index&req=getit&lid=47
6. COAST (Computer Operations, Audit, and Security Technology). *Internet Firewalls Resources*. Purdue University. (1996).
http://www.cerias.purdue.edu/coast/firewalls/
7. W.R. Cheswick, S. M. Bellowin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison Wesley Professional Computing Series. (1994).
http://www.foo.be/docs/firewall_and_internet_security/
8. S.M. Bellowin. *Security Problems in the TCP/IP Protocol Suite*. AT&T Bell Laboratories. (1989).
http://www.research.att.com/~smb/papers/ipext.pdf
9. CheckPoint Firewall-1
http://www.checkpoint.com/products/protect/firewall-1.html
10. Phoneboy's Firewall-1 Unofficial Page. (2001)
http://www.phoneboy.com/fw1/
11. ICAT Vulnerability database, mantenida por el NIST, National Institute of Standarts and technology.
http://icat.nist.gov/icat.cfm
12. FAQ: Network Instrusion Detection Systems
http://www.robertgraham.com/pubs/network-intrusion-detection.html
13. FAQ: Firewall Forensic
http://www.robertgraham.com/pubs/firewall-seen.html

7.3 Libros.

1. S. Feit. *TCP/IP, arquitectura, protocolos e implementación además de IPv6 y seguridad de IP*. Osborne McGraw-Hill. (1998).
2. K. Siyan, C. Hare. *Internet Firewalls and Network Security: Master the Complexities of Network Security*, New Riders Publishing, (1995).
3. D.B. Chapman, E.D. Zwicky, *Construya Firewalls para Internet.* O'Reilly & Associates, Inc., (1995).
4. W.R. Cheswick, S.M. Bellovin, *Firewalls and Internet Security: Repelling the Wiley Hacker*. Addison-Wesley Publishing Company, (1994).
5. S.L. Shaffer, A.R. Simon, *Network Security.* AP Professional, (1994).
6. M. Gasser, *Building a Secure Computer System.* Van Nostrand Reinhold, (1988).