Parte II
Estudio previo

5. Estado del Arte

Como se comentó en el apartado introductorio de esta memoria, el proyecto que estamos documentando se centra en un campo especifico de la seguridad de la información: los servidores de seguridad perimetrales. En este apartado aclararemos los conceptos básicos necesarios para abordar este campo. También se discute en esta sección el conjunto de características que debe cumplir un servidor de seguridad perimetral y las distintas clasificaciones bajo las que podemos agruparlos. Por último se dará una visión de los productos que actualmente se encuentran disponibles, tratándose tanto las herramientas comerciales como las herramientas licenciadas como software libre.

5.1. Arquitectura de red

Aunque existen muchas configuraciones de red posibles, en redes de datos (TCP/IP) medianas o pequeñas, la estructura habitual es similar a la representada en la figura 1. Podemos aprovechar está arquitectura "*tipo*", para aclarar las distintas zonas que encontramos y la ubicación del servidor de seguridad perimetral.

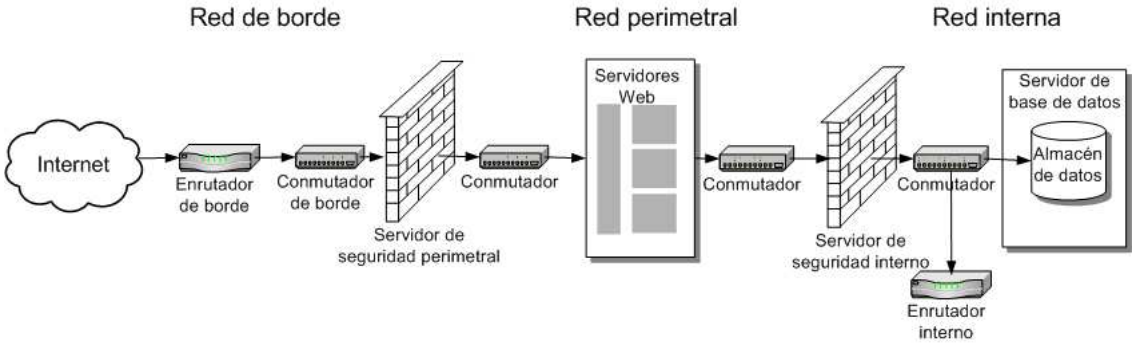

Figura 1: Arquitectura de red típica.

Estas zonas son normalmente tres:

Red de borde: Esta red está conectada directamente al exterior, Internet, a través de un enrutador que no representa un mecanismo de protección fiable. El enrutador transmite datos hacia la red perimetral atravesando del servidor de seguridad perimetral (cortafuegos de DMZ). En la red de borde no es frecuente encontrar servidores, en ocasiones pueden colocarse detectores de intrusiones o equipos de monitorización.

Red perimetral: Esta red, también conocida como DMZ (zona desmilitarizada), contiene los servidores accesibles desde el exterior. Es una zona de seguridad moderada, no lo suficientemente segura como para contener equipos de usuarios de la red local.

Redes internas: Esta red segura contiene a los equipos de usuarios y ciertos servidores solo accesibles por estos o por equipos de la red perimetral. Es una red protegida por distintos filtros de seguridad: servidor de seguridad perimetral y servidor de seguridad interno.

Queda claro pues cual es la ubicación del servidor de seguridad perimetral, entre la red de borde y la red perimetral. Es por tanto la primera barrera defensiva seria de una red de datos.

5.2. Ataques y defensas del sistema

Haremos en este apartado un resumen de algunos de los ataques al sistema conocidos, es fundamental conocer los riesgos antes de implementar las protecciones. Trataremos de exponer las razones por las cuales se considera al servidor de seguridad perimetral como primera linea de defensa contra ellos.

Una primera clasificación puede hacerse teniendo en cuenta el origen del ataque:

Ataques externos

La mayoría de los ataque externos registrados son parte de reconocimientos o intentos de explotación de vulnerabilidades automatizados, que se ejecutan contra miles de equipos y no por ello dejan de ser peligrosos Hay millones de potenciales atacantes en Internet, los más experimentados que posiblemente solo intente una intrusión si la red le resulta de interés o si puede usarla para obtener equipos "zombies" desde los que perpetrar otros ataques, los aprendices conocidos como "script-kiddies" que se limitan a ejecutar programas que otros crearon y tratan de aprovechar vulnerabilidades conocidas y otras clases de delincuentes que aprovechan la red de redes para conseguir dinero fraudulentamente con ataques de *phising* o enviando *spam.*

Ataques internos

Además de proporcionar protección frente a ataques desde Internet, también se debe proteger la información importante. La mayoría de las organizaciones tienen información importante que se debe proteger de determinados usuarios de la red interna, incluyendo no sólo a los empleados, sino también a los proveedores y clientes. Aunque un servidor de seguridad perimetral tiene la función principal de proteger contra intrusiones externas, también debe suponer un freno para los ataques internos por ejemplo impidiendo el tráfico de vuelta de un troyano que resida en un equipo interno o impidiendo el acceso a sitios peligrosos por parte de los usuarios de la red interna.

Según las características del ataque podemos encontrarnos con diversos tipos de ataque, algunos los listamos a continuación:

Rastreador de paquetes (sniffer) Un rastreador es una aplicación de software o un dispositivo de hardware que se conecta a la red y captura información de las tramas de datos. La intención original de estos sistemas era solucionar problemas y analizar el tráfico de Ethernet o profundizar en las tramas para examinar paquetes IP individuales. Los rastreadores funcionan de modo promiscuo; es decir, están atentos a todos los paquetes que atraviesan el medio físico, en redes conmutadas pueden utilizarse técnicas de envenenamiento de la caché ARP para capturar el tráfico que de otra manera no sería visible. En muchos protocolos, como telnet, smtp, pop3, se envía la información de nombre de usuario y contraseña en texto no cifrado que los productos rastreadores pueden leer, por lo tanto, un intruso con rastreador puede obtener acceso a muchas aplicaciones.

Suplantación de direcciones Se pueden suplantar direcciones a distintos niveles, por ejemplo IP y MAC (ethernet). La suplantación de IP se produce cuando se cambia la dirección de origen de un paquete IP para ocultar la identidad del remitente. Puesto que el enrutamiento en Internet utiliza sólo la dirección de destino para enviar un paquete y omite la dirección de origen, un intruso puede enviar un paquete destructivo al sistema disfrazando el origen para que no sepa de dónde proviene. La suplantación no es siempre destructiva, pero indica una intrusión cercana. La dirección puede ser externa (para ocultar la identidad del intruso) o una de las direcciones internas de confianza con acceso privilegiado. La suplantación se utiliza habitualmente para ataques de denegación de servicio, descritos posteriormente en este documento.

Denegación de servicio Los ataques de denegación de servicio (DoS) se encuentran entre los más difíciles de prevenir. Difieren de otros tipos de ataque en que no causan un daño permanente a la red, sino que intentan que ésta deje de funcionar bombardeando un equipo determinado (un servidor o un dispositivo de red) o reduciendo el rendimiento de los vínculos de red hasta el punto en que éste es tan pésimo que provoca descontento en los clientes y pérdida de negocio para la organización. Un ataque DoS distribuido (DDoS) es un ataque iniciado desde muchos otros equipos que se concentran en el bombardeo a su sistema. Puede que los equipos atacantes no hayan iniciado el ataque ellos mismos, sino que debido a sus propios problemas de seguridad, hayan permitido que se infiltrara un intruso que los ha llevado a enviar grandes volúmenes de datos a la red, congestionando, así, el vínculo al ISP o uno de los dispositivos.

Reconocimiento de redes (scanner) Son métodos y procedimientos de búsqueda de equipos y servicios publicados en esos equipos. Existen programas que automatizan estas búsquedas, uno de los scanners más potentes y utilizados es *nmap*. Estos programas son capaces de distinguir el sistema operativo, versiones de servidores, etc, a partir del comportamiento de estos ante la recepción de peticiones diversas. Un nivel más elevado ocupan los analizadores de vulnerabilidades que además de identificar los sistemas y servicios tratan de encontrar vulnerabilidades en ellos realizando pruebas automáticas y buscando en bases de datos de software vulnerable. Nessus es uno de estos programas, quizá el más extendido a la fecha de redacción de esta memoria.

Virus Gusanos y Troyanos Un virus informático es un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo; por otro lado un gusano (worm) es un programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él; un troyano es un programa que realiza funciones distintas a las que aparenta, por ejemplo recogida de datos del usuario o apertura de comunicaciones con el exterior. Generalmente, los servidores de seguridad no pueden detectar los virus, aunque algunos incluyen capacidades de detección de código malicioso en correo y tráfico http. Aunque la defensa principal contra los virus siempre es mantener el software antivirus actualizado en el dispositivo, el servidor de seguridad perimetral puede ser útil para limitar la efectividad de virus, gusanos y troyanos.

Ataques contra aplicaciones (Exploits) Del inglés to exploit (explotar, aprovechar), es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa. El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

Spam Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de spam incluyen grupos de noticias usenet, motores de búsqueda, wikis y blogs. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

5.3. Definición del dispositivo

Un servidor de seguridad es un mecanismo que sirve para controlar el flujo de tráfico IP entre dos redes. Los dispositivos de servidor de seguridad funcionan habitualmente en la capa de red (nivel 3) del modelo OSI, aunque algunos modelos, cada vez más, también pueden funcionar a niveles superiores (filtrado de contenidos, filtrado antivirus, filtrado anti-spam, proxy de aplicaciones).

Generalmente, los servidores de seguridad ofrecen las siguientes ventajas:

- Defienden los servidores internos de ataques a la red
- Aplican las directivas de uso de la red y acceso a la misma
- Supervisan el tráfico y generan alertas cuando se detectan patrones sospechosos

Es importante destacar que los servidores de seguridad mitigan sólo algunos tipos de peligros. Generalmente, un servidor de seguridad no evita el daño que se puede infligir a un servidor con un problema de seguridad de software. Los servidores de seguridad se deben implementar como parte de una arquitectura de seguridad completa de la organización.

5.4. Características del servidor de seguridad

Según las características que admita un servidor de seguridad, el tráfico se permitirá o bloqueará por medio de distintas técnicas. Dichas técnicas ofrecen varios grados de protección, según las capacidades del servidor de seguridad. En general, los servidores de seguridad que proporcionan características complejas ofrecen también características más sencillas. Las características siguientes del servidor de seguridad se enumeran de menor a mayor complejidad:

Filtros de entrada del adaptador de red El filtrado de entrada del adaptador de red examina las direcciones de origen o destino y otra información del paquete entrante y lo bloquea o lo deja pasar. Se aplica sólo al tráfico entrante y no puede controlar el tráfico de salida. Compara las direcciones IP, los números de puerto para UDP y TCP, así como el protocolo del tráfico, TCP, UDP y otros como la encapsulación de ruta genérica (GRE). Por ejemplo, para un servidor de seguridad perimetral que protege un servidor Web, el tráfico entrante válido debe permitir sólo el acceso a la dirección IP del servidor Web y, habitualmente, a un intervalo limitado de números de puerto, como 80 para HTTP o 443 para HTTPS. Aunque el servidor de seguridad perimetral debe tener este control, es recomendable que también se implemente en el enrutador de borde.

El filtrado de entrada del adaptador de red permite una denegación rápida y eficiente de los paquetes entrantes estándar que cumplan los criterios de las reglas configurados en el servidor de seguridad. Sin embargo, esta forma de filtrado se puede eludir fácilmente, puesto que sólo compara los encabezados del tráfico IP, funciona con la suposición de que el tráfico que se filtra sigue los estándares IP y no se ha diseñado para eludir el filtrado.

Filtros de paquetes estáticos Los filtros de paquetes estáticos son similares a los filtros de entrada del adaptador de red en cuanto a que simplemente comparan los encabezados IP para determinar si debe o no permitir que el tráfico pase por la interfaz. Sin embargo, los filtros de paquetes estáticos permiten el control sobre las comunicaciones salientes y las entrantes con una interfaz. Además, los filtros de paquetes estáticos suelen permitir una función adicional sobre el filtrado del adaptador de red, que es comprobar si el bit de reconocimiento (ACK) está establecido en el encabezado IP. El bit ACK proporciona información acerca de si el paquete es una solicitud nueva o una solicitud devuelta de otra original. No comprueba que el paquete lo enviara de origen la interfaz que lo recibió, simplemente, comprueba si el tráfico que entra a la interfaz parece tráfico devuelto, según las convenciones de los encabezados IP. Esta técnica sólo se aplica al protocolo TCP y no al protocolo UDP.

Al igual que el filtrado de entrada del adaptador de red, el filtrado de paquetes estático es muy rápido, pero sus capacidades son limitadas y el tráfico manipulado para eludirlo lo consigue. Igual que el filtrado de entrada del adaptador de red, el filtrado de paquetes estático se debe implementar en el enrutador de borde además del servidor de seguridad perimetral.

Traducción de direcciones de red En el intervalo de direcciones IP de todo el mundo, algunos intervalos se designan como direcciones privadas. Dichas direcciones están concebidas para su uso en la organización y no tienen ningún significado en Internet. El tráfico con destino

a estas direcciones IP no se puede enrutar a través de Internet, por lo que asignar una dirección privada a sus dispositivos internos puede proporcionarles cierta protección frente a los intrusos. Sin embargo, a menudo estos dispositivos necesitan tener acceso a Internet, por lo que la Traducción de direcciones de red (NAT) convierte la dirección privada en una dirección de Internet.
Aunque NAT no es estrictamente una tecnología de servidor de seguridad, ocultar la dirección IP real de un servidor evita que los atacantes consigan información de rastreo valiosa acerca del servidor.

Inspección con estado En la inspección con estado, todo el tráfico de salida se registra en una tabla de estado. Cuando el tráfico de conexión vuelve a la interfaz, se comprueba la tabla de estado para garantizar que el tráfico se ha originado en ésta. La inspección con estado es un poco más lenta que el filtrado de paquetes estático; sin embargo, garantiza que sólo se permita el tráfico si coincide con las solicitudes de tráfico de salida. La tabla de estado contiene elementos como la dirección IP de destino, el paquete IP de origen, el puerto al que se llama y el host de origen.
Algunos servidores de seguridad pueden almacenar más información en la tabla de estado que otros (como fragmentos IP enviados y recibidos). El servidor de seguridad puede comprobar que el tráfico se procesa cuando vuelve toda la información fragmentada o una parte de ésta. Los servidores de seguridad de distintos proveedores implementan la característica de inspección con estado de forma distinta.
La característica de inspección con estado ayuda a mitigar el peligro que supone el reconocimiento de redes y la suplantación de IP.

Inspección de circuitos El filtrado de circuitos permite inspeccionar sesiones, en lugar de conexiones o paquetes. Las sesiones se establecen sólo como respuesta a una solicitud de usuario y pueden incluir varias conexiones. El filtrado de circuitos proporciona compatibilidad integrada para protocolos con conexiones secundarias, como FTP y multimedia de transmisión por secuencias. Suele ayudar a reducir el peligro que suponen los ataques de suplantación de IP, DoS y reconocimiento de redes.

- Servidores de seguridad proxy Los servidores de seguridad proxy solicitan información en nombre de un cliente. A diferencia de las tecnologías de servidor de seguridad tratadas anteriormente, la comunicación no se efectúa directamente entre el cliente y el servidor que aloja el servicio, sino que el servidor de seguridad proxy recopila información en nombre del cliente y devuelve los datos que recibe del servicio de nuevo al cliente. Puesto que el servidor proxy recopila esta información para un cliente, también almacena en caché el contenido en el disco o la memoria. Si otro cliente realiza una solicitud de datos idéntica, ésta se puede satisfacer desde la caché, por lo que se reduce el tráfico de la red y el tiempo de procesamiento del servidor.
  Para sesiones no cifradas, como las sesiones de sólo lectura de FTP y HTTP, un servidor de seguridad proxy crea sesiones individuales reales con el cliente y el servidor, por lo que no hay nunca una conexión directa entre los dos. Por otra parte, para las sesiones cifradas, el servidor proxy comprueba que la información de encabezado se ajuste a los estándares de comunicación de Nivel de socket seguro (SSL) antes de permitir que pase el tráfico. Sin embargo, el proxy no puede inspeccionar los datos que pasan, porque están totalmente cifrados por el cliente y el servidor.
  Las ventajas de un servidor proxy por encima de las tecnologías de servidor de seguridad tratadas anteriormente incluyen:

  - No hay conexiones directas entre el cliente y el servidor. Aunque si lo hacen (como con SSL), se lleva a cabo la inspección del tráfico y el encabezado del protocolo.
  - El servidor puede almacenar en caché el contenido de los sitios solicitados con frecuencia, esto supone ahorro ancho de banda y evita que salgan del entorno solicitudes innecesarias.

- Además de validar el número de puerto a través del cual viaja la comunicación, los servidores proxy validan también los protocolos que pasan por estos. Los protocolos más habituales inspeccionados son FTP de sólo descarga, HTTP, SSL y algunos servicios de mensajes de texto (por ejemplo, sólo texto, sin vídeo, audio o transferencia de archivos).
- Los servidores proxy se pueden configurar a menudo para reenviar solicitudes basadas en la identidad del usuario (es decir, se pueden establecer restricciones sólo para determinados usuarios), en lugar del puerto, protocolo o IP de origen.

El principal inconveniente de un servidor proxy es que requiere mucha más capacidad de procesamiento para realizar una inspección de protocolo. Sin embargo, la capacidad de procesamiento aumenta siempre, por lo que esto es cada vez menos problemático. De todas formas, los servidores proxy no tienen el rendimiento de un servidor de seguridad de filtrado de paquetes o con estado. Se podría decir que las ventajas adicionales de la inspección de protocolo son necesarias en un mundo donde las redes de alta velocidad abundan para los usuarios domésticos y donde la conectividad a Internet está cada vez más disponible para nodos no confiables conectados por ISP con una obligación mínima o inexistente de proporcionar servicios de Internet confiables.
En general, la característica de proxy ayuda a mitigar el peligro que suponen los ataques de suplantación de IP, DoS y reconocimiento de redes, los virus o troyanos y algunos ataques a aplicaciones.

Filtrado de aplicaciones El nivel más sofisticado de inspección de tráfico del servidor de seguridad es el filtro de aplicaciones. Los filtros de aplicaciones de buena calidad permiten analizar un flujo de datos para una aplicación concreta y proporcionar el procesamiento específico de aplicaciones, incluida la inspección, el filtrado o el bloqueo, la redirección y la modificación de datos en su paso por el servidor de seguridad.
Este mecanismo se utiliza para proteger contra elementos como los comandos SMTP no seguros o los ataques contra los servidores del sistema de nombres de dominio (DNS). Generalmente, las herramientas de terceros para el filtrado de contenido, como la detección de virus, el análisis léxico y la categorización de sitios, se pueden agregar al servidor de seguridad.
Un servidor de seguridad de aplicaciones tiene la posibilidad de inspeccionar muchos protocolos distintos según el tráfico que pasa por éste. A diferencia del servidor de seguridad proxy, que habitualmente inspecciona el tráfico habitual (como HTTP, descarga de FTP y SSL), el servidor de seguridad de aplicaciones tiene un control mucho mayor sobre la forma en que el tráfico viaja por él. Por ejemplo, un servidor de seguridad de aplicaciones sólo puede permitir el paso al tráfico UDP que se origina dentro de sus límites. Si un host Internet explorara el puerto de un servidor de seguridad con estado para ver si ha permitido el tráfico DNS en el entorno, el resultado probablemente mostraría que el puerto conocido asociado con DNS estaba abierto, pero una vez preparado un ataque, el servidor de seguridad con estado rechazaría las solicitudes porque no se originaron de forma interna. Un servidor de seguridad de aplicaciones abre puertos de forma dinámica en función de si el tráfico se origina internamente o no.
La característica del servidor de seguridad de aplicaciones ayuda a mitigar el peligro que suponen los ataques de suplantación de IP, DoS, de aplicaciones, de reconocimiento de redes y los ataques de virus o troyanos.
Los inconvenientes de un servidor de seguridad de aplicaciones son similares a los del proxy, en cuanto a que requieren mucha más capacidad de procesamiento y habitualmente son mucho más lentos al transferir el tráfico que los servidores de seguridad con estado o de filtrado estático.
La característica de aplicaciones garantiza que el tráfico que pasa por un puerto es el apropiado. A diferencia del servidor de seguridad de inspección con estado o de filtrado de paquetes que mira simplemente al puerto y a las direcciones IP de origen y destino, los servidores de seguridad compatibles con la función de filtrado de aplicaciones tienen la capacidad de inspeccionar tanto los comandos como los datos que se transmiten en una y otra dirección.

La mayoría de los servidores de seguridad compatibles con la característica de aplicaciones sólo dispone del filtrado para el tráfico de texto no cifrado, como un servicio de mensajería, HTTP o FTP preparados para proxy. Es importante tener en cuenta que un servidor de seguridad compatible con esta característica puede regir el tráfico que entra y sale del entorno. Otra ventaja de esta característica es la posibilidad de inspeccionar el tráfico DNS al pasar por el servidor de seguridad para buscar comandos específicos de DNS. Este nivel adicional de protección garantiza que usuarios o atacantes no podrán ocultar información en los tipos de tráfico admitidos.

5.5. Productos existentes en el mercado

Cualquier red de datos actual necesita un servidor de seguridad perimetral, ante esta demanda han surgido en los últimos años diversas soluciones que tratan de simplificar la gestión de las distintas funcionalidades necesarias.

Es posible implementar un servidor de seguridad perimetral instalando distintos programas en un equipo existente, integrarlos y configurarlos uno a uno. Sin embargo el coste de implantación en este caso crece, es complicado configurar y mantener cada módulo del servidor por separado, cada uno con su interfaz de configuración y gestión.

Por tanto son las soluciones integrales las más demandadas, ya que facilitan al usuario final (el cual no tiene por que ser un experto en la seguridad de redes y sistemas) la implantación y mantenimiento del servidor de seguridad.

Los requerimientos en cuanto a rendimiento variaran enormemente según el tamaño de la red a proteger, según el número de equipos, el tráfico generado por estos que atravesará el dispositivo y el tipo de servicios (por ejemplo el tráfico interactivo exigirá más potencia de proceso).

Con el fin de acotar el estudio que nos atañe, optamos por mostrar aquí algunos productos diseñados principalmente para redes medianas (en cuanto a número de equipos y tráfico generado) y para tráfico genérico y heterogéneo.

En primer lugar, haremos una breve mención a dispositivos comerciales "cerrados". Es decir, dispositivos hardware en los que se instala un sistema operativo y unos programas diseñados específicamente para actuar como servidor de seguridad perimetral. Estos dispositivos conocidos comúnmente por el nombre inglés "appliance", suelen ejecutar en muchos casos sistemas operativos con núcleo Linux, y son adaptados para cumplir su función especifica añadiéndoseles interfaces de gestión y configuración gráficas.

En segundo lugar, presentaremos distintas distribuciones de sistemas operativos libres (Linux, OpenBSD, FreeBSD, etc.) diseñadas específicamente para cubrir las necesidades de un servidor de seguridad perimetral. Algunos de estos sistemas están diseñados para ejecutarse en dispositivos sin disco duro, ya sean dispositivos embebidos o en servidores corrientes en los que se carga el sistema desde un disco auto-arrancable (Live-CD).

Por lo tanto esta segunda aproximación al servidor de seguridad perimetral puede ser más versátil, pues permite partiendo de un mismo software, elegir el hardware más adecuado a las necesidades de la red que queramos proteger. Por ejemplo, en una pequeña oficina en la que los usuarios solo navegan y miran el correo electrónico bastará con instalar alguno de estos sistemas operativos en un ordenador personal. Sin embargo en una empresa cuya principal actividad este relacionada con las tecnologías de la información, y en la que sus servidores presentan un tráfico elevado de datos podremos instalar el mismo sistema operativo en un servidor con las prestaciones y el rendimiento adecuados.

5.5.1. Appliances

Symantec SGS300-400 Appliance de seguridad integrada con la posibilidad de añadir conexión inalámbrica 802.11 b/G. Ofrece un sólo punto para controlar toda la seguridad de la red en una organización.

Se mantiene actualizado gracias a tecnología Live Update. Comparte su conexión a Internet y es capaz de filtrar virus en navegación y correo, armar redes privadas virtuales (VPNs) (IPSec), ofrece además filtrado de contenidos y detección de intrusión.

La seguridad no consiste en cerrar el paso a la información, sino en abrirlo a las personas correctas, por eso este dispositivo de frontera permite tener la información disponible en el lugar que usted la necesite y tiene una administración sencilla.

Los modelos de la familia 300 se recomiendan para empresas entre 25 y 50 usuarios. Los modelos de la familia 400 se recomiendan para empresas de mayor tráfico o número de usuarios cercano a 100.

D-Link DFL-700 El DFL-700 de D-Link es un cortafuegos de fácil uso, diseñado para pequeñas y medianas empresas, grupos de trabajo, y departamentos que requieran una buena relación precio/rendimiento. Este dispositivo es una potente solución de seguridad que integra traducción de dirección de red (NAT), cortafuegos, filtrado de contenidos, protección IDS, gestión del ancho de banda y soporte de red privada virtual (VPN). El DFL-700 incluye soporte de enlace WAN, puerto LAN de confianza y puerto DMZ para correo electrónico local y servidores Web. Además, por su tamaño puede colocarse en cualquier lugar. Gracias a la intuitiva interfaz basada en Web, el proceso de instalación del DFL-700 resulta fácil y sencillo para el usuario.

ZyXEL ZyWall 2/2+ El ZyWALL 2 pertenece a la robusta familia de cortafuegos de ZyXEL. Dotado con la certificación ICSA y IPSec VPN, garantiza la seguridad además de interoperatividad con productos de otras marcas que cumplan la certificación ICSA. Las características de VPN están mejoradas en el ZyWALL 2, ofreciendo cifrado de datos 3DES a 2 Mbps y dos conexiones VPN.

Como características de valor añadido, incluye Marcado Backup y Redirección de Tráfico, características que aumentan su fiabilidad soportando múltiples conexiones a Internet. El ZyWALL 2 soporta certificación ICSA IPSec VPN conveniente para conexiones desde un punto al servidor central remoto. El cifrado de datos sobre Internet asegura la transmisión segura entre dos puntos, eliminando la necesidad de costosas líneas dedicadas y permitiendo interconectividad global a un mínimo coste. La certificación Firewall ICSA dota al robusto cortafuegos de protección y seguridad fiable. Basado en la tecnología de Inspección de Estado de Paquetes y Denegación de Servicio (Dos), proporciona la mejor defensa contra los intrusos de la red y otras amenazas peligrosas. El ZyWALL 2 está equipado con un switch Ethernet de 4 puertos 10/100 Mbps, permitiendo a múltiples usuarios compartir una conexión a Internet de banda ancha sin el coste adicional de switches o hubs externos.

SonicWall TZ150/170 SonicWALL es proveedor de soluciones de seguridad para Internet y ofrece seguridad en transacciones y seguridad en servicios para las pequeñas y medianas empresas, e-commerce, escuelas y gobierno. La plataforma tecnológica de SonicWALL incluye cortafuegos, VPN, SSL, alta disponibilidad, antivirus, autenticación con certificados digitales, evaluación de vulnerabilidad y filtrado de contenido. Estos productos y tecnologías proveen una solución de seguridad completa.

Nokia IP45 Nokia IP45 es una solución de seguridad para redes de tamaño moderado. Este appliance combina el software de cortafuegos Check Point con una plataforma hardware diseñada específicamente para su uso.

Proporciona un filtro de paquetes con estado, protección ante ataques de denegación de servicio y facilidad en la implantación, configuración y gestión.

Cisco PIX 501 El PIX 501 cuenta con recursos de seguridad de clase empresarial, incluyendo protección por inspección integral, red virtual privada y protección en caso de intrusión, además de ofrecer soporte de filtrado por URL, filtrado por contenido y a otras soluciones que ofrecen los equipos compatibles con la arquitectura AVVID de Cisco. Incluye un switch 10/100 Mbps con cuatro puertos para compartir conexiones en entornos de red residencial o de pequeñas empresas.

Además, el PIX®501 ofrece varias herramientas para su administración remota, incluyendo la administración individual vía Internet a través del PIX Device Manager, la administración escalable de varios dispositivos firewall por interfaz gráfica a través del Cisco Secure Policy Manager y la posibilidad de administrar el dispositivo por syslog, SNMP y telnet/SSH.

5.5.2. Distribuciones de servidor de seguridad

monowall m0n0wall es un cortafuegos especialmente pensado para dispositivos embebidos. Está basado en una versión para "bare-bones" de FreeBSD y proporciona todas las funcionalidades importantes de un cortafuegos comercial, incluyendo facilidad de uso. Todo esto en tan solo 6 MB de espacio, por tanto puede ser almacenada en una tarjeta de memoria.

La configuración del dispositivo se realiza por medio de una interfaz web, programada con scripts PHP y toda la configuración del sistema se almacena en formato XML.

A continuación listamos las principales funcionalidades de m0n0wall:

- interfaz web de configuración y gestión (soporta SSL)
- consola serie para recuperación en caso de fallo
- soporte inalámbrico (puntos de acceso con chipset PRISM-II/2.5/3, BSS/IBSS con otros incluido Cisco)
- portal cautivo (captive portal)
- soporte VLAN 802.1Q
- filtro de paquetes con estado (ipfilter)
- NAT/PAT (incluido 1:1)
- túneles VPN IPsec y PPTP
- otros: cliente DHCP, PPPoE, PPTP y Telstra BigPond Cable en la interfaz WAN, rutas estáticas, servidor DHCP, caching DNS forwarder, cliente DynDNS y actualizador RFC 2136 DNS, agente SNMP, formateado de tráfico, gráficos de tráfico basados en SVG, actualización de firmware desde la interfaz web, cliente "Wake on LAN", copia de seguridad de configuración y restauración.

Sin embargo, una de las restricciones de diseño de m0n0wall es su tamaño. Esta restricción impone un limite en el número de funcionalidades que tiene e imposibilita incluir otras iteresantes como filtros de paquetes, antivirus, antispam, proxy, etc.

pfsense pfsense es un cortafuegos de fuentes abiertas, derivado del proyecto m0n0wall y con objetivos radicalmente diferentes. Por ejemplo usa el filtro de paquetes de openBSD Packet Filter (pf), el uso de FreeBSD 6.1 ALTQ (HFSC) para la gestión de colas de tráfico y un gestor de paquetes de software integrado que permite extender el sistema con programas de terceros de forma modular.

Al igual que m0n0wall la configuración del sistema es sencilla y se realiza por medio de formularios web. Pfsense también está diseñado pensando en optimizar su tamaño para dispositivos embebidos, dispone de una versión de 32MB para estos y otra de mayor tamaño para ejecutarla desde un CDROM o ser instalada en disco duro.

Sus características son similares a las de m0n0wall pero incluye algunas más como por ejemplo el sistema de gestión de paquetes. Este permite integrar paquetes desarrollados por terceros en el sistema pfSense.

A pesar de ser una grán aplicación, el código de la interfaz de configuración web de PfSense es poco modular. Esto dificulta las posibles ampliaciones del sistema siendo la única forma "asequible" la creación de paquetes de terceros.

redWall RedWall se distribuye en un cdrom autoejecutable (LiveCD), su objetivo es simplificar la configuración del dispositivo por medio de una interfaz web, así como una interfaz que represente de forma sencilla y legible los ficheros de registro.

Algunas características destacables de redWall son:

- La configuración se almacena en un disquete floppy, en una memoria USB o en un disco duro, también puede ser enviada por correo electrónico.
- Para almacenar los registros (logs) se usa una base de datos Mysql (excepto para los informes del proxy squid), esto hace posible usar la consola para otros cortafuegos o programas de monitorización o detección de intrusiones.
- Basada en redhat 9.0
- Soporta el modo puente
- Registro de correos en busca de virus o spam.
- Durante el arranque se pueden configurar algunos parámetros, como las direcciones IP, dirección del servidor DNS, etc...

Al igual que en el caso de pfSense, redWall no ha sido diseñado y desarrollado teniendo en cuenta los principios básicos de escalabilidad. Por tanto es difícil y costoso ampliar o modificar el sistema.

Devil-Linux Devil-Linux es una distribución que arranca desde CDROM. La configuración del dispositivo puede ser almacenada en un disquete o una memoria usb. Devil Linux pretendía inicialmente ser una distribución especifica para hacer funciones de cortafuegos y encaminador, sin embargo actualmente integra otros servidores.

Sin embargo, Devil-Linux aun no dispone de una interfaz de configuración gráfica, aunque si de algunos scripts asistentes que facilitan las tareas de configuración.

floppyfw Floppyfw es un router con capacidades avanzadas de cortafuegos que se ajusta al tamaño de un disquete flexible. Puede ejecutarse en equipos anticuados facilitando su reutilización y ahorrando costes.

Algunas características de floppyfw que destacan son su implementación de listas de acceso y enmascaramiento de IP (NAT), el filtrado de paquetes con estado y encaminamiento avanzado. También permite el formateado de tráfico.

Requiere un procesador 386sx o superior, con 2 interfaces de red, disquetera 1.44MB y 12MByte de RAM. Y permite el registro de eventos por klogd/syslogd, local y remoto.

Floppyfw es un buen router y cortafuegos básico, pero sus funcionalidades son muy limitadas. Carece completamente de funcionalidades de cortafuegos de aplicación y por tanto pertenece a otro nivel distinto del objetivo de este proyecto.

6. Estudio de viabilidad

Comenzando con el proceso de definición del proyecto, en esta primera fase se trata de ver el sistema en su conjunto y de describir una primera solución que puede incluir o no desarrollos a medida, y/o adoptar productos estándares del mercado.

Puesto que se trata de la realización de un Proyecto de Fin de Carrera, es obvio que se pretende realizar desarrollos allá donde sea necesario, así como reutilizar productos estándares (tales como librerías y componentes de software) para facilitar la construcción y propiciar la finalización del mismo en un tiempo razonable con el esfuerzo (y especialmente la dedicación) del que se dispone que suele ser limitado en estos casos. Se tendrá en cuenta por tanto la inclusión de productos estándares y reutilizables allá donde sea posible (y cuya licencia de uso lo permitan).

Como ya se ha comentado anteriormente, en una vista general del proyecto se observa que el objeto de trabajo es la realización de un sistema de seguridad perimetral similar a los anteriormente descritos (con algunas ventajas si cabe). Este trabajo pues, se puede dividir en dos partes bien diferenciadas, las cuales son:

1. Interfaz de usuario
2. Sistema Operativo / distribución instalable

Mientras que la primera parte tiene un componente importante de Desarrollo, la segunda se centra más en la integración de componentes software estándares y el empaquetamiento de todo el sistema en lo que se llama una *distribución instalable* (que no es más que una distribución de Linux –en nuestro caso basada en **Debian GNU/Linux**–, personalizada para incluir únicamente lo necesario para los requisitos de este proyecto –por motivos de seguridad, rendimiento y espacio– , y automatizada en la medida de lo posible tanto en el proceso de instalación –con objeto de facilitar su empleo como producto final, y solución "cerrada", por parte del usuario– como en el funcionamiento autónomo).

Este "Servidor de seguridad" proporcionará una serie de herramientas al Administrador de Red para implantar una política de seguridad perimetral en el ámbito de una red local con conexión al exterior (típicamente Internet).

Por tanto la Interfaz de Usuario tiene como misión la de permitir a este Administrador de Red (en adelante Usuario) la revisión del estado de funcionamiento, por una parte, y la realización de tareas de configuración y ajuste de parámetros por otra, para lograr hacer efectiva dicha implantación de la política de seguridad deseada.

El conjunto de Sistema Operativo y componentes de Software que llevan a cabo, de forma efectiva, la funcionalidad de Seguridad a la que hace mención su título (funcionalidad cuya parametrización se lleva a cabo a través de la Interfaz de usuario) se empaquetan mediante una Distribución Instalable: ésta no es más que la suma de estos elementos junto con la Interfaz de usuario desarrollada, en un formato empaquetado (similar al de las distribuciones Linux) y disponible para su instalación sobre un hardware estándar (PC).

6.1. Módulos de los que se compone el sistema

Para que se disponga de una funcionalidad mínima que permita al usuario el control de la seguridad de la red a nivel perimetral, se han considerado convenientes integrar una serie de componentes que constituyan un primer conjunto de herramientas de fácil integración y funciones complementarias. También de esta forma se consigue construir un sistema que resulte, al menos, competitivo en el mercado. Estos componentes son:

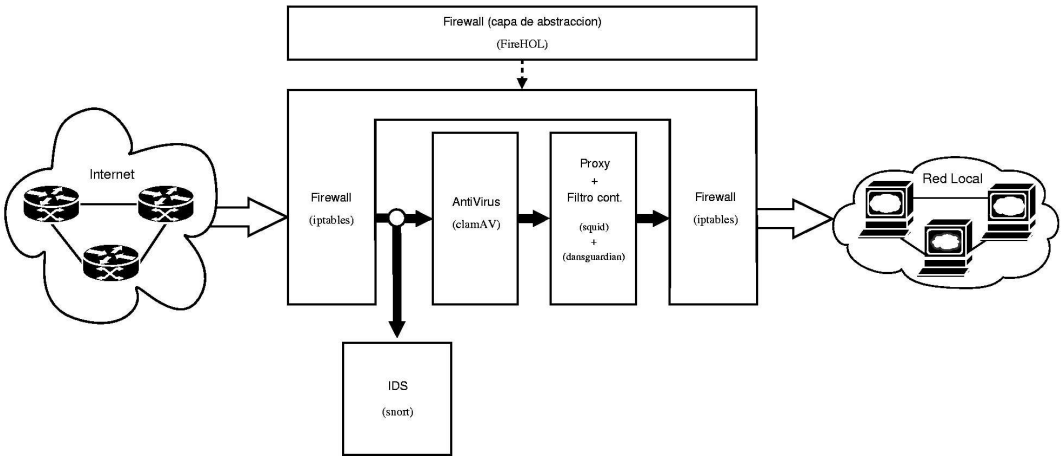

Figura 2: Módulos del sistema

- **Cortafuegos** (iptables, ipchains o similar)
- **Proxy** (Squid, Polipo, Privoxy, TinyProxy o similar)
- **Filtro de contenidos** (Dansguardian, SquidGuard, o similar)
- **Detector de intrusiones** (Snort, Prelude, o similar)
- **Antivirus** (ClamAV –open source– o algún otro del mercado)

En la figura 2, se representan gráficamente estos módulos y el flujo de datos a través de ellos en el sistema.

Si bien la primera parte del proyecto (interfaz de usuario) se centrará principalmente en el desarrollo, la segunda parte (distribución instalable) tendrá como objetivo principal la integración de estos componentes Software –que proporcionen las funcionalidades de seguridad requeridas–, y su empaquetamiento en forma de distribución Linux.

Volviendo a la Interfaz, se tratará pues de generar un producto a medida (ya que se ha visto que no hay disponible en la actualidad una aplicación que realice la tarea requerida con el nivel de detalle y automatización deseados, ajustándose a los componentes software que consideremos convenientes).

Tomadas estas decisiones, el estudio continuará en esta línea, primero a nivel más genérico, y posteriormente centrándonos en las alternativas elegidas.