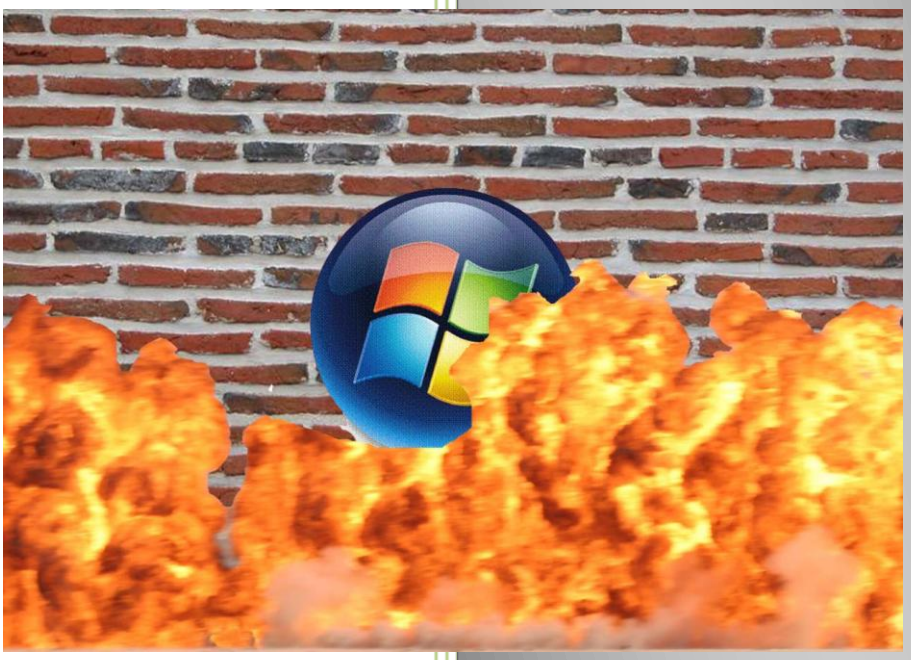
EiPE

FIREWALLS



INFORME PROFESIONAL

Armando Orera Gracia

Vicente Soriano Sarrió

INDICE

1. INTRODUCCIÓN: EMPRESA Y SEGURIDAD CON LAS TECNOLOGÍAS DE LA INFORMACIÓN

1.1. La empresa: dispositivos de acceso y redes

En el entorno de las empresas españolas, el teléfono móvil y el ordenador son los terminales informáticos y de acceso a las redes de comunicaciones preferentes, a la par en penetración, alcanzando cada uno de ellos a casi dos terceras partes de las microempresas y la totalidad del resto de empresas. La incorporación de esta infraestructura favorece a las empresas a la hora de llevar a cabo su actividad empresarial, permitiendo beneficiarse de todas las utilidades derivadas de la tecnología (acceso a Internet, mayor y mejor conectividad a través del correo electrónico, aplicaciones de gestión logística, rapidez de información y gestión, etc.). [1] [2] [3]

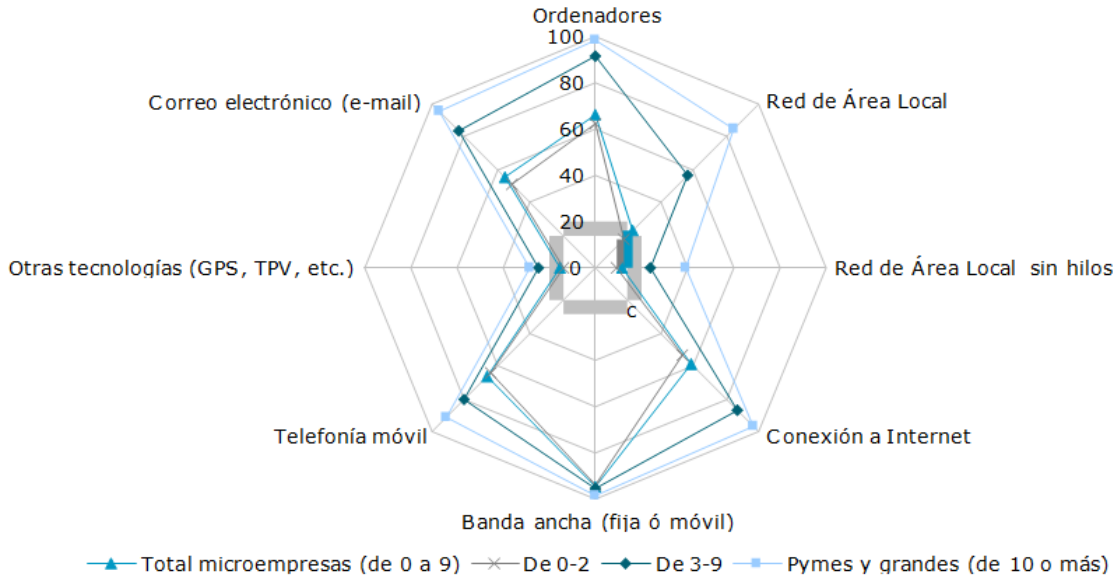


Ilustración 1 Infraestructura y conectividad TIC por tipo de empresa

1.2. Seguridad en PYMEs

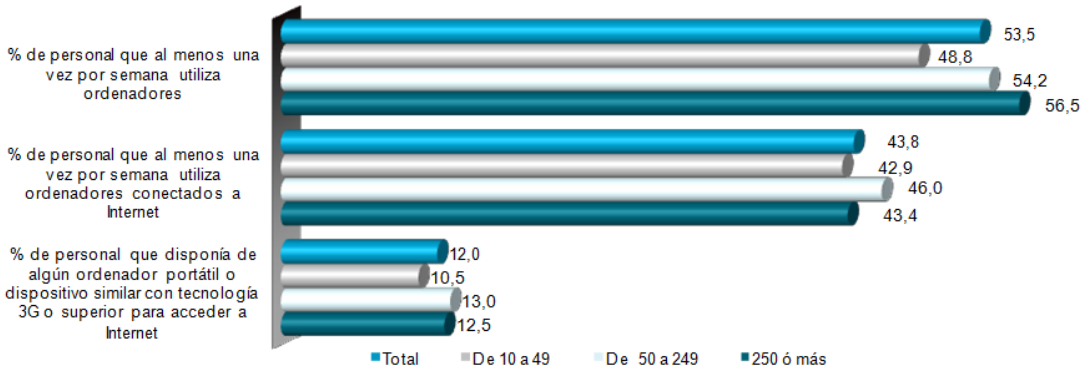
Generalmente, las pequeñas y medianas empresas no tienen una visión global sobre la situación de su seguridad. La falta de recursos provoca, a veces, que muchas PYMES cuenten con una seguridad insuficiente o no sepan exactamente cuáles son las medidas que tienen que adaptar para estar protegidos.

Las empresas españolas sufren más infecciones que las europeas: un 64% de las españolas ha sido infectada alguna vez, frente a un 58% de media en Europa.

Por esta causa, el 14% de los negocios en España, 30% en Europa, ha tenido que detener su negocio. [3] [4] [5]

1.3. Uso de las TIC por las empresas.

El porcentaje de personal que utiliza ordenadores de manera semanal en las microempresas es casi del 56% de los empleados, prácticamente igual a las de mayor tamaño. En el caso de que el ordenador disponga además de acceso a Internet los porcentajes son del 49,4% en microempresas frente al 44,9% en pymes y grandes empresas. [1]



[1]

Ilustración 2 Personal que utiliza ordenadores y ordenadores conectados a Internet, al menos una vez por semanas y disponibilidad de dispositivo móvil con tecnología 3G o superior.

2. AMENAZAS DE INTERNET

Estas infecciones se produjeron pese a que el 92% de las PYMEs españolas y el 93% de las europeas cuentan con algún sistema de seguridad.

En lo referente al tipo de protección instalada, el 26% de los negocios que cuentan con un sistema de seguridad en España tienen instalado software gratuito.

En lo que se refiere al papel que juega la seguridad en las empresas, las cifras coinciden y así, el 55% en España y en Europa consideran la seguridad muy importante para sus empresas. Sin embargo, sólo un 52% de las primeras y un 64% de las segundas cuentan con una persona dedicada en exclusiva a la seguridad.

Finalmente, respecto a un aspecto tan importante como es la formación sobre seguridad informática y amenazas cibernéticas, el 52% de las empresas españolas no recibe ningún tipo de formación de este tipo, siete puntos por encima de la media europea. [6]

El 53,5% del total de empleados de empresas de 10 o más empleados utiliza al menos una vez por semana ordenadores para desempeñar las tareas que requieren sus puestos de trabajo.

El 43,8% de los trabajadores de las empresas de 10 o más empleados utiliza al menos una vez por semana ordenadores conectados a Internet uso éste que asciende al 46% del personal de empresas medianas (50 a 249 trabajadores). [7]

En relación a los problemas que fueron causados por incidentes relacionados con los sistemas TIC en la empresa durante el año precedente, el 12,4% de las microempresas con ordenador ha tenido problemas de funcionamiento de los servicios TIC, destrucción o alteración de la información, debidos a fallos del software o del hardware.

En relación a las empresas de mayor tamaño, se encuentra que la tasa de microempresas que tuvo problemas de funcionamiento de los servicios TIC debidos a fallos del software o hardware (12,4%) es inferior a la de pymes y grandes empresas (19,1%). [1] [3] [8]

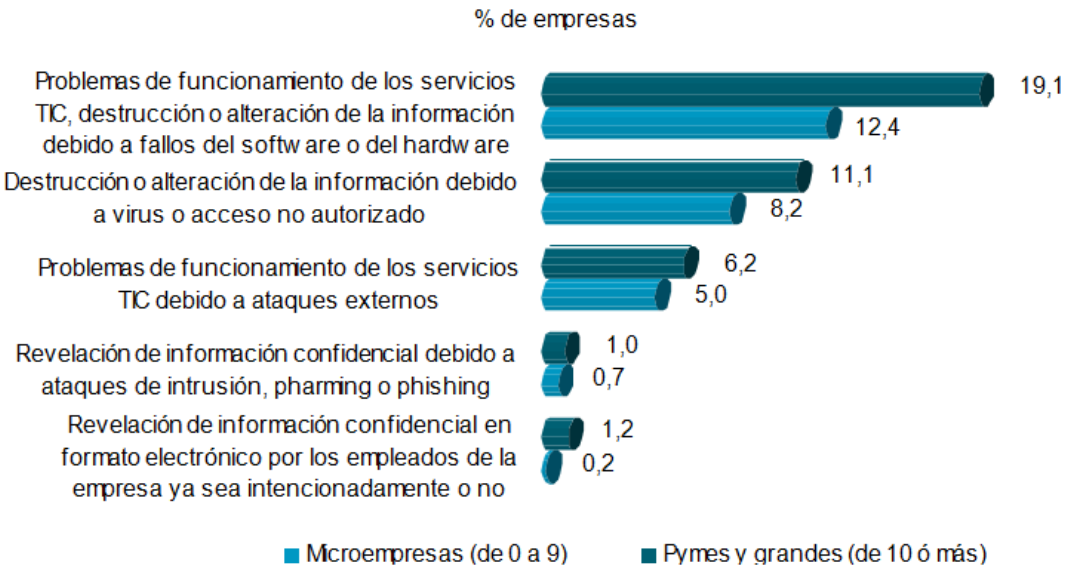


Ilustración 3 Problemas por incidentes relacionados con los sistemas TIC en la empresa

2.1. El ataque informático

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización, y persona, que tenga equipos conectados a la World Wide Web.

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

La seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos.

Afortunadamente, en la actualidad existe una gama muy amplia de herramientas de seguridad lo suficientemente eficaces que permiten obtener un adecuado nivel de seguridad ante intrusiones no autorizadas haciendo que la labor de los atacantes se transforme en un camino difícil de recorrer. [9]

2.2. El arma infalible: la ingeniería social

En el mundo de la seguridad de la información, el "arte de engañar" es utilizado para dos fines específicos, principalmente:

- El usuario es tentado a realizar una acción necesaria para vulnerar o dañar un sistema: esto ocurre cuando el usuario recibe un mensaje que lo lleva a abrir un archivo adjunto, abrir la página web recomendada o visualizar un supuesto video.

Un caso de "éxito" de este tipo de infecciones es el gusano Sober que, mediante un sencillo mensaje, logró ser el de mayor propagación del año 2005. Este malware alcanzó una distribución masiva con asuntos de correos tales como "Re:Your Password" o "Re:Your email was blocked".

- El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos. Este es el caso del Scam y el Phishing, en los que el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza o con un pretexto de que obtendrá algo a cambio, generalmente un "gran premio".

Estos casos evidencian otra importante característica de la Ingeniería Social: la excelente relación costo- beneficio obtenida con su aplicación, la convierte en una técnica de lo más seductora: con sólo una llamada telefónica, un correo electrónico o un mensaje de texto vía SMS el atacante puede obtener acceso a información valiosa del usuario, la empresa o incluso acceder a una red de sistemas.

Si bien se podría entrar en particularidades según cada caso, es fundamental comprender que no hay tecnología capaz de proteger contra la Ingeniería Social, como tampoco hay usuarios ni expertos que estén a salvo de esta forma de ataque. La Ingeniería Social no pasa de moda, se perfecciona y sólo tiene la imaginación como límite. [10] [9]

2.2.1. El tipo de amenaza con mayor incidencia

La amenaza que más afectó a las empresas que habían sufrido una infección, el 59% de las PYMES españolas señaló el malware –lo que comúnmente se conoce como "virus"- como principal amenaza, cifra un punto por debajo del porcentaje de empresas europeas que señalaron esta opción. [6]

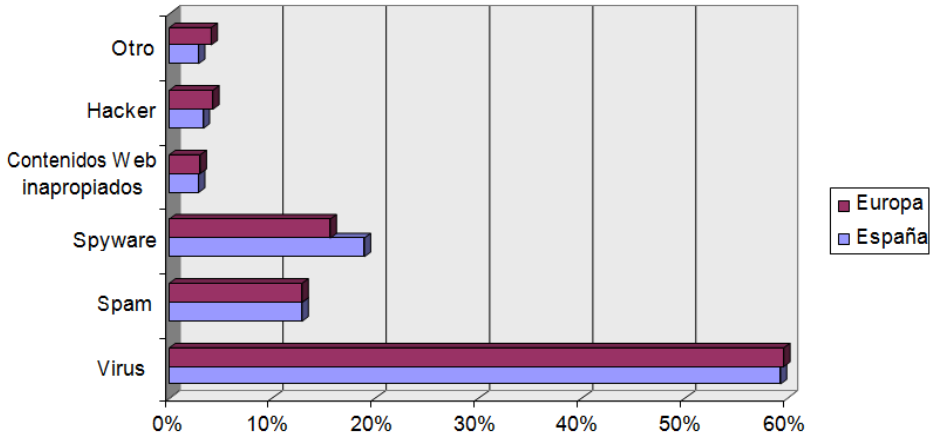


Ilustración 4 Incidencia en la empresa de las amenazas de internet

Las incidencias de seguridad declaradas por las pymes españolas suponen un problema crítico para el desarrollo del negocio. Cada vez más, los ataques son dirigidos por intereses económicos que provocan pérdidas de dinero o información confidencial. [4] [11]

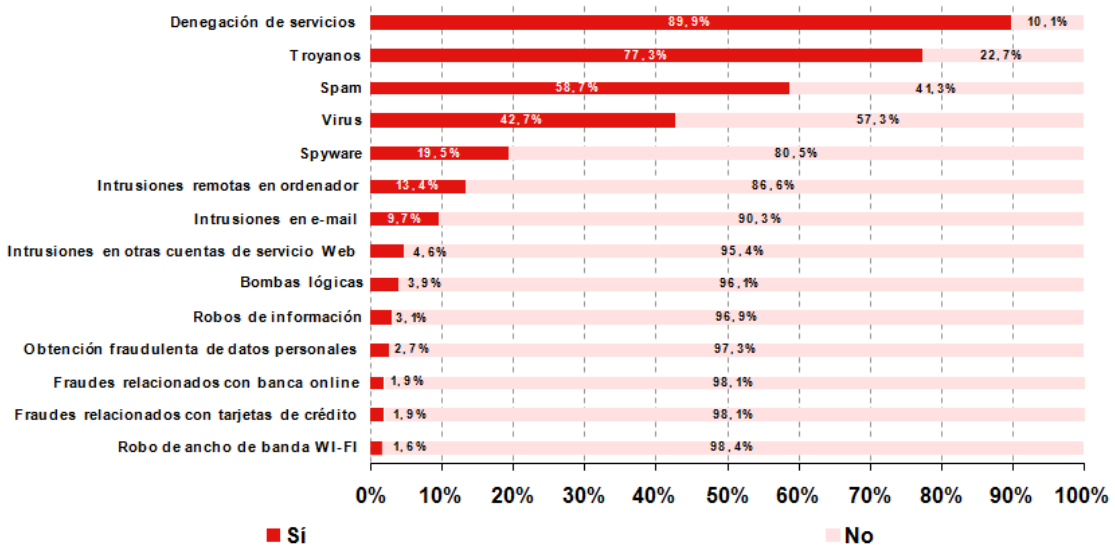


Ilustración 5 Percepción de incidencias de seguridad por las pymes.

2.2.2. El mercado negro del cibercrimen

Hoy en día nadie –ni usuario doméstico ni empresa- es inmune ante el robo de información confidencial y su posterior venta.

Además, aunque no hay datos exactos, creemos que este tipo de negocio ha proliferado con la crisis económica.

Donde sin duda se nota la necesidad de dinero de estas mafias es en la proliferación de ofertas de venta, en la guerra de precios y en la diversificación de negocio. Hace unos años, sólo vendían unos pocos datos de tarjetas de crédito. Ahora, además de que ofrecen hasta la fecha de nacimiento de la mascota familiar de la víctima robada, se ofrecen a realizar otro tipo de servicios en nombre del comprador, como duplicar físicamente las propias tarjetas o realizar compras anónimas y enviarlas al domicilio del ordenante.

Según el FBI, las organizaciones cibercriminales funcionan como empresas, contando con expertos especializados para cada tipo de trabajo y ocupación. A diferencia de una organización empresarial, estos cibercriminales trabajan sin horarios, sin vacaciones y sin fines de semana.

Este tipo de mercado tiene todos los ingredientes necesarios para satisfacer la ley de la oferta y la demanda: compiten en precios, ofrecen servicios añadidos, dan pruebas sin compromiso, garantizan la devolución si los datos no son operativos (o si la cuenta no tiene un capital mínimo garantizado)… incluso hacen compras anónimas para los vendedores. [12]

Tarjetas de crédito	Precio
Tarjetas de crédito Tarjetas de	Desde 2$ hasta 90$
crédito físicas Máquinas	Desde 180$ + coste de los datos
duplicadoras de tarjetas Cajeros	Desde 200 hasta 1.000 $
automáticos falsos Credenciales	Hasta 3.500$
bancarias	Desde 80 y hasta 700$ (con garantía de saldo)
Transferencias bancarias y cobro de cheques	Entre el 10 y el 40% del total a transferir o cobrar 10$ para cuenta simple sin saldo verificado
Cuentas de tiendas online y pasarelas de pago	Entre 80 y 1.500$ con saldo verificado
Diseño e implementación de falsas tiendas online	Según proyecto (sin especificar)
Compra y envío de productos	Entre 30 y 300$ (dependiendo producto)
Alquiler envío de spam	A partir de 15$
Alquiler SMTP	A partir de 20$. 40$ para uso durante 3 meses
Alquiler VPN	20$ para utilización para 3 meses

Ilustración 6 Principales características del funcionamiento del mercado negro.

2.3. El panorama de la seguridad de las TIC en la empresa española

Las incidencias de seguridad declaradas por las pymes españolas suponen un problema crítico para el desarrollo del negocio. Cada vez más, los ataques son dirigidos por intereses económicos que provocan pérdidas de dinero o información confidencial.

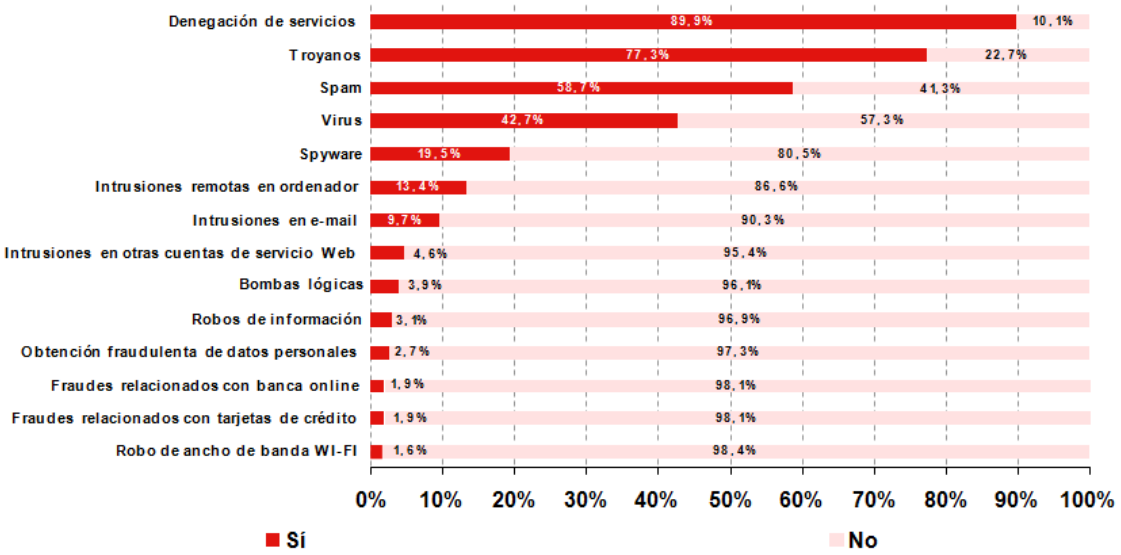


Ilustración 7 Percepción de incidencias de seguridad por las pymes

Las **grandes empresas** muestran un nivel de alto de preocupación y concienciación por la seguridad TIC. En los últimos años han invertido en tecnología y han implantado procesos y organizaciones para mejorar sus niveles de seguridad. El presupuesto dedicado a la seguridad ha crecido notablemente hasta llegar a superar el 15% del total dedicado a TIC [11]

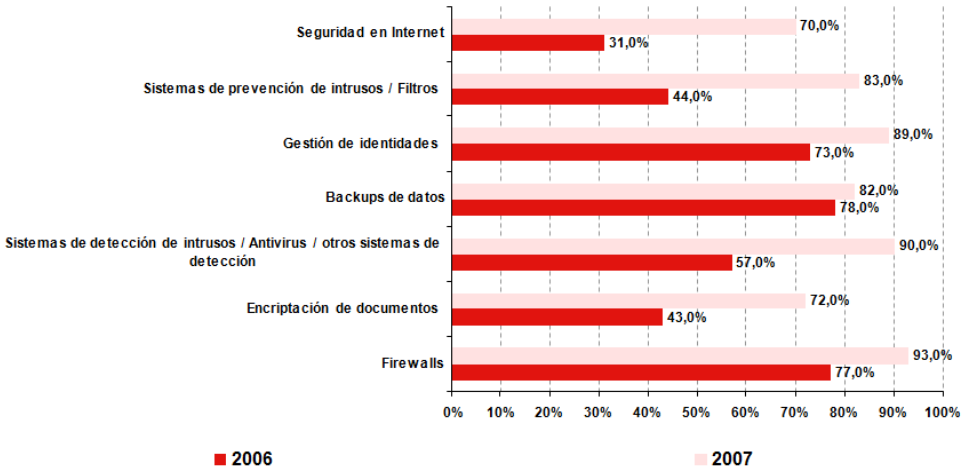


Ilustración 8 Porcentaje de empresas que tienen emplementadas herramientas de seguridad

2.3.1. Microempresas. Riesgos que contemplan las políticas de seguridad de las empresas

Las empresas que disponen de una política de seguridad definida y sujeta a revisión periódica, la utilizan para tratar, en primer lugar, los riesgos de destrucción o alteración de la información debido a accidentes inesperados o ataques (un 89,3% de las microempresas con política definida). En menor proporción, pero en porcentajes elevados también, se contemplan aspectos como los problemas de funcionamiento de los servicios TIC debido a ataques externos (82,9%) o casos en los que se revele información confidencial debido a intrusión, pharming, phishing o por accidente (77,2%).

Como se aprecia en la siguiente tabla, los sectores financiero e informático, telecomunicaciones y audiovisuales, son los que contemplan en mayor medida los tres tipos de riesgo en sus políticas de seguridad. [1] [2] [8]

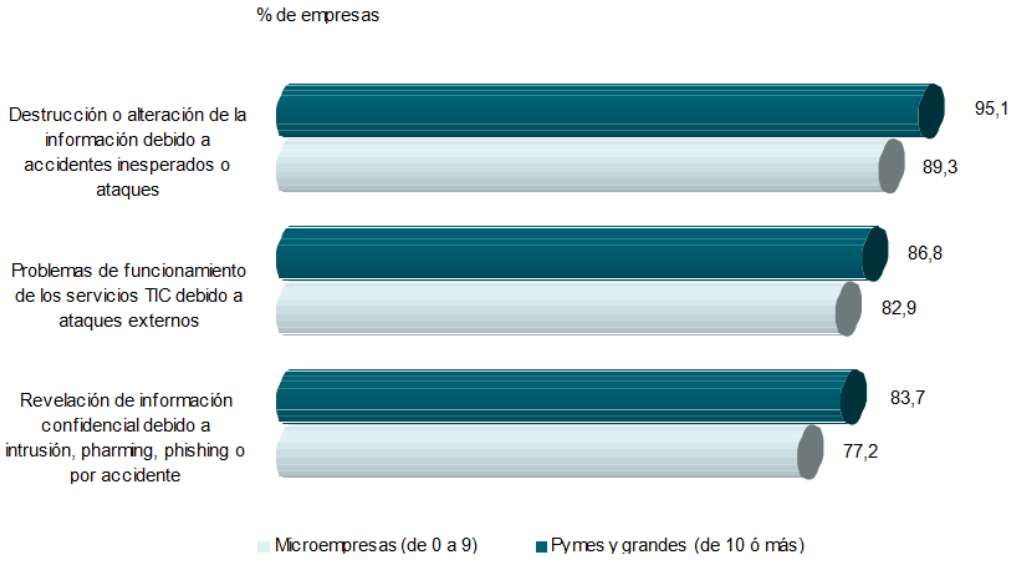


Ilustración 9 Riesgos que contemplan las políticas de las empresas.

2.3.2. Pequeña y mediana empresa. Percepción de la importancia de la seguridad

El gráfico siguiente denota que las pymes no tienen la formación necesaria para combatir las nuevas amenazas. Esta falta de conocimiento puede estar motivada por la ausencia de personal cualificado en materia de seguridad TIC en las pymes españolas: únicamente el 16% de las pymes encuestadas declara disponer de expertos en seguridad TIC en su plantilla. [11]

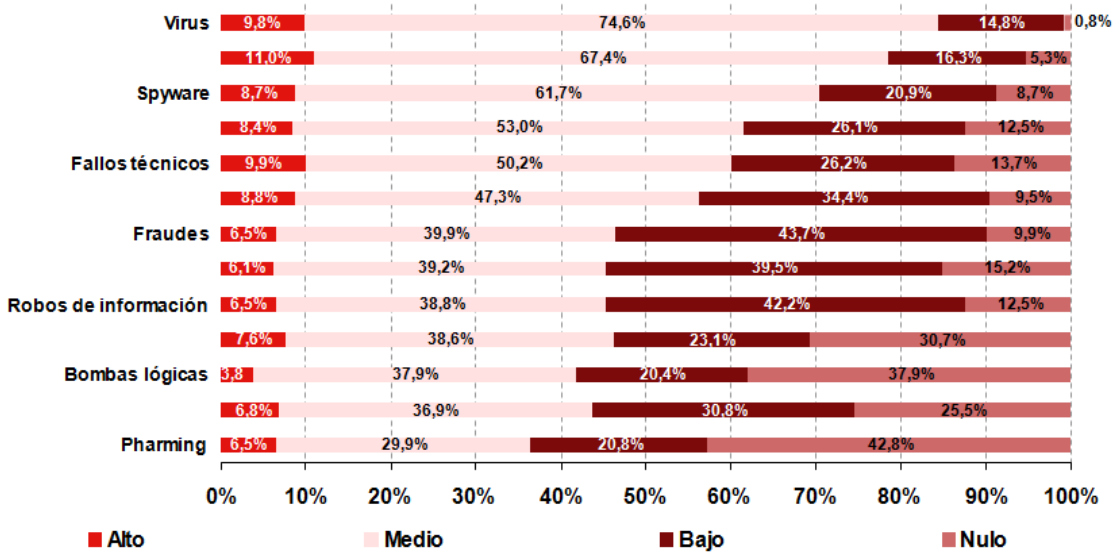


Ilustración 10 Grado de conocimiento de las incidencias de seguridad

2.3.3. Pequeña y mediana empresa. Qué tipo de amenaza le afectó más

Respecto a la amenaza que más afectó a las empresas que habían sufrido una infección, el 59% de las PYMES españolas señaló el malware –lo que comúnmente se conoce como "virus"- como principal amenaza, cifra un punto por debajo del porcentaje de empresas europeas que señalaron esta opción. [4]

	%	
	España	Europa
Virus	59%	60%
Spam	13%	13%
Spyware	19%	16%
Contenidos Web inapropiados	3%	3%
Hacker	3%	4%

Ilustración 11 Amenazas que afectaron a las pymes

2.3.4. Las TIC en empresas de menos de 10 trabajadores

El 69,7% de las empresas de menos de 10 empleados dispone de ordenadores y el 25,0% tiene instalada una Red de Área Local (LAN).

En cuanto al uso de Internet, el 64,1% de las empresas pequeñas dispone de acceso a Internet, lo que supone un incremento del 10,4% respecto a enero de 2010. El 96,8% de estas empresas con conexión a Internet acceden mediante alguna solución de Banda ancha.

En cuanto a las comunicaciones, el 70,7% las empresas con menos de 10 empleados son usuarias de telefonía móvil y el 17,9% utilizan otras tecnologías (GPS, TPV,...).

En cuanto a la presencia en la Red, el 25,9% de las empresas pequeñas con conexión a Internet dispone de página web, lo que supone un incremento del 3,7% respecto a enero de 2010 [13] [3] [8]

Porcentajes

	Enero de 2010	Enero de 2011
Ordenadores	66,2	69,7
Red de Área Local	22,9	25,0
Red de Área Local sin hilos	11,4	14,1
Conexión a Internet	58,1	64,1
Conexión a Internet mediante banda ancha (fija o móvil)1	94,3	96,8
Telefonía móvil	66,3	70,7
Otras tecnologías (p.e. GPS, TPV, etc.)	15,5	17,9
% de empresas con conexión a Internet y sitio/página web.1	25,0	25,9

[1] Porcentaje sobre el total de empresas con conexión a Internet

Ilustración 12 Infraestructuras TIC de las empresas de menos de 10 empleados.

2.3.5. Las TIC en empresas de más de 10 trabajadores

El porcentaje de empresas con conexión por Banda ancha fija ha aumentado del 98,2% en enero de 2010 al 99,3% en enero de 2011. Por su parte, el porcentaje de empresas con conexión a Internet y página web ha pasado del 63,9% al 67,0%, mientras que la interacción de las empresas con las Administraciones Públicas vía Internet se ha incrementado del 70,1% al 84,0%.

El 40,5% de las empresas realizan intercambio electrónico de datos con otros sistemas TIC externos. Los mensajes intercambiados con más frecuencia son el envío de instrucciones de pago a entidades bancarias (75,5%) y el envío o recepción de información con la Administración Pública (64,8%).

Las ventas a través de comercio electrónico representaron el 11,5% del total de ventas efectuadas por las empresas españolas. El 89,4% de las ventas por comercio electrónico tuvieron como destino otras empresas (*Business to Business*, B2B).

Las compras a través de comercio electrónico representaron el 15,6% de las compras totales efectuadas por las empresas, un 0,9% más que en el año anterior. [3] [14]

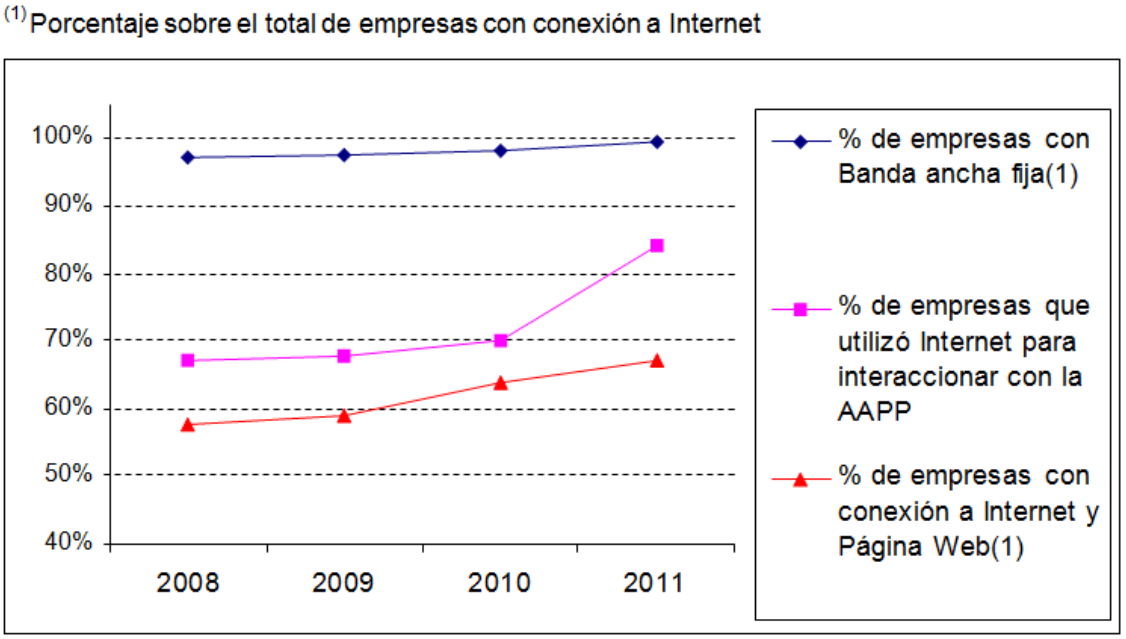


Ilustración 13 Evolución de las TIC 2008-2011

2.4. La defensa mínima

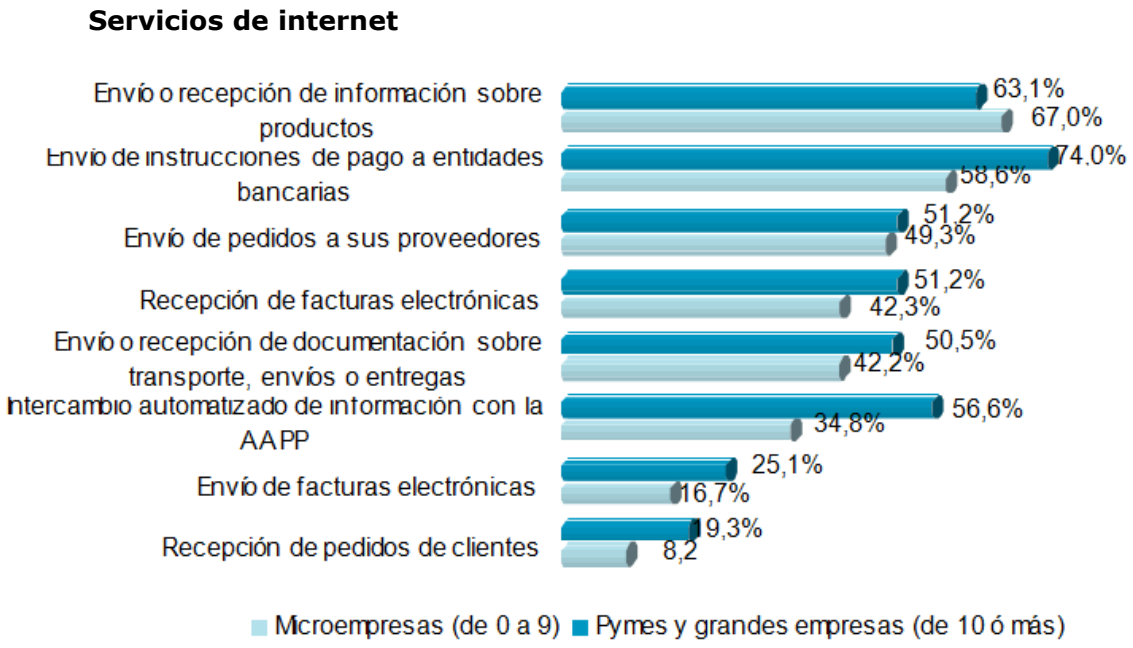


Ilustración 14 Tipo de intercambio electrónico de datos con otras empresas.

2.4.1. Tipos de defensas /ataques

El motivo de que se creen más troyanos, keyloggers y bots que ningún otro tipo de malware es porque resultan los más útiles para el robo de identidad. En el año 2005, casi la mitad de los nuevos códigos maliciosos eran troyanos:

Ilustración 15 Nuevo malware por tipo.

Al cierre de 2010, la situación es mucho peor, ya que los troyanos suponen más del 71 por ciento del nuevo malware.

Los hackers buscan el beneficio económico, y la venta de los datos que consiguen mediante las infecciones, redes de bots, phishing, etc., prueba que no se trata de un argumento del último éxito de hollywood, sino de una realidad. [12]

2.4.2. Ataques de negación de servicio.(DoS, Denial of Service)

Los ataques DoS son puramente maliciosos. No producen ningún beneficio para el "hacker", mas que el "placer" de que las redes, o parte de ellas, queden inaccesibles para sus usuarios. Un ataque DoS sobre- carga el sistema de manera que lo deja inhabilitado, negando así la posibilidad de utilizar los servicios de la red. Los "hackers" envían grandes paquetes de datos o programas que requieren que el sistema responda continuamente a comandos falsos. [1]

2.4.3. Fugas internas de información

La amenaza también puede provenir de la propia empresa, bien por errores humanos, bien por acciones deliberadas de los usuarios del *cloud*. Estos incidentes desencadenan pérdidas de información, con los consiguientes daños en la imagen de la empresa y las posibles consecuencias legales y/o jurídicas. Para evitar estas situaciones, las organizaciones utilizan medidas como la incorporación de cláusulas de confidencialidad en los contratos la- borales o el establecimiento de políticas de seguridad [15]

2.4.4. Autenticación y certificación digital

Son productos definidos en torno a los certificados digitales para aportar mayor seguridad a procesos, aplicaciones y sistemas que los utilizan. Estos productos permiten aplicar los certificados digitales en distintos escenarios y situaciones.

Los certificados digitales se usan también en tarjetas inteligentes, o *smart cards*, en las cuales se pueden almacenar, y por tanto en esta categoría se recogen los productos relacionados con dispositivos lectores de este tipo de tarjetas. El DNI electrónico, o DNIe, es un ejemplo de tarjeta inteligente que incluye certificados digitales para autenticación y firma.

Así mismo, se incluyen en esta categoría todo tipo de productos que permiten la creación y emisión de certificados digitales.

2.4.5. Gestión y control de acceso e identidad

Son productos destinados a dotar a las empresas y organizaciones de mecanismos que permitan: gestionar usuarios y sus datos de identificación; asociar roles, perfiles y políticas de seguridad; y controlar el acceso a los recursos. Suelen ser integrados con mecanismos de autenticación que posibilitan el control de acceso lógico de los usuarios en los sistemas informáticos.

2.4.6. Anti-fraude

Las herramientas *anti-fraude* están destinadas a proteger a los usuarios de ataques que utilizan prácticas denominadas de ingeniería social. Uno de los objetivos de la ingeniería social es conseguir, mediante engaños, datos de los usuarios (contraseñas, cuentas de correo,…) para realizar con ellos actividades fraudulentas en internet.

Estos ataques consisten, entre otros, en el robo de información personal y de datos bancarios y la suplantación de identidad, utilizando para ello técnicas como intentos de fraude bancario *(phishing)*, redirección de páginas web *(pharming)*, correo electrónico no deseado *(spam)* o *malware* diseñado al efecto (programas que capturan las pulsaciones de teclado – *keyloggers, recolectores de contraseñas,…*).

Los intentos de fraude más frecuentes llegan a través de mensajes falsos (accesos a servicios financieros, ofertas de trabajo fraudulentas, loterías, premios o regalos,…). Los datos así obtenidos se utilizan para realizar fraudes o comerciar con esta información para ser usada en actividades que persiguen obtener un beneficio económico, generalmente con perjuicio del usuario engañado.

El fraude *on-line* es una amenaza que utiliza múltiples técnicas y distintas vías de entrada (servicios en Internet, *malware*) pero sobre todo se caracteriza por explotar la confianza de los usuarios y su dificultad para diferenciar aquello que es legítimo de lo que no lo es.

2.4.7. Anti-malware

Son herramientas destinadas a la protección de sistemas informáticos: servidores, ordenadores de sobremesa, portátiles, dispositivos móviles, etc., frente a todo tipo de software malicioso que pueda afectarles (virus, troyanos, gusanos, *spyware*, etc.)

El software malicioso o *malware* es una amenaza que utiliza múltiples técnicas y vías de entrada: páginas web, correo electrónico, mensajería instantánea, descarga de ficheros de redes P2P, dispositivos de almacenamiento externos (memorias USB, discos duros externos, CDs, DVDs,…) y puertos abiertos en nuestro ordenador. Entre otras, estas vías, son utilizadas por el *malware* para infectar a los sistemas informáticos y propagarse por ellos, afectando de distintas formas al uso para el que están destinados (impidiendo acciones, vigilando usos, ralentizando sistemas, ejecutando acciones no permitidas,…). Las herramientas anti-malware son de uso generalizado y las más antiguas que existen.

2.4.8. Control de contenidos confidenciales

Son herramientas que previenen la difusión, accidental o intencionada, de cualquier tipo de información o datos fuera de una organización. Evitan la fuga de información a través de correo electrónico, mensajería instantánea, transferencia de ficheros mediante FTP, redes P2P, chats, blogs o mediante dispositivos externos de almacenamiento, como es el caso de las memorias USB.

Actúan monitorizando todo tipo canales de comunicación, desde y hacia el exterior de la organización, evitando la fuga de información e implementando políticas de uso de información sensible.

Se incluyen en estas herramientas aquellos sistemas que gestionan el ciclo de vida de información, controlando el uso autorizado de documentos electrónicos y facilitando la destrucción de los mismos cuando estén en desuso.

2.4.9. Sistemas y herramientas criptográficas

Son herramientas destinadas a proteger la confidencialidad de la información tanto en tránsito como almacenada. Permiten el cifrado y descifrado de la información mediante técnicas criptográficas, lo que impide un uso indebido de la misma por personas no autorizadas y permite el intercambio de la información de forma segura a través de medios o sistemas de comunicación inseguros, por ejemplo a través de correo electrónico o transferencia de ficheros.

Así mismo, no sólo protege la confidencialidad de la información, sino que además incorpora mecanismos para detectar modificaciones, cambios o manipulaciones durante su envío o almacenamiento. Por tanto, son herramientas que también protegen la integridad de la información.

2.4.10. Contingencia y continuidad

Son herramientas cuyo objetivo es facilitar el proceso de implantar planes de contingencia y continuidad en las organizaciones en todas sus fases. Por tanto, son herramientas que facilitan y posibilitan la gestión de los planes de contingencia y continuidad, desde su concepción y diseño hasta su implementación, pasando por su seguimiento, mejora continua y gestión de los incidentes que se puedan dar y que pondrán a prueba dichos planes. Entre estas herramientas, las de recuperación de sistemas, tras un incidente que afecta a la disponibilidad de la infraestructura TIC y las herramientas de copias de seguridad, son fundamentales para la implantación de planes de contingencia y continuidad en las organizaciones.

Para que un plan de contingencia y continuidad funcione correctamente es importante un buen diseño del plan, establecimiento de los tiempos de recuperación necesarios, implementación de medidas y políticas y valoración del impacto.

Estas herramientas están muy enfocadas a la recuperación ante desastres e incidentes de seguridad. La externalización se ha convertido en un elemento fundamental de este tipo de herramientas, como son las soluciones de copia de seguridad remota. Por otra parte, la virtualización está cobrando importancia a la hora la de conseguir reducir lo máximo posible los tiempos de despliegue y puesta en marcha de infraestructuras de respaldo, con el objetivo de reducir los tiempos de interrupción de la actividad.

2.4.11. Cortafuegos / VPN / IDS, IPS

Son productos destinados a proteger los sistemas y dispositivos conectados a una red. Son herramientas que permiten establecer un perímetro de seguridad y garantizar las comunicaciones seguras para evitar accesos no autorizados y ataques provenientes de de redes externas y de internet.

Esta categoría agrupa a productos que aseguran que las comunicaciones hacia y desde la red, corporativa o doméstica, cumplen las políticas de seguridad establecidas.

Para ello rastrean y controlan las comunicaciones, bloqueando el tráfico, detectando comportamientos anómalos y ataques y evitando intrusiones no autorizadas. También se integran en esta categoría las herramientas que permiten extender la red corporativa a entornos distantes (sedes remotas, oficinas) creando enlaces de comunicación seguros.

2.4.12. Seguridad en movilidad

Son herramientas destinadas a la protección de redes inalámbricas y dispositivos móviles o de dispositivos en movilidad (portátiles, PDAs, *Smartphones*,…) de forma que se minimicen o reduzcan los incidentes de seguridad. Un ejemplo es la protección de los datos en caso de sustracción o la pérdida de dispositivos.

Así mismo, son herramientas que protegen no solo a los dispositivos en movilidad, sino que además proporcionan protección y seguridad a aquellos dispositivos e infraestructuras a las cuales se conectan dichos dispositivos, proporcionando mecanismos de acceso y autenticación robustos, que posibilitan el uso de redes de comunicaciones desde cualquier localización o situación de forma segura.

Algunas de estas herramientas disponen además de hardware adicional de autenticación, como lectores biométricos de huella digital, lectores de tarjeta, etc.

2.4.13. Control de tráfico de Red

Son herramientas destinadas al control de la actividad de las infraestructuras de comunicaciones de una organización con distintos objetivos: cumplimiento de políticas de seguridad de la organización, seguridad perimetral y disponibilidad y uso adecuado de los recursos.

Permiten controlar el tráfico generado y recibido mediante el empleo de sondas o sistemas que recolectan información en tiempo real de los elementos de la red, realizando también un análisis de los datos recogidos para detectar situaciones que están fuera de los parámetros normales de operación. Se realiza así un control sobre el uso del ancho de banda, los usuarios, el tipo de tráfico y del rendimiento en general.

Son herramientas centradas en proteger la disponibilidad de las infraestructuras de comunicaciones de las organizaciones.

2.4.14. Gestión de eventos

Son productos que permiten llevar a cabo la gestión de eventos o incidentes de seguridad en cualquiera de sus fases, ya sea antes, durante o después de que se produzca un incidente. Recogen, cotejan y hacen informes con los datos de los registros de actividad (*logs*) de los dispositivos de seguridad o de red instalados en la red de área local (LAN): *routers* (enrutadores), *switches* (conmutadores), cortafuegos, UTMs,… Así mismo, permiten establecer un flujo para la gestión de los eventos de seguridad de forma que sea posible tratar los incidentes de forma organizada y siguiendo un

procedimiento cuyo objetivo es la resolución del incidente en el menor tiempo posible y con las menores consecuencias para las organizaciones.

Son herramientas que posibilitan actuar en la prevención, detección, mitigación, análisis y aplicación de contramedidas.

2.4.15. Auditoría técnica y forense

Son herramientas destinadas a la realización de auditorías de sistemas, aplicaciones y datos, para determinar posibles fallos de seguridad o brechas que pudieran ser fuente de un incidente de seguridad y, por tanto, de un riesgo para los activos de una organización. Por tanto, de forma general, son herramientas de prevención.

Por otro lado, en esta categoría se incluyen las herramientas de auditoría forense que, a diferencia de las anteriores, están orientadas a determinar qué ocurrió y cómo se ocasionó un incidente de seguridad, una vez que éste ya ha tenido lugar. Por tanto, son herramientas de análisis posteriores a un incidente.

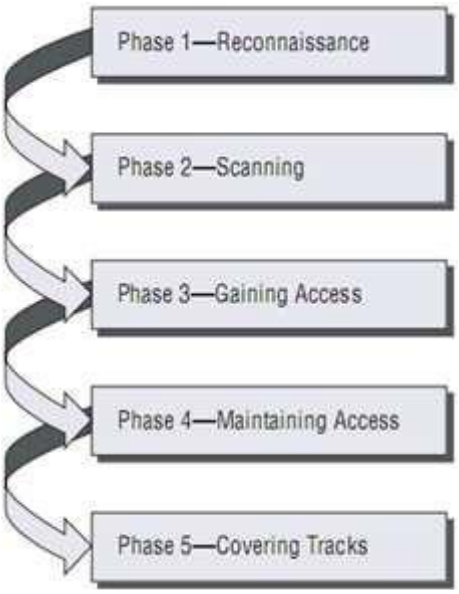
En la realidad, ambos tipos de herramientas se pueden combinar y, en algunos casos, se pueden usar de forma indistinta tanto antes como después de un incidente, puesto que muchas de sus funcionalidades son similares o realizan las mismas tareas, pero en un momento distinto del tiempo.

Las herramientas más orientadas a auditoría forense hacen uso de los *logs* o registros que quedan almacenados en los sistemas para establecer la historia del incidente, así como de los rastros de la actividad del incidente que puedan encontrarse en otro tipo de registros. [14]

2.5. Anatomía de un ataque informático: Fases

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

La siguiente imagen[1] muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado:



- Fase 1: Reconnaissance (Reconocimiento)

Esta etapa involucra la obtención de información (*Information Gathering*) con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el *Dumpster Diving*, el *sniffing*.

- Fase 2: Scanning (Exploración)

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el *network mappers*, *port mappers*, *network scanners, port scanners*, y *vulnerability scanners*.

- Fase 3: Gaining Access (Obtener acceso)

En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (*Flaw exploitation*) descubiertos durante las fases de reconocimiento y exploración.

Algunas de las técnicas que el atacante puede utilizar son ataques de *Buffer Overflow,* de *Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking*.

- Fase 4: Maintaining Access (Mantener el acceso)

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

- Fase 5: Covering Tracks (Borrar huellas)

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS). [9]

3. LA SEGURIDAD EN LA RED

3.1. Introducción

Desde que las empresas e individuos comenzaron a comunicarse mediante Internet ha surgido un problema de seguridad que afecta a los datos que mantienen en sus sistemas privados así como aquellos que son enviados a sitios remotos de la red mundial.

Los firewalls ofrecen una solución a estos problemas y ha surgido una amplia variedad de tecnologías y estrategias de entre las cuales se encuentran, como innovación de los últimos tiempos, los firewalls distribuidos, que permiten establecer políticas más flexibles y robustas que los sistemas convencionales que dependen fuertemente de la topología de la red sobre la cual se implementen.

Considero necesario introducir las tecnologías utilizadas en la implementación de un firewall tradicional ya que estas son la base sobre la cual se desarrollaron los firewalls distribuidos [16] [1]

3.1.1. Necesidad de seguridad

El uso de las computadoras se ha convertido en la herramienta esencial para el manejo de información en nuestra vida cotidiana y más aún en la realización de los negocios de hoy en día.

Como consecuencia ha surgido una necesidad de compartir información entre usuarios y entre estos y organizaciones o empresas. Esta necesidad ha sido dirigida por dos fuerzas: los laboratorios y proyectos de investigación, que ante la necesidad de colaboración necesitaron compartir información entre diferentes grupos situados en lugares remotos y desarrollaron protocolos y métodos para transferir datos (como por ejemplo TCP/IP); y por otro lado los intereses de las empresas, la necesidad de mejorar el intercambio de información corporativa entre oficinas o edificios llevó al desarrollo de varios protocolos desarrollados para estos fines.

Luego, la necesidad de comunicación se extendió a grandes áreas y surgieron nuevas industrias en la manipulación de routers, gateways y otros dispositivos para posibilitar tal transmisión de datos. Así mismo se estableció una tendencia al uso de protocolos estándares de uso común entre multitud de organizaciones que les permitiría intercomunicarse de forma apropiada.

Muchas organizaciones ofrecen servicios mediante sus sistemas de comunicación, la efectivización de tales servicios requiere el acceso a recursos críticos del sistema de información de la empresa (archivos, dispositivos de almacenamiento, líneas telefónicas, etc). Dichos recursos deben ser protegidos contra el uso indiscriminado y malicioso por parte de usuarios no deseados. Si un sistema de comunicación es vulnerable a estos tipos de ataques, el riesgo de pérdida de datos es importante. Este

riesgo potencial de seguridad aumenta junto con el nivel de dependencia en tecnología de información, lo que requiere el uso sistemas de seguridad más confiables y robustos.

Las redes son riesgosas por tres razones:

- Existen muchos puntos vulnerables desde donde puede ser lanzado un ataque,
- El perímetro físico del sistema de comunicación se ha extendido, existiendo mensajes de entrada y salida, manteniendo contacto con todos los otros sistemas conectados a la red,
- Las redes ofrecen múltiples servicios de conexión, cada uno con un punto de acceso propio. Cada uno de estos requiere una protección adecuada contra intrusos y cada una ofrece una complejidad y dificultad propia.

Las organizaciones poseen un conjunto de computadoras conectadas a la red propia y al exterior (no son simples computadoras conectadas unas a otras), que deben ser capaces de establecer comunicaciones confiables con cualquier dispositivo en la red (completa). Puesto de esta forma, parece ser una tarea bastante complicada en lo que a seguridad se refiere. Afortunadamente la red puede ser configurada de manera que solo una computadora necesite comunicarse con el exterior. Tal dispositivo dedicado es llamado "compuerta cortafuegos" (firewall gateway) y suele ser el principio de una estrategia de seguridad. [7] [16]

3.1.2. Requerimientos funcionales de una solución de seguridad

La implementación de un buen sistema de seguridad requiere el uso de ciertas funciones que permitirán asegurar la confidencialidad e integridad de los recursos de nuestra red contra los ataques de intrusos. De este planteo surgen algunas cuestiones [Ches-Bell], previas a la elección de las tecnologías a utilizar, que deberán se resueltas al momento de implementar un mecanismo de seguridad efectivo para una red:

¿Que recursos tratamos de proteger? Un determinado host posee ciertos recursos y tiene acceso a otros recursos de la red. Deben determinarse qué recursos son críticos para la organización y deben, por lo tanto, ser protegidos contra el acceso de intrusos. Tales recursos pueden ser archivos confidenciales, dispositivos de almacenamiento u otro tipo, líneas de conexiones, etc. Estas decisiones determinarán las medidas a tomar o estrategia que asegurarán la aplicación de los permisos de acceso a los recursos para cada posible usuario (host confiable o no); por ejemplo, si queremos proteger todos esos recursos, debemos efectuar un control en un punto previo a la entrada a la red local.

Estas decisiones deben tomar en consideración otra cuestión referida a dónde se originan los problemas de seguridad, es decir ¿contra quien defendemos nuestros sistemas?. Es posible que un intruso asuma la identidad de un host confiable para la red y tenga acceso a recursos que de otra forma no tendría. Además debemos tener en cuenta qué tan severo sería que la seguridad sea quebrada y los recursos de la red sean accedidos por usuarios no deseables. El objetivo es que esto nunca suceda por lo que

podríamos decidir implementar una estrategia severa con mecanismos de alta calidad, pero estamos dejando de lado otro importante factor. [13] [17] [16]

3.2. Seguridad en Tránsito

Todas las comunicaciones entre sitios que forman parte de una red pública son vulnerables a ataques de escuchas, éste riesgo está asociado con la importancia que tiene la información para quien tenga la habilidad de interceptar dicha comunicación.

La seguridad en tránsito enfatiza la necesidad de mantener los datos seguros mientras transitan una red pública como Internet. Así, disponemos de ciertas funciones o servicios que cubren distintos puntos de este aspecto. [1] [7] [18] [17] [16]

3.2.1. Limitar la exposición de la red interna

De esta forma podemos ocultar "todo" lo que sucede dentro de la red de la organización de la red pública, que de otra forma significaría un riesgo en la seguridad de las comunicaciones y los recursos.

Mediante este servicio es posible ocultar el esquema de direcciones de la red interior, para evitar que cualquier host no confiable efectúe comunicaciones de forma directa con alguno de los host de nuestra red, así como también asegurar que todo el tráfico entre hosts confiables de la red privada que atraviese una red pública se mantenga de esa forma (es decir, solo accesible a aquellos hosts a quienes está destinada la comunicación). Estas funcionalidades pueden ser logradas mediante el uso de la Traducción de Direcciones de Red (NAT) y de Redes Privadas Virtuales (VPN) respectivamente.

3.2.2. Criptografía

La necesidad de comunicarnos nos ha llevado a un nivel de conexión que nos permite enviar datos a cualquier sitio del mundo. Surge entonces el riesgo de que cualquiera pueda interceptar nuestros mensajes; si nuestros datos tienen cierta confidencialidad sería entonces deseable que nadie, que intercepte dicha comunicación, pueda acceder a ellos, sino solo el receptor deseado.

La criptografía es la transformación de un mensaje, mediante mecanismos y claves, en una forma ilegible y sin sentido propio. De esta forma, quien intercepte un mensaje encriptado no será capaz de saber qué es lo que tiene en su poder. Los mecanismos de encriptación utilizados en la actualidad aseguran que solo el receptor deseado sea capaz de leer el mensaje recibido aplicando el proceso inverso de encriptación.

La criptografía ofrece una segunda funcionalidad: autenticación. ¿Sabemos con quién nos comunicamos en Internet? ¿Es confiable la otra parte? La criptografía agrega a las comunicaciones sobre Internet un aspecto de seguridad muy importante, la certeza de la identidad de aquellos terceros con quien se establecen comunicaciones y se intercambia información. El hecho de poder desencriptar un mensaje correctamente,

por parte del receptor deseado, le da la seguridad de quién lo ha enviado ya que solo dicha entidad pudo encriptar el mensaje que ha sido recibido (aunque existen algunas consideraciones a este respecto que serán tratadas más adelante).

3.2.3. Tunneling de Tráfico, Puntos de control y Monitoreo

La transmisión de paquetes entre dos sistemas finales remotos en Internet involucra la intervención de varios sistemas intermedios que pueden tener acceso a la información transmitida si no se considera ningún esquema de privacidad.

Un túnel es un tipo especial de conexión entre dos sistemas a través de una red.

3.3. Regulación de Tráfico

Otro de los aspectos importantes acerca de la seguridad de las redes es regular de cerca qué tipos de paquetes pueden viajar entre redes. Si un paquete que puede hacer algo malicioso a un host remoto nunca llega a él, el host remoto no se verá afectado. La regulación del tráfico provee este servicio entre hosts y sitios remotos. Esto sucede en tres áreas básicas de la red: routers, firewalls y hosts. Cada uno provee servicios similares en diferentes puntos de la red. De hecho, la línea que los diferencia es arbitraria y difusa. [19] [20] [21] [16]

3.3.1. Política de seguridad

Una política de seguridad es un conjunto de decisiones que determinan, de forma colectiva, la postura asumida con respecto a las medidas de seguridad implementadas (o a implementar) en una red de computadoras.

No existe una fórmula para la política de seguridad de una red privada sino que cada responsable debe diseñarla según el caso.

Las consideraciones de una política de seguridad están dirigidas por las necesidades estructurales, de negocios o tecnológicas de la organización y pueden involucrar decisiones tales como restringir el tráfico de salida de red que permita a los empleados exportar datos valiosos, restringir el software importado por los empleados sin permiso de la compañía, impedir el uso de un determinado protocolo de comunicación porque no puede ser administrado de forma segura, entre otras. Este es un proceso iterativo que permite modificar la filosofía para ajustarse a las necesidades del momento.

El funcionamiento de un firewall está fuertemente asociado a la política de seguridad elegida. Definir los límites de comportamiento es fundamental para la operación de un firewall. Por lo tanto, una vez que se haya establecido y documentado apropiadamente una sólida política de seguridad, el firewall debe ser configurado para reflejarla y es su trabajo aplicarla como parte de una defensa de perímetro (siguiendo el enfoque tradicional). Consecuentemente se configura un firewall para rechazar todo, a menos que hayamos elegido explícitamente aceptarlo y correr el riesgo. Tomar el camino opuesto de rechazar solo a los ofensores conocidos es una opción

extremadamente peligrosa. Por último, cualquier cambio hecho al firewall debería se corregido en la política de seguridad y viceversa.

3.3.2. Filtros y listas de acceso

Los filtros son programas que generalmente se encuentran situados en los sistemas que proveen conectividad entre redes, es decir los puntos de acceso a la red, routers, firewalls y gateways

Con la utilización de un filtro es posible bloquear toda comunicación con ciertas partes (sitios) de la red externa para evitar determinados comportamientos no deseables en los sistemas finales de la red privada; permite restringir todas las comunicaciones entrantes a ciertos servicios de la red para evitar el acceso a recursos privados; y habilitar alarmas o avisos que adviertan que paquetes entran, salen o son rechazados. Por lo tanto el filtro de paquetes puede actuar tanto para la entrada como para la salida de paquetes de la red.

3.4. Modelo de Referencia

Partiendo de la necesidad de implantar estos servicios para una solución firewall, se ha definido un modelo de referencia [Peri] que establece los diferentes componentes que deben estar presentes (*ver Figura 18*)

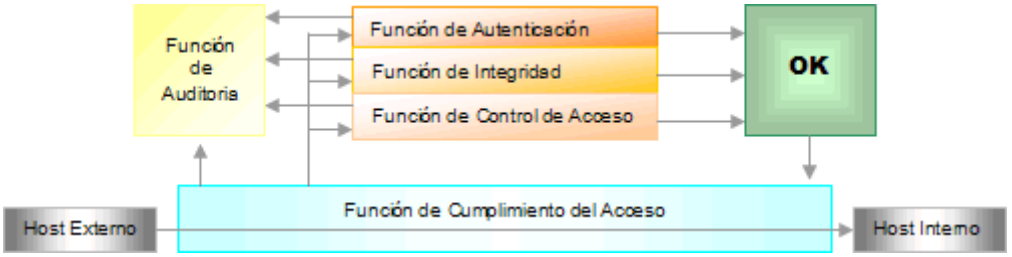


Ilustración 18 Modelo de referencia para firewalls

Función de Auditoría o Monitoreo: permite el registro de eventos relevantes del sistema, muy útil para la detección de intrusos.

Función de Autenticación: permite la identificación certera de la entidad con la cual se establece una comunicación.

Función de Integridad: asegura que el paquete ha sido recibido tal cual fue enviado y que no ha sido falseado en el transcurso de su transmisión.

Función de control de Acceso (filtrado de paquetes): en base a información dentro del paquete, se verifican las reglas de seguridad para determinar el destino del paquete.

Función de cumplimiento del Acceso: realiza el control final de los datos entrantes derivando la decisión a los módulos apropiados; éste es un servicio de la misma

naturaleza que el de control de acceso, solo que a un nivel superior (referido a la aplicación responsable de procesar el paquete). [7] [19] [21] [16]

3.4.1. Tecnologías y aspectos de seguridad

Anteriormente se vieron cuáles son los servicios de seguridad que debería ofrecer una solución firewall. Para poder implementar y llevar a cabo estos servicios se necesita de una arquitectura de hardware apropiada sobre la cual se configurarán los diferentes servicios.

Existen diferentes formas de configurar una solución (que se tratarán en la tercera parte), pero básicamente lo componentes principales de cualquier sistema de comunicaciones protegido por un firewall son: *Routers*, *Gateways*, *Proxies* y *Hosts* o *Sistemas finales* que conforman la red, todos ellos comunicados por algún medio de transmisión. A continuación se describe brevemente cada uno de estos sistemas. Luego se describirán las tecnologías que hacen posible ofrecer los servicios mencionados, sobre qué componente pueden ser instaladas y cómo.

3.4.2. Routers

Un router es un dispositivo que reenvía o retransmite paquetes entre dos o más redes (ver Figura 19). Operan sobre la capa de red por lo que no necesitan implementar los niveles superiores de la arquitectura de red (aunque también es posible encontrar la capa de Transporte lo que permite extender algunos servicios).

A medida que los paquetes son recibidos por el router, utiliza información de direccionamiento de los paquetes IP para determinar la mejor ruta que puede tomar para llegar a su destino final. El paquete es ruteado a través de la red mediante un algoritmo que utiliza una tabla de ruteo que contiene información de todas las redes conocidas por él, el número de nodos hasta una red determinada, y la dirección del router en la dirección de la red destino.

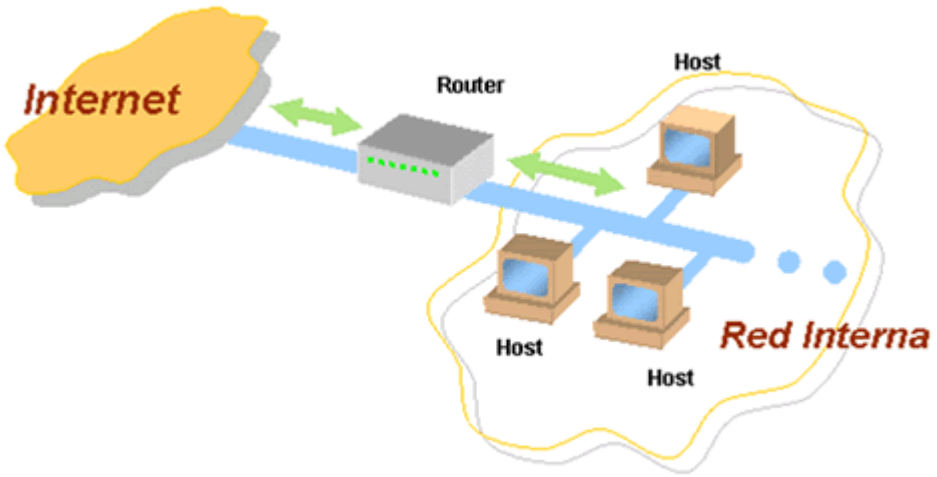


Ilustración 19 Funcionamiento básico de un router

3.4.3. Gateways y Proxies

Un *gateway* o *puerta de enlace* es un sistema que actúa como intermediario o compuerta entre una red privada y una red a la cual está conectada (generalmente Internet), es decir que todo el tráfico existente entre ambas redes pasa por esta compuerta (ver Figura 20). Está encargado de capturar y redirigir todos los mensajes y solicitudes de conexión provenientes de la red pública, destinados a servicios ofrecidos por sistemas finales (servidores de aplicación, por Ej. Web, FTP, HTTP, etc) dentro de la red privada y vise versa. Este servicio es implementado en el gateway mediante el uso de aplicaciones de software llamadas *proxies*.

Un *servidor proxy* es una aplicación situada entre una aplicación cliente y un servidor real

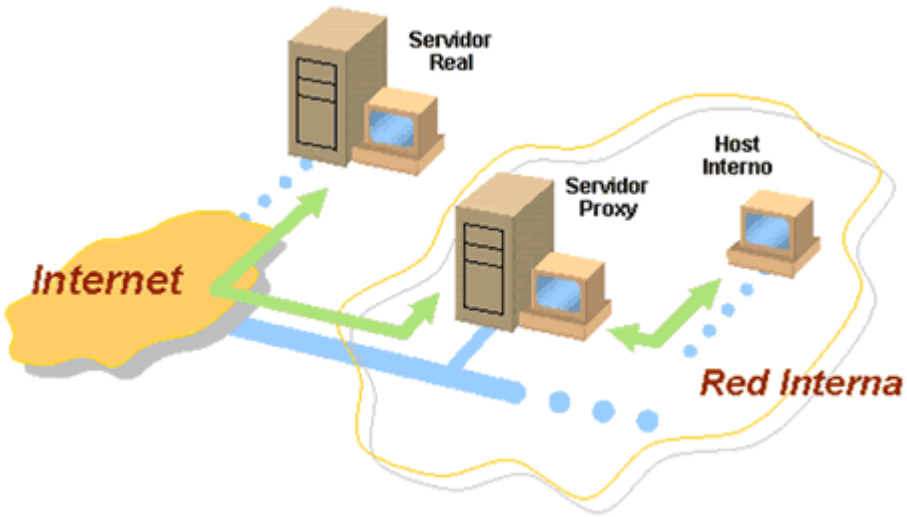


Ilustración 20 Funcionamiento básico de un Servidor Proxy

Los proxies comprenden la sintaxis de un protocolo pero no implementan ninguna de sus funcionalidades. Simplemente verifican que un mensaje proveniente de un host externo es apropiado, y luego lo envía al sistema encargado de procesar los datos (el servidor real al cual estaba dirigido el mensaje).

El uso de un proxy tiene dos propósitos: mejorar *el desempeño de la red:* los servidores proxy pueden mejorar en gran medida el desempeño para un grupo de usuarios ya que ahorra la obtención de los resultados (consultas al servidor real) de todas las solicitudes para una cierta cantidad de tiempo; y *filtrar solicitudes:* de esta forma puede ofrecer un servicio de seguridad básico y muy importante para proteger una intranet o un sistema de información conectado a una red pública.

Otra ventaja de utilizar estos sistemas es que permite monitorear y controlar toda actividad de la red que involucre comunicación con el exterior (en ambas direcciones).

Cuando este sistema actúa como firewall, verifica si tales solicitudes o mensajes son permitidos y las rechaza en caso de que así lo determine, en función a las reglas que se le hayan impuesto.

El gateway está asociado con un router para determinar dónde son enviados los paquetes en función de tablas de ruteo e información del paquete.

3.4.4. Sistemas finales

Los sistemas finales de una red son tanto aquellos equipos destinados a ofrecer un servicio, como por ejemplo un servidor Web, un servidor FTP, un servidor de Correo Electrónico, etc., como aquellos sistemas utilizados por los integrantes de la organización que posee la red, para administración o simple uso de los recursos existentes. Estos también son conocidos como *hosts*.

Cuando se habla de seguridad en una red, la idea es proteger a los sistemas finales de ataques o intrusos que intenten tomar provecho de los recursos disponibles a través de la red, y no de impedir que atraviesen los puntos de acceso; éste es el medio por el cual se logra el objetivo final (comunicarse).

Todos los dispositivos de una red son capaces de soportar e implementar los servicios de seguridad necesarios para proveer protección a los sistemas finales (inclusive ellos mismos). El lugar (dispositivo) en la red donde se instalen los distintos servicios de seguridad determina la flexibilidad y granularidad de la protección. Un ataque puede provenir desde cualquier sitio de la red, tanto interna como externa por lo que los sistemas finales deberían protegerse por sí mismos de los intrusos.

La literatura suele referirse a diferentes tipos de hosts según la función que cumplen, como por ejemplo, un host gateway es aquel que cumple la función de un gateway o host firewall, aquel que realiza funciones de un firewall. Un término de particular importancia es el de "*host bastión*". Éste es un sistema de cómputo altamente protegido ya que está expuesto a Internet y es el principal punto de contacto con usuarios de la red interna por lo que es vulnerable a los ataques. Generalmente implementan varias funciones y mecanismos de control combinando funciones de filtrado de paquetes y servicios proxies.

Existen diferentes estrategias y configuraciones para implementar una solución de seguridad que deberá responder a las necesidades de protección de los sistemas finales y a las restricciones impuestas por los recursos disponibles para llevarla a cabo.

3.5. Traducción de Direcciones de Red

3.5.1. Seguridad en Tránsito

A continuación se presentan las tecnologías que hacen posible proteger los datos que viajan a través de una red pública. [7]

- NAT: Traducción de Direcciones de red

La traducción de direcciones de red (NAT por *Network Address Translation*) fue creada, inicialmente con el propósito de resolver el problema de escalabilidad de direcciones IP y su agotamiento para la asignación de nuevas números IP; otra ventaja de NAT es que permite ocultar el esquema de direcciones de una red privada al exterior ofreciendo un importante servicio para una solución de seguridad.

La estrategia utilizada por la aplicación de esta tecnología está basada en la distribución topológica de la asignación de futuras direcciones IP de cada espacio de direcciones de red a los distintos dominios de ruteo de tránsito de datos (redes privadas). Las direcciones IP dentro de un red privada no son únicas globalmente, sino que son reusadas en otros dominios, resolviendo así el problema de agotamiento de direcciones. [16]

Ilustración 21 Mapeo de direcciones NAT

3.6. Túneles

Un túnel es un canal virtual, configurado entre dos sistemas remotos que se encuentran en diferentes redes, sobre una conexión real que involucra más de un nodo intermedio.

La técnica de "tunneling" consiste en encapsular un mensaje de un protocolo dentro de sí mismo aprovechando ciertas propiedades del paquete externo con el objetivo de que el mensaje sea tratado de forma diferente a como habría sido tratado el mensaje encapsulado. De esta forma un paquete puede "saltar" la topología de una red. Por ejemplo, un túnel puede ser usado para evitar un firewall (con los peligros consecuentes de esta decisión). Esta es una consideración a tener en cuenta al configurar un túnel.

De esta forma, el túnel es simplemente la ruta que toman los paquetes encapsulados (y encriptados), dentro de un paquete del mismo protocolo, entre las dos redes. Un atacante puede interceptar los mensajes que viajen por el túnel, pero los datos encapsulados están encriptados y solo pueden ser recuperados por el destinatario final.

En el sistema de destino, el mensaje encapsulado es extraído del paquete recibido, desencriptado, y reinyectado en la red a la que pertenece el receptor (en el caso de un gateway). [16] [18]

3.7. Criptografía

La criptografía consiste en la modificación de un mensaje a una forma no comprensible directamente de forma tal que solo quienes establezcan una comunicación cifrada puedan tener acceso a los datos originales.

Por lo tanto es deseable un esquema de obtención y administración de claves robusto, para que emisor y receptor puedan comunicarse de forma segura, y que impida que algún atacante obtenga la clave con la cual se encriptarán los mensajes. [16] [7]

3.8. Firmas digitales y funciones de resumen y certificados

3.8.1. Firmas Digitales

El mecanismo de encriptado ofrece otra facilidad en seguridad: hace posible un método para utilizar *firmas digitales* y *certificados* para proporcionar *autenticidad* a los mensajes transmitidos.

Mediante el cifrado de un mensaje, podemos asegurar la privacidad de los datos enviados. Pero, ¿sabe realmente el receptor de quién proviene tal mensaje? El origen de un mensaje es tan importante como su contenido. [7]

3.8.2. Certificados

¿Que sucede si alguien mal intencionado publica sus claves diciendo ser alguien más? Es necesario proveer algún mecanismo de autenticación para las claves publicas que son distribuidas. Esto se logra mediante el uso de *certificados*.

Un certificado es un documento digital que acredita que la clave pública que contiene es de quien dice ser.

Básicamente, un certificado consta de la clave publica que certifica, el nombre del propietario, un período de validez, el nombre de la Autoridad de Certificación que lo emite, un número de serie, entre otros datos adicionales. [16]

3.9. Redes Privadas Virtuales

La comunicación entre sitios a través de Internet es vulnerable a ataques de "escuchas". El uso de una red privada virtual garantiza que todo el tráfico existente entre diferentes puntos de comunicación remotos interconectados mediante una red pública sea privado.

Una red privada virtual consiste de un conjunto de sistemas o dispositivos interconectados a través de canales seguros, sobre una red pública, permitiendo el acceso remoto de los recursos y servicios de la red de forma transparente y segura como si los usuarios estuvieran conectados de forma local.

Ofrece una alternativa sobre el acceso remoto tradicional y líneas dedicadas ya que utiliza los canales de comunicación ya existentes de la red de redes (Internet) permitiendo conectar usuarios remotos mediante el uso de servidores de VPN habilitando el uso compartido de los recursos ya que diferentes usuarios y conexiones pueden establecerse en diferentes momentos y compartir la misma infraestructura.

Generalmente, los servidores VPN se encuentran situados detrás del firewall "perimetral" para proteger la red de la organización. [18] [16]

3.9.1. Redes Privadas Virtuales y Firewalls

Es común que un firewall implemente un servicio VPN, de esta forma, es posible conectar dos redes con protección perimetral mediante túneles de firewall a firewall, con lo cual se obtiene una red privada conformada por dos redes remotas.

Existen varias tecnologías para implementar Redes Privadas Virtuales, la principal es criptografía.

3.10. Control de Acceso y Filtros

Una de las funciones más importantes de un firewall es el filtrado o control de acceso de toda la información que sea recibida en los distintos puntos de acceso a la red interna o a los sistemas finales, que son administrados por aquél.

El filtrado de datos permite controlar la transferencia segura de datos basado principalmente en: la dirección de donde provienen los datos, la dirección de destino de los datos y los protocolos de transporte y aplicación utilizados.

Esta función puede ser implementada en diferentes niveles de la arquitectura de red, con lo cual se logran diferentes niveles de granularidad, es decir, qué tan minucioso es el control de seguridad efectuado. Sobre la base del nivel donde se efectúe el filtrado, la función se implementará en diferentes dispositivos[1]. Los niveles mencionados son tres[2]: *filtrado de paquetes*, *control de acceso de conexiones* y *filtrado de datos de aplicación*. [7] [20] [21] [16]

3.10.1. Filtrado de paquetes (a nivel de red)

Los filtros de paquetes operan al más bajo nivel de abstracción en el cual, los datos son transmitidos en paquetes y analizados como tales. En la familia de protocolos TCP/IP, los filtros son aplicados al nivel de transporte (TCP, UDP) y al nivel de red (IP) (ver Figura 22).

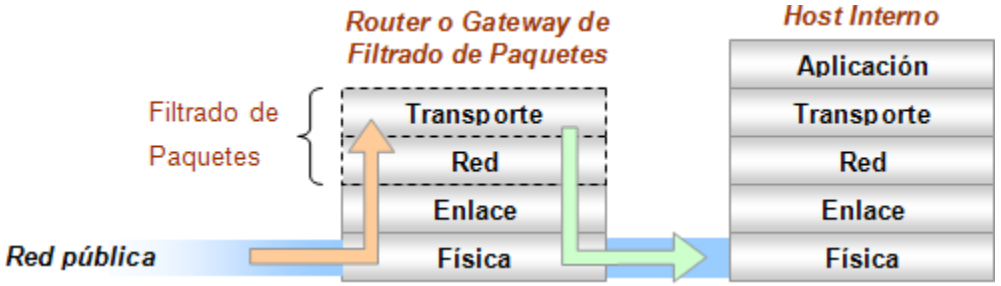


Ilustración 22 Filtrado de paquetes en un Router o Gateway

Este mecanismo es implementado por lo general en los sistemas intermedios (*gateways* o *routers*) que conectan la red interna con la red pública. Cada paquete que ingresa a la red es interceptado y analizado por la función de filtrado, implementada por un filtro de paquetes en estos dispositivos intermedios. Suelen ser llamados *Router de Filtrado de Paquetes* o *Gateways de Filtrado de Paquetes*.

El filtro rechaza o reenvía los paquetes al destinatario original, según reglas especificadas en Listas de Control de Acceso (ACL), que son almacenadas en el router o gateway, basadas en los datos de los encabezados de los paquetes TCP e IP. Básicamente los datos analizados son las direcciones IP y puertos TCP de origen y destino de los paquetes.

Un filtro de paquetes no mantiene información de contexto para los paquetes que sean parte de una conexión; todos los paquetes son tratados de forma independiente, sin ser relacionados con ningún otro.

- Implementación

La función de filtrado de paquetes puede implementarse en varios sitios de la red interna. La forma más directa y simple es utilizar un *router* que la soporte.

Un router tendrá dos interfaces, una que conecte a la red externa y la otra a la red interna. Los filtros pueden aplicarse en una de las dos interfaces, o en ambas. Además puede aplicarse al tráfico de entrada como al de salida, o a ambos. Estas características varían con los diferentes routers. Tales consideraciones reflejan diferentes políticas más o menos flexibles, con más o menos puntos de control. Una buena política a respetar es que si un paquete ha de ser rechazado, que sea cuanto antes.

3.10.2. Control de Acceso de Conexiones

Este mecanismo controla y retransmite conexiones TCP manteniendo registro del estado de todos los paquetes que agrupan tal conexión, de forma que solo aquellos hosts externos confiables puedan establecer conexiones con aquellos dispositivos habilitados a ofrecer un servicio a tales usuarios. De la misma forma es posible restringir las conexiones originadas en la red interna con destino a ciertos sitios de la red externa. Esta función es realizada por un *proceso proxy* instalado en un gateway que interconecta la red interna con la red pública. Estos dispositivos son llamados *gateways a nivel de circuitos*. (*ver Figura 23*)

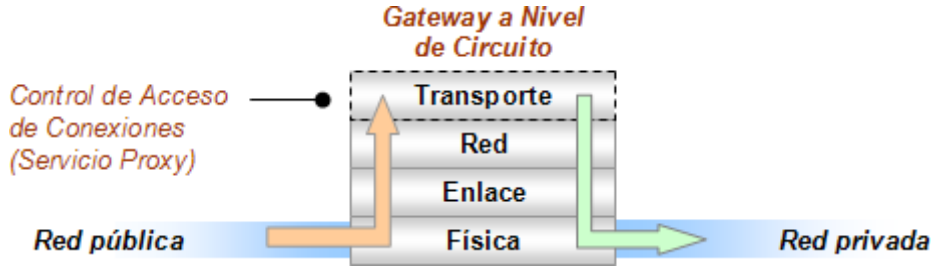


Ilustración 23 Control de acceso de conexiones en un Gateway

3.10.3. Filtrado de Datos de Aplicación

Este mecanismo interpreta los datos encapsulados en los paquetes correspondientes a protocolos de aplicación particulares para determinar si deben o no deben ser procesados por la aplicación correspondiente, ya que pueden contener datos que afecten el buen funcionamiento de las mismas. La función de seguridad ofrecida por este mecanismo es mucho más segura que las anteriores (*ver Figura 24*)

Son implementados por servicios proxies instalados en gateways, llamados *gateways a nivel de aplicación*. Proveen una barrera de seguridad entre los usuarios internos y la red pública. Los usuarios de la red interna se conectan al filtro de datos de

aplicación, quien funciona como intermediario entre diferentes servicios de la red externa y el usuario interno.

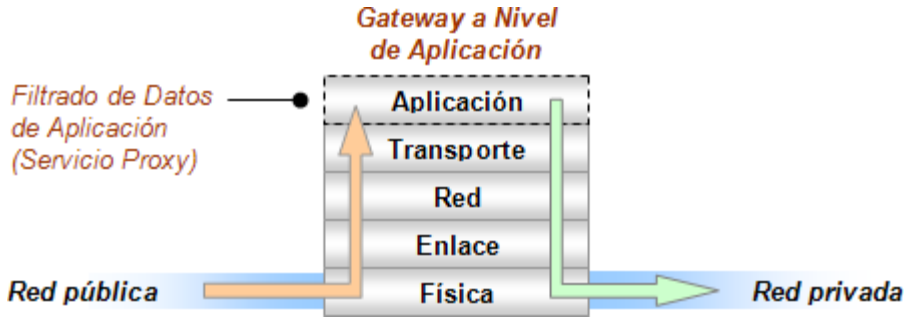


Ilustración 24 Filtrado de datos de aplicación en un gateway

Presentan otra ventaja, que en algunos ambientes es bastante crítica: el registro de todo el tráfico de entrada y salida es simple implementar.

3.11. Políticas de Seguridad

- ¿Qué es una Política de Seguridad?

Las decisiones en cuanto a medidas de seguridad para un sitio determinan, obviamente, que tan segura será la red y, además, qué nivel de funcionalidad ofrecerá y qué tan fácil será de usar.

Estas decisiones deben ser antecedidas por la determinación de los objetivos de seguridad, que permitirán resolver la selección de las herramientas que harán efectivos tales objetivos. Estos objetivos serán diferentes para cada organización porque dependen de sus necesidades. Están muy relacionados con algunos puntos de equilibrio claves tales como:

Servicios ofrecidos vs. La seguridad provista: cada servicio ofrecido a un usuario tiene su propio riesgo de seguridad.

Facilidad de uso vs. Seguridad: un sistema muy fácil de usar permitirá el acceso a casi todos los usuarios y por lo tanto serán menos seguro.

Costo de la seguridad vs. Riesgo de pérdida: existen muchos costos de seguridad: monetarios, de desempeño y facilidad de uso. Los riesgos de pérdida pueden ser de privacidad, de datos, y servicios. Cada tipo de costo debe ser balanceado con respecto a cada tipo de perdida.

Una vez definidos los objetivos, deben ser comunicados a todos los usuarios de la red de la organización e implementados a través de un conjunto de reglas de seguridad, llamadas "**política de seguridad**".

"Una política de seguridad es un enunciado formal de las reglas que los usuarios que acceden a los recursos de la red de una organización deben cumplir" [RFC-2196].

El *objetivo principal* del uso de una política de seguridad es:

- Informar a los usuarios de la red sus obligaciones para proteger a los recursos de la red.
- Especificar los mecanismos a través de los cuales estos requerimientos pueden ser logrados.
- Proveer una guía que permitirá implementar, configurar y controlar los sistemas de la red para determinar su conformidad con la política.

Una política de seguridad debe asegurar cuatro *aspectos fundamentales* en una solución de seguridad: *autenticación*, *control de acceso*, *integridad* y *confidencialidad*. A partir de estos, surgen los *principales componentes* de una política de seguridad:

Una política de privacidad: define expectativas de privacidad con respecto a funciones como monitoreo, registro de actividades y acceso a recursos de la red.

Una política de acceso: que permite definir derechos de acceso y privilegios para proteger los objetivos clave de una pérdida o exposición mediante la especificación de guías de uso aceptables para los usuarios con respecto a conexiones externas, comunicación de datos, conexión de dispositivos a la red, incorporación de nuevo software a la red, etc.

Una política de autenticación: que establece un servicio de confiabilidad mediante alguna política de contraseñas o mecanismos de firmas digitales, estableciendo guías para la autenticación remota y el uso de dispositivos de autenticación.

Un sistema de IT (tecnología de la información) y una política de administración de la red: describe como pueden manipular las tecnologías los encargados de la administración interna y externa. De aquí surge la consideración de si la administración externa será soportada y, en tal caso, como será controlada.

Al diseñar la política de seguridad de una red se deben responder algunas *cuestiones claves* para poder llevar a cabo una sólida definición. Las preguntas básicas sobre la cual desarrollar la política de seguridad son las siguientes:

- ¿Que recursos se tratan de proteger? (objetivos clave)
- ¿De quién se trata de proteger los recursos?
- ¿Cuáles y cómo son son las amenazas que afectan a tales recursos?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas pueden ser implementadas para proteger el recurso?
- ¿Cuál es el costo de tal medida y en qué tiempo puede ser implementada?
- ¿Quién autoriza a los usuarios?

Las empresas y organizaciones raramente mantienen sus servicios constantes, sino que continuamente introducen nuevas tecnologías para mejorarlos. Es por esto que tales cuestiones (y por tanto, la política de seguridad) deben ser revisadas periódicamente para adaptarse a las necesidades de seguridad reales, ya que la introducción o modificación de algún recurso puede generar fallas en la arquitectura de seguridad actual. [1] [7] [19] [21] [17] [16] [13]

3.11.1. Análisis de riesgo

En cuanto a la tarea de determinar dónde se requiere enfocar las decisiones (1 y 2) se puede lograr mediante un Análisis de Riesgo que permite determinar qué se necesita proteger, de qué protegerlo, y cómo protegerlo. Es decir, se examinan todos los riesgos posibles y se clasifican por nivel de severidad. Dos de los elementos importantes del análisis de riesgo son: la identificación de los objetivos clave e identificación de las amenazas.

- Identificar los objetivos clave

Se debe identificar todo aquello que será protegido, es decir, que puedan ser afectadas por un problema de seguridad. Entre algunas de las más importantes encontramos:

Hardware: Unidades de procesamiento, terminales, impresoras, unidades de almacenamiento, servidores, routers, etc.

Software: Programas fuentes, utilidades, sistemas operativos, etc.

Datos: archivos en línea, bases de datos, datos siendo trasmitidos por algún medio, etc.

- Identificar las amenazas

Consiste en determinar aquellas amenazas que afecten los objetivos clave a ser protegidos. Pueden ser examinadas considerando el potencial de perdida existente. Las amenazas a considerar dependerán de las características del sitio y servicios a ofrecer, sin embargo existen algunas amenazas comunes que deben ser consideradas:

  - Acceso no autorizado a recursos y/o información
  - Exposición no autorizada de información
  - Ataques de Rechazo del servicio (DoS – Denial of Service)

3.12. Planes de seguridad

Para mantener una visión clara e integral de las políticas de seguridad a definir, es útil establecer un *plan de seguridad* que ofrezca un marco de guías generales para tales políticas. De esta forma, las políticas individuales serán consistentes con toda la arquitectura de seguridad.

Un plan de seguridad debe definir:

- La lista de servicios que serán ofrecidos por la red de la organización
- Qué áreas de la organización proveerán tales servicios
- Quién tendrá acceso a esos servicios
- Cómo será provisto el acceso
- Quién administrará esos servicios
- Cómo serán manejados los incidentes

Al igual que un plan de seguridad ofrece un marco de diseño para una política de seguridad, éstas se definen a diferentes niveles de especificación o abstracción lo que ofrece una visión más clara y coherente del esquema de seguridad completo resultante.

Cada iteración o nivel, especifica requerimientos de seguridad más detallados enfocados en diferentes aspectos. Las diferentes políticas se refieren a: seguridad del sitio, acceso a servicios de red, diseño del firewall, políticas específicas del sistema.

3.12.1. Política de Diseño de Firewall

Es una política de bajo nivel que describe cómo el firewall controlará el acceso a los servicios restringidos como se definió en la política de acceso a servicios de red.

La política de diseño es específica de cada firewall. Define las reglas utilizadas para implementar la política de acceso a servicios de red. Debe ser diseñada en relación a, y con completo conocimiento de características tales como las limitaciones y capacidades del firewall, y las amenazas y vulnerabilidades asociadas con las tecnologías utilizadas (como TCP/IP). Los firewalls generalmente implementan una de dos políticas de diseño básicas:

- Permitir todo servicio, a menos que sea expresamente restricto, o
- Denegar todo servicio, a menos que sea expresamente permitido.

La primera política es menos deseable, ya que ofrece más vías por las cuales puede accederse a un servicio, evitando el firewall, mientras que la segunda es más fuerte y segura, aunque es más restrictiva para los usuarios. Ésta última es la clásicamente usada en todas las áreas de seguridad de la información.

Por lo tanto, dependiendo de los requerimientos de seguridad y flexibilidad, ciertos tipos de firewalls son más apropiados que otros, haciendo muy importante que la política sea considerada antes de implementar un firewall. De otra forma, el firewall podría no cubrir las funcionalidades esperadas. [1] [7] [19] [21] [17] [13]

4. FIREWALLS

Luego de haber decidido una estrategia de seguridad y, en función de ella, una política de seguridad para una red, es necesario llevar estas especificaciones a la implementación. Tal implementación corresponde a un ***Firewall***, [1] [7] [19] [21] [16] [13]

4.1. Definición de firewall

Un firewall es la combinación de diferentes componentes: dispositivos físicos (hardware), programas (software) y actividades de administración, que, en conjunto, permitirán aplicar una política de seguridad de una red, haciendo efectiva una estrategia particular, para restringir el acceso entre ésta red y la red pública a la cual esté conectada. El objetivo es protegerla de cualquier acción hostil proveniente de un host externo[1] a la red.

La función de un firewall es tal que todo el tráfico de entrada y salida de la red privada debe pasar a través de él; el tráfico permitido por el firewall es autorizado mediante su evaluación en base a la política de seguridad.

En general no existe una terminología completamente consistente para arquitecturas de firewalls y sus componentes. Diferentes autores usan términos de diferentes formas (o incluso conflictivas). Es apropiado referirse como “firewall” al conjunto de estrategias y políticas de seguridad y como “sistema firewall” a los elementos de hardware y software utilizados en la implementación de esas políticas (hablar de políticas incluye implícitamente una estrategia ya que se ve reflejada en la primera).

El enfoque de firewalls está basado en el concepto de permitir a los usuarios locales el uso de todos los servicios de red internos a su red local y otros servicios ofrecidos por la Internet, controlando, además, el acceso de los usuarios externos a los recursos de la red local.

4.2. Funciones principales de un Firewall

Un firewall permite proteger una red privada contra cualquier acción hostil, al limitar su exposición a una red no confiable[2] aplicando mecanismos de control para restringir el acceso desde y hacia ella al nivel definido en la política de seguridad. Generalmente un firewall es utilizado para hacer de intermediario entre una red de una organización e Internet u otra red no confiable.

Estos mecanismos de control actúan sobre los medios de comunicación entre las dos redes, en particular, sobre la familia de protocolos utilizada para la comunicación de sistemas remotos. La más comúnmente usada es TCP/IP ya que dispone de amplios desarrollos de mecanismos estándares para su uso en varios aspectos, incluyendo en seguridad.

La tarea de un firewall consiste en inspeccionar y controlar todo el tráfico entre la red local e Internet. De esta forma se intenta detectar y rechazar todo el tráfico potencialmente peligroso antes de que alcance otras partes de la red interna, en algunos casos también se efectúan registros de tales actividades. La determinación de qué es peligroso para la red local, es especificada en la política de seguridad adoptada por el sitio.

La protección que provee un firewall es de diferentes tipos:

- Bloquea tráfico no deseado;
- Redirecciona tráfico de entrada a sistemas internos de más confianza;
- Oculta sistemas vulnerables, que pueden ser fácilmente asegurados, de Internet;
- Puede registrar el tráfico desde y hacia la red privada;
- Puede ocultar información como ser nombres de sistemas, topología de la red, tipos de dispositivos de red, e identificadores de usuarios internos, de Internet;
- Puede proveer autenticación más robusta que las aplicaciones estándares;
- ... entre otros.

4.3. Estrategia de un firewall

Generalmente un firewall se encuentra situado en los puntos de entrada a la red que protege. Este es un enfoque tradicional que surge a partir de la forma más simple de conexión de una red privada a Internet: mediante un único enlace. Aunque es posible utilizar otros enfoques para diferentes topologías de interconexión. Pero en cada caso, cada conexión (punto de acceso) de la red local a Internet estará equipada con un firewall.

Ya que todo el tráfico debe pasar por él, puede considerarse como el foco de todas las decisiones de seguridad. Concentrando las defensas en este punto, es posible reducir la sobrecarga de seguridad del sistema interno ya que el esfuerzo se limita a unos pocos dispositivos de toda la red (los que forman parte del firewall).

De esta forma, un firewall centraliza el control de acceso. Los usuarios remotos pueden acceder a la red interna de forma controlada y segura, pasando a través del firewall.

Un firewall será transparente a los usuarios si no advierten su existencia para poder acceder a la red. Los firewalls generalmente son configurados para ser transparentes para los usuarios de la red interna, mientras que para los usuarios de la red externa, no.

4.4. Fundamento de los firewalls

Alguien podría cuestionarse lo siguiente: si queremos proteger nuestra red privada porque permitimos que una red de dominio público como Internet, pueda acceder a ella? La respuesta es simple: porque queremos que nuestra red acceda a ella. Muchas compañías dependen de Internet para publicitar sus productos y servicios. Por lo que es necesario proteger los datos, transmisiones y transacciones de cualquier incidente, ya sea, causado por actos maliciosos o no intencionales.

En el caso de una red local directamente conectada a Internet sin un firewall, la red entera está sujeta a ataques (*ver Figura 25*). La experiencia práctica muestra que es muy difícil asegurar que todo host de la red esté protegido. Una contraseña mal elegida puede comprometer la seguridad de toda la red.

Ilustración 25 Red local sin firewall

Si la red local está protegida por un firewall, solo existe acceso directo para un conjunto seleccionado de hosts y la zona de riesgo es reducida al firewall en sí mismo o a un conjunto seleccionado de hosts de la red interna. (*ver Figura 26*)

Ilustración 26 Red local con firewall

Un firewall no es tanto una solución de seguridad sino una respuesta al problema de ingeniería/administración: configurar un gran número de sistemas de hosts para una buena seguridad. Un firewall solo no asegurará una red. Solo es parte de un área más amplia dedicada a proteger un sitio y efectuar operaciones de red.

4.5. Limitaciones de los firewalls

En el enfoque tradicional comentado, un firewall no puede ofrecer protección contra conexiones que no pasen a través de él, por lo que el firewall no puede proteger la red contra atacantes internos.

Adicionalmente un firewall restringirá el acceso a ciertos dispositivos o funcionalidades, si existen conexiones no protegidas que pueden comunicar los

sistemas de la red interna con la externa, es posible que algún usuario no autorizado intente saltear el firewall para obtener acceso a esas funcionalidades. Este tipo de amenaza solo puede ser tratada por procedimientos de administración que estén incorporados a las políticas de seguridad de las organizaciones y aseguren la protección o eliminación de estas conexiones.

Obviamente un firewall no ofrecerá protección contra aquellas amenazas que no hayan sido consideradas en el diseño de la estrategia y la política de seguridad.

4.6. Ventajas y Desventajas de los firewalls

Obviamente, la principal ventaja de un firewall es que permite la interconexión segura de una red privada con una red pública para aprovechar los beneficios que ésta ofrece. Un firewall puede resultar en una reducción de costos si todo el software de seguridad puede ser situado en un único sistema firewall, en lugar de ser distribuido en cada servidor o máquina de la red privada.

Existen algunas desventajas de los firewalls: cosas de las cuales los firewalls no puede proteger, como ser amenazas de puntos de acceso alternativos no previstos (backdoors) y ataques originados en el interior de la red. El problema de los firewalls es que limitan el acceso desde y hacia Internet, pero es un precio que se debe pagar y es una cuestión de análisis de costo / beneficio al desarrollar una implementación de seguridad.

4.7. Implementación

Para asegurar una red privada, se debe definir qué idea se tiene del “perímetro” de red. En base a éstas y otras consideraciones se define una política de seguridad y se establecen los mecanismos para aplicar la política y los métodos que se van a emplear. Existe una variedad de mecanismos para la implementación de firewalls que pueden incrementar en gran medida el nivel de seguridad.

Antes de definir qué tipo de firewall se ajusta a las necesidades de la red, se necesitará analizar la topología de la red para determinar si los componentes tales como hubs, routers y cableado son apropiados para un modelo de firewall especifico.

La red debe ser analizada en base a las diferentes capas del modelo de red. Un firewall pasa a través de todas estas capas y actúa en aquellas responsables del envió de paquetes, establecimiento y control de la conexión y del procesamiento de las aplicaciones. Por eso, con un firewall podemos controlar el flujo de información durante el establecimiento de sesiones, inclusive determinando que operaciones serán o no permitidas.

- El término “externo” hace referencia a un host que no pertenece lógicamente a la misma red de la organización ya que puede tratarse de usuarios conectados de forma remota como usuarios confiables de la red.

- En este contexto, el término “confiable” se refiere a la confianza que se tiene a los usuarios conectados a dicha red para el uso de los recursos de la red privada.

4.8. Componentes de un Firewall

Toda solución firewall necesita de ciertos componentes básicos en los cuales residirán las funciones de seguridad de control de acceso y otras como protección de tráfico, autenticación, etc. [1] [7] [19] [21] [16]

4.8.1. Screening Router

Éste es un router utilizado para el filtrado de paquetes. Son configurados para bloquear o filtrar los protocolos y direcciones de forma transparente en los puntos de acceso a la red externa a la cual se conectan directamente.

El router permite el acceso selectivo a los sistemas y servicios del sitio, dependiendo de la política. Usualmente, los usuarios tienen acceso directo a Internet y el acceso a los sistemas del sitio desde Internet es restringido.

El screening router retransmite o rechaza un paquete IP basándose en la información contenida en el encabezado del paquete. Aunque también es capaz de basar las decisiones de ruteo en información que no se encuentra en el encabezado del paquete, por ejemplo, las interfaces de origen y destino.

Un router de filtrado de paquete puede implementar cualquier estrategia de seguridad, sin embargo tiene algunas desventajas

- La capacidad de registro de sucesos es mínima o nula por lo que es difícil determinar si un router ha sido comprometido por un ataque;
- Las reglas de filtrado de paquetes son difíciles de testear, lo que puede dejar un sitio abierto a vulnerabilidades no testeadas;
- Si se necesitan reglas de filtrado complejas, puede volverse inmanejable;
- Cada host directamente accesible desde Internet requerirá su propio conjunto de medidas de autenticación avanzadas.

Estas desventajas se ven aumentadas a medida que las necesidades de seguridad del sitio se vuelven más complejas y rigurosas. El uso de un screening router como único componente de seguridad es considerado como inadecuado para una solución efectiva.

Los hosts protegidos por un screening router son llamados screened hosts. De forma similar una subred protegida es llamada screened subnet o “zona desmilitarizada”.

- ¿Como se filtran los paquetes?

La decisión de filtrado se lleva a cabo de acuerdo con una Lista de Control de Acceso (ACL) asociada a cada interfaz física por la cual se recibe el paquete. Cada entrada de esta lista especifica valores para campos particulares de los encabezados de los paquetes, y acciones a ser tomadas si el paquete conforma con dichos valores. (*ver Figura 27*)

Las tareas de inspección de un screening router se realizan previas a que el paquete alcance la capa de red (la capa que procesa el protocolo que se está filtrando).

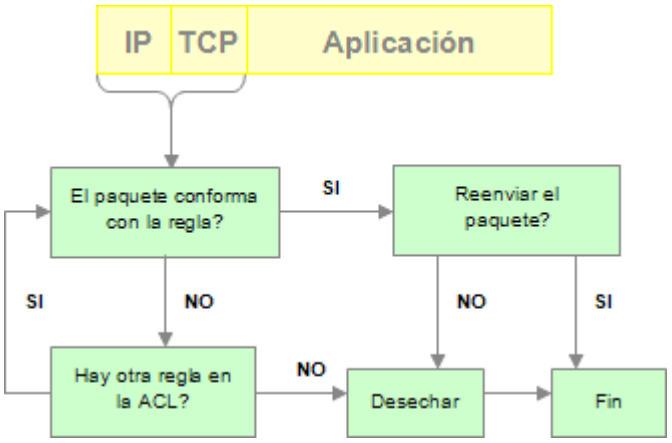


Ilustración 27 Un polible funcionamiento del filtrado de paquetes en un screemin router (responde a la estrategia de rechazar aquello desconocido)

Los datos analizados por el router corresponden al encabezado IP y de los protocolos de transporte TCP y UDP (dependiendo de cada producto). Los campos comúnmente analizados son:

- *Dirección IP origen y destino*: Basándose en las direcciones IP, el router es capaz de bloquear el acceso desde o hacia algún sitio o hosts no confiable.
- *Tipo de protocolo*: indica si los datos encapsulados corresponden a TCP, UDP o ICMP
- *Puerto TCP o UDP de origen y destino*: el router hace uso de los puertos "bien conocidos" de TCP para permitir, denegar o rutear el acceso a servicios de Internet particulares. Por ejemplo, es posible bloquear todo el trafico de entrada excepto para correo electrónico, rechazando todos los paquetes cuyo puerto de origen sea diferente a 25, el puerto por defecto para SMTP. También podría rutear todo el tráfico Web (puerto 80) a un host en particular (por ejemplo, un servidor web).
- *Bit ACK*: que indica si el paquete es una confirmación de un paquete TCP recibido

De todas formas, no todos los routers soportan todos estos campos o listas de control para cada interfaz física.

4.8.2. Gateway a Nivel de aplicación

Son aplicaciones específicas para cada aplicación o programas servidores de propósito especial que se ejecutan en un host para formar parte de un firewall; ofrecen un medio de extender el control de acceso del tráfico de red a las capas de aplicación. Son también llamados aplicaciones o servidores proxies.

Estos programas proveen una barrera segura entre los usuarios internos e Internet actuando como intermediarios para cada sesión de comunicación. En lugar de conectarse directamente a Internet, por ejemplo con un browser Web el usuario interno se conecta al gateway de aplicación, quien establece la conexión con el servidor Web en Internet y actúa como intermediario en el intercambio de datos.

Ya que estos gateways operan sobre la capa de aplicación pueden proveer control de acceso al nivel de los protocolos de aplicación y pueden administrar contenido almacenándolo (mediante el uso de memoria cache) para mejorar el desempeño de la red o intercambiándolo de forma interactiva entre el cliente y el servidor final.

Ya que todos los datos entre el cliente y el servidor son ruteados a través del proxy de aplicación, además de controlar la sesión, puede proveer funciones de registro de sucesos detalladas. Esta habilidad es una de las principales ventajas de un gateway de aplicación.

La principal desventaja de los gateways de aplicación es que requieren código de propósito especial para proveer cada servicio. Pero esto hace que deban implementar la política de rechazar todo a menos que sea explícitamente permitido, que se considera un enfoque ventajoso desde el punto de vista de seguridad. Adicionalmente y dado que efectúan un detallado análisis de los paquetes, son los filtros más costosos en términos de tiempo y capacidad de cómputo.

De las consideraciones del uso de servidores proxy pueden surgir dos cuestiones: primero, como evitar que un host externo intente contactarse con otro host local diferente al servidor proxy? Y segundo, como instruir al host interno que contacte al servidor proxy y no al servidor real de forma directa?.

- Comunicación cliente externo / servidor proxy

Posiblemente, el servidor proxy se encuentre conectado a la red local. Los hosts externos no deberían conocer la topología de la red local y por lo tanto las direcciones IP o nombres de las maquinas conectadas a la misma. Solo deben conocer la dirección de la red o sitio, correspondiente al host que interconecta la red local con la red externa, que será el responsable de redirigir los paquetes al gateway.

Si un host externo conoce esta dirección podría intentar contactarlo y aprovecharse de la situación. Para prevenir esto se dispone de funciones de seguridad en el dispositivo que interconecta la red local para prevenir cualquier intento de acceso no permitido.

- Comunicación cliente interno / servidor proxy

De la misma forma que en el caso anterior, se evita la conexión directa entre el cliente en la red local y el servidor real.

Existen dos tecnologías proxy para lograr esto, *clásica* y *transparente*. En la tecnología proxy clásica, se modifica el software cliente o se instruye al usuario de efectuar procedimientos especiales para contactar al servidor real a través del servidor proxy. En la tecnología proxy transparente, se configuran las tablas de ruteo de la red local para que todos los paquetes destinados a un servidor externo sean redirigidos a gateway de aplicación que sabrá interceptar los paquetes y crear ambas conexiones.

4.8.3. Gateway a Nivel de circuitos

Al igual que los gateways a nivel de aplicación, los gateways a nivel de circuitos son aplicaciones proxies pero se diferencian en los datos sobre los cuales aplican la función de filtrado.

Un gateway a nivel de circuitos no interpreta el contenido de los protocolos de aplicación, sino que determina si una conexión entre dos puntos es permitida, de acuerdo con un determinado conjunto de reglas, manteniendo el estado a lo largo de la transmisión, agrupando los paquetes que pertenecen a la misma conexión.

4.9. Firewalls: Tipos

4.9.1. Alternativas y Estrategias de Seguridad

Los firewalls pueden ser configurados de diferentes formas, utilizando diferentes componentes, logrando varios niveles de seguridad a diferentes costos de instalación y mantenimiento. Esta decisión dependerá de las necesidades y de la evaluación de costo/beneficio de llevar a cabo tal implementación.

Las tecnologías de filtrado de paquetes y gateways a nivel de circuito y aplicación son los principales componentes de una solución firewall. [7] [19] [16]

El filtrado de paquete permite controlar de forma eficiente y transparente el tráfico de una red. El impacto que produce su introducción en una arquitectura de red es mínimo, ya que no requiere grandes cambios en la configuración de los dispositivos de la red. Ofrecen protección a nivel de transporte y red.

Los gateways a nivel de aplicación y circuitos amplían la protección de los filtros de paquetes ya que tienen conocimiento de los protocolos que trabajan sobre la capa de transporte por lo que pueden implementar mecanismos a un nivel más detallado.

A continuación se presentan las principales arquitecturas de un enfoque perimetral y algunas variaciones de las mismas.

- Arquitectura Screening Router

En esta configuración, el firewall consiste de un único router que realiza la función de filtrado de paquetes (*ver Figura 28*). Es una de las estrategias más simples de implementar. El router posee dos interfaces de red, una conectada a la red interna y la otra conectada a la red externa. Intercepta todo el tráfico (de entrada y salida) y lo redirige a su destinatario dependiendo de las reglas del filtro.

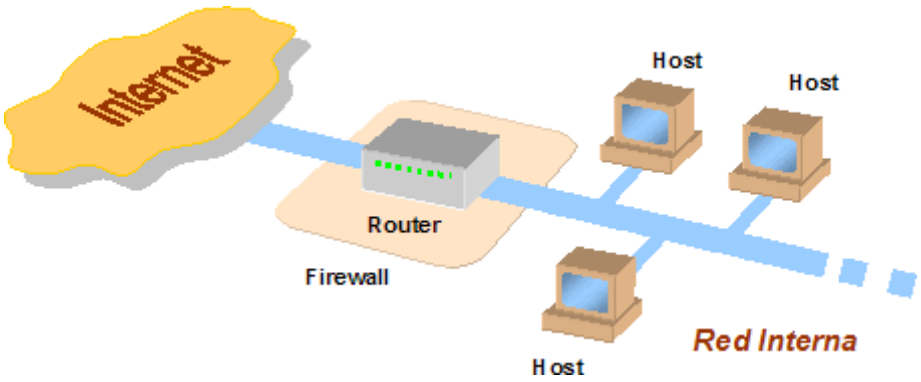


Ilustración 28 Arquitectura screening router

Los hosts de la red interna se comunican entre sí directamente, mientras que la comunicación entre hosts de la red privada y la red publica está restringido a aquellos paquetes que sean permitidos por el router (según el conjunto de reglas de control que reflejan la política de seguridad).

Es una buena configuración para una primer línea de defensa para un firewall, pero para una solución definitiva. En esta configuración, la seguridad de toda la red depende por completo de las reglas definidas en el router. Si un atacante logra atravesar este sistema, tendrá acceso a toda la red interna. Además, esta estrategia no permite ocultar las direcciones IP de la red interna y las capacidades de monitoreo y registro no son muy buenas.

- Arquitectura Dual-Homed Host

En esta arquitectura el firewall consiste de un único hosts bastión dual-homed que implementará funciones de filtrado tanto de red como de aplicación (*ver Figura 29*). Este sistema posee dos interfaces de red, donde cada interfaz se conecta lógica y físicamente a segmentos de red separados y diferentes. Una interfaz de red se conecta a una red externa, no confiable (como Internet), la otra se conecta a la red privada.

Un principio clave de seguridad de esta arquitectura es no permitir que el tráfico de red desde la red externa sea ruteado directamente a la red interna. El firewall deberá, en todos los casos, actuar como un intermediario. Es por esto que en este sistema, la función de ruteo está deshabilitada por lo que el host aísla las dos redes entre ellas al bloquear todo paquete IP que capture. Los sistemas conectados a cada lado del host no pueden comunicarse directamente sino a través de éste.

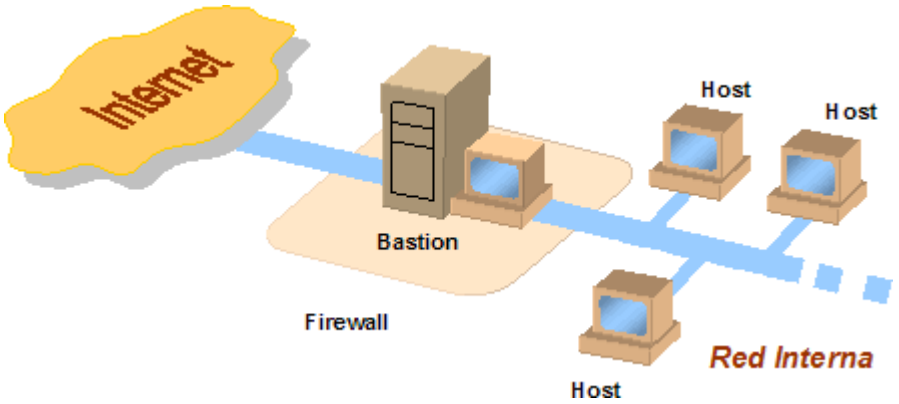


Ilustración 29 Arquitectura Dual-Homed Host

La forma de proveer servicios por parte del host bastión puede ser realizada de dos formas:

- Si los usuarios de la red local poseen cuentas en el host bastión, las mismas le permiten iniciar sesiones (logearse) para poder utilizar los servicios de Internet. Este aspecto presenta un serio riesgo de seguridad ya que la protección depende de que el usuario haya elegido bien su contraseña. Si un usuario externo puede iniciar una sesión, logra tener acceso a la red local completa.
- La alternativa es que el host ejecute servicios proxy para cada servicio que se desee permitir, de esta forma el usuario se desliga de la responsabilidad de la seguridad de la red.

Este host puede proveer un alto nivel de control al permitir que los hosts internos deban comunicarse sólo con este host. Es posible que el dual-homed host rechace conexiones en base a los datos que contenga. Aunque se requiere de mucho trabajo para lograr el máximo potencial de esta configuración.

En esta arquitectura, este dispositivo es critico para la seguridad de la red ya que es el único sistema que puede ser accedido (y atacado) desde Internet, por lo que debe poseer un alto nivel de protección a diferencia de un host común de la red interna. Es por esto que a estos host suele llamárseles *bastión*. Debe instalarse en este host la mínima cantidad necesaria de software para reducir el riesgo de que sea vulnerado.

Implementar servicios proxies ofrece una ventaja sobre el filtrado de paquetes, pero puede no estar disponible para todos que se deseen.

Esta arquitectura es mucho mas segura que la anterior, pero aún si el bastión es traspasado, la red local completa queda sin protección.

- Arquitectura Screened Host

La arquitectura Screened Host posee un firewall compuesto por un router para el filtrado de paquetes y un host bastión para el filtrado de conexiones a nivel de circuito y aplicación (*ver Figura 30*). La primer línea de protección corresponde al router con filtrado de paquetes, el host bastión se encuentra conectado a la red interna como un host más.

El router está configurado para dirigir todo el trafico proveniente de la red externa al host bastión por lo que es el único que puede ser accedido directamente desde fuera de la red local, por esto, el bastión debe estar altamente protegido. Así mismo, éste último dirige todo el tráfico proveniente de la red interna al router por lo que es el único que puede establecer una conexión con el exterior. Adicionalmente, el bastión solo permite ciertos tipos de conexiones y protocolos.

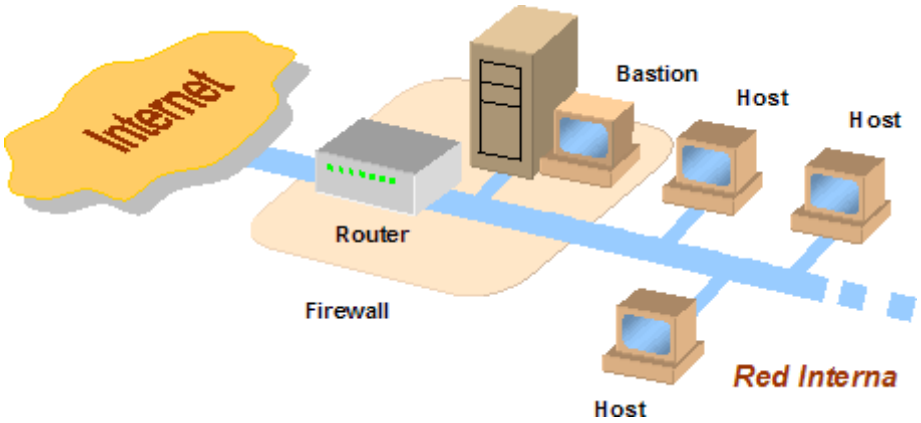


Ilustración 30 Arquitectura screened Host

El router de filtrado de paquetes puede ser configurado de diferentes formas

- Permitir que ciertos hosts internos puedan abrir conexiones a Internet para ciertos servicios;
- Deshabilitar todas las conexiones desde los hosts internos habilitando solo al host bastión para establecer estas conexiones;
- También es posible que algunos paquetes sean dirigidos, por el router, directamente a los hosts internos.

Estos aspectos dependen de la política de seguridad elegida.

Gracias a esta posibilidad, esta arquitectura es más flexible ya que permite que algunos servicios no soportados por el proxy puedan se dirigidos a los hosts internos directamente por el router.

Ya que el bastión bloquea todo el tráfico entre la red externa y la red local, esta se mantiene oculta para cualquier host externo.

Como en la arquitectura anterior, el bastión administra las conexiones mediante una aplicación proxy, Los hosts de la red local están configurados para dirigir todas las solicitudes al servidor proxy, en el host bastión, para poder comunicarse con la red externa.

Esta arquitectura es más segura ya que agrega una capa de seguridad a la arquitectura anterior: un atacante tiene que pasar primero por el router y luego por el host bastión (por supuesto, esto depende siempre del uso de una política de seguridad correctamente diseñada)

Por otro lado, esta arquitectura presenta una desventaja: si un atacante logra vulnerar al host bastión, podrá tener acceso a toda la red interna.

En el modelo presentado, el host bastión se conecta a la red como otro host más. Es posible configurar a éste host para que se conecte al router y a la red interna por medio de interfaces de red diferentes; de esta forma se crea una división física entre la red interna y el router.

- Arquitectura Screened Subnet

El riesgo presente en las arquitecturas anteriores de que el host bastión sea comprometido puede ser reducido configurando una *red de perímetro* a la cual se conecte el mismo. Esta red suele ser llamada Zona Desmilitarizada.

Para lograr esta arquitectura se introduce un router de filtrado de paquetes entre el host bastión y la red interna, por lo que el host bastión se encontrará entre los dos routers (interno y externo, uno se encuentra entre la red perimetral y la red externa y el otro entre la red perimetral y la red interna) y estará conectado a un segmento de red diferente al que están conectados los hosts de la red privada. Con esta configuración no existe un único punto vulnerable que ponga en riesgo toda la red interna (*ver Figura 31*)

Con esta arquitectura se agrega una nueva capa de seguridad a la arquitectura anterior que aísla la red local de Internet. Aislando al host bastión en una red de perímetro, es posible reducir el impacto de que el bastión sea vulnerado por algún ataque.

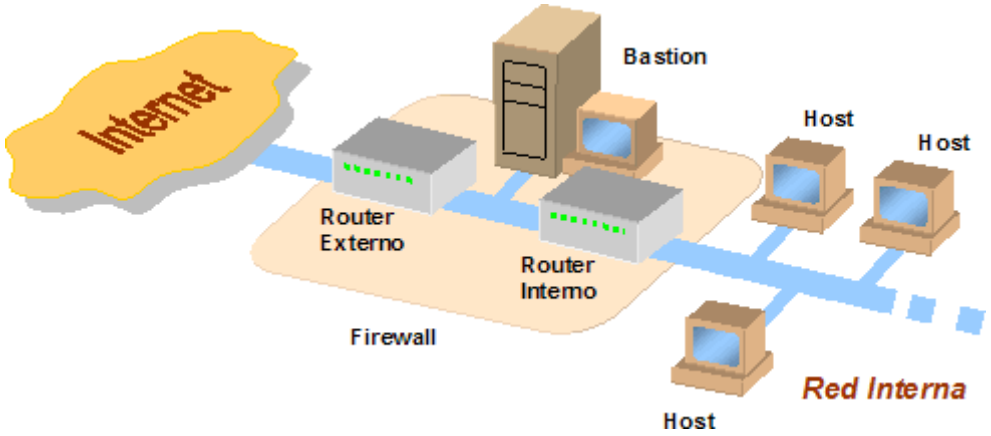


Ilustración 31 Arquitectura sceened subnet

Si un atacante logra vencer la protección del host bastión, solo podrá acceder a la red perimetral ya que la red interna sigue protegida por el router interno. De esta forma el atacante solo tendrá acceso a la red perimetral, ocultando todo el trafico de la red local.

Esta arquitectura es la más segura de las presentadas hasta ahora ya que la ***red perimetral*** soporta aspectos de seguridad a nivel de red y de aplicación y provee un sitio seguro para conectar servidores públicos. Ésta red establece una capa de seguridad adicional, entre la red externa y la red interna protegida. Si un atacante penetra el host bastión de la red perimetral, solo será capaz de ver el tráfico en dicha red. Todo el tráfico en esta red deberá ser desde o hacia el host bastión, o desde y hacia la red externa. Ya que el tráfico de la red interna no pasa por la red perimetral, estará a salvo de ser "escuchado" por un intruso, inclusive si el host bastión es vulnerado.

El ***router externo*** ofrece protección contra ataques provenientes de la red externa y administra el acceso de Internet a la red perimetral. De esta forma, protege tanto a la red perimetral como a la red interna.

En la practica, estos routers permiten casi todo el tráfico que provenga de la red perimetral y realizan pocas tareas de filtrado de paquetes. Las reglas más importantes de este router son aquellas que protegen a los dispositivos situados en la red perimetral, aunque estos estén protegidos a sí mismos pero la redundancia es importante al momento de proteger un sistema. Una de las tareas mas importantes del router externo es bloquear todo paquete que provenga de la red externa "diciendo" que proviene de la red interna.

Para soportar servicios proxy el router externo permitirá el paso de los protocolos si provienen del host bastión. Estas reglas proveen un nivel extra de seguridad, aunque en situaciones normales, estos paquetes ya habrán sido bloqueados por el router interno.

El ***router interno*** protege la red interna de la red externa y de la perimetral administrando el acceso de ésta a la red interna; provee una segunda línea de defensa si el router externo es comprometido.

Realiza la mayor parte del filtrado de paquetes del firewall. Permite que ciertos servicios salgan de la red interna hacia Internet. Estos servicios son aquellos que el sitio puede soportar y proveer de forma segura usando filtrado de paquetes en lugar de servicios proxy (por ejemplo, Telnet, FTP, etc).

Los servicios que permite entre el host bastión y la red interna no son necesariamente los mismos que permite entre la red externa y la red interna. La idea es reducir el número de máquinas que puedan ser atacadas desde el host bastión.

Los servicios permitidos entre el host bastión y la red interna deberían limitarse solo a aquellos que sean necesarios (como por Ej. SMTP, para que el bastión pueda reenviar correo entrante). Inclusive sería apropiado que solo sean permitidos a algunos hosts de la red interna (para el mismo ejemplo, servidores de mail internos)

El **host bastión** conectado a la red perimetral es el principal punto de contacto para conexiones de entrada desde la red externa, por ejemplo, sesiones de correo electrónico (SMTP), conexiones FTP al servidor anónimo del sitio, consultas DNS al sitio, etc.

Los servicios externos son administrados por el host bastión de la misma forma que en la arquitectura anterior, solo que en este caso existe un router más que configurar. En cualquier caso, el host bastión solo se comunicará directamente con los routers que delimitan a red perimetral.

Además del host bastión que actúa como servicio proxy, la red perimetral también podrá contener servidores para distintas aplicaciones (HTTP, Correo electrónico). Inclusive es posible agregar un sistema de detección de intrusos y así poder detectar los problemas antes de que se conviertan en un riesgo para la red.

El host bastión podría ser configurado de tal forma que divida físicamente la red perimetral en dos subredes si se conecta a los router interno y externo mediante dos interfaces de red diferentes (dual-homed) con lo que se obtiene un nivel más de seguridad.

- Variaciones de Arquitecturas Firewall

Hasta aquí se han presentado las arquitecturas básicas y principales que pueden ser encontradas en un firewall. Existen diversas configuraciones partiendo de estas arquitecturas que permiten cubrir las necesidades básicas de una organización que desee proteger su red privada de los ataques provenientes de la red externa (en muchos casos pública) a la cual están conectadas.

Una de las posibles variaciones es utilizar más de un host bastión ya sea para mejorar el desempeño de los servicios de la red ampliando la capacidad de procesamiento paralelo de distintos servicios, introducir redundancia para obtener un

soporte de apoyo (ya sea de servicios o de datos) o separar servicios por razones de seguridad.

También es posible crear una red perimetral utilizando un solo router que cumpla las funciones de un router externo y otro interno. Para esto, el router debe ser lo suficientemente capaz de procesar todo el tráfico que reciba. Esta configuración tiene la misma desventaja de la arquitectura screened host ya que existen un único punto de falla.

El host bastión puede ser utilizado como router externo si se conecta a dos redes mediante dos interfaces de red diferentes. De esta forma, el filtrado de paquetes y los servicios proxy son ejecutados en el mismo host. Esta decisión involucra un costo en el desempeño de estos servicios aunque las tareas de filtrado de un router externo son mínimas. Esta configuración no introduce vulnerabilidades pero sí queda más expuesto en host bastión por lo que deben considerarse medidas de seguridad mayores para tal host. La alternativa opuesta sería aquella que utilice un host con dos interfaces de red para actuar como bastión (servidor proxy) y router interno pero de esta forma se está eliminando el nivel de seguridad provisto por el router interno si los niveles de seguridad más expuestos fallan.

Si la red privada se conectará a más de una red externa, puede utilizarse para cada una un router externo diferente, de esta forma se mantendrá el desempeño de cada router independientemente agregando conectividad.

Una alternativa a este enfoque es utilizar una red perimetral (un firewall) para cada red externa a la cual se conecte la red privada.

Si la red interna es de una dimensión importante tal que pueda sobrecargar al router interno (el más importante), es posible utilizar múltiples routers internos conectados a dos subredes, es decir, a segmentos diferentes correspondientes a la red interna.

4.9.2. Firewalls Distribuidos

Las organizaciones han abierto el ambiente de sus redes para ofrecer sus servicios a otras compañías y a los usuarios interesados, lo que implica un riesgo de seguridad ya que también se encuentra abierta a ataques destinados al uso no permitido de ciertos recursos privados de la red de la organización, inclusive con un perímetro de seguridad.

Los firewalls tradicionales introducen limitaciones de desempeño en la capacidad de tráfico de paquetes en una red, además de no proveer protección contra ataques provenientes de la red privada o que hayan podido pasar la protección perimetral.

Existen ciertos aspectos de las redes actuales que dejan de lado a los firewalls convencionales como una opción de seguridad:

- Debido al incremento de la velocidad de las líneas y los protocolos que requieren más capacidad de cómputo que el firewall puede soportar, las redes tienden a convertirse en puntos de congestión;
- Existen protocolos que son difíciles de procesar por el firewall, ya que no dispone de cierto conocimiento que sí está disponible en los sistemas finales de una red;
- No todos los hosts internos son confiables;
- Varias formas de túneles, conexiones inalámbricas, y métodos de acceso telefónicos permiten establecer puntos de acceso no autorizados a la red que traspasen los mecanismos de seguridad provistos por un firewall tradicional (backdoors);
- Las grandes redes tienden a tener un gran número de puntos de entrada. Muchos sitios emplean firewalls internos para proveer alguna forma de sectorización. Esto hace la administración particularmente difícil, desde un punto de vista práctico con respecto a la consistencia de la política, pues no existe un mecanismo de administración global y unificado;
- La encriptación punto a punto puede ser una amenaza para un firewall convencional ya que evita que éste pueda inspeccionar el paquete para realizar tareas de filtrado;
- Existe una necesidad incremental de un control de acceso más especializado y detallado que los firewall estándares no pueden realizar sin incrementar en gran medida los requerimientos de complejidad y procesamiento, causando una degradación del desempeño de las comunicaciones de la red.

La falta de funciones tales como control de acceso y prevención de intrusos en muchos de los sistemas operativos utilizados en una red (tales como Windows NT o Windows 2000), dejan vulnerables los servidores y dispositivos críticos a una amplia diversidad de herramientas de ataque de fácil acceso por cualquier usuario situado en una red pública.

Ante estas dificultades es necesario un mecanismo de seguridad que permita proteger a estos sistemas sin afectar el desempeño total de la red, considerando la variedad de dispositivos que pueden encontrarse en una red y la topología de la misma.

La introducción de los *firewalls distribuidos* ofrece un conjunto de herramientas que permiten desplegar una configuración de seguridad flexible, transparente, efectiva y robusta para proteger todos los dispositivos de una red, tanto a servidores críticos como usuarios remotos, de cualquier ataque, externo o interno, de forma que no afecte el desempeño de la red. Además, este enfoque se destaca por ofrecer una protección basada en múltiples capas, un mecanismo de administración integrado y un desempeño escalable. [7] [13] [16]

- ¿Que es un firewall distribuido?

Los firewalls distribuidos son aplicaciones de software de seguridad situadas en los sistemas finales críticos de una red que se desean proteger contra posibles ataques, es general, sus servidores y las computadoras de los usuarios.

La principal diferencia con el enfoque tradicional es el sitio de la red donde se efectúa la aplicación de los mecanismos de seguridad. En un firewall de perímetro estos mecanismos están situados en los puntos de acceso a la red, mientras que en un firewall distribuido, se aplican principalmente en cada sistema final que compone la red (si se desea protegerlo).

Las principales características de esta arquitectura son:

- Las tareas de administración y monitoreo son realizadas de forma **central e integrada**, haciéndola más práctica y optimizando recursos;
- La aplicación de los mecanismos de seguridad **se sitúa en los sistemas finales** de la red.

- Administración central

Un firewall distribuido provee herramientas para desplegar tecnología de firewall sobre los dispositivos de la red. Estas herramientas permiten a los administradores de red establecer políticas y monitorear aspectos de seguridad en toda la red, ya sea en sistemas de usuario o en servidores, e inclusive en equipos remotos.

La transparencia de un firewall distribuido mejora la función de administración central. Las políticas son enviadas y embebidas remotamente en los sistemas finales, sin la necesidad de interfaces visibles al usuario; esto mantiene protegido al firewall de malas configuraciones por parte de un usuario no autorizado. De esta forma, solo el personal entrenado para las tareas de administración de seguridad es capaz de trabajar con reportes de actividad y alertas por actividad sospechosa.

- Aplicación de políticas de seguridad situada en los sistemas finales

Los usuarios remotos de una red, que no se encuentran conectados directamente, pueden ser utilizados como punto de entrada por intrusos, inclusive si se utilizan líneas protegidas, tales como redes privadas virtuales, para establecer la conexión ya que es posible que eviten ser detectados por firewalls perimetrales.

Un firewall distribuido sitúa los aspectos de seguridad en cada maquina individual y se mantiene en ellos sin importar donde sean instalados. De esta forma, protegen a cada sistema individual en la misma forma que un firewall de perímetro protege a la red completa. Cada sistema final es capaz de efectuar el control de acceso del trafico de paquetes que reciba basado en las reglas derivadas de la política de seguridad definida. Las políticas pueden ser aplicadas de forma independiente o a nivel de grupos, aunque siempre son administradas de forma centralizada.

A diferencia de los firewalls de perímetro, que deben tomar un enfoque más general para poder proteger a todos los servidores de la red, los firewalls distribuidos pueden ser configurados para optimizar la seguridad de cada servidor y sistema final individual

y de las aplicaciones que soportan ofreciendo un control de acceso especializado, lo que permite crear políticas de seguridad detalladas. Éstas pueden ser configuradas y distribuidas a través de la red a los dispositivos de la red como a aquellos conectados de forma remota a través de interfaces con Internet (cable modem o DSL). Estas actividades son realizadas de forma transparente de modo que el usuario no debe preocuparse por la aplicación de las políticas o el funcionamiento del firewall. De esta forma solo se permite el tráfico esencial en la máquina que protegen, prohibiendo otro tipo de tráfico que pondría en riesgo la integridad de los recursos del sistema.

Los firewalls distribuidos, también llamados agentes de firewall, están basados en la misma tecnología que los firewalls personales pero están enfocados al mercado empresarial ya que permiten integrar una solución distribuida. Las soluciones de firewalls distribuidos permiten proteger empleados remotos y redes de comunicación. También son usados para proteger PCs personales de los usuarios de la red. En principio, son como firewalls personales excepto que ofrecen varias ventajas importantes: administración central, registro, y en algunos casos, granularidad de control de acceso. Estas características son necesarias para implementar políticas de seguridad en redes de grandes empresas de forma uniforme e integrada.

Los firewalls distribuidos son apropiados para todos los sistemas de la red interna y pueden ser aplicados en varios aspectos como ser:

- Fortalecer los servidores de infraestructura e información contra ataques de red;
- Ocultar la información departamental y servidores de aplicación del acceso no deseado;
- Fortalecer sistemas finales críticos.

Pueden proveer ya sea una capa adicional de defensa para servidores localizados detrás de un firewall de perímetro o proteger los servidores directamente expuestos a Internet.

- Componentes y ventajas de un firewall distribuido:

  - Componentes de un firewall distribuido

En función del comportamiento presentado de un firewall distribuido, son necesarios tres componentes principales para el funcionamiento de ésta arquitectura (*ver Figura 32*).

Primero se necesita de *un lenguaje para expresar las políticas y resolver consultas* para determinar si una determinada comunicación será o no permitida.

Como segundo componente, es necesario un *mecanismo para distribuir de forma segura las políticas de seguridad* (un protocolo de administración de claves u otro).

Por ultimo se necesita de un *mecanismo que aplique la política de seguridad asignada a cada host*. Este debe poder reconocer el lenguaje en el que estén expresadas las políticas para poder aplicarlas. Existen, además, para este componente, cuestiones de compatibilidad con respecto a las plataformas donde se utilice.

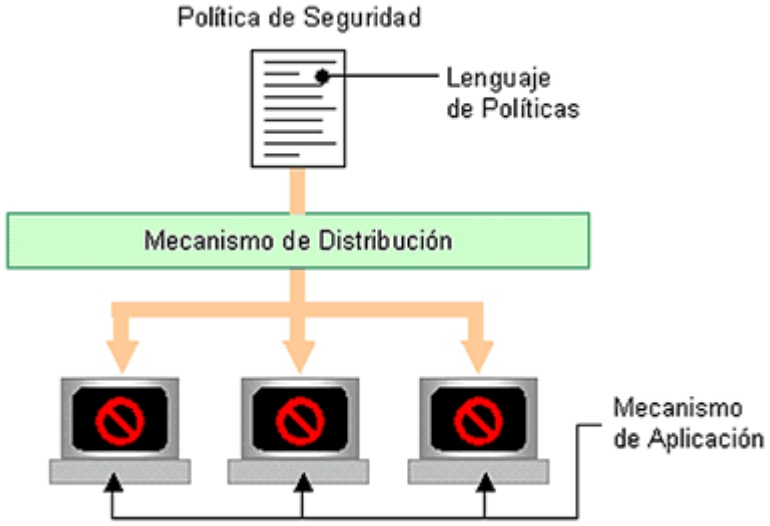


Ilustración 32 Interacción de los componentes principales de un Firewall Distribuido.

Básicamente, la instalación de un firewall distribuido consiste en la instalación del mecanismo de aplicación de la política, que según el producto podrá efectuarse de forma distribuida o individualmente en cada sistema final, pero en general, esta tarea es relativamente simple, similar a la instalación de cualquier producto de software. También se instalará el modulo de administración central en una de las máquinas de la red privada.

Luego, toda tarea de configuración y administración posterior será dirigida desde la consola central. Allí se especificará la política de seguridad para cada sistema o grupo de sistemas, de acuerdo a la definición decidida, que luego será distribuida automáticamente a los dispositivos de la red. Una vez instalada cada política, el mecanismo situado en cada sistema final será el encargado de realizar la función principal del firewall: el control de acceso. Las tareas de monitoreo serán llevadas a cabo por el sistema de administración central.

- Ventajas sobre el enfoque tradicional

La arquitectura que propone un firewall distribuido ofrece ciertas ventajas sobre el enfoque tradicional.

A diferencia de un firewall perimetral, un firewall distribuido, residente en los sistemas finales, puede filtrar el tráfico proveniente tanto de la red externa como de la red interna ya que se ha movido el punto de control de acceso del perímetro a cada host de la red. El concepto de “red no confiable” se extiende, de esta forma, a aquellos hosts situados en la red privada, para responder a la necesidad de ofrecer una

protección contra uno de los ataques más comunes: aquellos que provienen de la red interna, ya sea originados dentro de la red de la organización o por acción de un ataque que ha simulado una de las identidades de la red interna.

Ya que los firewalls distribuidos son exclusivamente sistemas de software pueden ser desplegados sobre una arquitectura de red existente, y cuestan una fracción del precio de un dispositivo para un firewall tradicional. Además el costo de instalación (en tiempo y dificultad) es mucho menor, ya que no requiere una reconexión de la red actual de una organización y consecuente interrupción de las aplicaciones que se ejecutan en la red.

La forma de protección de un firewall distribuido permite que la solución de seguridad sea totalmente escalable en cualquier medida a una multitud y variedad de sistemas conectados a la red, permite ofrecer una solución de seguridad en ambientes heterogéneos. Además elimina al firewall tradicional como único punto de falla ya que la seguridad de cada host depende de sí mismo, es decir, cada host debe aplicar las reglas de control de acceso asignadas según la política de seguridad diseñada para él.

De todas formas, la introducción de un firewall distribuido en una red no elimina por completo la necesidad de un firewall tradicional, ya que éste es útil para ciertas tareas:

- Es más apropiado para proteger la red de ataques de infraestructura aunque ésta es una característica de implementación, no hay razón para que un firewall distribuido no pueda operar en capas básicas arbitrarias;
- La protección contra ataques de denegación de servicio es más efectivas en los puntos de ingreso a la red;
- Los sistemas de detección de intrusos son mas efectivos cuando son situados en un firewall perimetral, donde se dispone de información de tráfico completa;
- El firewall tradicional puede proteger hosts finales que no soporten los mecanismos de los firewalls distribuidos. La integración con la especificación de la política y mecanismos de distribución es especialmente importante aquí, para evitar filtros duplicados y puntos de acceso vulnerables;
- Un firewall tradicional puede actuar como mecanismo de seguridad a prueba de fallos.

Ya que la mayoría de las funciones de seguridad han sido movidas a los hosts, la tarea de un firewall tradicional operando en una infraestructura de firewall distribuido es más simple.

5. TIPOS DE FIREWALLS EN EL MERCADO

La elección de un firewall en el mercado tiene que encajar con todo el Plan Estratégico de Tecnología de Información (TI) de la empresa (si existiese). Si no existe, convendría hacer uno previo a la Auditoría de Seguridad (una Auditoría que no esté alineada a un plan, sería como revisar un coche de carreras que no sabemos el presupuesto para arreglar cosas, ni quién lo va a conducir, ni en qué circuito va a correr, ni si está siquiera asfaltado).

5.1. Pasos para elegir una solución de firewall

Para la elección del tipo de defensa necesaria y el firewall hay que seguir los siguientes pasos:

El primero realizar una auditoría de seguridad que encaje en el Plan Estratégico de Tecnología de información.

El segundo elegir un suministrador ,generalmente lo recomienda el Auditor, de hadware y software.

El Tercer paso es contratar un servicio de gestión de la seguridad.

5.2. El firewall de hadware o dedicado. Ampliances.

El software de firewall para pequeñas empresas es un método utilizado para proteger los equipos de los ataques de piratas informáticos y otras amenazas de Internet. Otro método es desplegar un firewall de hardware (que también utiliza software). A continuación se ofrece una guía para comprender las diferencias entre un software de firewall y un firewall de hardware para pequeñas empresas.

5.2.1. Software de firewall para pequeñas empresas: Cómo funciona

Las soluciones de hardware y software de firewall para pequeñas empresas están diseñadas para bloquear el acceso no autorizado a los equipos. Los firewalls le ayudan a impedir que los piratas informáticos intercepten datos privados o introduzcan troyanos u otras amenazas de Internet en los equipos en red.

Los programas de software de firewall para pequeñas empresas se instalan en cada equipo que se desee proteger. Por tanto, para proteger todos los equipos de la empresa, cada uno debe tener un firewall de software instalado. Esto puede resultar costoso y dificultar el mantenimiento y el soporte.

Además, el software de firewall para pequeñas empresas puede exigir que cada usuario tome decisiones sobre permitir o denegar un acceso solicitado de un programa a Internet (lo que ayuda a impedir que el software malicioso envíe información patentada desde el equipo por Internet, entre otras cosas). Los usuarios sin mucha

experiencia en informática o seguridad pueden sentirse incómodos gestionando las solicitudes y alertas que el software de firewall para pequeñas empresas les presenta.

5.2.2. Firewalls de hardware

Los firewalls basados en hardware protegen todos los equipos de la red. Un firewall basado en hardware es más fácil de mantener y gestionar que los firewalls de software individuales.

La solución ideal para las pequeñas empresas es un firewall de hardware integrado en una solución de seguridad completa. Además de un firewall, la solución debe incluir soporte para red privada virtual (VPN), antivirus, antispam, antispyware, filtrado de contenido y otras tecnologías de seguridad.

Busque una solución de seguridad fácil de usar que esté diseñada para pequeñas empresas y que puede crecer con sus necesidades de seguridad.

5.3. Servicios que da el firewall.

Todos los tipos de empresas se enfrentan a muy diversas amenazas a la seguridad, ante las que deben reaccionar con rapidez y con recursos de TI limitados. Para gestionar estas amenazas hay soluciones de seguridad para necesidades empresariales, como conexiones en red, comunicaciones sitio a sitio, trabajo a distancia, transacciones de PDV o sitios Web seguros. Estas soluciones satisfacen los objetivos de las empresas conectadas por Internet actuales.

5.3.1. Dispositivos móviles seguros.

Las soluciones de movilidad ofrecen acceso remoto con políticas de seguridad aplicadas a recursos de red desde diversas plataformas de dispositivos móviles, incluidos Apple Mac OS®, iOS, Google Android® y Windows Mobile. Las distintas soluciones brindan a los usuarios de teléfonos inteligentes y tabletas un acceso superior al nivel de red para recursos académicos y corporativos a través de conexiones VPN SSL encriptadas, y así asegura la confidencialidad e integridad de los datos para los usuarios externos de la red corporativa cuando se encuentran de viaje o usando enlaces directos.

5.3.2. Movilidad.

Los smartphones y tablets —en especial los dispositivos con iOS tales como Apple® iPhones® e iPads®— han emergido como una potente plataforma para empresas móviles y dispositivos informáticos académicos. Los usuarios esperan contar con acceso en todo momento y en cualquier lugar a través de redes 3G/4G o WiFi tanto para sus actividades corporativas como las privadas. Las soluciones de ofrecen un enfoque de políticas de cumplimiento y servicios de seguridad potentes y simples de utilizar que mejoran la administración de seguridad de las redes de dispositivos móviles.

5.3.3. Conexión de red distribuida

En el modelo empresarial distribuido, las sucursales y las instalaciones de PDV amplían la influencia de una empresa a los mercados principales, pero este vínculo de comunicación debe estar disponible las 24 horas del día, los 7 días de la semana, y debe ser compatible siempre con las aplicaciones de la empresa. Las soluciones de VPN y GMS deben permitir permitir a las empresas centralizar el control de los puntos de acceso remoto y aportar el alto nivel de seguridad y rendimiento necesario para la permanencia de la empresa. Las soluciones de VPN y cortafuegos deben posibilitar las comunicaciones seguras de alta velocidad entre múltiples ubicaciones.

5.3.4. Protección de red.

Lla protección de lu red particular no consiste únicamente en impedir el acceso de las amenazas de Internet, sino también rechazar las amenazas internas. Los dispositivos de seguridad de Internet deben basarse en tecnologías SSL VPN y VPN IPSec cortafuegos de inspección profunda de paquetes con prestaciones de antivirus de pasarela, anti-spyware, comprehensive anti-spam, prevención de intrusiones, antivirus de escritorio forzoso, filtrado de contenidos y seguridad inalámbrica. Al aplicar el usuario soluciones como soluciones específicas o como soluciones integrales el usuario puede simplificar en gran medida la gestión de los servicios de redes locales, remotos y móviles, y proteger la información clave y los recursos de comunicaciones de un modo rentable. Además, gracias a los controles granulares de políticas de limitación de acceso a la red, sólo los usuarios autorizados podrán consultar los datos restringidos.

5.3.5. Acceso remoto seguro.

Cada vez más empresas están basando su red de comunicaciones en Internet de acceso público con el objetivo de ahorrar costes y mejorar la flexibilidad y el rendimiento. Gracias a las tecnologías VPN, ahora es posible transmitir los datos hasta su destino de forma segura, sin riesgo de que se roben o se corrompan los datos. La amplia gama de soluciones de seguridad de Internet basadas en VPN facilita la informática móvil y el trabajo a distancia. Tanto si trabaja desde su casa y busca una alternativa segura a su poco fiable red de casa como si es un habitual de los hoteles que se conecta desde una habitación, se debe tener la solución idónea para satisfacer sus necesidades empresariales específicas.

5.3.6. Gestión Unificada de Amenazas.

La completa solución UTM brinda protección de red inteligente y en tiempo real frente a los sofisticados ataques basados en contenido y en capas de aplicaciones. La solución, que incluye servicios de antivirus de pasarela, anti-spyware, comprehensive anti-spam y prevención de intrusiones, rechaza las amenazas tanto internas como externas mediante la administración de múltiples puntos de amenazas y la exploración minuciosa de todas las capas de red. Gracias al motor de inspección profunda de paquetes de elevado rendimiento, se brinda protección frente a las amenazas

directamente en la pasarela de seguridad, explorando diversos protocolos y tipos de aplicación y comparando los archivos con una extensiva base de datos de firmas que se actualiza de manera continua.

5.3.7. Voz sobre IP (VoIP).

Muchas empresas que quieren reducir los costes de comunicación están volviendo la vista hacia las tecnologías de voz sobre IP (VoIP). No obstante, con frecuencia no se consideran los riesgos a la seguridad asociados con las redes de datos y voz integrados. Las empresas sucumben a la tentación de las ventajas que suponen la reducción de las facturas telefónicas, la gestión centralizada y la rápida instalación y, en ocasiones, no tienen en cuenta la seguridad de VoIP y su impacto en la integridad de la red. Los productos de las empresas de seguridad, proporcionan una completa solución que brindan niveles únicos de seguridad para la infraestructura de VoIP, así como compatibilidad basada en los estándares e interoperabilidad con muchos de los principales dispositivos de comunicaciones y pasarelas de VoIP del mundo.

5.3.8. Clean Wireless.

Se ofrece conexión inalámbrica segura para organizaciones de todos los tamaños de dos maneras: integrada como parte de los dispositivos de seguridad de red (NSA o como puntos de acceso que amplían el alcance de dichos dispositivos. Los puntos de acceso son gestionados por un dispositivo de, que controla a los usuarios de cable o inalámbricos con varias zonas de acceso, al tiempo que otorga a los administradores control total sobre los recursos de red a los que tienen acceso los usuarios. Con la integración de los estándares inalámbricos, las empresas pueden implementar Puntos de acceso en toda la red para establecer seguridad con cable de confianza en toda la organización.

5.3.9. CDP.

Una copia de seguridad es fiable en la medida en que es capaz de restaurar datos y aplicaciones empresariales cuando más se necesitan. Las pequeñas y medianas empresas (PYME) no sólo necesitan proteger sus datos, sino también los sistemas de acceso a ellos, como Exchange, SQL Server y Active Directory. Las PYMES necesitan rendimiento para que la copia de seguridad y restauración de grandes volúmenes de datos se realice rápidamente, al tiempo que deben cumplir con estrictas normativas para el archivo histórico de los datos. Y, en caso de desastre, las PYMES necesitan flexibilidad para recuperar inmediatamente los datos más actuales en nuevas ubicaciones o plataformas de ordenador.

5.4. Alternativas de firewall, servicios y tamaños de empresas.

Para ver la amplitud de de presupuestos hay que tener en cuenta que lógicamente a mayor sistema a defender mayor presupuesto.

He tomado como ejemplo los precios basados en solución panda suministrada por INFODASA con el rango de precios y de una solución particular utilizando hardware sonicwall.

Infodasa vende diferentes marcas de antivirus y firewall, siendo Partner preferentemente de Panda Security. Dependiendo de la naturaleza de la empresa se nosotros combinamos los siguientes productos.

Para la protección individual de los equipos:

- Panda Cloud Office Protection (Seguridad SaaS para todos sus equipos, portátiles y servidores. La solución ligera, segura y fácil)
- Para soluciones perimetrales disponemos de:
- Panda GateDefender Integra (Prevención perimetral centralizada contra todo tipo de amenazas)
- Panda GateDefender Performa (Protección perimetral en tiempo real para su tráfico Web y correo electrónico)
- Panda Virtual GateDefender Performa (Consolide el cloud en su Infraestructura IT virtualizada)

La protección individual de lo equipos siempre la incluimos y dependiendo de la empresa se incluye una solución perimetral. Podéis encontrar toda la información de los productos (funcionalidades, casos de éxito, hoja de producto) en la web http://www.pandasecurity.com/spain/enterprise

El detalle de precios es el siguiente:

Descripción Producto	Licencias	PVPR
Panda Cloud Office Protection 1 año gestionado por Partner	501-1000	51,88 €
Panda Cloud Office Protection 2 años gestionados por Partner	501-1000	88,19 €
Panda Cloud Office Protection 3 años gestionados por Partner	501-1000	124,50 €
Panda Cloud Office Protection 1 año gestionado por Partner	1001-3000	44,47 €
Panda Cloud Office Protection 2 años gestionados por Partner	1001-3000	75,59 €
Panda Cloud Office Protection 3 años gestionados por Partner	1001-3000	106,72 €
Panda Cloud Office Protection 1 año gestionado por Partner	+3000	40,76 €
Panda Cloud Office Protection 2 años gestionados por Partner	+3000	69,29 €
Panda Cloud Office Protection 3 años gestionados por Partner	+3000	97,83 €

Descripción de Producto	PVPR
GateDefender Performa SB Hardware unit + Total Protection 1 año	2.980 €
GateDefender Performa 9100 Lite Hardware unit + Total Protection 1 año	5.560 €
GateDefender Performa 9100 Hardware unit + Total Protection 1 año	9.075 €
GateDefender Performa 9500 Lite Hardware unit + Total Protection 1 año	21.780 €
GateDefender Performa 9500 Hardware unit + Total Protection 1 año	39.200 €

Descripción de Producto	PVPR
Virtual GateDefender Performa 50 users - Total protection 1 año	1.190,00 €
Virtual GateDefender Performa 100 users - Total protection 1 año	1.890,00 €
Virtual GateDefender Performa 250 users - Total protection 1 año	2.590,00 €
Virtual GateDefender Performa 500 users - Total protection 1 año	3.080,00 €
Virtual GateDefender Performa 1000 users - Total protection 1 año	6.595,00 €
Virtual GateDefender Performa 2500 users - Total protection 1 año	16.450,00 €
Virtual GateDefender Performa 5000 users - Total protection 1 año	33.870,00 €
Virtual GateDefender Performa 10000 users - Total protection 1 año	54.869,00 €

Clínica Ruber:

El Hospital Ruber Internacional está situado en Madrid en la zona residencial de Mirasierra. Se puede acceder desde la M30 o la M40 por la Avda. del Ventisquero de la Condesa. Cuenta con 174 confortables habitaciones individuales con terraza.

El Hospital Ruber Internacional necesitaba migrar las actuales plataformas de seguridad con un sistema unificado de protección de la red, mejorar la gestión, aumentar los niveles de seguridad, rendimiento y disponibilidad del servicio. Todo un reto en un escenario complejo como Ruber Internacional.

El objetivo de la segmentación de la red en base a los servicios y las políticas de acceso, para inspeccionar los accesos de los distintos colectivos de usuarios a las distintas aplicaciones internas y externas

Solución:

2 Firewall de nueva Generación en alta Disponibilidad NSA 5500, con servicios de Seguridad:

Antivirus, Antimalware
IPS
Filtrado de Contenidos
Soporte 24x7

Además todo el Hospital esta dotado de Servicios de WI-FI segura, Gestionada por nuestro propio Firewall y un conjunto de 64 Sonicwpoint (puntos de Acceso) que dan cobertura a todo el Hospital.

Te adjunto la Información relativa a la Solución

Con respecto a la Oferta económica, realmente la desconozco en detalle, pero en cualquier caso y como precios de Referencia:

Firewall:

1.- NSA 5500 + Sevicios de seguridad de 1 año: 16.000€
1.- NSA 5500 HA, para alta disponibilidad: 6.500€
64.- Sonicpoint NI (p. Unitario: 415€): 26.560€

5.5. Agradecimientos

Para la realización del estudio de firewall comercial hemos consultado con distintas empresas, estas nos han pedido que los citemos en el estudio por esta razón realizamos este epígrafe:

CONTENTSORT .Ignacio Parres . C/ Núñez Morgado, 6 – 1º B 28036 – Madrid Tlf. 91 323 83 57 Fax. 91 323 51 77 . www.contentsort.com .

MAGRANA.NET Francisco Calvo Savall .Telf/fax: 965 88 08 61.C/Sant Francesc, 3.03510 Callosa d'en Sarrià – Alacant.http://www.magrana.net http://twitter.com/pacocalvo

INFODASA . Juan Manuel Orgaz Mascaraque**.** Responsable de Seguridad. Servicio Técnico. Móvil: 656 811 454. jorgaz@infodasa.com

SONICWALL . Nicasio de Tomas. Territory Account Manager. SonicWALL, Inc. ndetomas@sonicwall.com

T2CLIENT. Albert Clarà Milian. Pau Claris, 94 3ª. aclara@t2client.com 08010 Barcelona . Móvil: 687.87.41.51. www.t2client.com

6. ANEXO 1: TRABAJOS CITADOS

[1] 3com, «Seguridad de Redes:Una guía para implementar Firewalls,» 2010.

[2] INE, «Encuesta sobre el uso de TIC y del comercio Electrónico en las empresas 2010/2011,» 2011.

[3] INE, «Encuesta de uso de TIC y comercio electrónico (CE) en lsa empresas 2010/2011,» 2011.

[4] Panda Security, «Barómetro internacional de Seguridad en PYMEs,» 2009.

[5] PANDA, «II Barómetro internacional de seguridad en las PYMES,» 2010.

[6] Alberto Ureña y otros, «Tecnologías de la Información y las Comunicaciones en la microenpresa,» 2011.

[7] E. l. H. B.Alarcos, «Firewalls,» 2011.

[8] INE, «Indicadores de uso de TIC en empresas,» 2011.

[9] Jorge Mieres, «Ataques informáticos,» 2010.

[10] C. Borghello, «El arma infalible, la ingenieríaq social,» 2009.

[11] INTECO, «Estudio sobre el sector de la seguridad TIC en la empresa,» 2008.

[12] Panda Security, «El mercado negro del cibercrimen al descubierto,» 2010.

[13] P. A. Networks, «Guía para el comprador de firewall,» 2012.

[14] INTECO, «Catálogo de empresas y soluciones de seguridad TIC,» 2010.

[15] Pablo Pérez San-José, «Guía para las empresas: seguridad y privacidad del cloud coputing,» 2011.

[16] D. Medina, «Firewall Distribuido,» 2007.

[17] S. t. LTD, «Seguridad integral para los ambientes más exigentes,» 2006.

[18] Ignacio Cortés Delgado, «¿Qué es y para qué sirven un firewall y una VPN?,» 2007.

[19] R. D.Pantazis, «Firewalls de Internet,» 2003.

[20] G. I. V. Guerrera, «Transmisión de Datos en Internet,» 2007.

[21] INTECO, «Firewalls qué son y para qué sirven,» 2010.

[22] ONTSI, «Tecnologías de la Información y las comunicaciones en la empres española,» 2012.

[23] Varios, «Cluster,» Wikipedia, 2012.

[24] INTECO, «Riesgos y amenazas en Cloud Computing,» 2011.

[25] M. Interno, «Informe de Cliente,» 2011.

[26] verizon, «Cloud computing ¿Exageraciones publicitarias o buena estrategia comercial?,» 2010.

[27] J. A. Z. Urrea, «Diseño y configuración de una firewall humano,» 2007.

7. ANEXO 2: TABLA DE ILUSTRACIONES

8. ANEXO 3: GLOSARIO

ADSL: Línea de Subscripción Asimétrica Digital. Tecnología que mejora el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps (megabits por segundo) gracias a una serie de métodos de compresión.

Ancho de Banda: Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información.

Antivirus: Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

Bandwidth: Ver Ancho de banda.

Base de datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Buffer: El buffer contiene data que es almacenada por un corto periodo de tiempo, generalmente en el RAM de la computadora. El propósito del buffer es guardar data un poco antes que sea usada.

Bus :En una computadora, el bus es la ruta de data en el motherboard o tarjeta madre, que interconecta al microprocesador con extensiones adjuntas conectadas en espacios o slots de expansión, por ejemplo disco duro, CD-ROM drive y tarjetas de video.

Cache: Copia que mantiene una computadora de las páginas web visitadas últimamente, de forma que si el usuario vuelve a solicitarlas, las mismas son leídas desde el disco duro sin necesidad de tener que conectarse de nuevo a la red; consiguiéndose así una mejora muy apreciable en la velocidad.

Certificado Digital: Acreditación emitida por una entidad o un particular debidamente autorizada garantizando que un determinado dato (una firma electrónica o una clave pública) pertenece realmente a quien se supone. Por ejemplo, Verisign y Thawte

Ciberespacio: El conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el cual casi todo lo que contiene es información.

Cibermarketing: Mercadeo a través de la red.

Cliente :Aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red. Sistema o proceso el cual le solicita a otro sistema o proceso la prestación de un servicio.

Comercio electrónico: En inglés e-commerce. Es la compra y venta de bienes y servicios realizado a través del internet, habitualmente con el soporte de plataformas y protocolos de seguridad estandarizados.

Conmutación de Paquetes: Un portador separa los datos en paquetes. Cada paquete contiene la dirección de origen, la dirección de su destino, e información acerca de cómo volver a unirse con otros paquetes emparentados.

Contraseña: Password. Código utilizado para accesar un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

Cracker: Persona que trata de introducirse a un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio.

Criptografía: Se dice que cualquier procedimiento es criptográfico si permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, luego de haberlo descifrado.

CRM: Customer Relationship Management. Manejo de la Relación con el Consumidor. Sistema automatizado de información sobre clientes cuyo objetivo es que estos puedan ser atendidos de la manera más personalizada posible. Internet es uno de los soportes tecnológicos más importantes en CRM, a la vez que uno de sus principales canales de comunicación con los clientes.

DDoS: Acrónimo del inglés "Distributed Denial of Service," (Servicio Denegado Distrubuido). Es un ataque con una multitud de sistemas que han sido "hackeados" dirigido a un objetivo en particular. La cantidad excesiva de data "ahoga" el sistema atacado y lo tumba, causando un DoS.

Desencriptación: Descifrado. Recuperación del contenido real de una información previamente encriptada o cifrada.

Desfragmentar: Desfragmentar un disco duro es el proceso en el cual se reorganiza la data del disco duro para que este de una manera más eficiente, por lo tanto, el disco duro funciona más rapido y mejor.

Dominio: Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.

DoS : Denial Of Service (DoS), denegación de servicio, incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar.

e-commerce : Ver Comercio Electrónico.

Encriptación : Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Ethernet : Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10 Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

Extranet : Cuando una intranet tiene partes públicas, en donde posiblemente usuarios externos al intranet pueden llenar formularios que forman parte de procesos internos del intranet.

Firewall : Combinación de hardware y software la cual separa una red de área local (LAN) en dos o mas partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

Firma digital : Información cifrada que identifica al autor de un documento electrónico y autentica su identidad.

Gateway: Un gateway es un punto de red que actúa como entrada a otra red. En el internet, un nodo o "parada" puede ser un "nodo gateway" o un "nodo host".

Gusano : Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (Marzo 1982). El primer gusano famoso de Internet apareció en

Noviembre de 1988 y se propagó por sí solo a más de 6.000 sistemas a lo largo de Internet.

Hacker**:** Persona que tiene un conocimiento profundo acerca del funcionamiento de redes de forma que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

Host: Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas (ssh, FTP, www, email, etc.). Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

Intranet: Red privada dentro de una compañía u organización que utiliza el navegador favorito de cada usuario, en su computadora, para ver menus con opciones desde cumpleaños del personal, calendario de citas, mensajería instantánea privada, repositorio de archivos y las normativas de la empresa entre otras.

IP: Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10

IPv4: IPv4 es la cuarta revisión del Protocolo de Internet y la más usada hoy en día. Usa direcciones de 32 bits, con el formato "111.111.111.111." Cada sección puede contener un numero de 0 hasta 255, lo cual da un total de 4,294,967,296 (2^32) direcciones IP posibles.

IPv6: Con el crecimiento exponencial de las computadoras, el sistema de direcciones IP, IPv4, se va a quedar sin direcciones IP. Entra en acción IPv6, también llamado IPng (IP Next Generation - IP de Nueva Generación); es la siguiente versión planificada para el sistema de direcciones IP.

LAN: Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones.

Lista de Correo: Mailing List. Listado de direcciones electrónicas utilizado para distribuir mensajes a un grupo de personas y generalmente se utiliza para discutir acerca de un determinado tema.

Login: Clave de acceso que se le asigna a un usuario con el propósito de que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de Internet junto con la dirección electrónica de la computadora que utiliza.

Malware: Cualquier programa cuyo objetivo sea causar daños a computadoras, sistemas o redes y, por extensión, a sus usuarios.

Mensajería instantánea: Instant Messaging (IM), en inglés, es un sistema de intercambio de mensajes entre personas, escritos en tiempo real a través de redes.

Modelo Cliente-Servidor: Sistema que se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor).

Modem: Equipo que permite conectar computadoras por medio de una llamada telefónica, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información).

NAT: Network Address Translation o Network Address Translator es la traducción de IPs privados de una red en IP públicos, para que la red pueda enviar paquetes al exterior, y viceversa.

Network: Ver Red

Networking: Término utilizado para referirse a las redes de telecomunicaciones en general.

P2P: Peer-to-Peer. Comunicación bilateral exclusiva entre dos personas a través de Internet para el intercambio de información en general y de archivos en particular (ej, BitTorrent, eMule).

Paquete: Un paquete es un pedazo de información enviada a través de la red. La unidad de datos que se envía a través de una red la cual se compone de un conjunto de bits que viajan juntos.

Password: Ver Contraseña.

Phishing: "Phishing" (pronunciado como "fishing", "pescar" en inglés) se refiere a comunicaciones fraudulentas diseñadas para inducir a los consumidores a divulgar información personal, financiera o sobre su cuenta, incluyendo nombre de usuario y contraseña, información sobre tarjetas de crédito, entre otros.

PIN: Siglas del ingles Personal Identification Number (Numero de Identificación Personal). Es una contraseña numérica.

Portal: Pagina web con la cual un usuario empieza su navegacion por el WWW.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

Proxy: Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red.

Puerto: Número que aparece tras un nombre de dominio en una URL. Dicho número va precedido del signo (dos puntos). Canal de entrada/salida de una computadora.

Red de Area Local: Ver LAN

Red Privada Virtual: Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.

Router: Un router es un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino.

Servidor: Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

Spam: Envío masivo, indiscriminado y no solicitado de publicidad a través de email, aunque actualmente las personas se refieren como spam a publicidad que llega a los celulares por medio de mensajes de texto SMS, por ejemplo.

Spyware: Spyware son unos pequeños programas cuyo objetivo es mandar información, generalmente a empresas de mercadeo, del uso de internet, websites visitados, etc. del usuario, por medio del internet. Usualmente estas acciones son llevadas a cabo sin el conocimiento del usuario, y consumen ancho de banda, la computadora se pone lenta, etc.

TCP/IP: El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet.

Telefonia IP: La señal analógica de la voz es convertida en señal digital que puede transitar por Internet. La calidad del sonido en las redes TCP/IP depende del ancho de banda del que se dispone.

Telnet: Servicio de internet con el cual un usuario se puede conectar de forma remota a otra computadora, como si se hiciera desde un terminal local, usualmente por el puerto 23. Es preferible usar otros programas más actualizados como ssh2, ya que telnet tiene vulnerabilidades.

Tienda virtual: Página web donde se pueden realizar compras en línea.

Trojan Horse: Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema en el que se introduce de manera subrepticia (de ahí su nombre).

Tunneling: Tecnología que permite que una red mande su data por medio de las conexiones de otra red. Funciona encapsulando un protocolo de red dentro de los paquetes de la segunda red. Es el acto de encapsular un protocolo de comunicación dentro de otro a través de dispositivos y Routers.

USB : Universal Serial Bus. Estándar utilizado en las PCs con el fin de reconocer los dispositivos hardware (impresora, teclado, etc.) y ponerlos en funcionamiento de forma rápida y sencilla. Elimina la necesidad de instalar adaptadores en la PC.

Virus :Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas.

WAN: Siglas del inglés Wide Area Network (Red de Área Amplia). Es una red de computadoras conectadas entre sí, usando líneas terrestres o incluso satélites para interconectar redes LAN en un área geográfica extensa que puede ser hasta de miles de kilómetros.

WLAN: Acrónimo en inglés para Wireless Local Area Network. Red inalámbrica de área local permite que un usuario móvil pueda conectarse a una red de área local (LAN) por medio de una conexión inalámbrica de radio.

Worm: Ver Gusano.

Zipear: Se refiere a la acción de comprimir en un solo archivo a un grupo de archivos que por lo general se comprimen también para que ocupen el menor espacio posible en la computadora y aminore el tiempo en que se transmiten a través de Internet.

9. ANEXO 4: CASO DE UN INFORME PRIVADO OBTENIDO MEDIANTE EL BUSCADOR GOOGLE

“Informe de Cliente: **DATO BORRADO**

Datos actualizados a Abril de 2011

DATO BORRADO

Memorando Interno – Clasificación Confidencial – Para: Equipo de Consultoría

Informe de Cliente: ----------

Datos actualizados a Abril de 2011

INFORMACIÓN SOBRE LA COMPAÑÍA

Nombre de la Compañía: ----------.

Sector de Actividad: Fabricación de componentes informáticos (Routers, Switchs y Firewalls)

Facturación: 5 millones de € (en 2010)

Número de Empleados: 28

---------- tiene como actividades principales la fabricación y comercialización de routers, modems y elementos de conexión de red, así como elementos de seguridad

Entorno Global

Existe una gran competencia a nivel mundial, siendo los ciclos de vida del producto cada vez más cortos y los productos de prestaciones cada vez más elevadas

La tecnología inalámbrica se está imponiendo en los routers de pequeñas prestaciones y la seguridad y el control avanzados en los de grandes prestaciones.

Posición Competitiva

No hay productos sustitutivos de routers y firewalls y las amenazas provienen de los avances en la tecnología utilizada en su diseño y fabricación

Las redes de distribución existentes están controladas en su mayoría por empresas extrajeras de alta tecnología, con lo que existe de una gran presión hacia los canales tradicionales empleados por Inforouter

Seguridad

Routers

En las gamas bajas de producto la diferenciación es media o baja, centrada en prestaciones adicionales o seguridad. Sus precios han mermado considerablemente en los últimos años

En las gamas medias se compite en precio. El R6000 es un producto competitivo ya que posee unas prestaciones medias, pero un precio reducido.

En la gama baja existe mucha oferta y se compite básicamente en precios, aunque los firewalls de más prestaciones poseen una mayor cuota de mercado

En la gama media las empresas que distribuyen routers no suelen ser especialistas y los venden junto a otros elementos, teniendo un poder alto de negociación

Características del Mercado

Los clientes de gama baja de routers y firewalls suelen ser pequeñas empresas y profesionales, mientras que los clientes de las gamas medias suelen ser empresas medianas con cierta extensión en la utilización de TIC

La tendencia de fabricación es a diseñar routers inalámbricos en la gama baja y de mayores prestaciones de seguridad en la alta

El crecimiento nacional desde 2005 se ha mantenido sostenido en un 7% anual para los routers y un 11% en firewalls, no presentando variaciones considerables durante la presente crisis.

La aparición de empresas extrajeras es preocupante, acaparando la mayoría de la cuota de mercado generada por el crecimiento del sector

Las empresas españolas, salvo alguna excepción, se mantienen o bajan sus expectativas a medida que las prestaciones de routers y firewalls se

incrementan y sus precios descienden. La mayoría se convierten en meros distribuidores con servicio de mantenimiento.

El mayor porcentaje de las ventas se obtiene de la línea 300DSL. Es un mercado que puede crecer con el aumento de las redes de área local, aunque existe una fuerte presión de empresas extrajeras de más bajo coste

Existe un 24% aproximadamente de pedidos especiales en los modelos 300 y 6000, en los que se introducen modificaciones solicitadas por el cliente.

La exportación supone un porcentaje muy pequeño de ventas, inferior al 10%. El medio de promoción son las ferias internacionales.

La calidad de los productos de Inforouter es similar a la de sus competidores, pero a diferencia de estos no posee ninguna certificación de calidad u homologación.

Estrategia

Se utilizan tecnologías avanzadas pero no propias, en el diseño de los productos, adaptándolos a las tendencias del mercado.

Se pretende incrementar la presencia internacional, especialmente en Latinoamérica, donde el crecimiento del mercado es mayor que en Europa.

Organización

Organigrama: No existe un organigrama explícito, pero existen los siguientes puestos directivos:

D. **DATO BORRADO**,Gerente y propietario principal.

D. **DATO BORRADO**, Departamento Comercial

D. **DATO BORRADO**, Departamento de Marketing

D. **DATO BORRADO**, Producción y Compras

D. **DATO BORRADO**, Departamento de Personal

D. **DATO BORRADO**, Departamento Financiero

D. **DATO BORRADO**, Servicio Técnico

D. **DATO BORRADO**, Departamento de I+D

Planificación, Organización y Control

Se intenta mantener un buen nivel tecnológico, con el que abordar en el futuro nuevas gamas de productos afines. La dirección sabe que esto supone realizar un mayor esfuerzo en I+D, gestión de stocks, control de producción y en los plazos de entrega.

El proceso de planificación y seguimiento se lleva a cabo a partir de previsiones de ventas, cobros, beneficios, etc. La gestión diaria de fábrica se realiza mediante equipos informáticos independientes, no intercomunicados.

Almacenes

Existe un almacén de componentes y otro de producto terminado, que se controlan manualmente mediante sus respectivos archivos de fichas. Los productos semielaborados se apilan a la salida de una sección o entrada de la siguiente.

Los stocks se actualizan una vez al mes en la base de datos, por lo que es necesario comprobar las existencias físicamente

Producción

La fabricación de routers y firewalls se realiza bajo pedido

El departamento comercial, una vez recibido el pedido, emite un albarán cuyo destino es el departamento de Producción, a este albarán se le asigna un código y se registra en una base de datos, comprobándose si hay existencias en el almacén para servirlo de forma inmediata. En caso contrario, se genera la documentación necesaria para comenzar su fabricación.

Las secciones de fabricación manejan varios pedidos a la vez, cambiando los operarios de tarea/pedido según las

prioridades, los materiales disponibles, etc.

Se lleva a cabo un envejecimiento de

24 horas con objeto de reducir la tasa de fallos más alta en la etapa de funcionamiento inicial de los equipos. Los costes de producción no se conocen para cada producto. El director de fábrica es consciente de la importancia de determinarlos y se trabaja en esta línea.

Comercial

Las ventas se realizan a través de distribuidores en su mayor parte y directamente por Inforouter, especialmente en modelos de más prestaciones o con características especiales.

En momentos determinados se produce una saturación en los pedidos y en la comunicación comercial-producción-fabrica cuando se trata de pedidos especiales, ya que es necesario comunicarse varias veces con el cliente para concretar las modificaciones a su pedido

La compañía se está planteando entrar en Internet de forma más importante. Actualmente dispone de una página informativa en la que se detallan muy superficialmente los modelos y se especifica la dirección, correo electrónico y el teléfono del departamento comercial.

El director comercial afirma que la clientela de Inforouter no suele utilizar Internet como medio de contacto ni comunicación y que posiblemente nunca lo utilice con este fin.

El jefe de fábrica, por otra parte, opina que sería una herramienta indispensable para coordinar los pedidos a medida de los clientes y mejorar el servicio postventa

La principal problemática de una implantación de Internet en mayor profundidad reside en que si existe venta on-line es necesario contar con una logística de la cual carece y por otro lado, no se cuenta con los expertos necesarios en Internet ni con la tecnología suficiente para mantener un portal complejo

Recursos Humanos

Varios directivos y sobre todo el director Comercial, mostraron diferencias de criterio con el director de Marketing a lo largo de las entrevistas mantenidas

Una reciente reducción de la plantilla ha sensibilizado al personal, que en buena parte tiene una edad media cercana a los 40 años. La subsiguiente reorganización del trabajo provocó descontento, por diferencias de criterio entre el director de Recursos Humanos y los trabajadores

Capacidad Tecnológica

Los productos de Inforouter son tecnológicamente competitivos aunque no dispone de tecnología inalámbrica ni de software de control.

Las pequeñas modificaciones que se precisa introducir con frecuencia en los diseños de circuitos impresos, al ser subcontratadas, son lentas y restan flexibilidad de respuesta, y no se dispone de una estación de trabajo CAD que permitiese realizarlas internamente.

DATO BORRADO dispone de tres personas dedicadas a I+D y soporte de ingeniería de fábrica, lo cual hace poco viable aumentar su carga de trabajo. Ninguna de ellas es especialista en software o tecnologías inalámbricas.