# SIE - Firewall DMZ

## Protección perimetral para su red local

**por ALBA Software**

*SIE Firewall es un sistema pensado para proteger la red de su empresa de posibles ataques de Internet. El firewall actua de barrera separando la red de su empresa del servidor de aplicaciones Internet.*

## 1. Importancia de los firewalls

Para explicar la importancia que tienen los cortafuegos dentro de las redes corporativas incorporamos un fragmento de texto extraído del servicio de información de Panda Software:

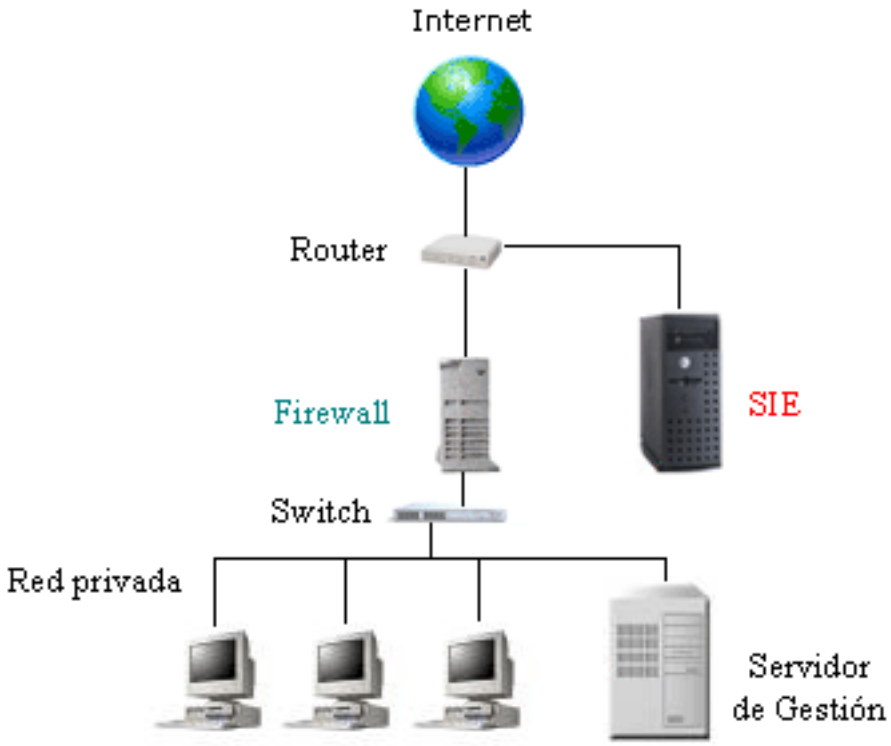
```
Los sistemas de redes de cierta envergadura suelen comprender dos áreas
bien diferenciadas: la red interna y la Zona Desmilitarizada.
La división tiene su origen en el hecho de que actualmente hay muchas
empresas que poseen servidores específicos para Internet (de web, correo,
DNS, etc.). Dichos sistemas terminan siendo de alto riesgo, ya que deben
estar accesibles para cualquier usuario de Internet y, como sus direcciones
son conocidas, suelen convertirse en los primeros objetivos de los
atacantes.

Si los servidores públicos se hospedan en el mismo segmento de red que el
resto de los equipos internos, un usuario malicioso que logre penetrar en
ellos podría, fácilmente, "pasearse" por la red corporativa y acceder a
recursos importantes y a datos confidenciales. Para evitar este problema se
crea la Zona Desmilitarizada, área perimétrica separada de la red interna
en la que se sitúan los servidores que deben ser visibles desde Internet.
```

## 2. Arquitectura de la red

El firewall actúa de barrera examinando todos y cada uno de los paquetes de información que

tratan de atravesar la red:

Para que el firewall funcione de forma efectiva, todo el tráfico de información tendrá que pasar por él, para poder ser inspeccionado mediante el uso de políticas de seguridad, y supervisar los registros de seguridad creando un perímetro de defensa (DMZ) diseñado para proteger la información.




Arquitectura de Red

## 3. ¿Necesito un firewall en mi red?

No hace falta tener enemigos para ser atacado. Los atacantes suelen ser entusiastas de la informática que buscan sus víctimas sin importar si son una empresa multinacional, una pequeña empresa o simplemente un usuario doméstico. De hecho, no son ni tan siquiera ellos mismos los que atacan, sino robots (aplicaciones) que tan sólo buscan una dirección IP que esté ofreciendo algún servicio en Internet y tratan de explotar alguna vulnerabilidad de las aplicaciones (Servidor Web, correo, ftp, etc...) que resida en los equipos expuestos a Internet.

Pensemos que quizá nuestros datos no sean demasiado importantes para otros, pero un

servidor vulnerable sobre el que se puedan lanzar ataques a terceros siempre es atractivo.

Si alguien accede de forma no autorizada a un equipo y toma el control, interesa que no pueda saltar a otros equipos de la red.

La forma de entrar en un equipo es a través de los servicios que ofrece, servidor de correo electrónico, servidor Web, etc. Por tanto si no ofrecemos servicios a internet puede bastar con una buena configuración del router y no haría falta un firewall.

Otro asunto a tener en cuenta es la confianza que tenemos en las aplicaciones que están dando servicios. En el apartado de arquitectura de red el esquema de red muestra un equipo SIE conectado a la red DMZ, pero aquí deben estar todos los equipos que ofrezcan servicios Web. En alguna de nuestras instalaciones hay aplicaciones ASP corriendo en equipos Windows y SIE Firewall está para evitar que cuando el servidor Windows coge un constipado (nimda, code red,...) infecte a la red local de la empresa.

Por ello creamos una red especial donde conectamos los servidores de Internet y la unimos a la red de la empresa mediante un firewall. Que no es más que un equipo con dos tarjetas de red con un software especial que filtra el tráfico que debe circular entre las dos redes.

# 4. Mitos y Ritos

**Cualquier firewall sirve.**

La administración del firewall consiste en establecer correctamente las políticas de acceso de Internet a la red interna y viceversa.

Depende de la arquitectura de la red de la empresa y de los servicios que estamos ofreciendo. No podemos instalar un firewall genérico y pensar que nuestra red está segura, esto solo funciona en casos estándar.

**Nota:**

La seguridad es una consecuencia de los servicios, hay que conocer que hacen, cuales pueden ser sus vulnerabilidades y configurar el firewall en consecuencia.

Esta labor es compleja y necesita un análisis basado en los servicios que estamos ofreciendo y la arquitectura de la red de la empresa. ALBA Software le dará el soporte necesario para configurar completamente las reglas de seguridad.

**El Firewall Hardware.**

El mito del firewall hardware es curioso, según cuenta la leyenda, parece ser que los firewalls hardware son más seguros, más rápidos y funcionan mejor que los implementados por

oftware.

Pero, ¿Que es un firewall hardware?. Aquí hay dos acepciones, unos llaman firewall hardware a aquellos que separan dos redes frente a los que proveen de servicios de firewall al equipo de trabajo.

Si nos basamos en la arquitectura para definirlos, a este tipo se le suele llamar firewall DMZ, porque se encargan de separar la red "desmilitarizada" (De Militarized Zone) o red externa donde se encuentran los equipos que dan servicio a Internet de la red local. Este es el caso que nos ocupa.

Por otro lado está el sentido de "equipo compacto a modo de caja negra que se encarga de la seguridad de mi red".

Por esta misma razón deberíamos llamar router hardware, hub hardware, switch hardware, etc., pero esto no lo hace más seguro o más rápido. De hecho los routers de gama media con capacidad de firewalling montan microprocesadores de las características del 386. Microprocesadores, luego ejecutan código, luego también "tienen software".

Son equipos con un sistema operativo sobre el que corren programas de routing, firewalling, etc., eso si se le llama firmware. Nosotros mismos hemos tenido problemas de "firmware" con routers baratos pero también con routers Cisco serie 800. No nos engañemos, cualquier programa puede contener errores.

Y esto nos lleva a nuestra elección.

SIE Firewall DMZ es **más seguro** porque su sistema operativo está más probado que cualquier otro sistema operativo del mercado. Muchos ven esto como un inconveniente puesto que Linux es código abierto y los hackers pueden inspeccionar su código para encontrar agujeros de seguridad. Ante esto unos comentarios:

- En cuanto se descubre un problema se publica e inmediatamente se soluciona. No hay que tener miedo a lo que conoce todo el mundo sino a lo que solo conocen unos cuantos.
- Windows no es un sistema operativo de código abierto y se descubren más agujeros de seguridad que en ningún otro.
- Un sistema poco probado no es un sistema más seguro, por la misma razón que un puente no es más seguro antes de hacerle la prueba de carga.

SIEDMZ es **más flexible**.

- Podemos instalar módulos de conectividad como VPN, videoconferencia y voz sobre IP, ASSR, etc.
- Permite autentificar servicios de acceso contra el directorio corporativo (LDAP).
- Permite monitorización y soporte remoto.
- Control de ancho de banda.

SIEDMZ es todo lo **rápido** que se necesite nuestra red y los servicios que implementemos puesto que el hardware de un pentium II es mucho más rápido que cualquier firewall "hardware" del mercado, y en muchos casos lo tenemos arrinconado porque ya no nos sirve para estación de trabajo.

**Para proteger el servidor de correo este debe estar detrás de un firewall.**

Este es un rito que no tiene mucho sentido, aunque está más extendido de lo que cabría suponer.

Si colocamos el equipo que está haciendo de servidor de correo dentro de la red local, y por tanto detrás del firewall, debemos abrir el puerto SMTP hacia adentro para que el servidor pueda recibir correo.

El que el servidor esté en una red u otra no evita que el propio servicio de correo tenga una vulnerabilidad, que por otra parte no es tan extraño y si no que se lo pregunten a los que utilizan Exchange Server, en cuyo caso el hacker no tendría el servidor de correo, tendría *toda la red de la empresa*.

# 5. Características de SIE-Firewall

1. Gestión automática del router.
2. Módulos opcionales de conectividad, y administración
3. Posibilidad de control de ancho de banda.

Una característica importante de SIE-Firewall es la posibilidad de control de ancho de banda por protocolos. Esto nos permitirá, por ejemplo, asegurar un ancho de banda mínimo para conexiones VPN entre otros centros con SIE-Firewall y reservar 20 K para voz sobre IP.

# 6. Hardware necesario

El único requisito es disponer de un equipo. Mínimo: Pentium, 32Mb/64 Ram, 1Gb de HD y 2 o 3 tarjetas de red.

# 7. Módulos opcionales.

SIE Firewall permite además incorporar una serie de módulos opcionales que lo convierten en mucho más que un firewall. Una empresa que tenga distintas delegaciones puede conectarlas mediante SIE-Firewall + VPN-IPSEC creando una red privada virtual.

Además, en cada delegación puede montar el módulo de proxy para controlar de forma centralizada los accesos a Internet desde cualquier punto de su red, Servicios de Acceso seguro como ASSR, control de ancho de banda, Etc.

Uno de los últimos módulos incorporados permite voz sobre IP entre centros sobre la VPN.