Que es un firewall y como funciona

La función principal de un **firewall** o **corta fuego** es bloquear cualquier intento de acceso no autorizado a dispositivos internos privados de nuestra red de datos (LAN) desde las conexiones externas de internet comúnmente llamado WAN.

Un **firewall** o **cortafuegos** proporciona un modo de filtrar la información que se comunica a través de la conexión de red. Cuando están presentes en un equipo individual, se denomina un **firewall personal**. Cuando los **firewalls** están presentes en una red empresarial para la protección de múltiples equipos se denomina **Firewall de red**.

Los **Firewalls** permiten o bloquean la comunicación entre equipos basados en reglas. Cada regla define un determinado patrón de **tráfico de red** y la acción a realizar cuando se detecta. Estas reglas personalizables proporcionan control y fluidez sobre el uso de la red.

Un **firewall** puede ser un programa **software** o **dispositivo hardware**. El sistema operativo Windows o Linux Firewall, son ejemplos de **firewalls de software**. ZyXEL ZyWALL USG o SonicWall TZ firewall son ejemplos de **firewall de hardware**.

¿Cómo funciona un firewall?

Un **firewall** actúa bloqueando el tráfico no autorizado y cada diseño de implementación se enfocara a las características y necesidades de cada tipo de empresa.

Existen varios métodos que se utilizan para **filtrar el tráfico de datos**, que pueden ser utilizados individualmente o combinados en un equipo firewall:

Políticas de Firewall

Aquí el firewall sólo permite las comunicaciones a la red protegida sobre la base de las peticiones que provienen de los equipos dentro de esa red. Nadie va poder escanear la red, desde el exterior sólo se ve la **dirección IP** del **cortafuegos**, no se ven recursos internos dentro de la red. Todos los puertos de enlace entrantes están cerrados y todos los puertos salientes están abiertos. Existe la posibilidad de permitir excepciones.

Filtrado de Contenido

Esta función permite el filtrado de paquetes, examina los paquetes de comunicación que intentan pasar a través del **firewall**, comparándolos con las reglas. Las reglas determinan cómo se maneja la comunicación. Estas reglas están basadas en la dirección IP de origen de los datos y el puerto a que se destina.

El **filtrado de contenidos** permite a los administradores bloquear fácilmente algunos tipos de contenido web sin tener que hacerlo manualmente con cada URL individual.
Se bloquean sitios web inapropiados y sitios web de redes sociales de forma rápida y sencilla.

Servicio Anti-Virus de red (AV)

En el caso de los firewalls **ZyWALL USG** se implementa con **Karsperky Anti-Virus (AV)**; es la primera línea de defensa para proteger tu red interna contra ataques que provengan de Internet o enlace WAN.

Las empresas deberían considerar activar el servicio de AV en el firewall, ya que en los ordenadores y

servidores los AV pueden ser fácilmente desactivados o manipulados por los usuarios, creando potenciales riesgos al propio ordenador e incluso a la red.

El AV en el **Gateway Firewall** proporciona una capa adicional de defensa contra las amenazas más recientes.

(AS) Anti-Spam del Firewall

Este servicio protege contra el spam, phishing y correos electrónicos cargados de virus.

La tecnología proviene de la detección de patrón recurrente (RPD).
Analiza la capacidad a través de millones de nuevos patrones a diario (24x7x365) para bloquear todos los mensajes infectados en tiempo real. Además, el antispam se aplica a la IP remitente basado en reputación para eliminar más del 80% del correo electrónico no deseado, evita mensajes sospechosos.

Servicio de IDP

IDP Intrusión Detección y Prevención, permite al administrador controlar aplicaciones específicas conocido como (troyanos y aplicaciones de puerta trasera que pueden infiltrarse en su red interna.
IDP utiliza la tecnología de inspección profunda de paquetes **DPI (deep packet inspectión)** y puede llegar a soportar más de 8.000 firmas.
Esto añade otra capa crítica de seguridad y proporciona al administrador la flexibilidad necesaria para bloquear programas específicos que no están permitidos en la red como el intercambio de archivos P2P o la mensajería instantánea.

También permite a los administradores identificar, categorizar y controlar más de 3.000 aplicaciones sociales, juegos, aplicaciones productivas, Los administradores pueden priorizar las aplicaciones productivas y bloquear las no productivas evitando el abuso del ancho de banda. Esta necesidad es muy frecuente en los casos de las empresas.

Servicio de cliente VPN SSL

Con esta función se logra crear un túnel de comunicación de datos encriptado entre el **firewall** y el usuario de forma rápida y segura sin tener que implementar software adicional en el equipo de usuario.

VPN software Cliente

Esta función se realiza a través de software instalado en el ordenador del cliente, con autenticación fuerte, soporta SHA-2 512 bits y tiene conexión rápida al ejecutarlo.

Servicio Gestionado AP

Debido a la gran demanda de **conexiones inalámbricas wifi** a través del **firewall en la empresa** se pueden controlar los dispositivos AP y lograr administrar el uso para usuarios autorizados y servicios definidos. De esta manera se mantiene la operatividad óptima del servicio.

Si necesitas más información sobre **qué es un firewall y cómo funciona**, puedes consultarlo con nuestros asesores.