****

Equipo:

**Aracely Alhelí Calles Osorio**

**Karen Itzel Alejandra Sánchez Pérez**

**Jorge Emanuel Morales López**

**Javier Adrián Jiménez Hernández**

**Víctor Rivera Diaz**

**Angel Francisco López olan**

Tarea:

**Investigación**

Asignatura:

**Seguridad en informática**

Profesor:

**María de la luz Valdez Ramos**

**¿Qué es un firewall?**

El cortafuegos, o firewall en inglés, es un sistema de seguridad cuyo objetivo es bloquear accesos no autorizados a un sistema, accesos de redes externas. Al mismo tiempo, nos deja seguir la comunicación de nuestro dispositivo con otros servicios y páginas que sí están autorizadas.

## ****¿Cómo funciona un firewall?****

El firewall se sitúa en el punto de unión entre Internet y un ordenador o red de ordenadores. Su mecanismo se basa en controlar toda la información y el tráfico que el router transmite desde una red hacia otra. Si el cortafuegos, realizando un análisis veloz, cree que dichos datos cumplen con ciertos parámetros de seguridad y protocolo, los permitirá entrar en la red.  Si el firewall detecta lo contrario, funcionará como una pared, y bloqueará los mismos para que no se conecten.

## ****Características de un Firewall****

* **Políticas de cortafuegos:** suspende las peticiones de conexión que no provengan de la misma red o sistema, y oculta detrás de una IP los recursos internos.
* **Filtrado de contenido:** identifica los contenidos que pueden dar problemas, siempre teniendo la palabra del usuario como decisión final.
* **Servicios antimalware:** algunos cortafuegos pueden también detectar los virus y evitar su expansión. Estos son un híbrido entre un firewall y antivirus. No son cortafuegos clásicos.
* **Servicios de DPI:**los procedimientos de *Inspección Profunda de Paquetes* suman una segunda protección al sistema, revisando exhaustivamente los paquetes de información que se reciben.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipos de Firewall** | **Descripción** | **Pros** | **Contras** |
| Firewall de red | Bloquea el tráfico no autorizado hacia una red empresarial. | Protección contra ataques externos. | No protege contra amenazas internas. |
| Firewall de aplicación | Se enfoca en los protocolos y puertos de aplicaciones específicas. | Mayor seguridad y control a nivel de aplicación. | Mayor costo y complejidad. |
| Firewall de estado | Analiza el estado de las conexiones de red y autoriza el tráfico de red seguro. | Mayor nivel de seguridad. | Mayor costo y complejidad. |
| Firewall de próxima generación | Ofrece seguridad de red integral con tecnología de última generación. | Mayor flexibilidad y control. | Mayor costo y complejidad. |
| Firewall de hardware | Proporciona seguridad de red en tiempo real mediante hardware dedicado. | Mayor rendimiento y estabilidad. | Mayor costo y complejidad. |
| Firewall de software | Proporciona seguridad de red mediante software instalado en un servidor o computadora. | Menor costo y fácil de implementar. | Menor rendimiento y estabilidad. |