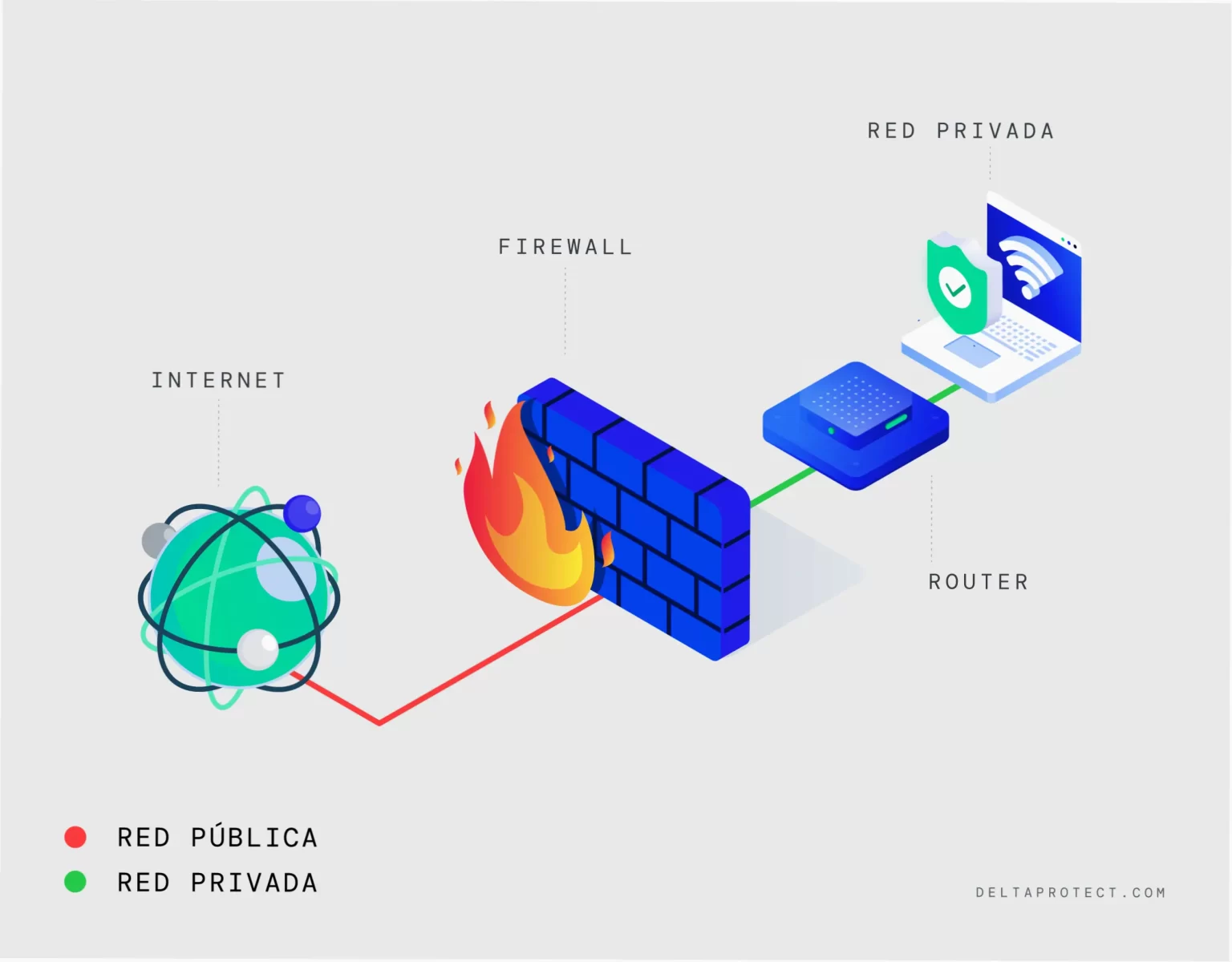
**1.-Realiza un trabajo de investigación sobre los cortafuegos que incluya la siguiente información:**

1. **Información general sobre el funcionamiento del cortafuego.**
2. **Componentes de un cortafuegos.**
3. **Clasificación de los cortafuegos: según la tecnología utilizada, según el área de influencia.**
4. **IPTABLES.**

**Que es un cortafuegos**

Un cortafuegos es un sistema de seguridad que se coloca entre una red interna segura y una red no confiable, como Internet.



Su función principal es permitir a los usuarios de la red interna acceder a recursos externos mientras impide que usuarios no autorizados accedan a la red interna.

Un cortafuegos actúa como una barrera de seguridad que controla el tráfico de red entre la red interna y la red externa.

Esto significa que cualquier tráfico que ingrese o salga de la red interna debe pasar a través del cortafuegos, que verifica si el tráfico es seguro o no antes de permitir que continúe.

Los cortafuegos pueden ser de hardware o software. Los de hardware son dispositivos físicos que protegen la red entre la red interna y externa, mientras que los de software se ejecutan en servidores o equipos individuales. Son utilizados en redes LAN, WAN, MAN, proveedores de servicios de Internet (ISP) y centros de datos para mejorar la seguridad.

**Funcionamiento de un cortafuegos**

El funcionamiento de un cortafuegos se basa en la capacidad de controlar y filtrar el tráfico de red entre la red interna y la red externa. Un cortafuegos actúa como una barrera de seguridad que se coloca entre la red interna segura y la red no confiable, como Internet.

Su función es permitir a los usuarios de la red interna acceder a recursos externos mientras impide que usuarios no autorizados accedan a la red interna. Se basa en tres principios fundamentales:

* **Control de acceso:** el cortafuegos controla quién puede acceder a la red interna y qué recursos pueden ser accedidos
* **Filtrado de tráfico**: el cortafuegos filtra el tráfico de red para bloquear paquetes de datos malintencionados o no deseados
* **Supervisión en tiempo real:** el cortafuegos supervisa el tráfico de red en tiempo real para detectar y responder a posibles amenazas

El cortafuegos actúa como un punto de control entre la red interna y externa, filtrando el tráfico y determinando qué datos pueden entrar o salir para garantizar la seguridad.

**Componentes de un cortafuegos**

Un cortafuegos está compuesto por dos componentes fundamentales: hardware y software. El hardware del cortafuegos se refiere al equipo físico que se utiliza para implementar la seguridad de la red.

Esto puede incluir routers, switches y servidores especiales diseñados para la seguridad de la red.

El software del cortafuegos implementa las políticas de seguridad y filtra el tráfico, mientras que el hardware proporciona la plataforma física. Juntos, impiden el acceso no autorizado a la red.

| **Componente** | **Descripción** |
| --- | --- |
| Hardware del cortafuegos | Equipo físico que se utiliza para implementar la seguridad de la red. |
| Software del cortafuegos | Programa que se ejecuta en el hardware del cortafuegos para implementar las políticas de seguridad de la red. |

**Tipos de cortafuegos**

Los cortafuegos se clasifican en tres categorías principales: cortafuegos de hardware, cortafuegos de software y cortafuegos híbridos. Cada tipo de cortafuegos tiene sus propias características y ventajas, y se utiliza según las necesidades específicas de la red.

# **Cortafuegos de hardware**

Los cortafuegos de hardware son dispositivos físicos diseñados para proteger una red de ataques externos. Estos dispositivos suelen ser routers especiales que se colocan entre la red interna y la red externa.

* **Seguridad física:** Los cortafuegos de hardware suelen ser dispositivos físicos que se colocan en un lugar seguro.
* **Rendimiento alto:** Los cortafuegos de hardware pueden manejar grandes cantidades de tráfico de red sin afectar el rendimiento.
* **Fácil de configurar:** Los cortafuegos de hardware suelen ser fáciles de configurar y administrar.

Los cortafuegos de hardware son adecuados para redes grandes y complejas, ya que ofrecen una alta seguridad y rendimiento.

# **Cortafuegos de software**

Los cortafuegos de software son programas que se instalan en un equipo o servidor para proteger la red. Estos programas monitorean y controlan el tráfico de red para impedir el acceso no autorizado.

* **Flexibilidad:** Los cortafuegos de software pueden ser configurados para adaptarse a las necesidades específicas de la red.
* **Costo efectivo:** Los cortafuegos de software suelen ser más baratos que los cortafuegos de hardware.
* **Fácil de actualizar:** Los cortafuegos de software pueden ser actualizados fácilmente para mantenerse al día con las últimas amenazas de seguridad

Los cortafuegos de software son adecuados para redes pequeñas y medianas, ya que ofrecen una buena relación calidad-precio.

# **Cortafuegos híbridos**

Los cortafuegos híbridos combinan las características de los cortafuegos de hardware y software. Estos dispositivos utilizan hardware especializado para mejorar el rendimiento y la seguridad.

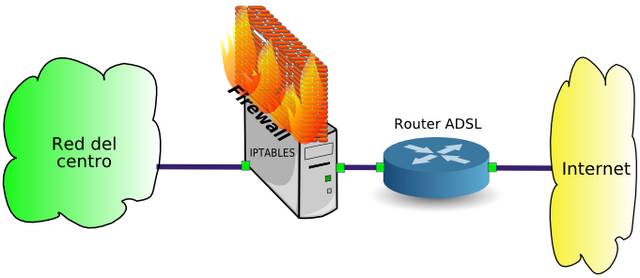
* **Mejora del rendimiento:** Los cortafuegos híbridos ofrecen un rendimiento alto y una baja latencia.
* **Seguridad avanzada**: Los cortafuegos híbridos ofrecen una seguridad avanzada gracias a la combinación de hardware y software.
* **Flexibilidad:** Los cortafuegos híbridos pueden ser configurados para adaptarse a las necesidades específicas de la red.

Los cortafuegos híbridos son adecuados para redes que requieren un alto nivel de seguridad y rendimiento.

La elección del tipo de cortafuegos adecuado dependerá de las necesidades específicas de la red y los recursos disponibles.

**Cortafuegos IPTABLES**

Iptables es el cortafuegos utilizado en Linux para gestionar conexiones. Permite crear reglas que analizan los paquetes de datos que entran, salen o pasan por la máquina, y en función de condiciones establecidas, decide si permitir o bloquear el tráfico. Aunque las posibilidades son casi infinitas y pueden ser configuradas de forma compleja, su función principal es filtrar el tráfico según las reglas definidas por el administrador.



# **¿Cómo funciona Iptables?**

Iptables utiliza una estructura de tablas para organizar y gestionar las reglas de filtrado. Las tablas se dividen en diferentes cadenas y reglas para definir el comportamiento del tráfico. Los paquetes de red pasan a través de estas tablas y, según las reglas configuradas, el cortafuegos decide si se permiten, se bloquean o se modifican. Las principales tablas son:

* **filter:** Es la tabla por defecto, encargada de filtrar el tráfico. Las reglas de esta tabla definen si un paquete es aceptado o rechazado.
* **nat**: Se utiliza para la traducción de direcciones de red (NAT), como la redirección de puertos o el enmascaramiento.
* **mangle**: Permite modificar los paquetes, como cambiar el tipo de servicio o los valores de los paquetes.
* **raw**: Permite excepciones para el seguimiento de conexiones y realizar manipulaciones específicas en el tráfico.
* **security**: Gestiona las políticas de seguridad, como el control de acceso

# **Cadenas principales**

Cada tabla tiene un conjunto de cadenas que especifican los puntos en los que se procesan los paquetes:

* **INPUT**: Gestiona el tráfico que entra al sistema.
* **OUTPUT**: Gestiona el tráfico que sale del sistema.
* **FORWARD**: Gestiona el tráfico que pasa a través del sistema (cuando no está destinado ni a la máquina de origen ni a la de destino).
* **PREROUTING y POSTROUTING**: Estas cadenas se utilizan en la tabla NAT y se encargan de la manipulación de los paquetes antes o después del enrutamiento.

# 

# **Reglas**

Las reglas en iptables definen el comportamiento frente al tráfico, como por ejemplo:

* **ACCEPT**: Permite que el paquete pase.
* **DROP**: Bloquea el paquete sin enviar ningún mensaje.
* **REJECT**: Bloquea el paquete y envía un mensaje de error.
* **LOG**: Registra el paquete en los logs del sistema.

# **Ejemplo básico de uso**

iptables -A INPUT -p tcp --dport 80 -j ACCEPT