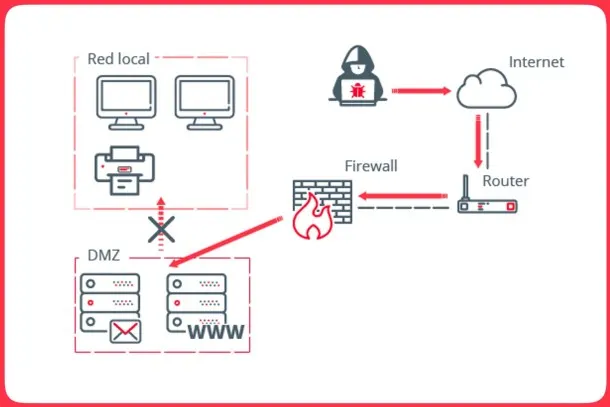
**5.-Realiza un trabajo de investigación sobre la DMZ, que incluya la siguiente información:**

1. **Información general sobre su funcionamiento.**
2. **Arquitectura débil de subred protegida (un firewall).**
3. **Arquitectura fuerte de subred protegida (dos firewall).**

**Que es DMZ**

La DMZ es una red perimetral en una infraestructura de red empresarial que actúa como una zona intermedia entre la red interna segura de la organización y redes externas, como Internet. La principal finalidad de la DMZ es aislar los sistemas expuestos a Internet de la red interna, proporcionando una capa de seguridad adicional para evitar que los atacantes puedan penetrar la red interna a través de servicios públicos como servidores web, servidores de correo electrónico o servidores DNS.



La DMZ no es una red completamente aislada, pero se configura para que los dispositivos y servicios que residen en ella sean accesibles desde el exterior, pero con restricciones para evitar que el tráfico no autorizado ingrese a la red interna. Es una estrategia clave en la segmentación de red y protección contra ataques cibernéticos.

# **Componentes para el Funcionamiento de DMZ**

* **Firewall de Perímetro**: Controla el acceso entre la red interna, la DMZ y la red externa, asegurando que solo el tráfico autorizado fluya entre ellas.
* **Servicios Expuestos**: Los servidores que ofrecen servicios públicos (web, correo, FTP) se alojan en la DMZ, exponiéndose de manera controlada.
* **Accesibilidad Controlada**: Los dispositivos en la DMZ pueden ser accesibles desde Internet, pero su acceso a la red interna se restringe.

**Arquitectura Débil de Subred Protegida**

En una arquitectura débil de DMZ, sólo se utiliza un firewall para controlar el tráfico entre la red interna, la DMZ y la red externa. Esta configuración es más simple y económica, pero tiene ciertas limitaciones en términos de seguridad.

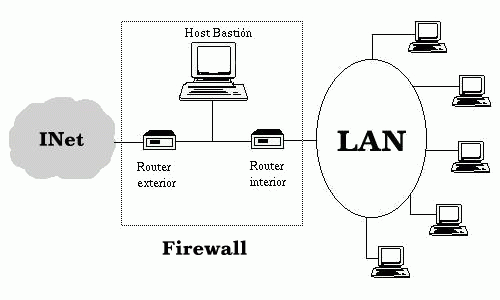
# **Características de la Arquitectura Débil**

Se utiliza un único firewall para filtrar el tráfico entrante desde Internet hacia la DMZ y el tráfico de la DMZ hacia la red interna. Este firewall se coloca en la "frontera" entre las redes.

Los servicios públicos, como servidores web, servidores de correo y DNS, se colocan dentro de la DMZ, pero solo pueden ser accedidos desde Internet y no desde la red interna.

* **Ventajas:**
  + **Económica**: La implementación es más simple y barata, ya que solo se necesita un firewall.
  + **Fácil de configurar**: Se configura de forma rápida y sencilla, lo que lo hace adecuado para redes pequeñas o con necesidades de seguridad menos estrictas.
* **Desventajas:** 
  + **Seguridad limitada**: Si el firewall de la DMZ es vulnerado, el atacante tiene acceso directo a la DMZ, lo que podría facilitar el acceso a la red interna.
  + **Menor control**: La ausencia de una segunda capa de defensa entre la DMZ y la red interna significa que un atacante podría explotar la DMZ para atacar los sistemas internos

En esta arquitectura, la DMZ se convierte en un área de riesgo potencial, aunque los servicios expuestos están segmentados de la red interna.



**Arquitectura Fuerte de Subred Protegida**

En una arquitectura fuerte de DMZ, se utilizan dos firewalls, creando una defensa en profundidad entre la red interna y la DMZ. Esta configuración mejora la seguridad al agregar una capa adicional de filtrado de tráfico entre las redes, asegurando que, incluso si un firewall es vulnerado, el acceso a la red interna sigue estando restringido.

# **Características de la Arquitectura Fuerte**

Se colocan dos firewalls en serie. El primer firewall filtra el tráfico que entra desde Internet hacia la DMZ, y el segundo firewall controla el tráfico entre la DMZ y la red interna

* **Firewall Externo:** Protege la red externa (Internet) de la DMZ, bloqueando accesos no autorizados desde el exterior.
* **Firewall Interno:** Filtra el tráfico entre la DMZ y la red interna, asegurando que incluso si un servicio en la DMZ es comprometido, no se pueda acceder directamente a la red interna

1. **Ventajas**
   1. **Seguridad Mejorada**: El uso de dos firewalls crea una defensa en profundidad, lo que significa que si un firewall es vulnerado, el otro sigue protegiendo la red interna.
   2. **Segmentación Rigurosa**: El tráfico entre la DMZ y la red interna está estrictamente controlado, lo que minimiza las posibilidades de que un atacante comprometa la red interna a través de un servidor en la DMZ.
   3. **Mayor Control y Monitoreo**: Esta arquitectura permite políticas de seguridad más detalladas y monitoreo más fino del tráfico.
2. **Desventajas:**
   1. Costo y Complejidad: Requiere más recursos tanto en términos de hardware como en la gestión y mantenimiento de las reglas de filtrado.
   2. Mayor Latencia: El doble filtrado de tráfico puede introducir una ligera latencia en las comunicaciones entre la red interna y la DMZ, aunque esto rara vez es un problema significativo en redes bien dimensionadas.

En esta configuración, la DMZ actúa como una zona altamente segmentada y protegida que asegura la red interna sin comprometer la accesibilidad de los servicios públicos.

