Seguridad perimetral

Álvaro González Sotillo

13 de noviembre de 2026

Índice

1. Introducción **1**

2. Sin seguridad perimetral **1**

3. Seguridad perimetral **2**

4. Medidas a a aplicar **2**

5. *Firewall* **3**

6. *Proxy* (pasarela) **3**

7. VPN **3**

8. Arquitecturas de cortafuegos **3**

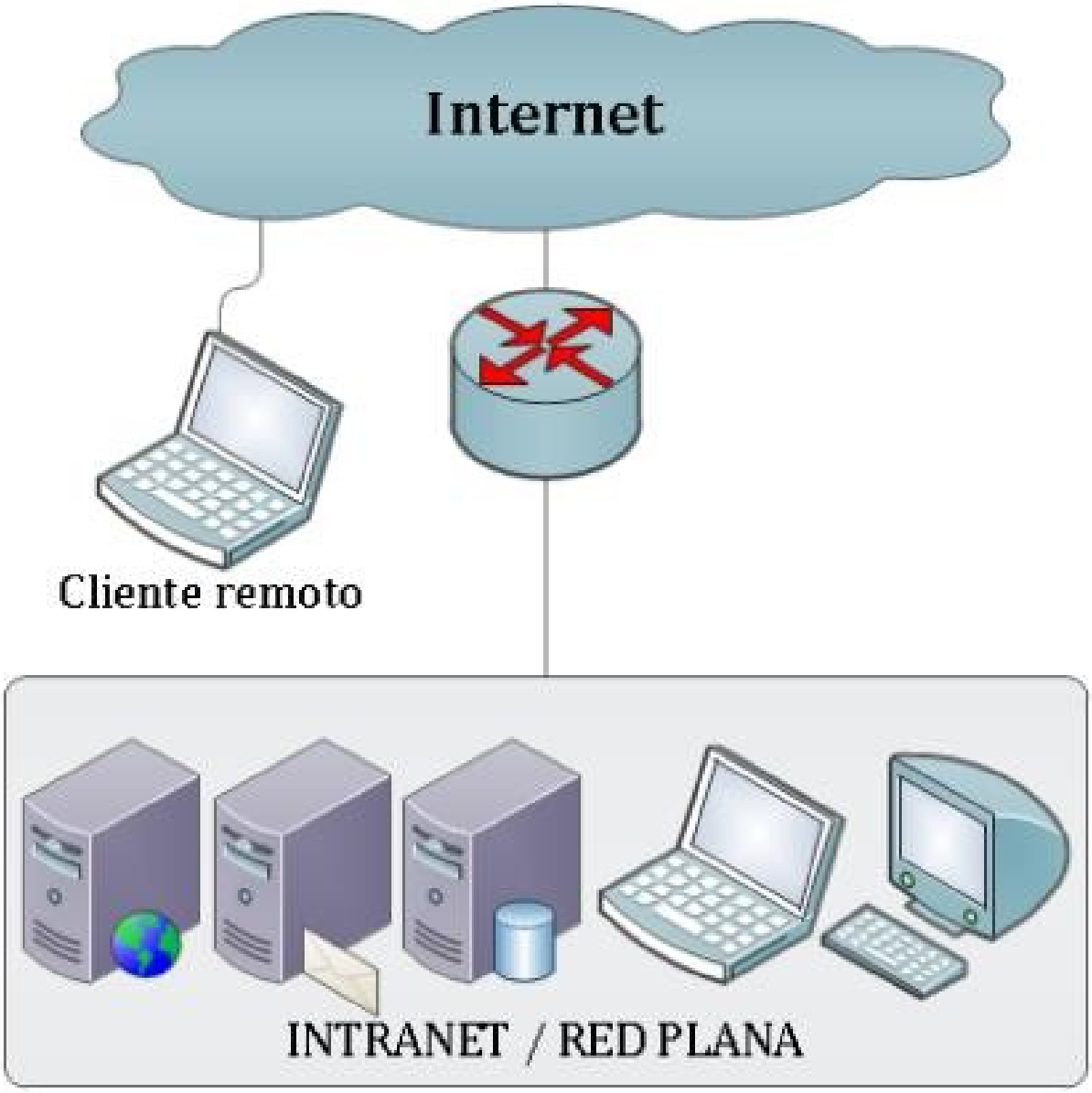
9. Referencias **7**

1. Introducción

- Las redes corporativas son LAN
  - Se asumen privadas
  - El administrador controla clientes, servicios, equipos de red
  - Pero es una red aislada
- Redes públicas
  - Tienen una utilidad evidente: consumir y proveer servicios a otras empresas o divisiones de la empresa
  - Tienen peligros evidentes: ataques a sistemas internos

2. Sin seguridad perimetral

- Se conecta la red corporativa a Internet mediante un router
- Sin *firewall*, simplemente enrutamiento
  - Publicación de servicios internos
  - No hay elementos de monitorización
  - No se filtra tráfico de entrada ni de salida
  - Clientes remotos acceden directamente a los servicios.



3. Seguridad perimetral

- La primera línea de defensa entre las redes públicas y privadas. ◦
- La seguridad perimetral implementa diferentes tipos de arquitectura
- Para proteger nuestra *red interna* o *subred protegida*.
- Hay varias posibilidades, que varían entre:
  - Configuración sencilla y poca protección. **Débil**
  - Configuración compleja y alta protección. **Fuerte**

4. Medidas a a aplicar

- La seguridad perimetral puede combinar varias medidas entre:
  - Cortafuegos (*firewall*) en *routers*

- Cortafuegos en equipos finales (servidores)
- Bastiones (*proxies* o pasarelas)
- VPN

5. *Firewall*

- Trabaja generalmente a nivel de red (IP) y transporte (TCP, UDP)
- Tipos
  - *firewalls* personales: integrados en las *workstations* y servidores
    - ufw
    - Windows firewall
  - *Firewalls* por *software*
    - Se instalan en sistemas operativos de servidor
    - Utilizan las mismas tecnologías que los *firewalls* personales, con extensiones para varias interfaces
  - *Firewalls* por *hardware*
    - Instalados en equipos de red (no terminales)
    - Ejemplo: ACL de Cisco
- En otro tema del curso trabajaremos los *firewall* implementados en linux.

5.1. *Firewalls* más allá de TCP/UDP

- Los bastiones (más adelante) pueden incluir reglas de acceso
- Puede haber configuraciones/plugins en servidores que cumplan función de filtro
  - Ejemplo: modsecurity para Apache/IIS/nginx

6. *Proxy* (pasarela)

- Equivalente a bastión
  - El bastión suele ser el servidor, el *proxy* el servicio
  - El bastión puede hacer funciones de *router*
- El *proxy* hace de MITM entre los clientes y los servicios reales
  1. El cliente está configurado para usar el *proxy*
  2. O bien el administrador de red ha configurado los DNS/routers para hacer creer al cliente que se comunica con el servicio (*proxy* transparente)

7. VPN

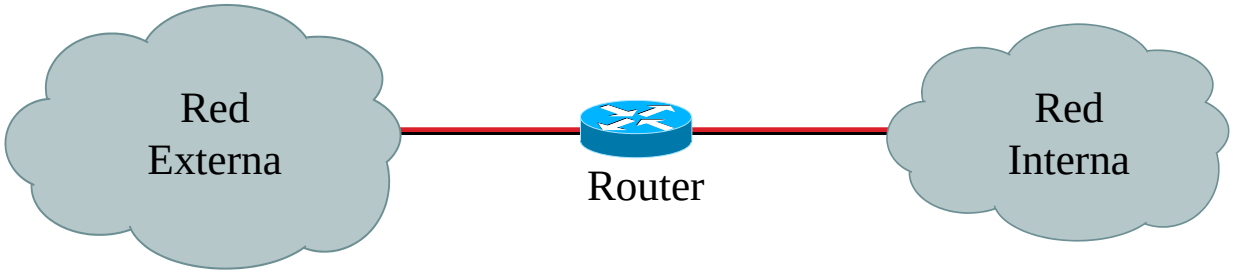
- Red privada virtual
- Descrito en esta presentación

8. Arquitecturas de cortafuegos

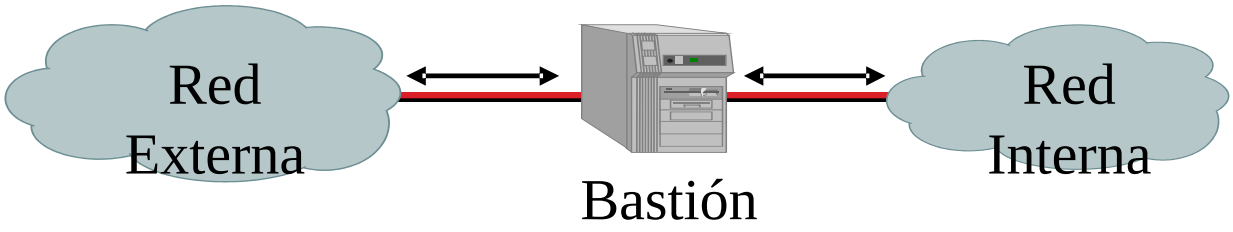
- *Screening router*
- *Screened host*
- *Screened subnet*

8.1. *Screening router*

- Configuración simple
- Poco *hardware* (barato)
- Los servicios al exterior están en la misma red que las *workstations*
  - Se mezcla tráfico interno y externo en la misma red *ethernet*
- La seguridad depende de un solo punto
  - Si un atacante consigue el control del router, controla toda la red

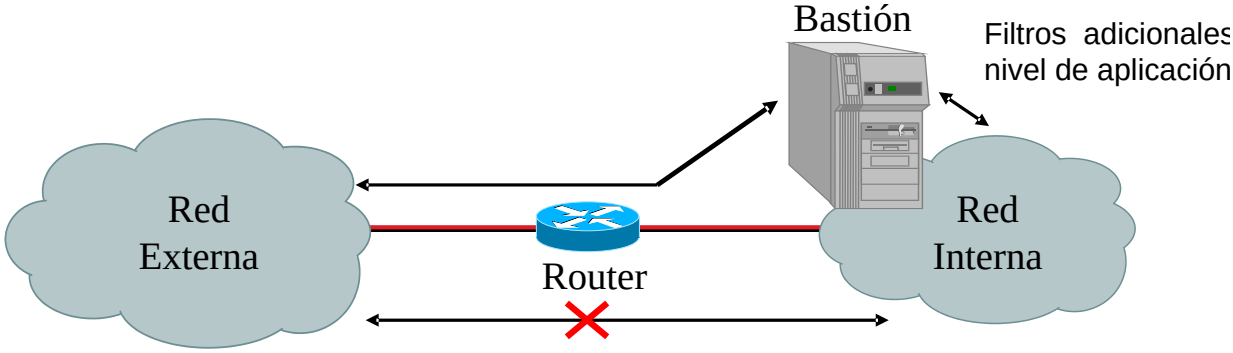


- El *router* puede cambiarse por un bastión
- Así puede controlarse también el nivel de aplicación
- Filtros más complejos, con más criterios
  - Usuario de aplicación
  - Recurso accedido (URL)
  - Límites de ancho de banda y tráfico total
  - Hora y día de acceso
  - ...

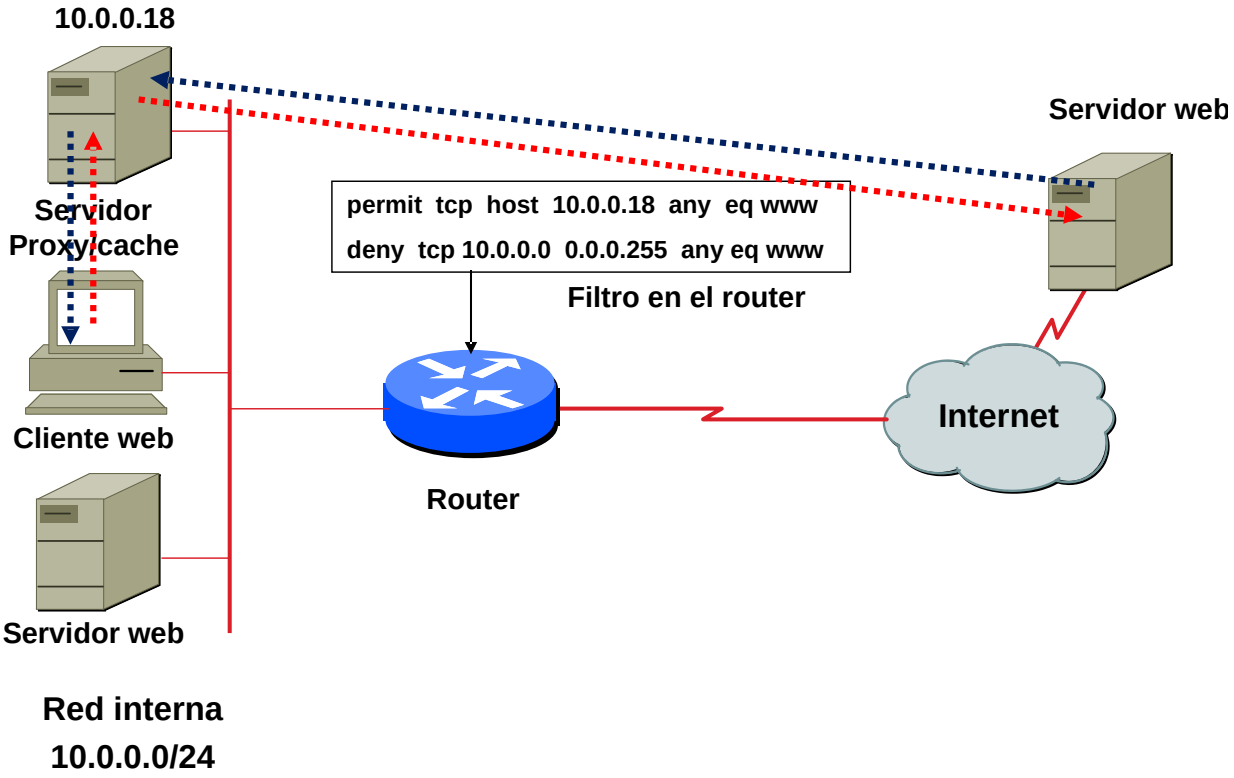


8.2. *Screened host*

- Se separa el *router* del bastión
- El *router* envía las peticiones externas al bastión
- La mayoría de los clientes no salen directamente por el router, sino que lo hacen a través del bastión

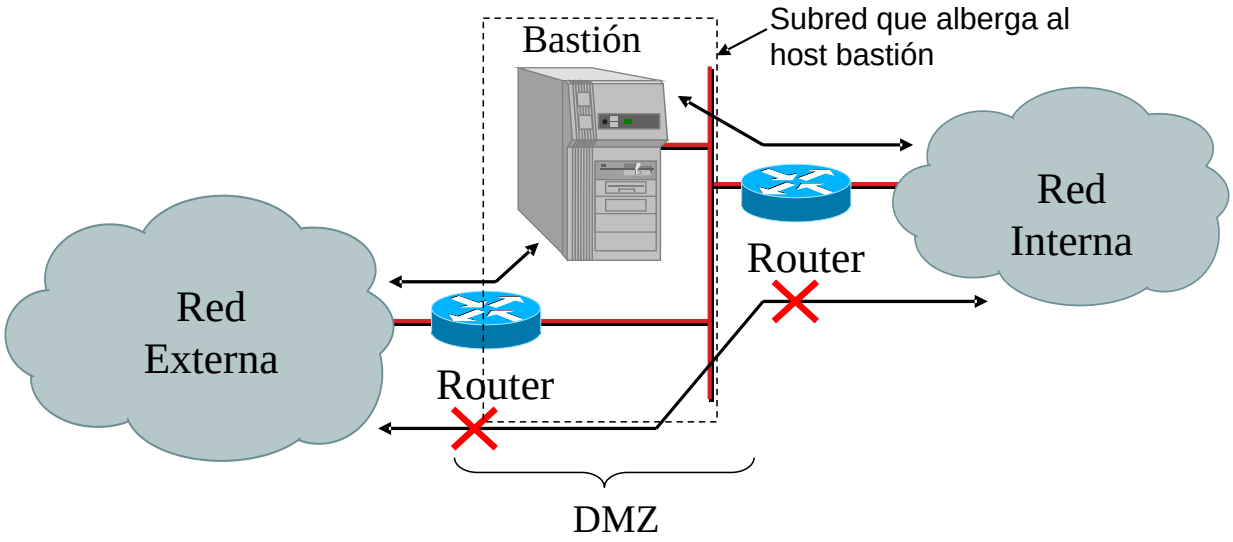


- Ejemplo con *router* Cisco, en el que todas las peticiones HTTP deben pasar por el *proxy*



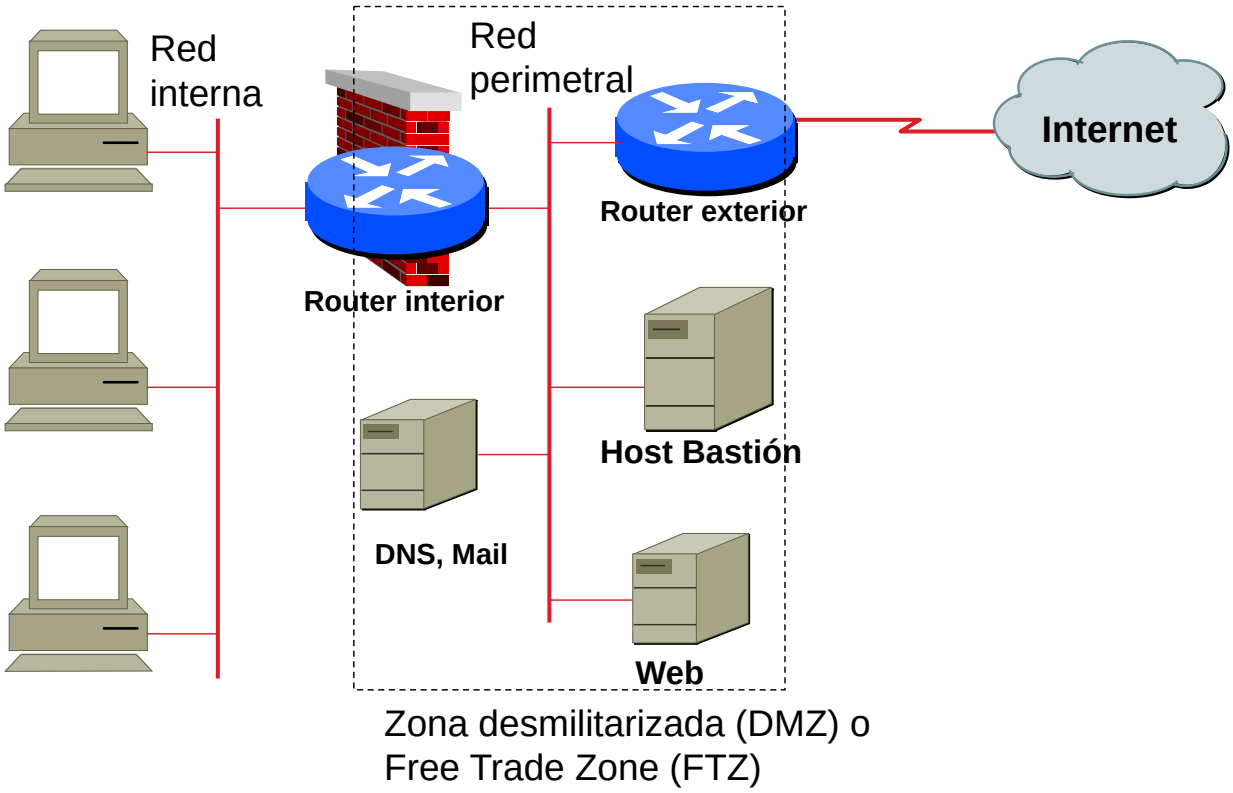
8.3. *Screened subnet*

- La red interna no se satura con peticiones del exterior
- Si el router externo o el bastión es *hackeado* queda otro nivel de protección
- Más caro, más complejo. Pero más difícil de comprometer.



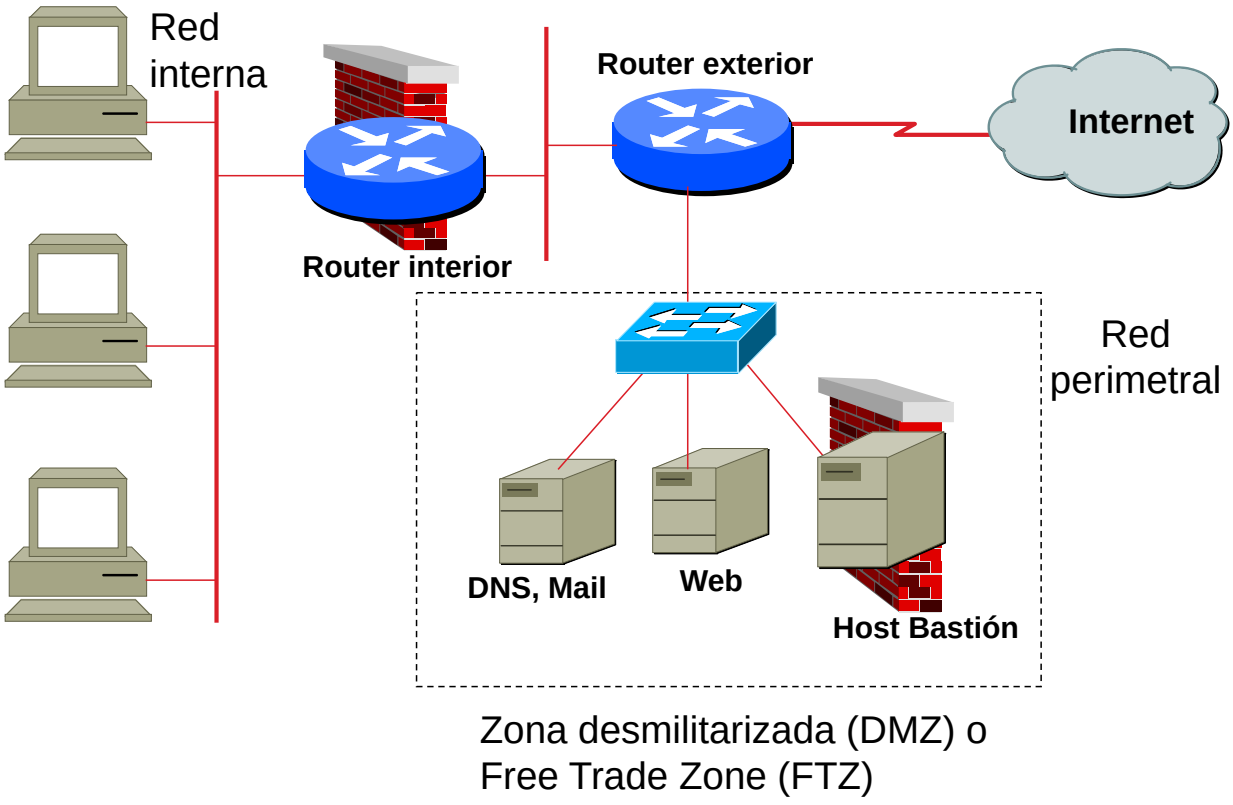
8.4. DMZ

- Los servicios al exterior no necesitan estar en la red interna
- Suelen colocarse entre los dos *routers*



8.5. DMZ (variante)

- Hay variantes según el número de routers y redes intermedias entre Internet y la red interna



9. Referencias

- Formatos:
  - Transparencias
  - PDF
  - Página web
  - EPUB
- Alojado en Github