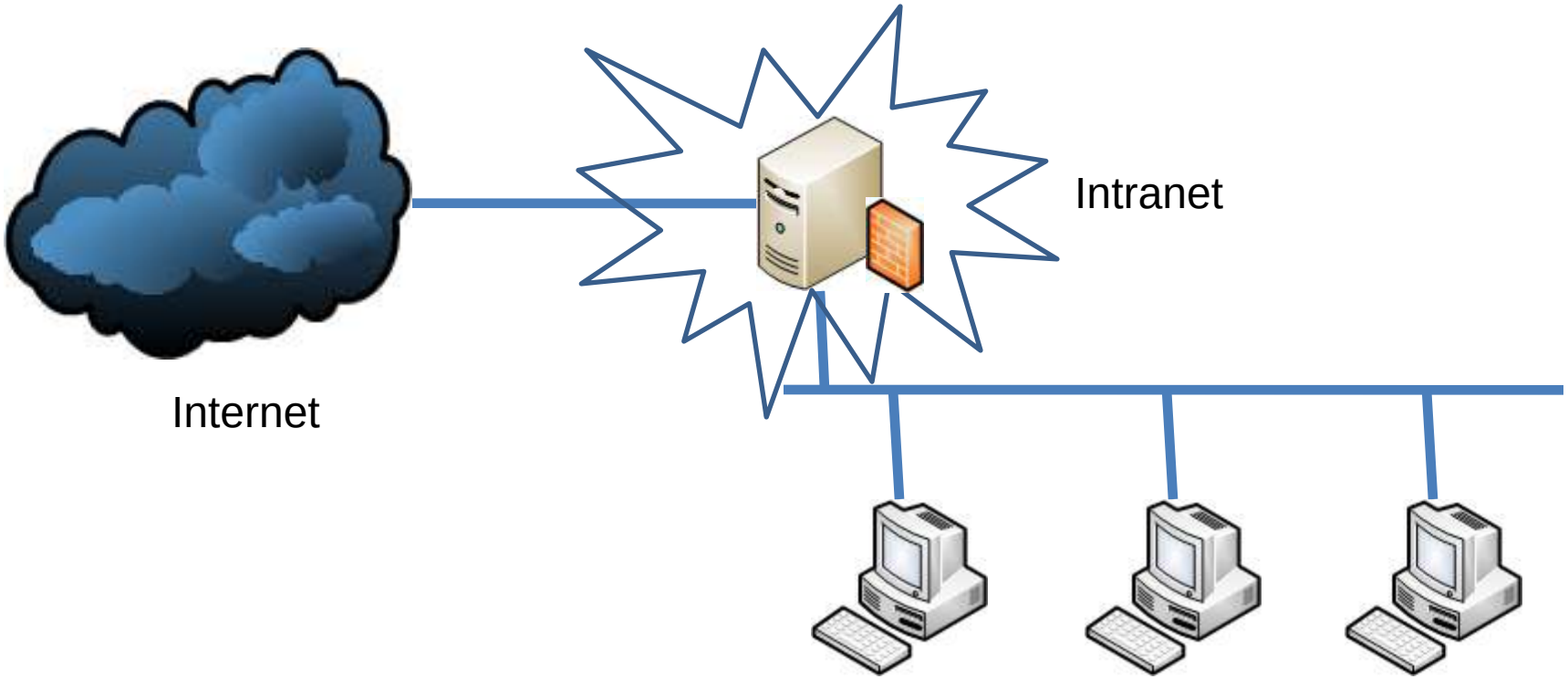
Tema 5. Topologías de red Seguras

Módulo I : Topologías de Red Seguras

Introducción

- Definición de Firewall:
  - Firewall o cortafuegos se denomina al elemento de enlace entre dos tramos de Red.



Introducción

- Características:
  - Aparecen entre políticas diferentes de seguridad de red.
  - Define zonas confiables por las que los datos pueden distribuirse sin peligro de su seguridad. Los pueden viajar por ellas sin la necesidad de identificarse a cada momento.
  - Centralizan la política de control relativa al acceso a terceras partes, entrada y salida.
  - Permiten separar el problema en dos partes política interna frente a política de interconexión.

Elementos Tecnológicos

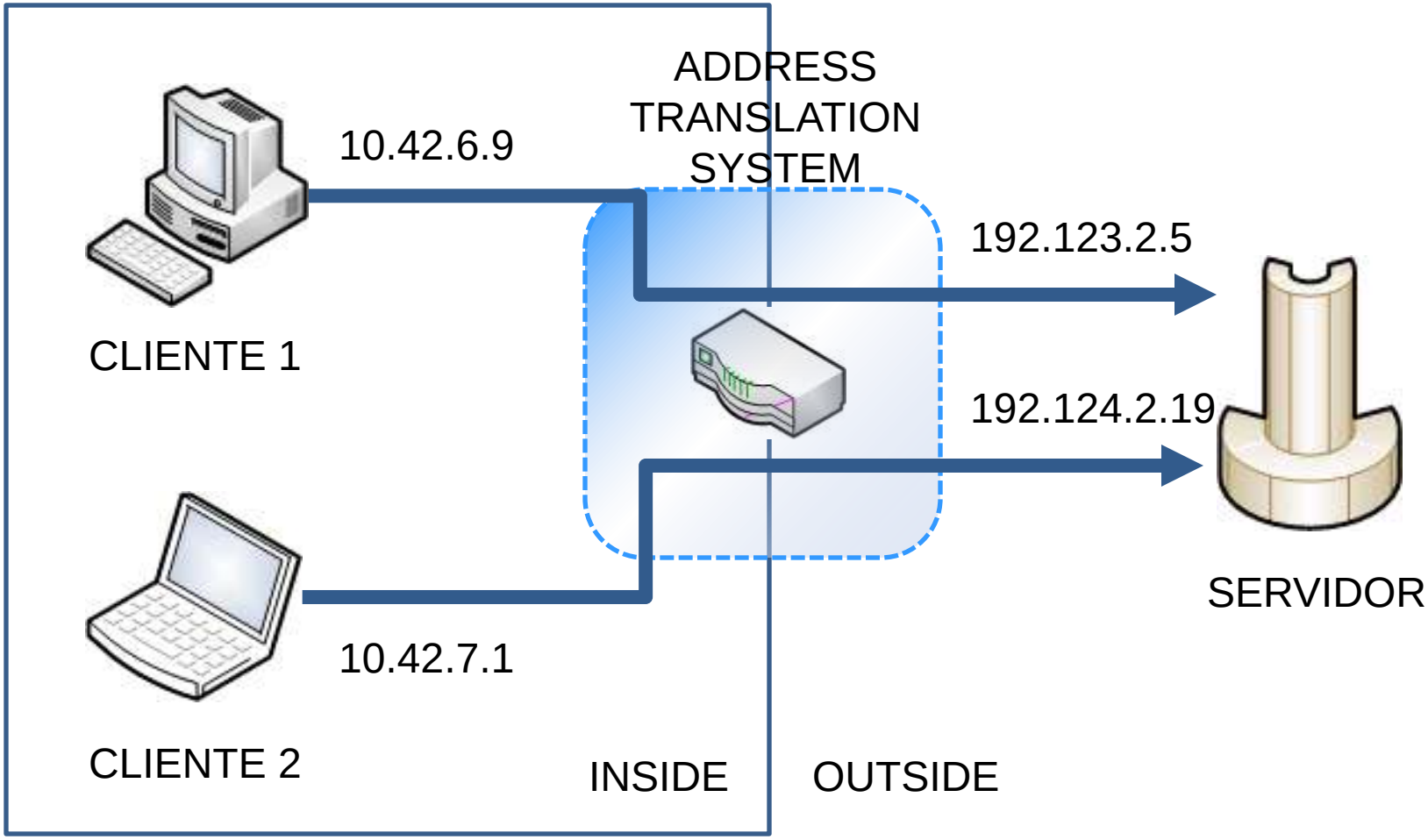
- Filtros a nivel de red
  - Las redes IP permiten el intercambio de paquetes. Cada conexión TCP o UDP está asociada a un equipo y a un puerto (asociado a un servicio).
  - Controlando los paquetes que van y vienen controlamos los servicios que están prestando.
  - Un cortafuegos a nivel de red suele incorporarse a un equipo encaminador (router).

Elementos Tecnológicos

- Direcciones IP de intranet
  - Los encaminadores (routers) precisan de direcciones válidas para ir acercando los paquetes a su destino.
  - La utilización de direcciones no válidas para las intranets favorece:
    - A la escasez de direcciones de Internet
    - La seguridad de las máquinas de la intranet.
  - De la traducción a direcciones legales puede hacerse cargo el cortafuegos. (NAT, Network Address Translation, rfc 1631)

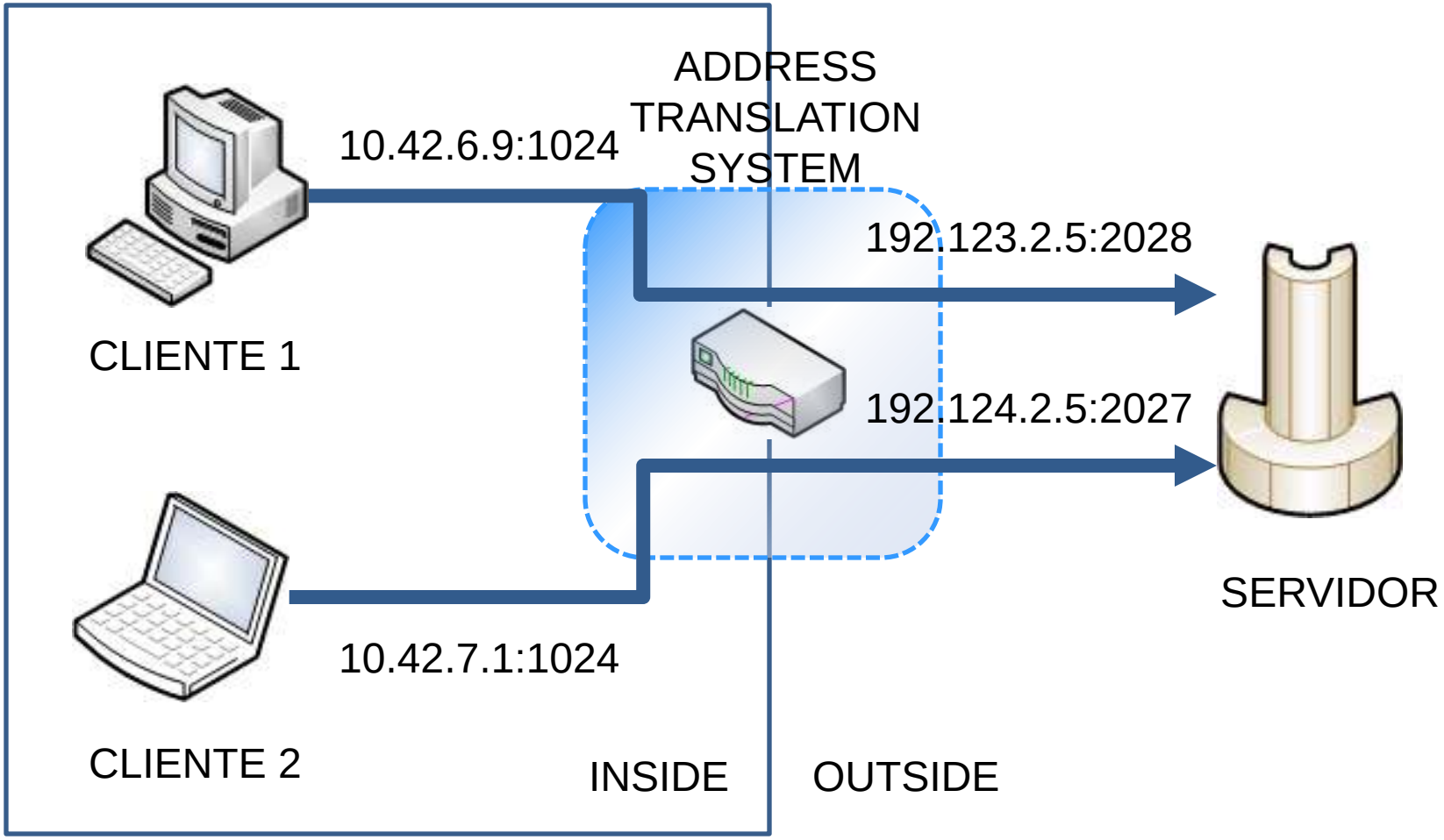
Elementos Tecnológicos

- NAT



Elementos Tecnológicos

- PAT

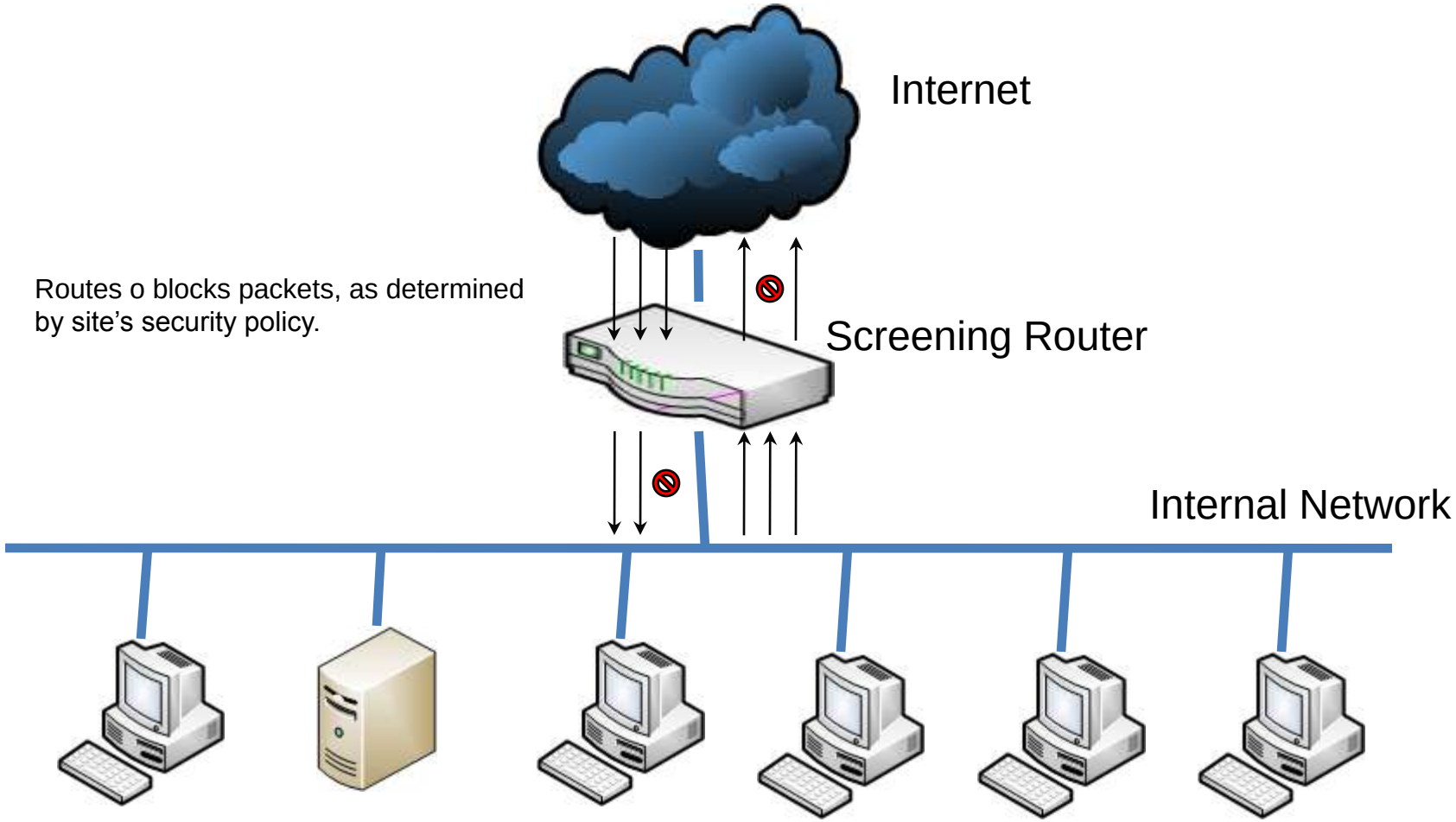


Elementos Tecnológicos

- Redes privadas virtuales
  - Se trata de canales seguros de comunicación entre cortafuegos extremos.
  - Establecen un túnel criptográfico que cifra los datos de salida los cuales son descifrados al llegar al otro extremo.
  - En las RPV se debe notar que:
    - Deben protegerse las infidelidades internas.
    - La seguridad de la RPV es la de la red mas insegura de las dos.
    - Los agresores pueden analizar el tráfico extremo a extremo.

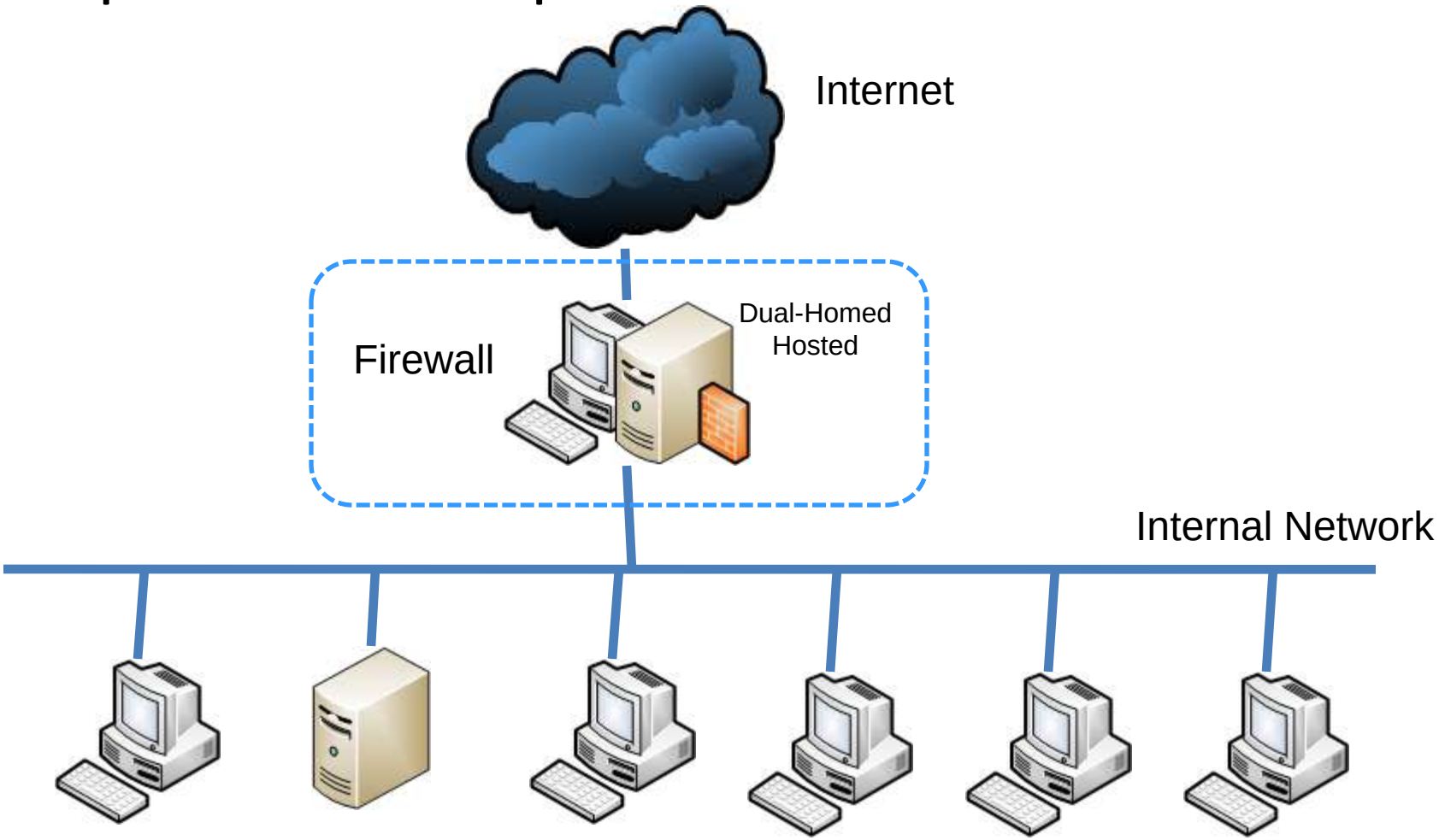
Arquitectura de cortafuegos

- Arquitecturas simples



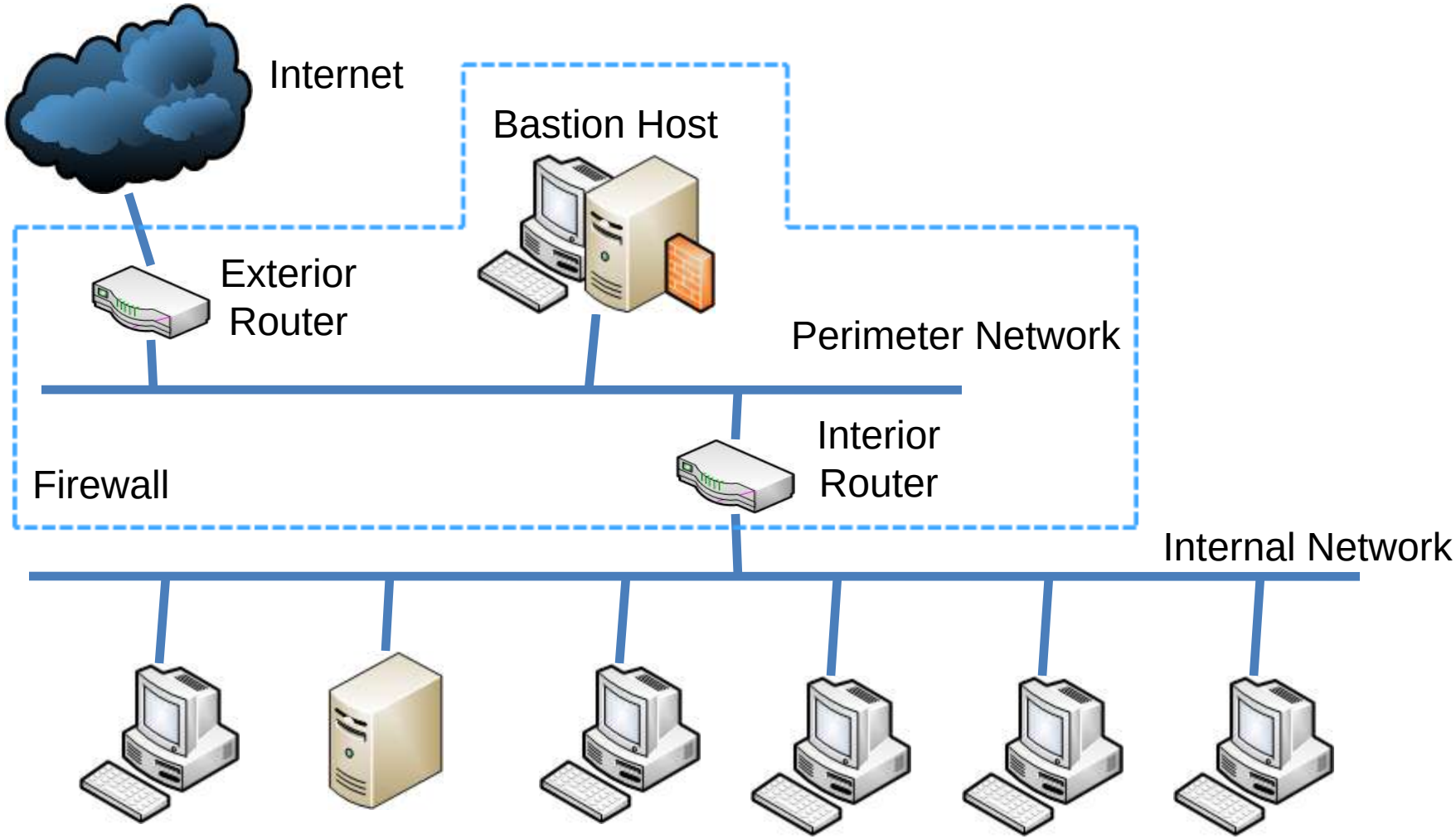
Arquitectura de cortafuegos

- Arquitecturas simples



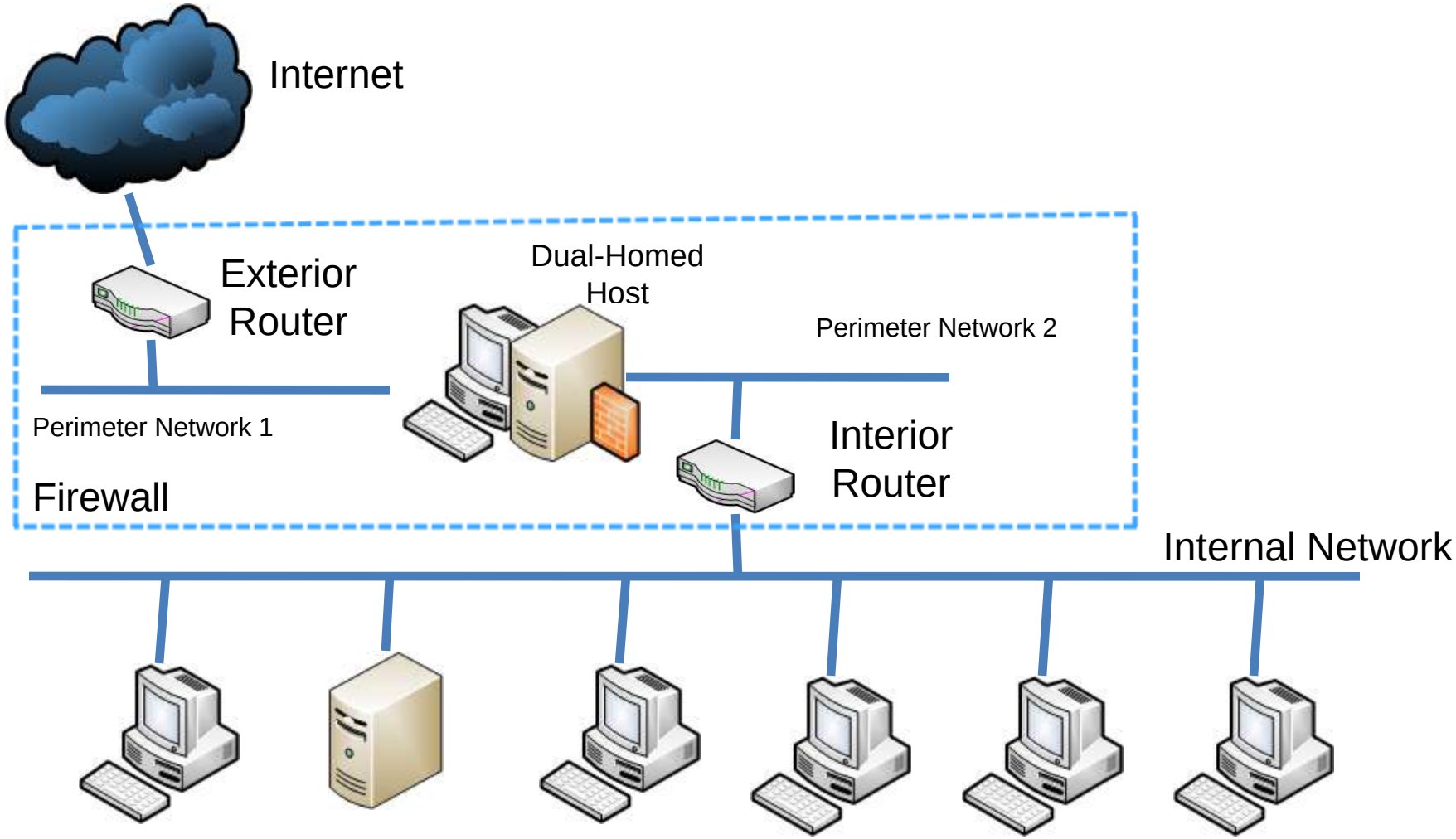
Arquitectura de cortafuegos

- Técnicas de defensa en profundidad



Arquitectura de cortafuegos

- Técnicas de defensa en profundidad



Planificación de una arquitectura

- La planificación no es trivial.
- No es una tarea imposible pero si delicada.
- Debe fundamentarse en:
  - Una política de seguridad definida por la corporación.
  - Determinar los responsables y beneficiarios de los servicios.
  - Ubicación del cortafuegos.
  - Control y mantenimiento del funcionamiento.

Planificación de una arquitectura

- Política permisiva.
  - Permite todo salvo orden
  - Exceso de tráfico
  - Problemas debidos a las interacciones de los servicios.
- Política prohibitiva.
  - Se prohíbe todo en principio y luego se van permitiendo poco a poco permisos y servicios.

Selección de un cortafuegos

- Fundamentar la decisión en:
  - Desarrollo interno del cortafuego.
  - Elegir un producto del mercado.
  - Analizar la carga de tráfico para determinar la capacidad del cortafuego.
  - Ubicar el cortafuego en un sistema operativo seguro. Los cortafuegos sin sistema operativo representan un gran avance en seguridad.
  - Interfaz gráfica de configuración.
  - Herramientas de análisis y registro.
  - Integración en un sistema SNMP.

IP Tables

- Sólo en Linux, hay paquetes similares para otros sistemas.
- Robusto y sencillo.
- Lista de reglas para controlar paquetes:
  - Aceptar
  - Denegar
  - Ignorar (denegar sin contestar)
- No permite acceso por usuarios, sólo por redes o estaciones.

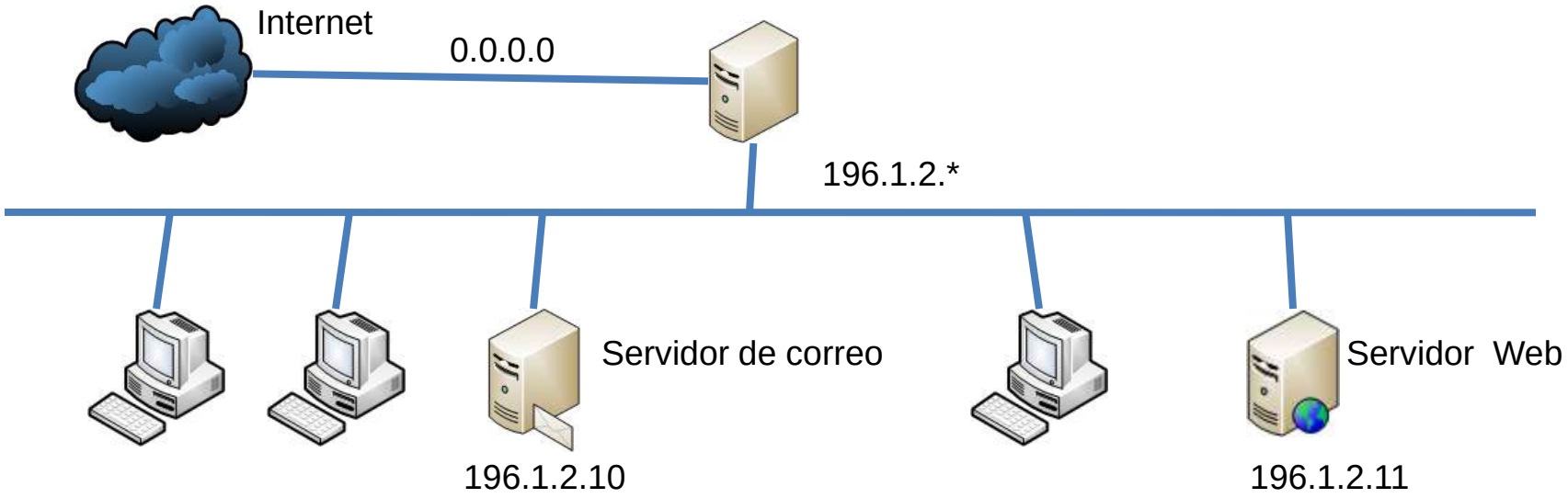
iptables

- Habilitar la opción de *forwarding* en el kernel.
- Es un comando del sistema. Es necesario ejecutarlo desde el arranque, pero es reconfigurable en cualquier momento.
- Establecer una política por defecto (acceso o rechazo) y especificar el resto de las normas de acceso por reglas adicionales.

iptables

- Parámetros:
  - Tipo de regla:
    - Entrada -I, Salida -O, Reenvío -F, Enmascaramiento -M, Registro del trafico –A.
  - Acción:
    - Aceptar, denegar o ignorar.
  - Protocolo a controlar:
    - ICMP, IP, UDP, TCP o todos.
  - Red de origen/destino del paquete y puerto o rango de puertos.

iptables




```
iptables -F -p deny       #denegar todos los accesos.
iptables -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 192.1.2.10 25
         #aceptar correo
iptables -F -a accept -b -P tcp -S 196.1.2.10 25 -D 0.0.0.0/0 1024:65535
         #permitir enviar correo.
iptables -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 196.1.2.11 80
         #aceptar conexiones a nuestra Web
iptables -F -a accept -b -P tcp -S 196.1.2.* 80 -D 0.0.0.0/0 1024:65535
         #permitir http a servidores externos
iptables -F -a accept -b -P udp -S 0.0.0.0/0 53 -D 196.1.2.0/24
                  #aceptar trafico DNS.
```