Seguridad: VPN, Cortafuegos, NAT, Proxies

Emilio Hernández

Redes Virtuales Privadas (VPN)

Conexión encriptada entre dos dispositivos que habilita la comunicación segura entre dos redes a través de un dominio inseguro

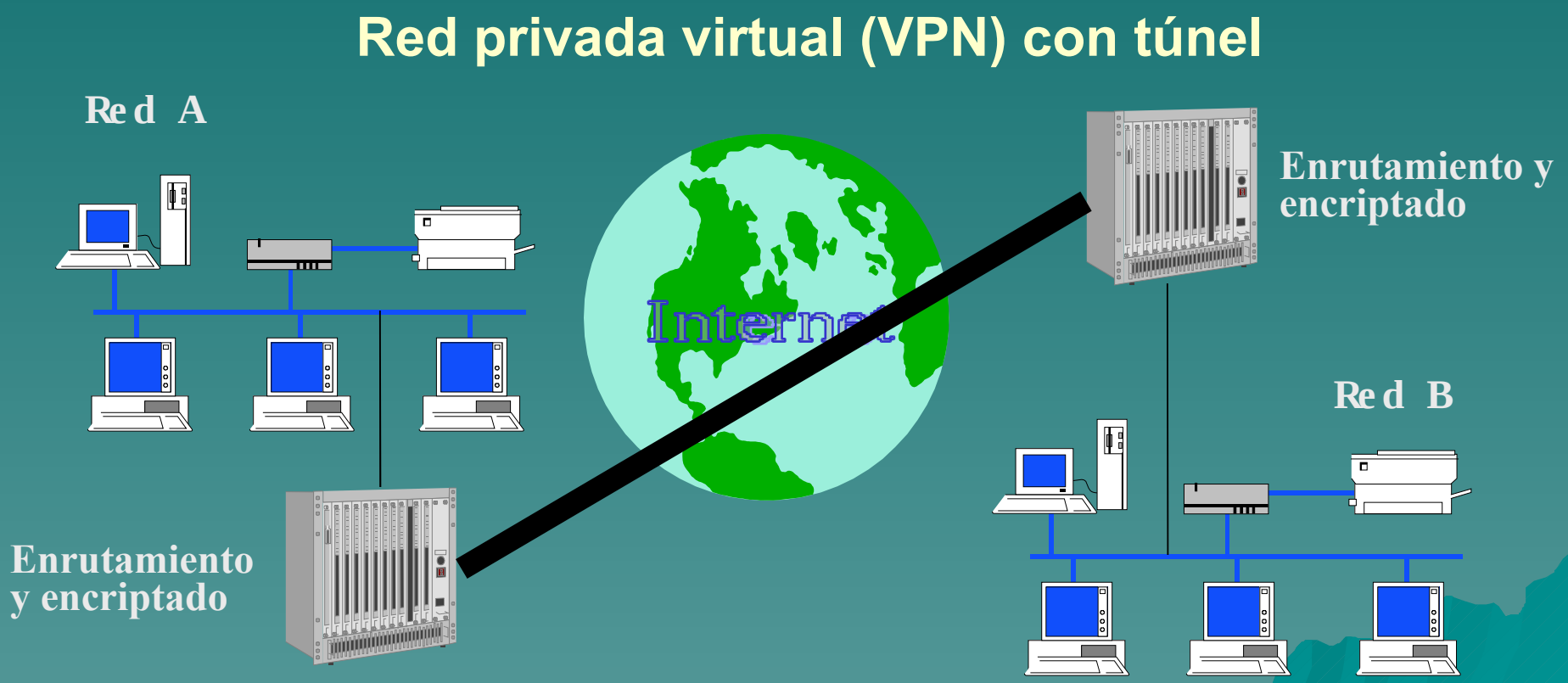
Qué conectamos?

- Clientes con servidores, servidores entre sí, enrutadores entre sí

Protocolos

- IPSec
- PPTP (Tunel PPP sobre IP, de Microsoft)

Ejemplo de VPN con Túnel



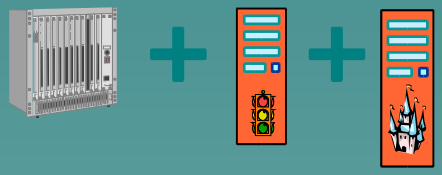
Filtrado: Definiciones básicas

Enrutador con filtro (EF): enrutador (*router*) que provee filtrado de paquetes

Máquina con capacidad de enrutamiento (MCE): máquina con varias conexiones a la red, puede tener software de filtrado de paquetes

Bastión: servidor expuesto al ataque (típicamente desde “afuera”)

Cortafuegos: solución integrada al problema de seguridad. Es una combinación de EF´s, MCE´s y bastiones.



Filtros de red

Seleccionan los paquetes que cruzan desde Internet hacia la red interna y viceversa

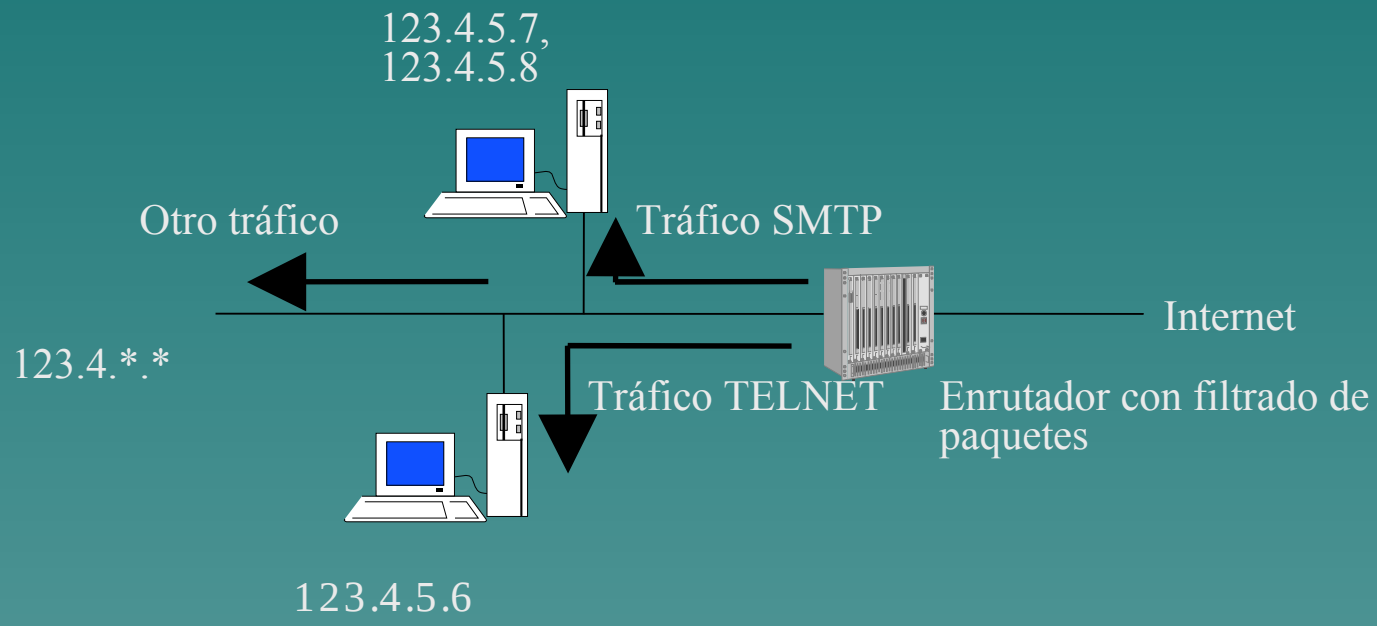
Funcionan al nivel de capa de red (IP) y, posiblemente, transporte (TCP/UDP)

Los paquetes que no pueden cruzar son descartados; pueden hacer ligeras modificaciones a los paquetes que las cruzan

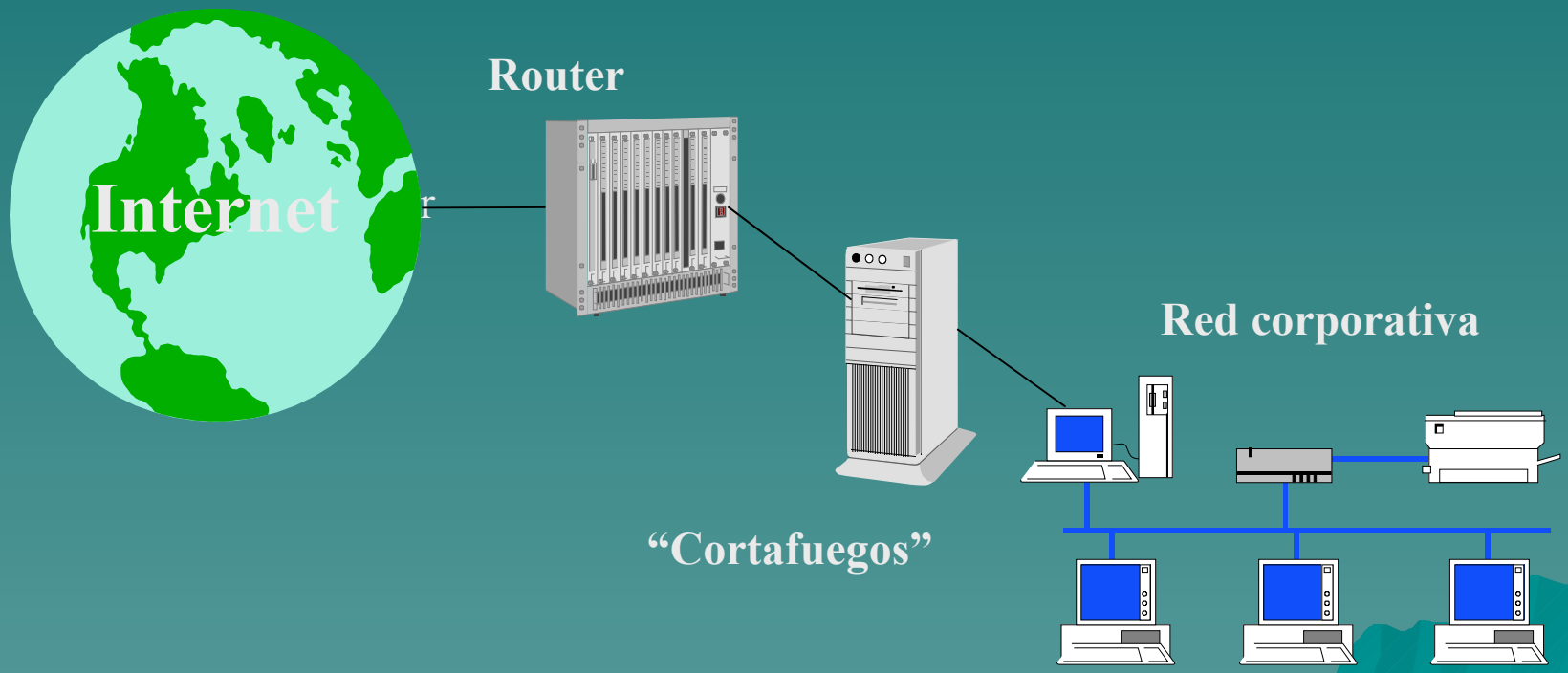
Usan: *IP source address, IP destination address, Protocol (TCP, UDP, or ICMP packet), TCP or UDP source port, TCP or UDP destination port, ICMP message type,* interfaz por donde llega, ...

Filtrado de paquetes

Ejemplo de filtrado de paquetes para TELNET y SMTP



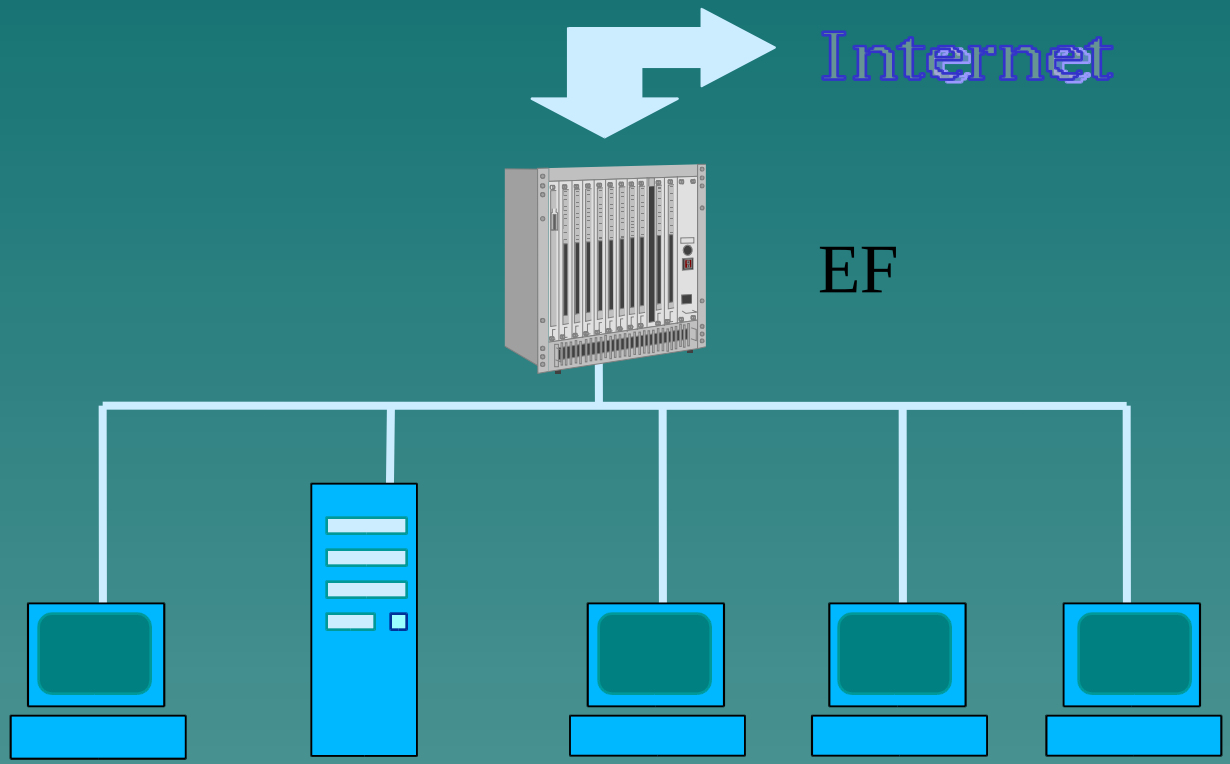
Cortafuegos. Escenario típico



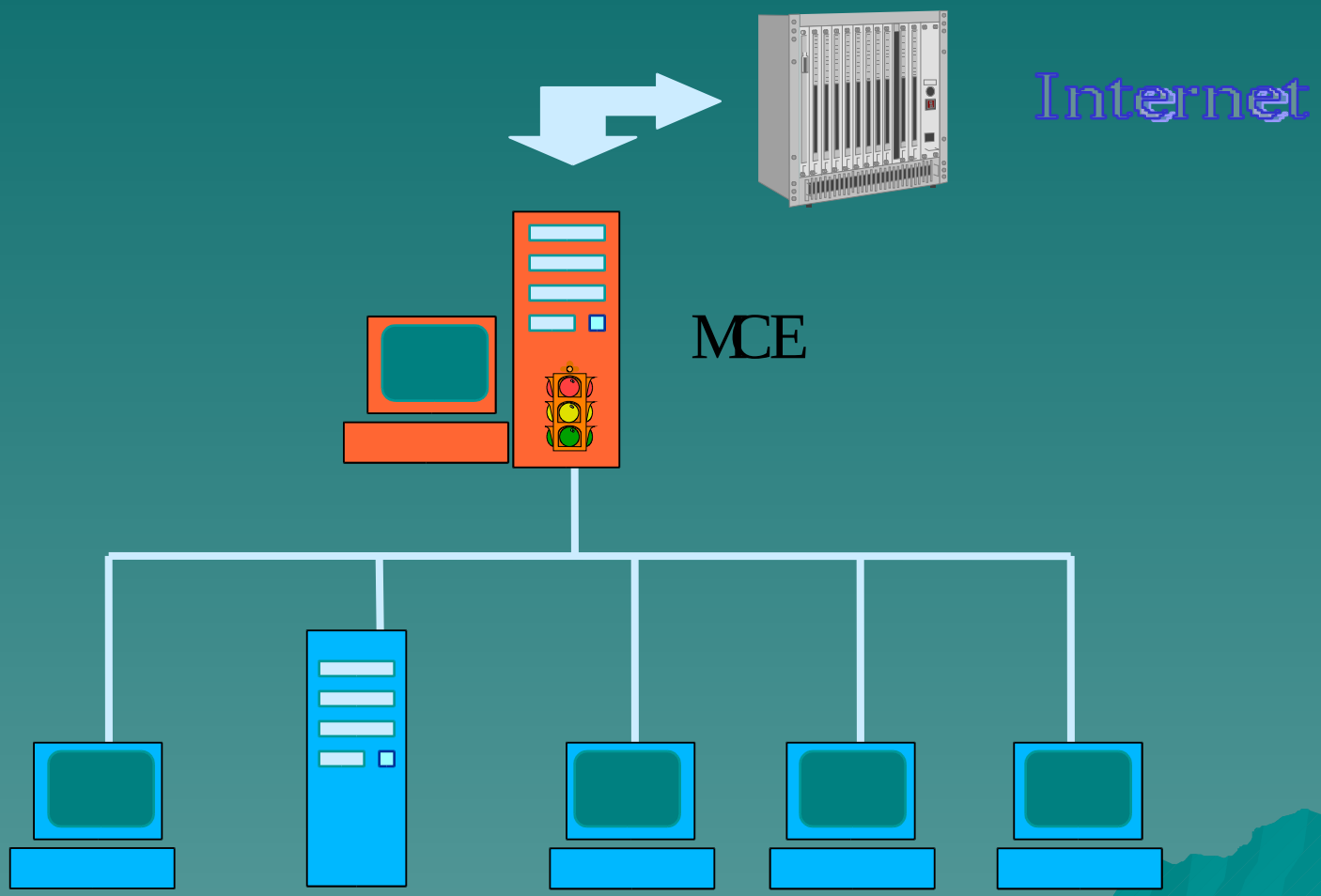
Objetivos del cortafuegos

- Rechazar conexiones a servicios comprometidos
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico) o entre ciertos nodos
- Ser el único punto de interconexión con el exterior
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- Mantener trazas (*logging*) del tráfico entre el exterior y el interior
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos...

Filtrado con EF



Filtrado con MCE



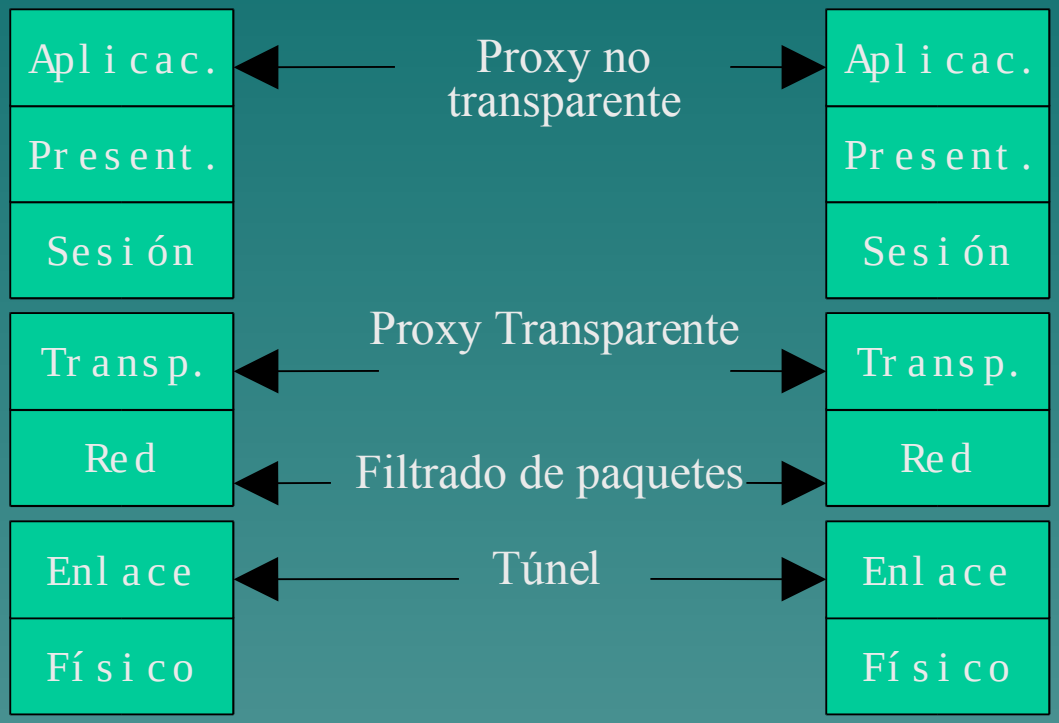
Sugerencias para el filtrado

- Usar *"reject"* o *"deny"* como política por defecto
- Estudiar los protocolos. Algunos, como FTP, requieren consideraciones especiales.
- Cuidado con las "optimizaciones" que provee el software de filtrado (validarlas o probarlas si es posible)
- Registrar información sobre paquetes aceptados y rechazados

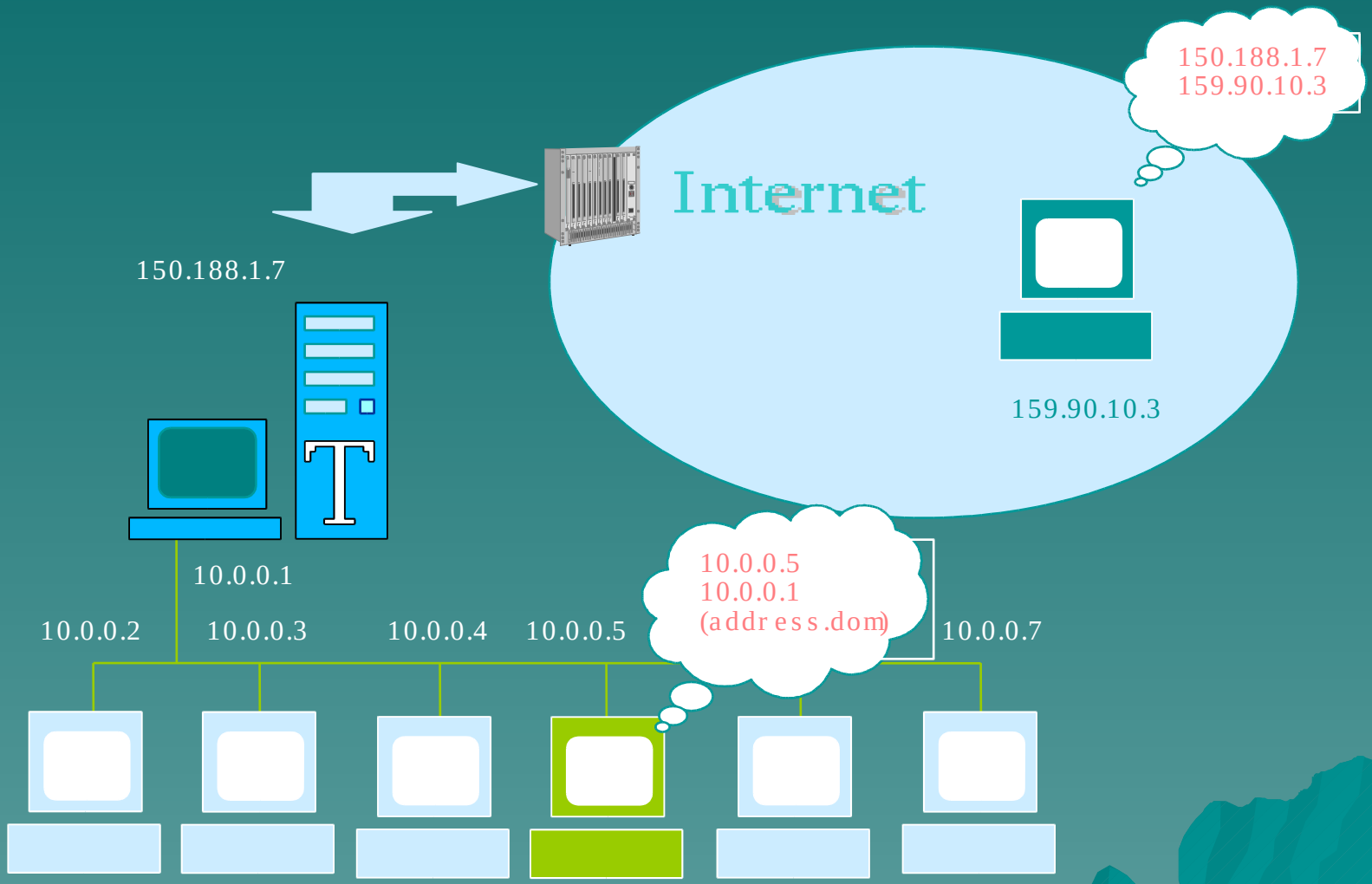
Escenarios de Filtraje

- Red interna con IP´s privados
  - Proxies
    - No transparentes
    - Transparentes
  - NAT
- Red interna con IP´s públicos
  - Enrutadores con filtro (EF´s)
  - MCE´s con filtrado de paquetes

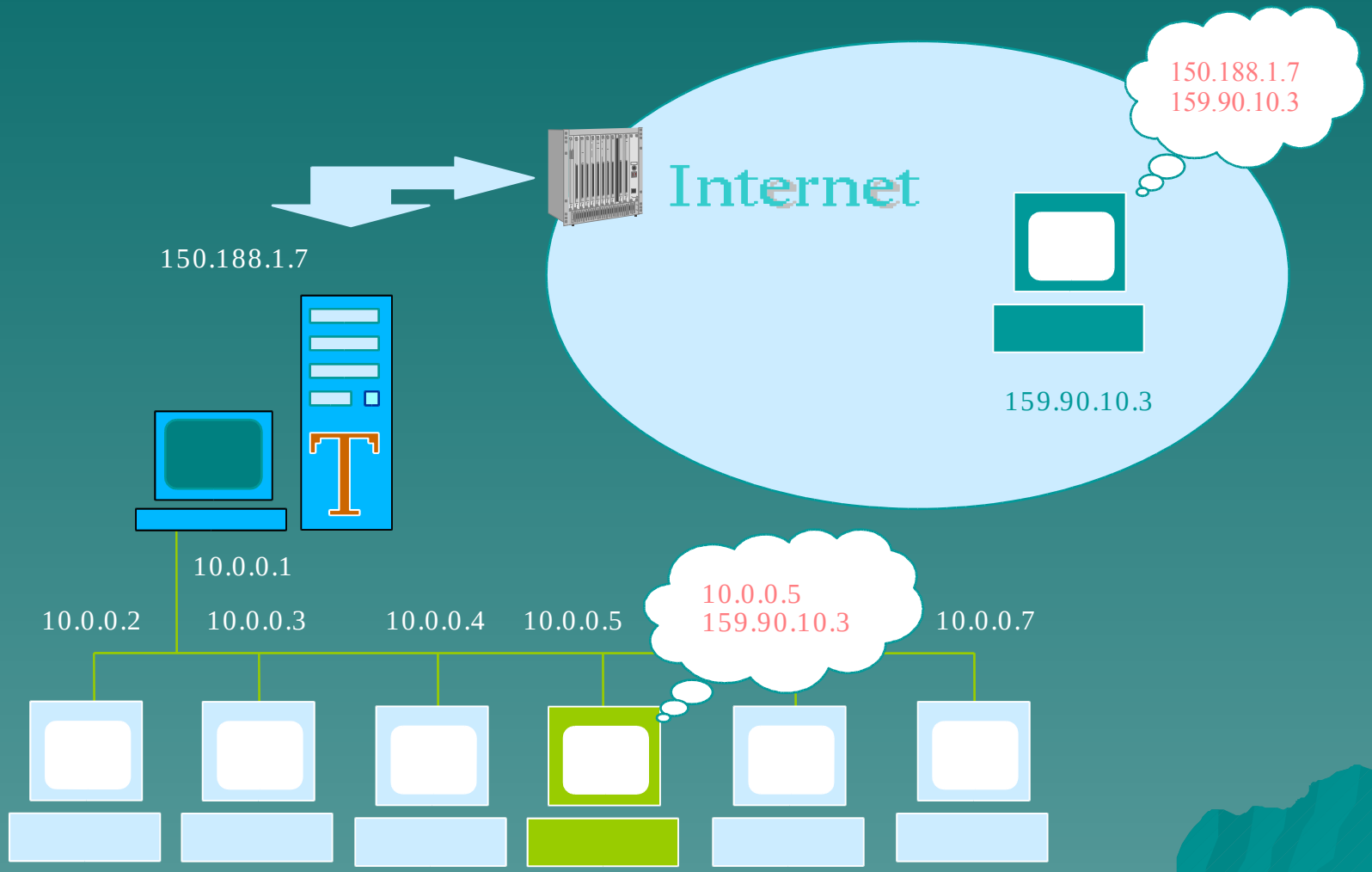
Escenarios de Filtraje



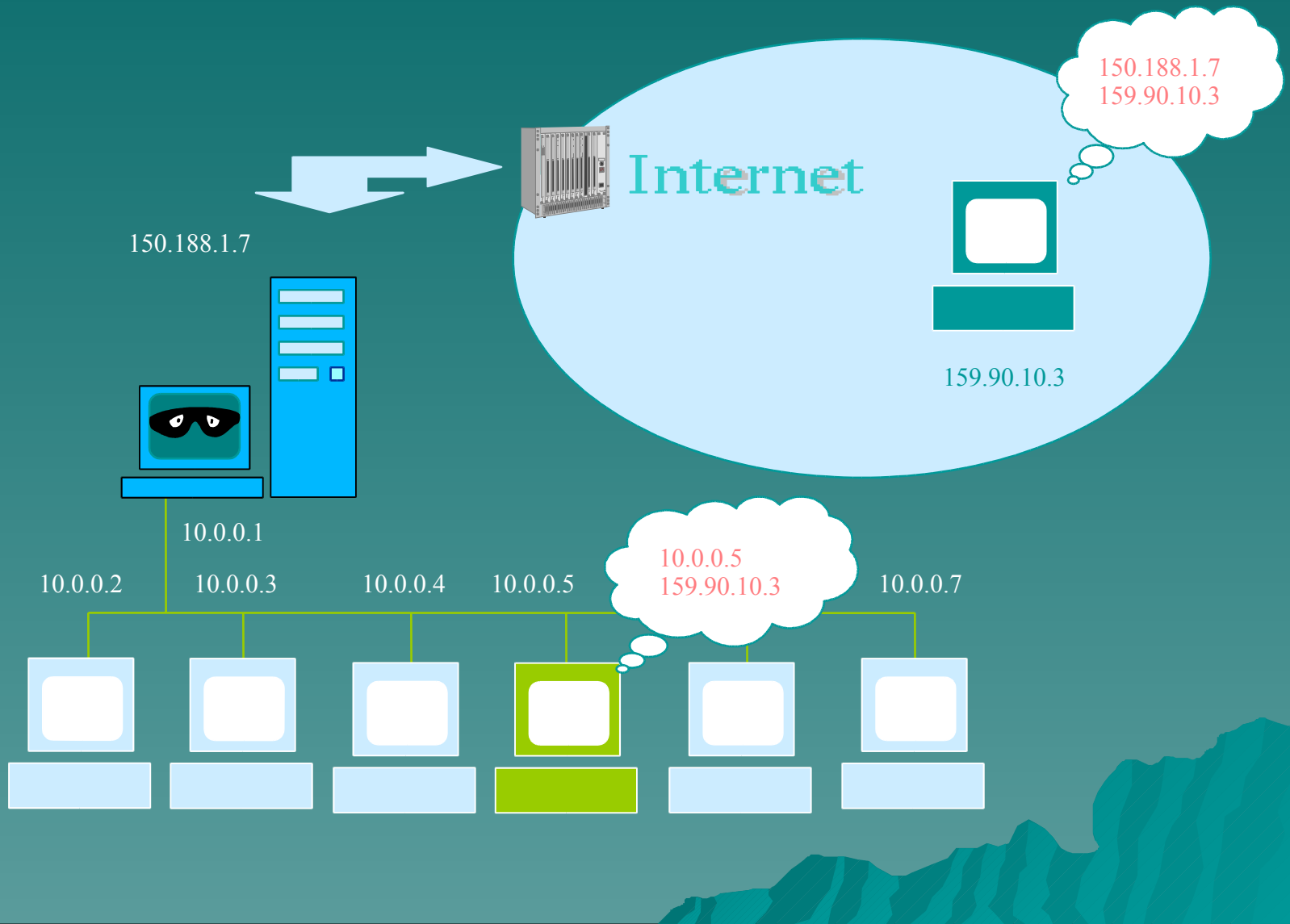
Proxies no transparentes



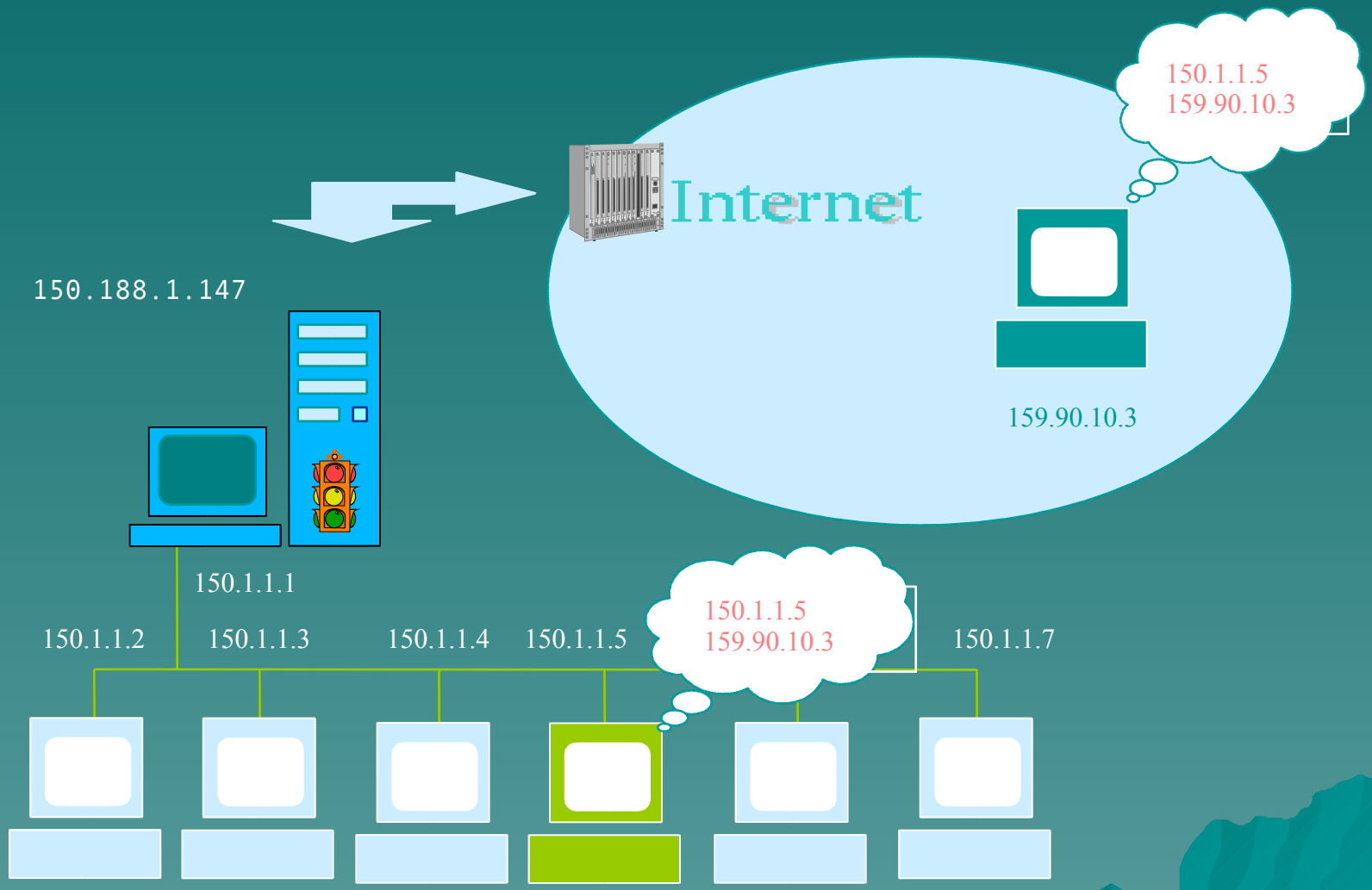
Proxies transparentes



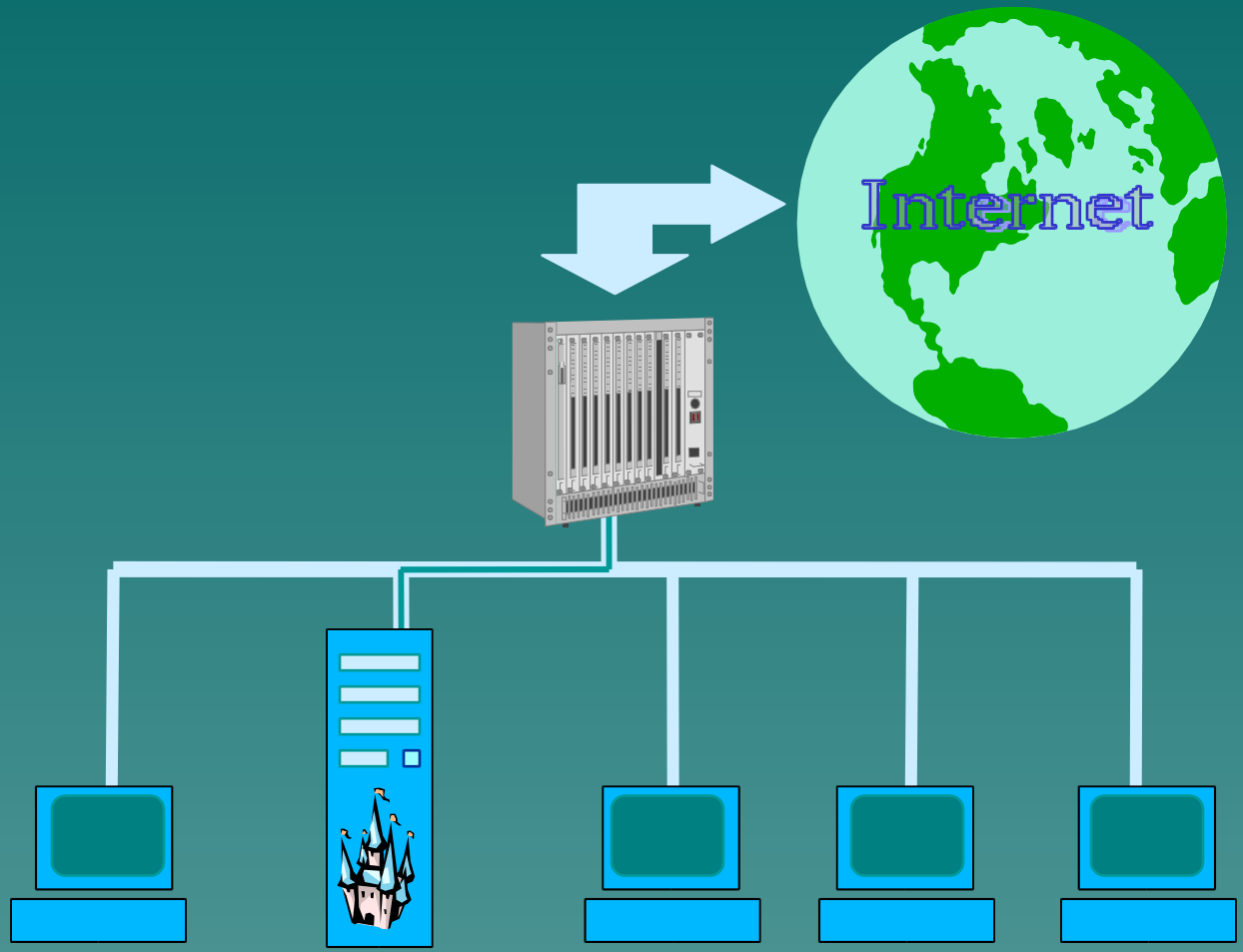
NAT


150.188.1.7
159.90.10.3
Internet
150.188.1.7
159.90.10.3
10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
10.0.0.5
10.0.0.5
159.90.10.3
10.0.0.7

Cortafuegos

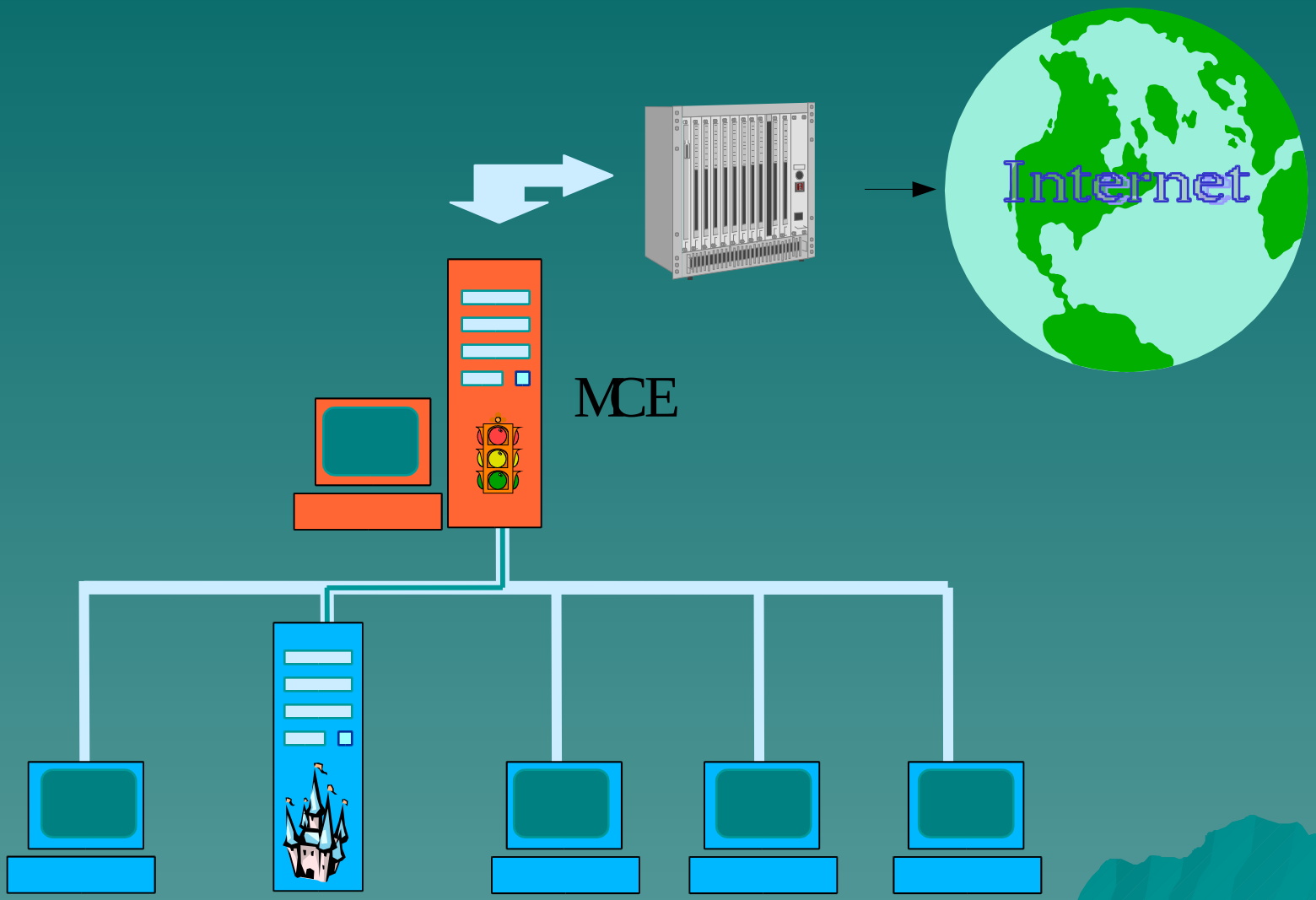


Uso de un bastión



(Esquema débil)

Uso de un bastión (II)

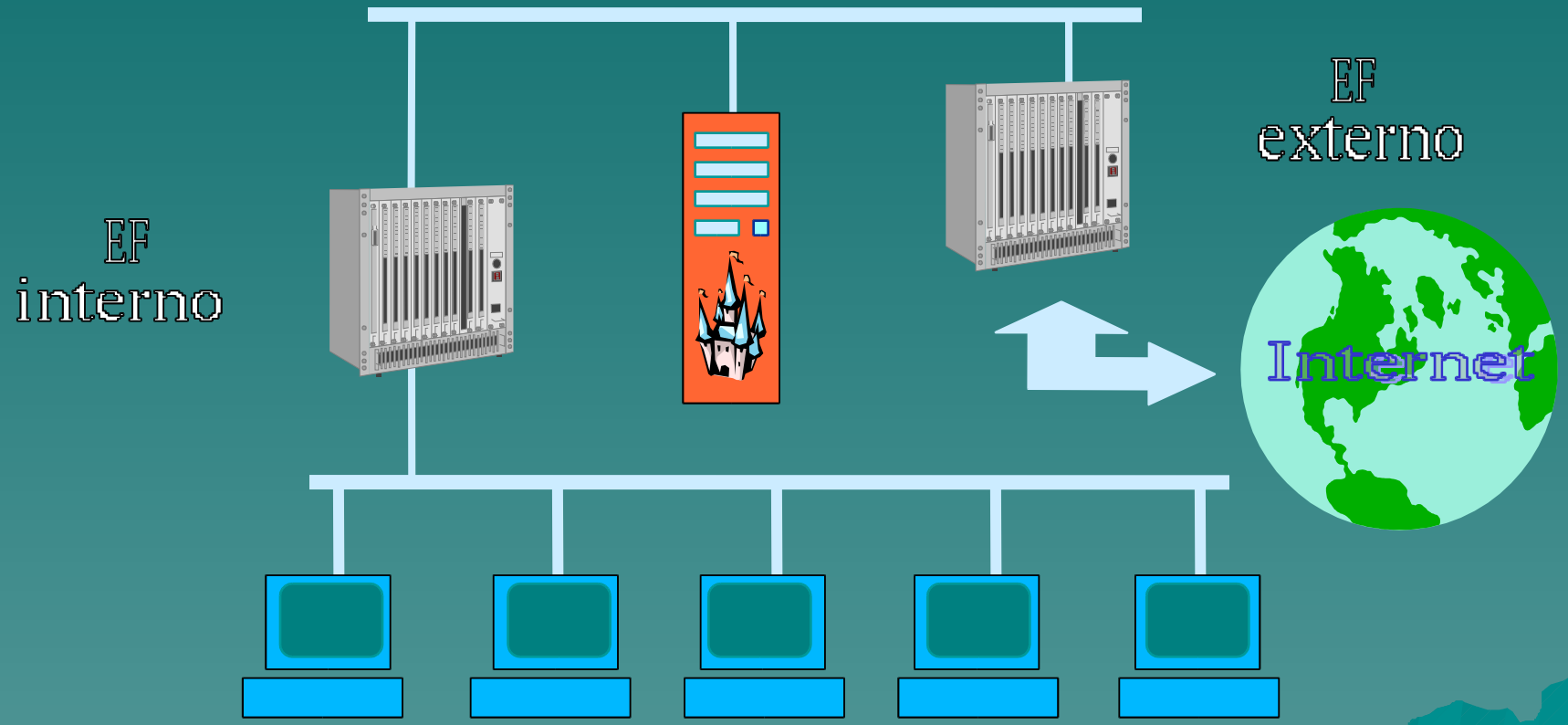


(Esquema débil)

Sugerencias para uso de bastiones

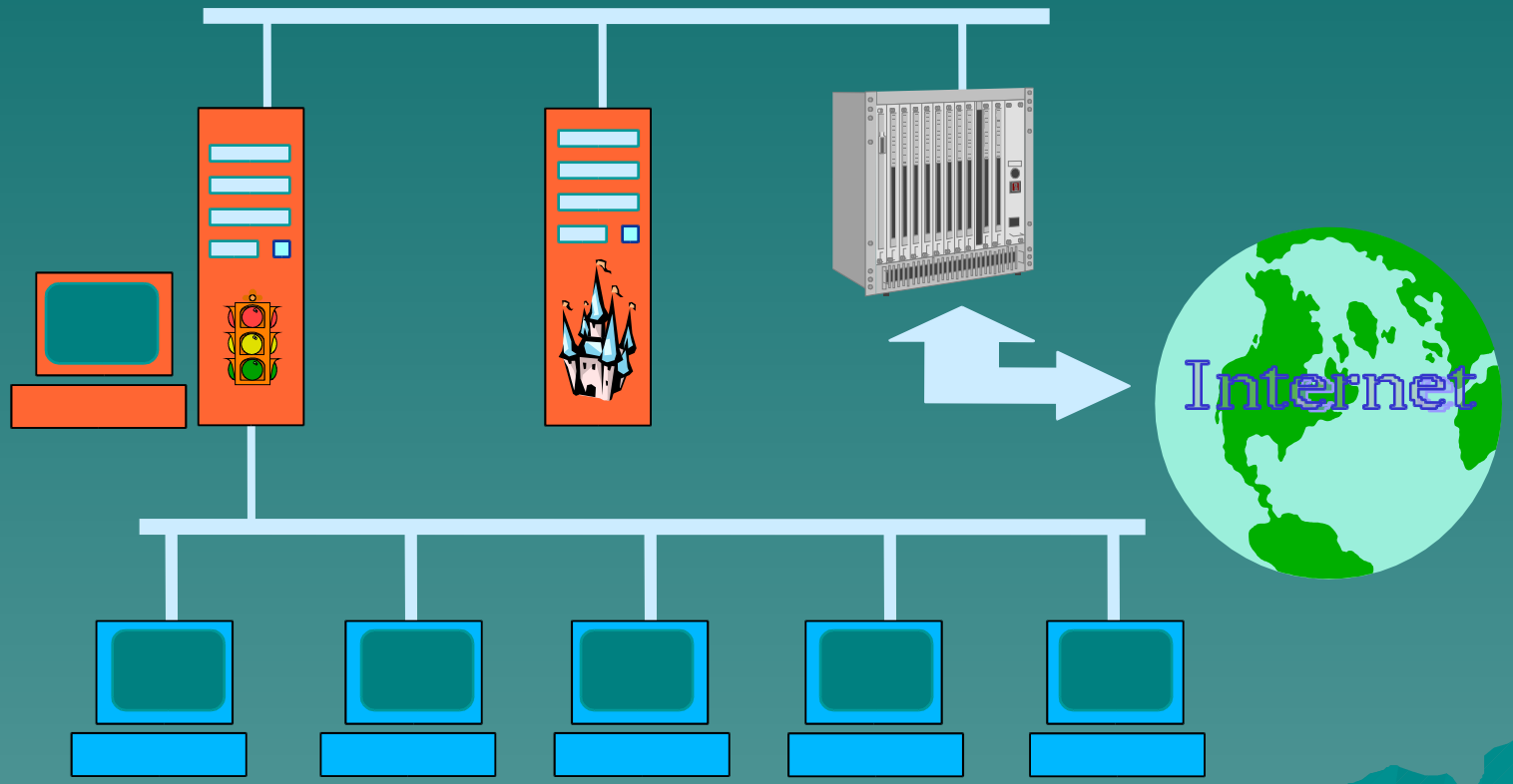
- Puede haber más de un bastión, si se desea repartir los servicios
- No es buena idea que el bastión sea la misma MCE que realiza el filtrado, a menos que haya un filtrado interno adicional
- Eliminar los servicios innecesarios dentro del bastión
- Usar *wrappers* para los servicios, como barricada de seguridad adicional

Red protectora



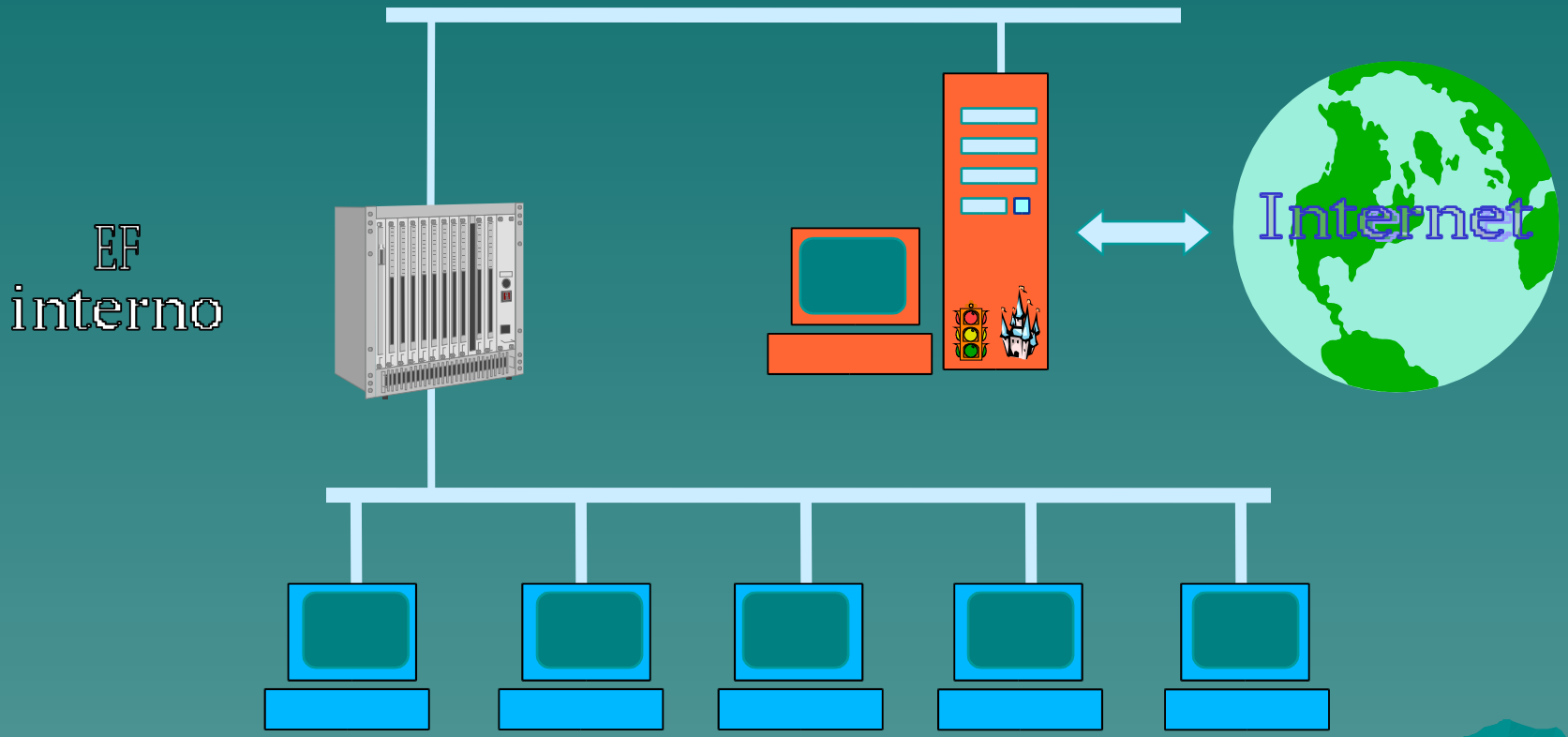
(Esquema fuerte)

Red protectora (II)



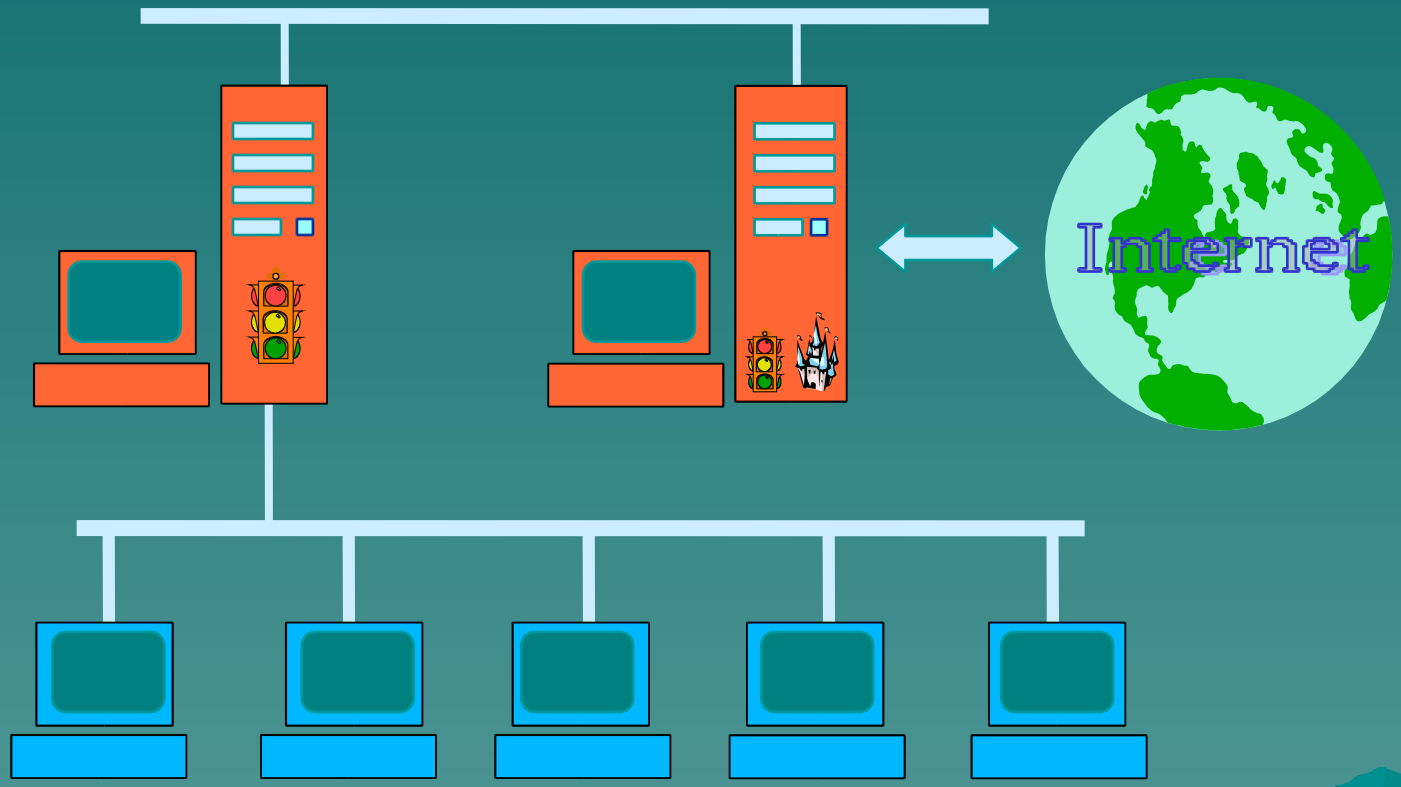
(Esquema fuerte)

Red protectora (III)



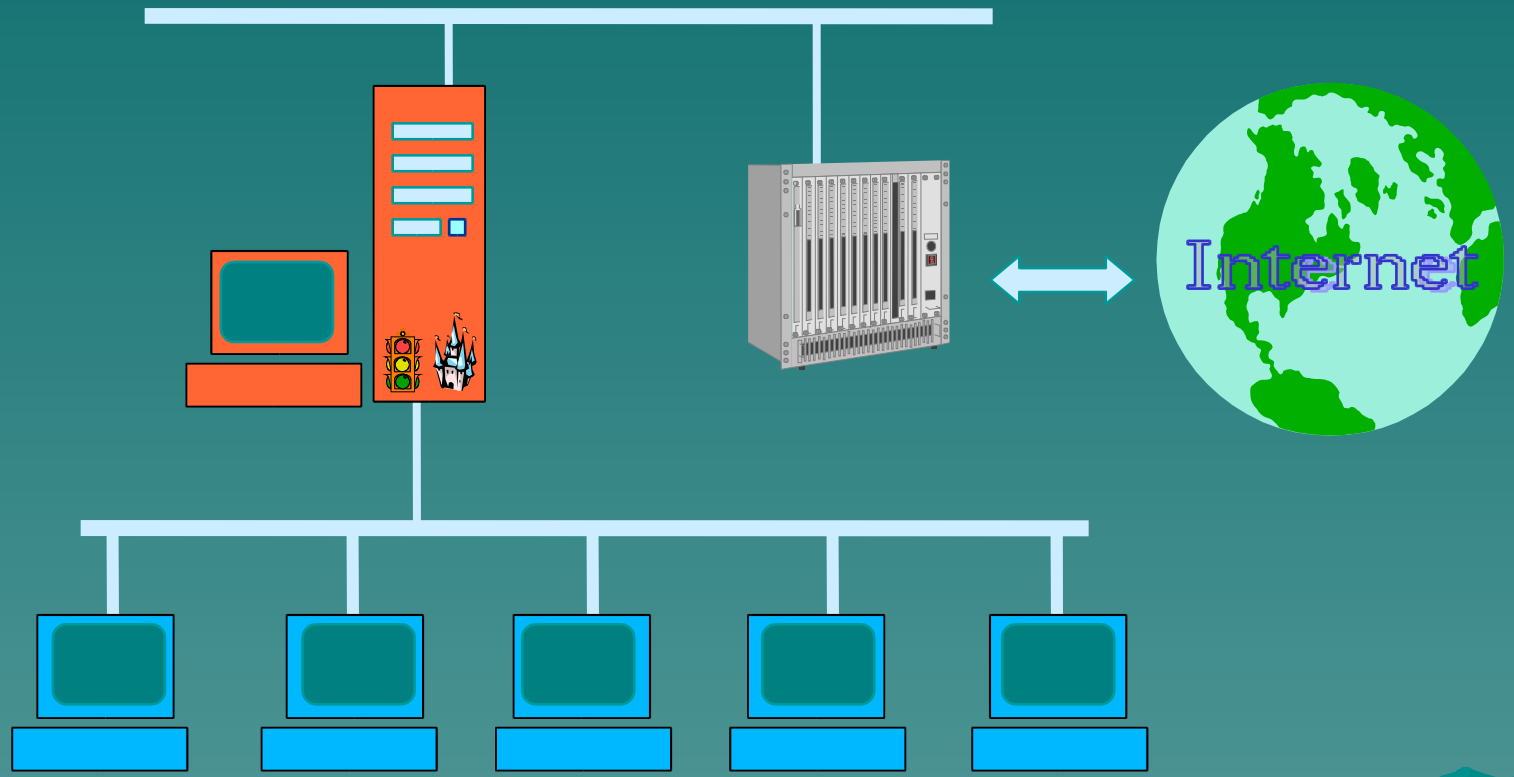
(Esquema fuerte)

Red protectora (IV)



(Esquema fuerte)

Red protectora (débil)



(Esquema débil)