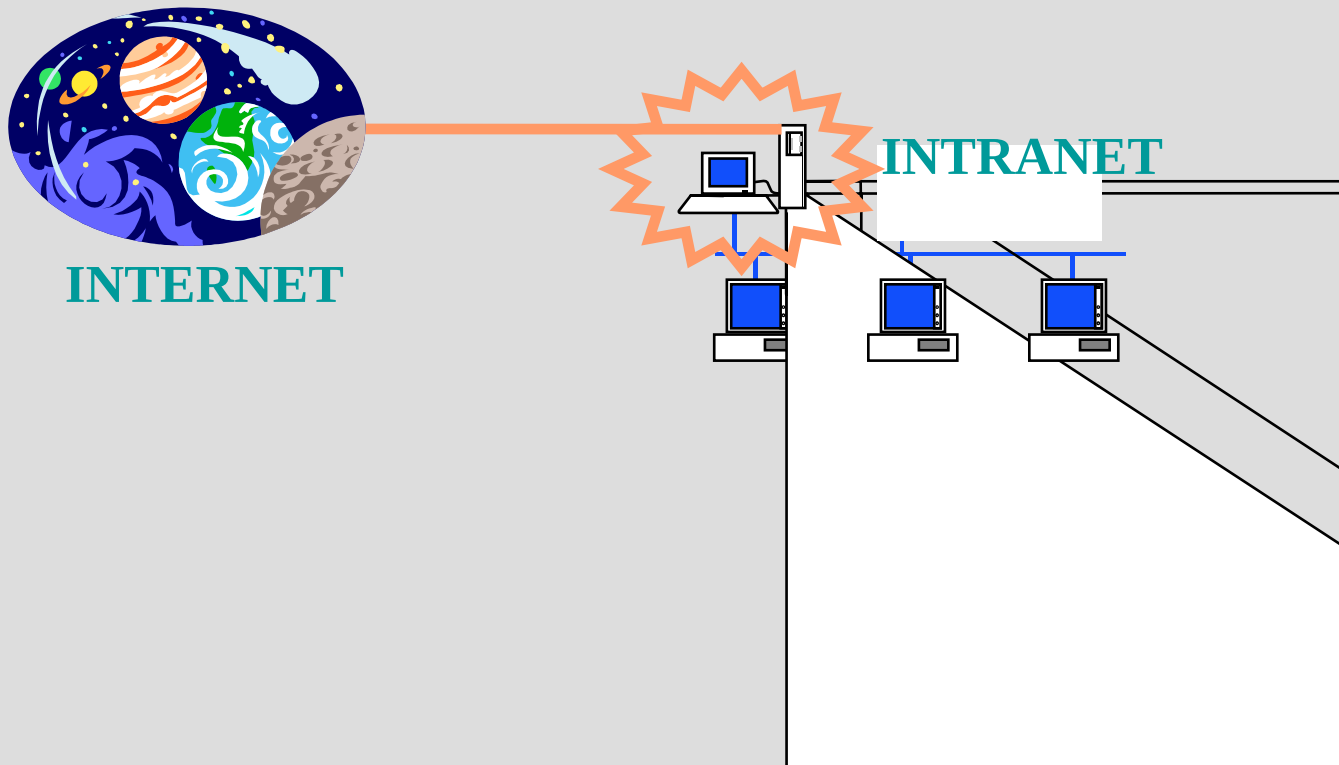
Curso de doctorado
Seguridad en Redes de Ordenadores

Tema 3b: Tecnologías de protección de redes internas

Introducción

- Cortafuegos

Firewall o cortafuego se denomina al elemento de enlace entre dos tramos de red.



Introducción

- Carácterísticas
  - Aparecen entre políticas diferentes de seguridad de red.
  - Define zonas confiables por las que los datos pueden distribuirse sin peligro de su seguridad

    Los usuarios pueden viajar por ellas sin la necesidad de identificarse a cada momento.
  - Centralizan la política de control de acceso relativa 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

- Intermediarios a nivel de aplicación
  - Los sistemas clientes-servidor se basan en el establecimiento de canales extremo a extremo.
  - El cliente se comunica con el servidor del propio cortafuegos. Este le identifica, registra sus peticiones y si lo considera oportuno lo encamina hasta el verdadero servidor.
  - Los cortafuegos a nivel de aplicación se basan en la instalación de intermediarios (proxies).

Elementos tecnológicos

- Direciones 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)

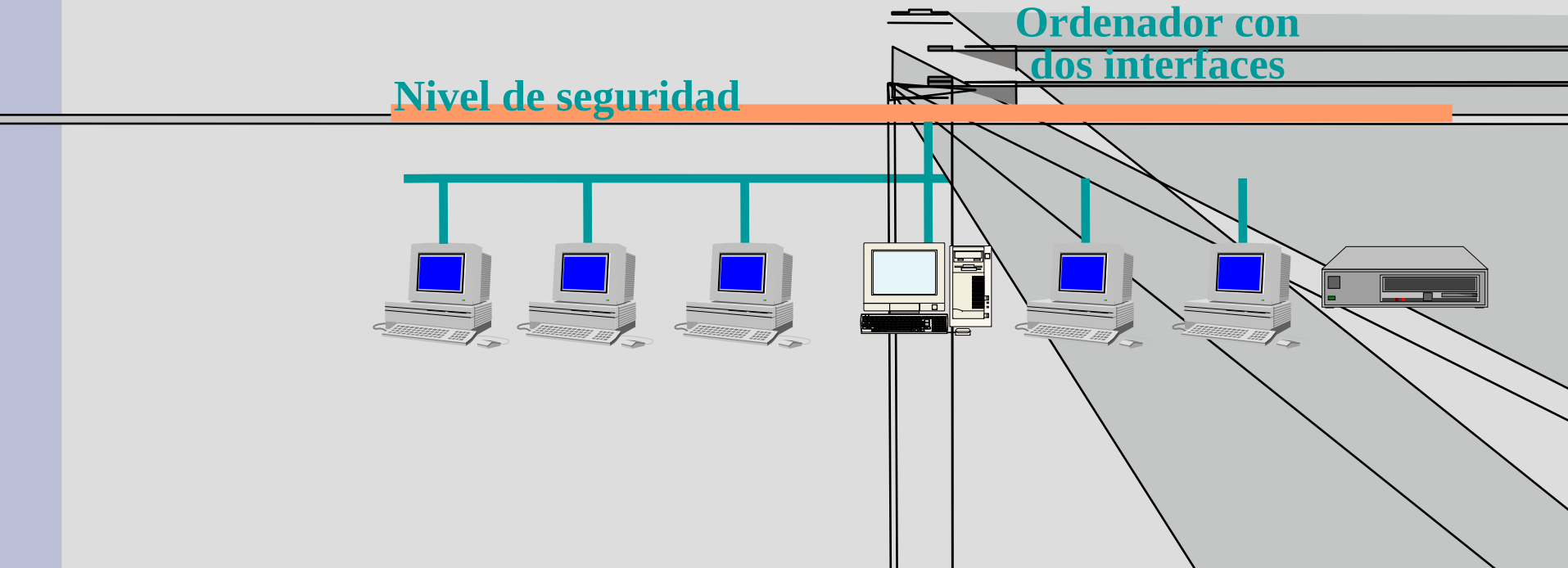
Elementos tecnológicos

- Redes privadas virtuales
  - Se trata de canales seguros de comunicación entre cortafuegos extremos.
  - Establecen un tunel 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 más insegura de las dos
    - Los agresores puede analizar el tráfico

Arquitecturas

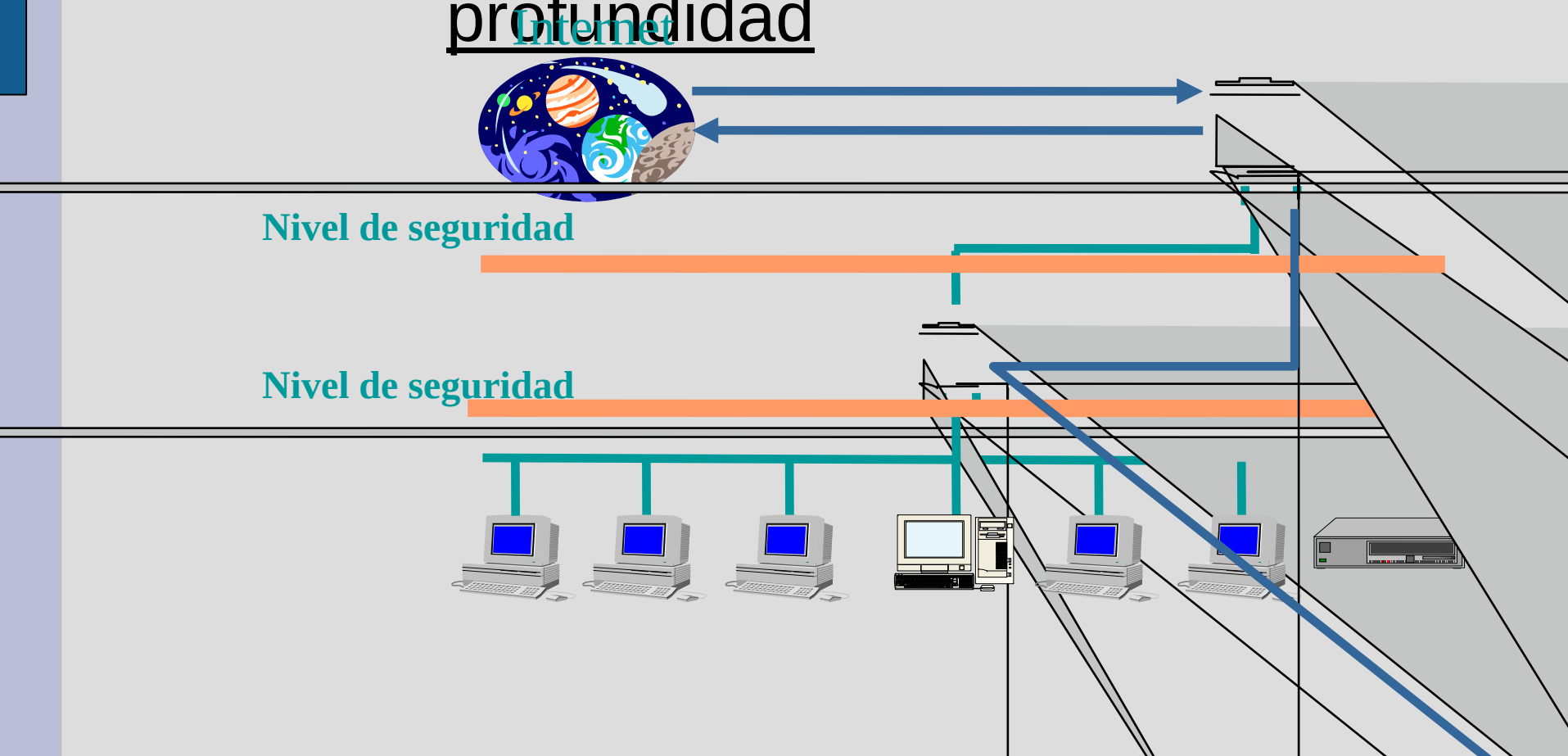
Arquitectura simple

Internet



Arquitecturas

Tecnicas de defensa en profundidad



Planificación

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

Planificación

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

Selección de cortafuego

- 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