Esquema Nacional de Seguridad

seguridad en las interconexiones

CCN-STIC 811 + *ITS en desarrollo*

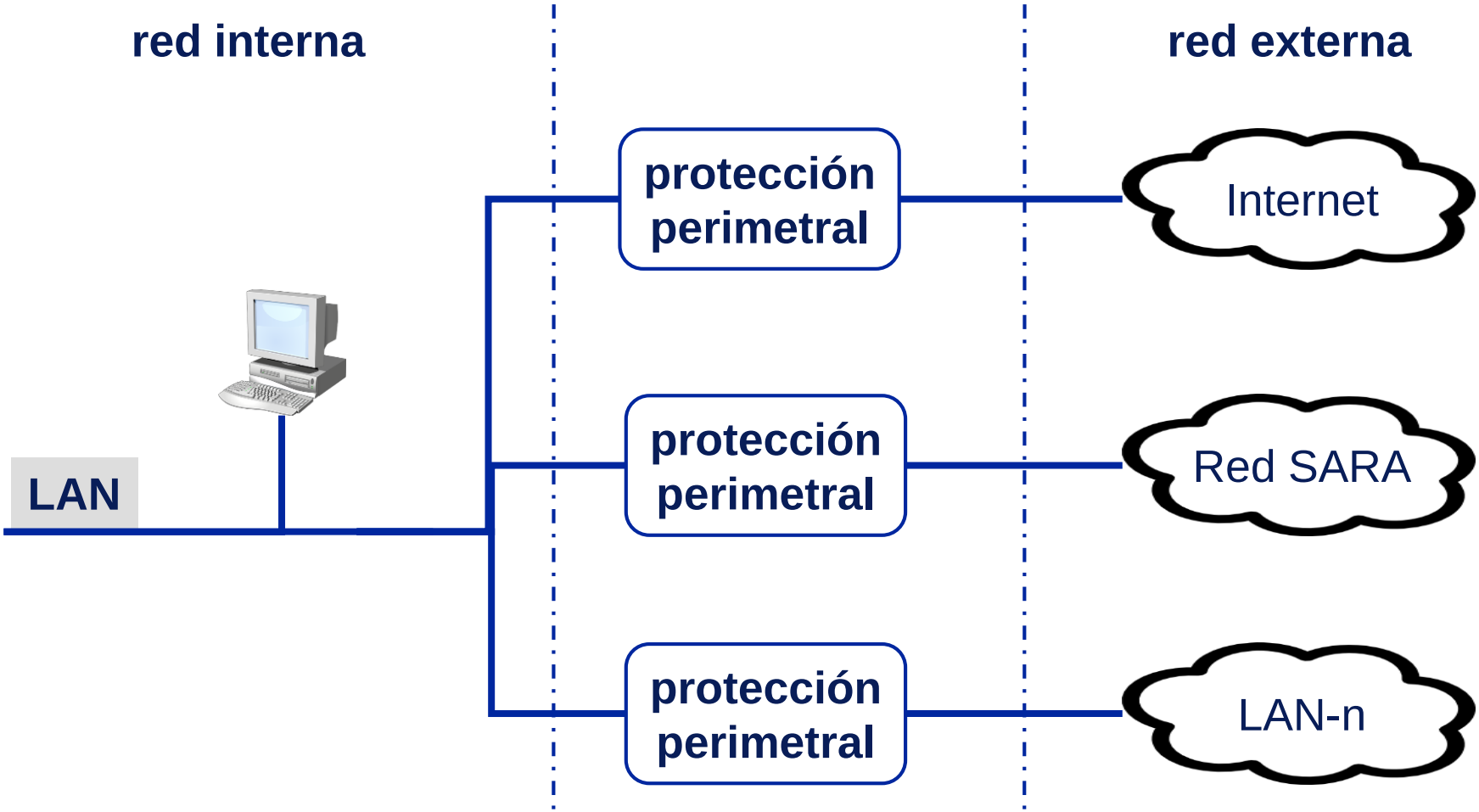
josé a. mañas

14.1.2017

definiciones

- Un sistema de información es un conjunto de equipos físicos, aplicaciones lógicas, soportes de información, comunicaciones, instalaciones y personal que se emplean para tratar información y prestar servicios.
- Se dice que tenemos una interconexión cuando un sistema de información se conecta a otro y se establece un flujo entrante o saliente de datos entre ellos.
- De las interconexiones nos interesa la frontera
  - BPS – SPP – Servicio de protección del perímetro
  - BPC – DPP – Dispositivo de protección del perímetro

interconexiones



principios

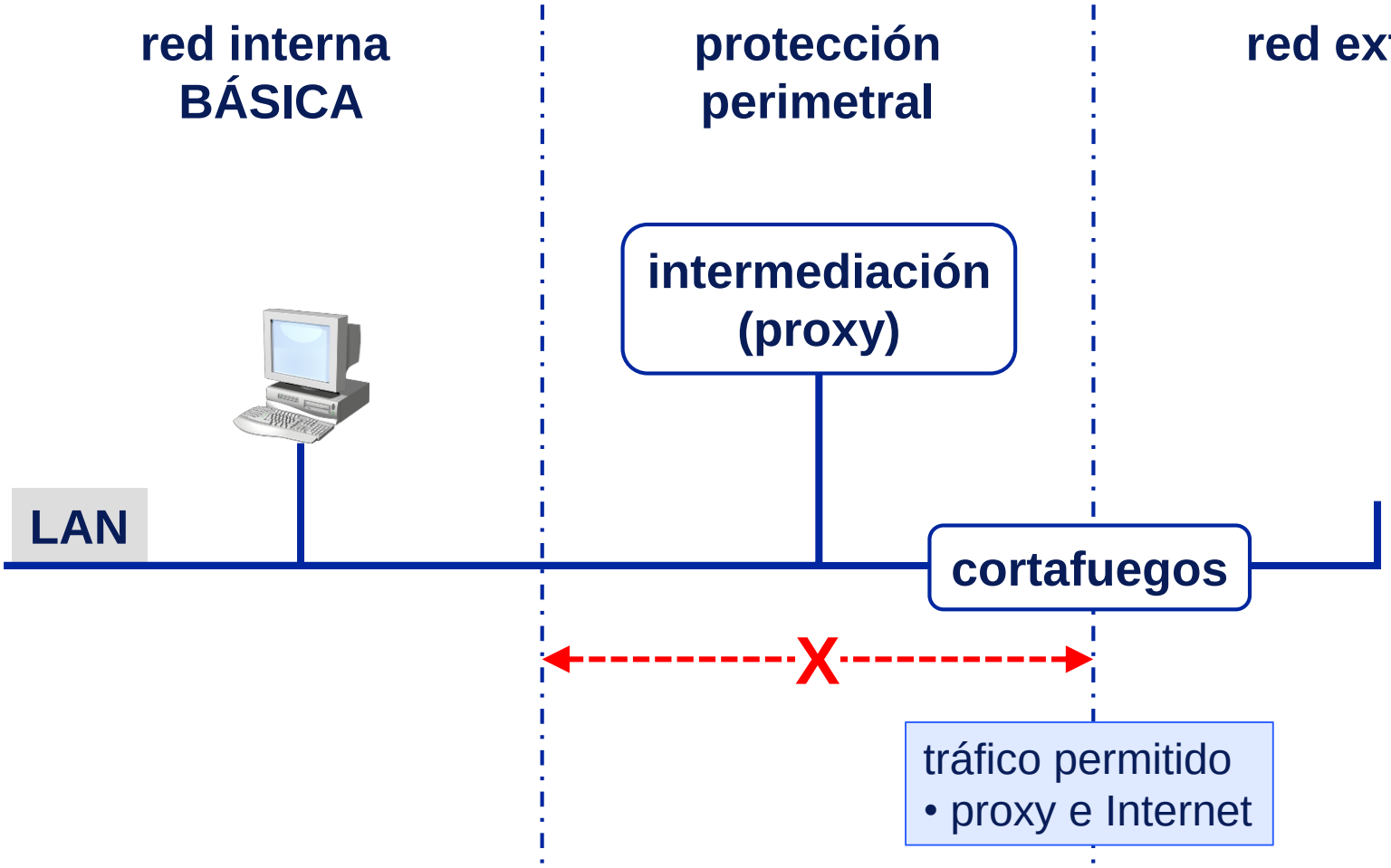
- **Mínima funcionalidad**
  - En el perímetro, solamente se instalan, configuran y usan los protocolos, servicios de red y flujos de información necesarios para la misión.
- **Mínimo privilegio**
  - Los usuarios y procesos autorizados a atravesar el perímetro solo disfrutan de los derechos mínimos imprescindibles para ello.
- **Nodo auto protegido**
  - Cualquier otro sistema de información se considera no fiable, realizándose un control local de los datos intercambiados.
    Nuestro sistema debe protegerse como si los demás estuvieran comprometido.
    Nuestra seguridad no puede depender de que los demás actúen correctamente.

ISA

- Acuerdo de Seguridad de la Interconexión
  - elaborado por los Responsables de los Sistemas
  - aprobado por los Responsables de la Seguridad

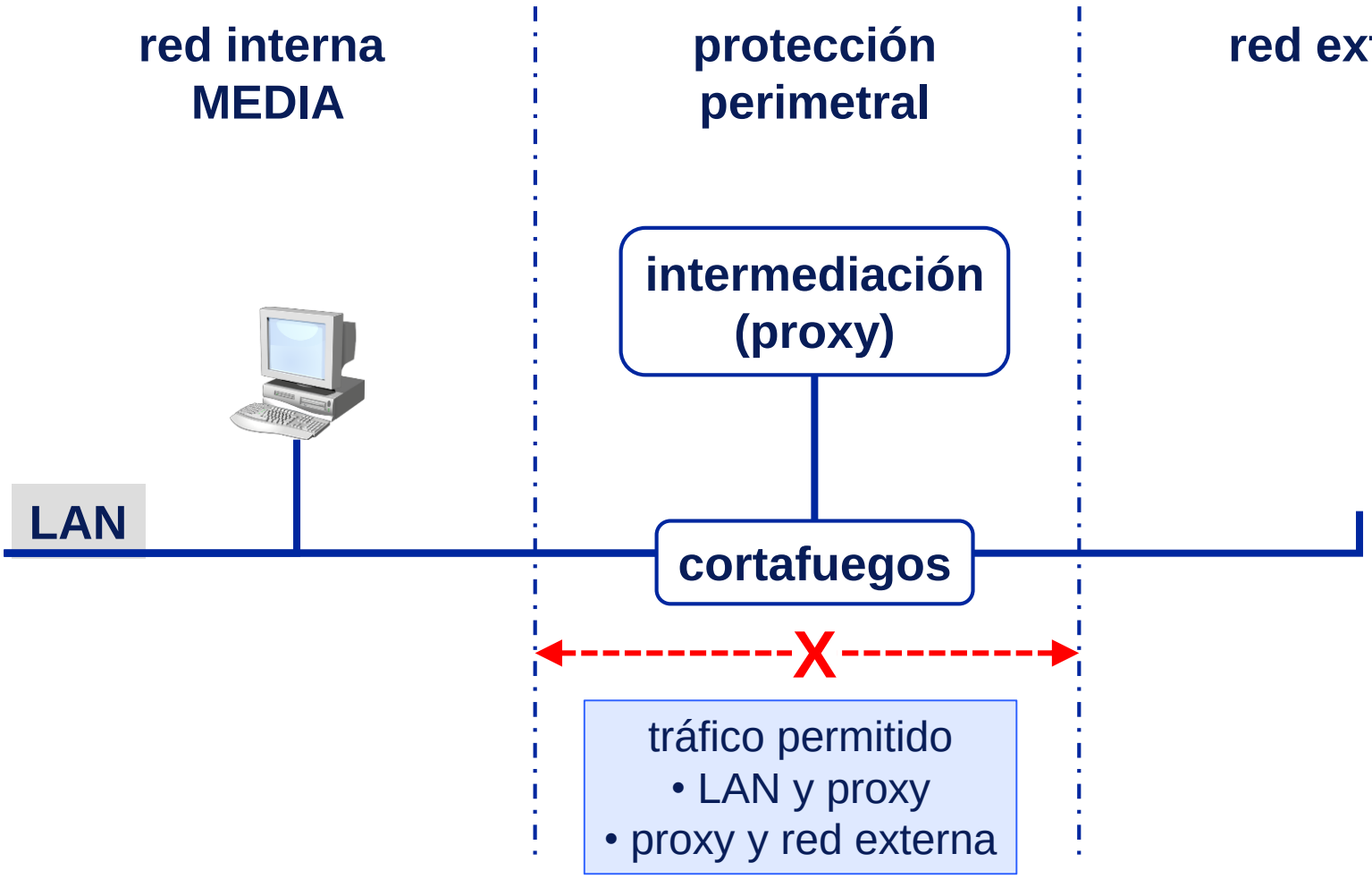
  - topología | arquitectura
  - datos y servicios: protocolos & formatos
  - flujos de información que se permiten
  - registro de actividad
  - procedimiento y responsabilidades para autorizar cambios

categoría BÁSICA



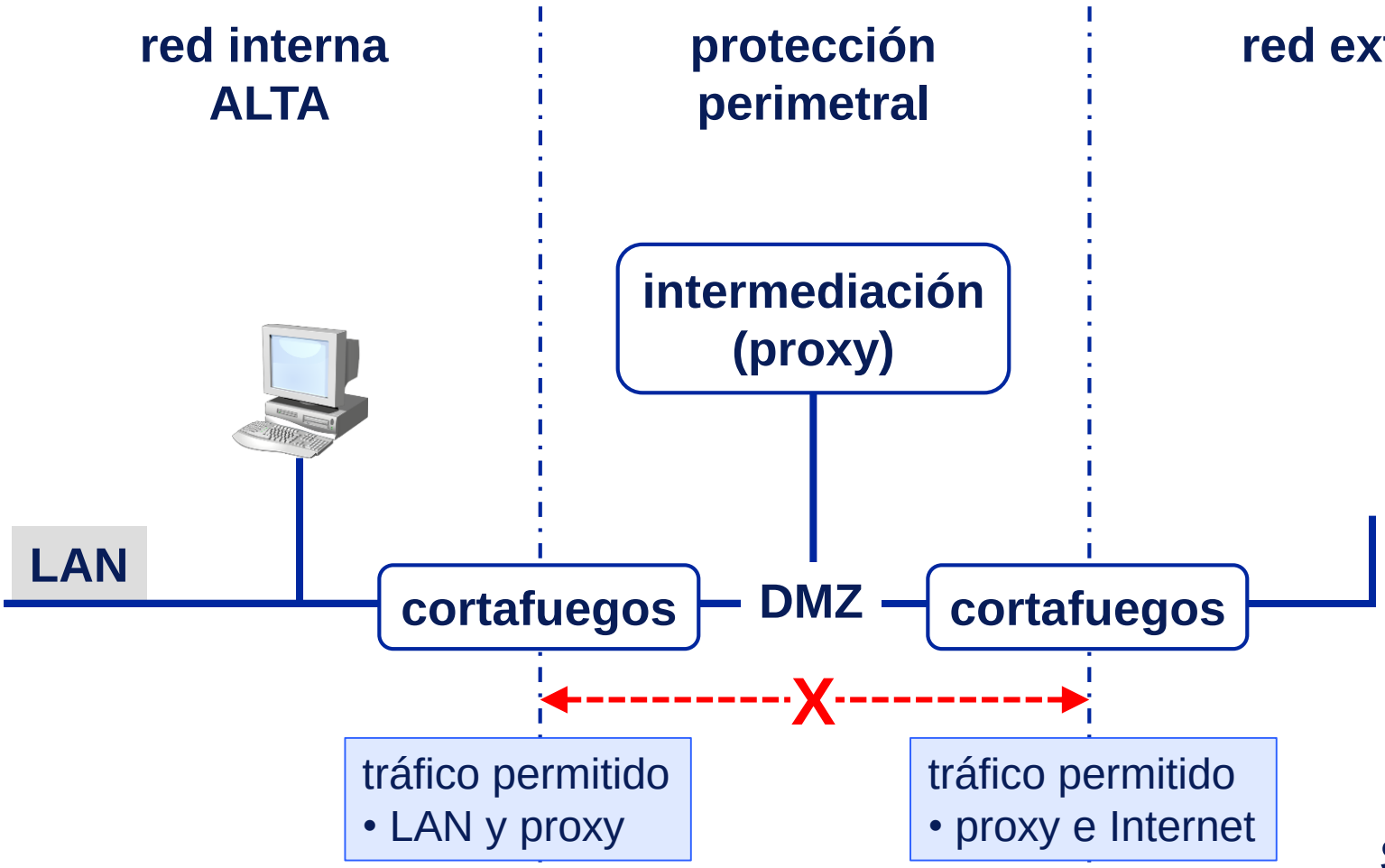
SPP-1

categoría MEDIA



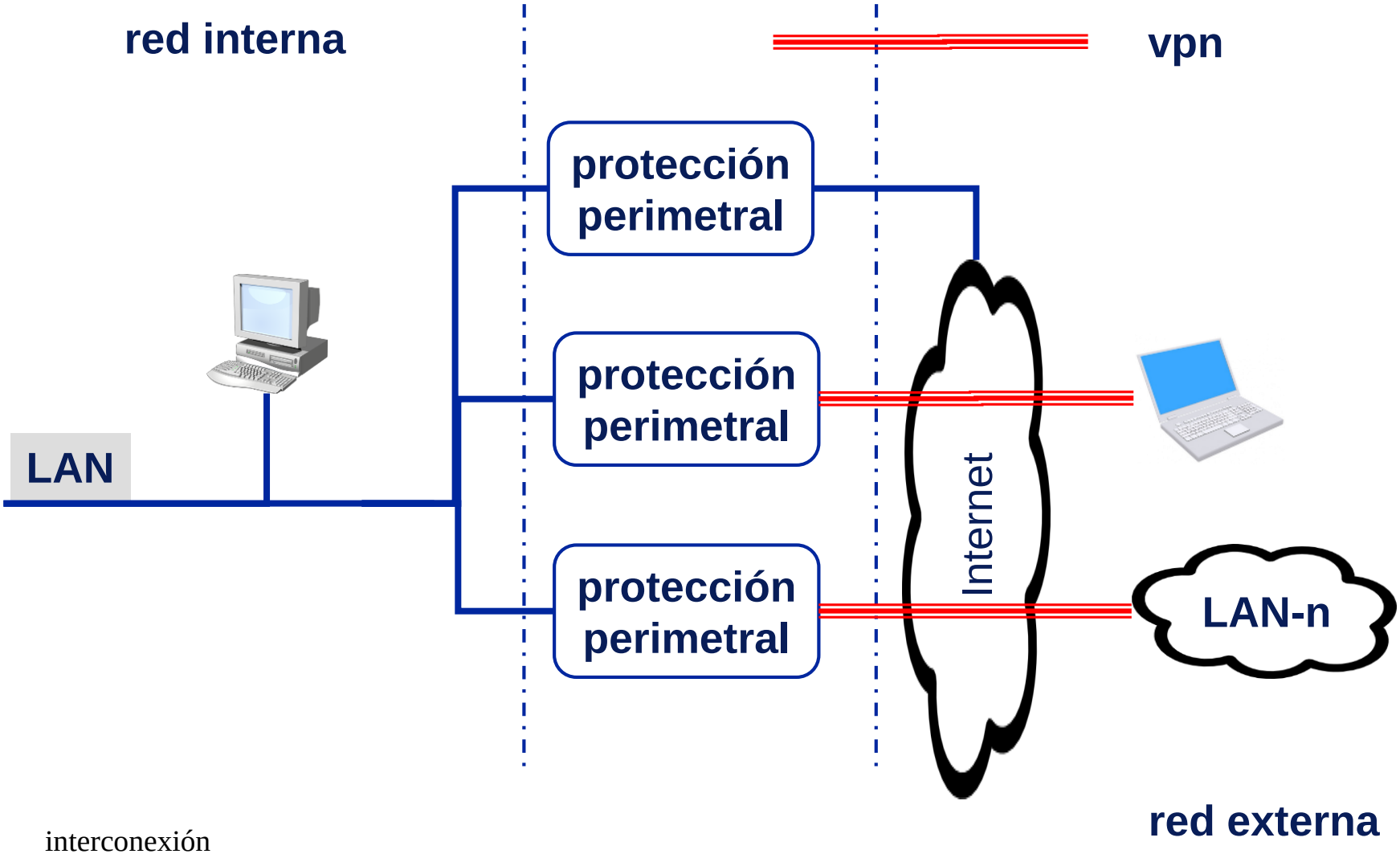
SPP-2

categoría ALTA



SPP-2*

redes privadas virtuales



redes privadas virtuales

- todos los datos que entran / salen deben ser intermediados en el proxy
  - TODOS puede implicar romper canales VPN
  - respeto a la legalidad vigente
- pueden aparecer vpn que atraviesan en negro la frontera
  - se establecerá un servicio proxy en la terminación interior

herramientas

	BÁSICA	MEDIA	ALTA
código malicioso	obligado 7d	obligado 48h	obligado 24h
análisis de vulnerabilidades	obligado 3m	obligado 1m	obligado 1s
análisis de logs	recomendado	obligado 1s	obligado 24h
IDS / IPS	opcional	obligado	obligado
monitorización de tráfico	opcional	recomendado	obligado
DLP (tráfico saliente)	opcional	opcional	obligado
escaneo de configuración	opcional	opcional	recomendado
verificación de funciones de seguridad	opcional	opcional	recomendado

equipos remotos

- Categoría BÁSICA
  - cortafuegos personal
  - administración de seguridad por personal autorizado
- Categoría MEDIA
  - white list : sitios a los que se puede conectar
- Categoría ALTA
  - el usuario no puede instalar sw
  - DLP local

para acabar

- La frontera de un sistema
  - está sujeta a lo prescrito en el ENS
  - tiene requisitos específicos de topología
  - tiene requisitos adicionales de protección
    - preventivos (dificultar los ataques)
    - monitorización: reaccionar & analizar