CENTRE DE SUPERCOMPUTACIÓ
DE CATALUNYA

CESCA

Mesa redonda:

Experiencia en arquitecturas de seguridad

Carles Fragoso i Mariscal

VII Foro de Seguridad RedIRIS, UCLM Ciudad Real

13 de marzo de 2009

Agenda

- ✓ ¿Qué es la arquitectura de seguridad?
- ✓ Problemáticas de una arquitectura tradicional
- ✓ Criterios de diseño
- ✓ Arquitectura de seguridad en el CESCA

Qué es la …

Arquitectura de seguridad

Arquitecto de seguridad

Técnica

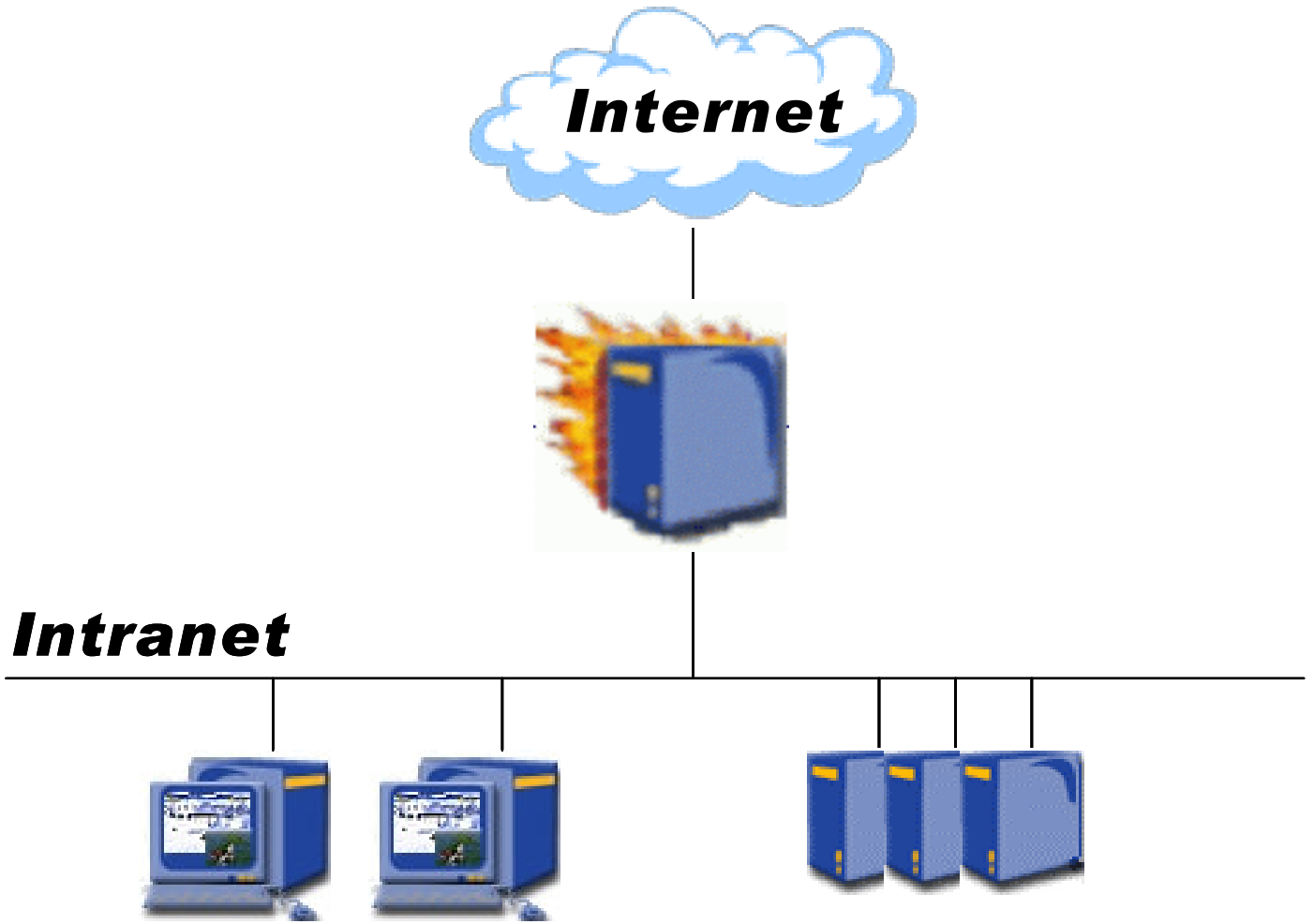
Creatividad

Experiencia

CESCA

- ✓ Red académica y de investigación: Anella Científica
- ✓ Punto Neutro de Internet en Cataluña (CATNIX)
- ✓ Supercomputación
- ✓ Repositorios y portales
- ✓ Alojamiento de servidores
- ✓ Red corporativa
  - CESCA
  - CBUC

Arquitectura plana



Problemáticas

- ✓ Política: permitir todo y denegar algunas cosas
- ✓ Listas de control de acceso complejas de gestionar
- ✓ Exposición en incidentes de seguridad
- ✓ Impacto alto de problemas de red de nivel 1 y 2
- ✓ Falta de documentación sobre los sistemas y servicios
- ✓ Cambios en entorno de producción

Oh…

¡Dios mío!

Ingeniería inversa TIC

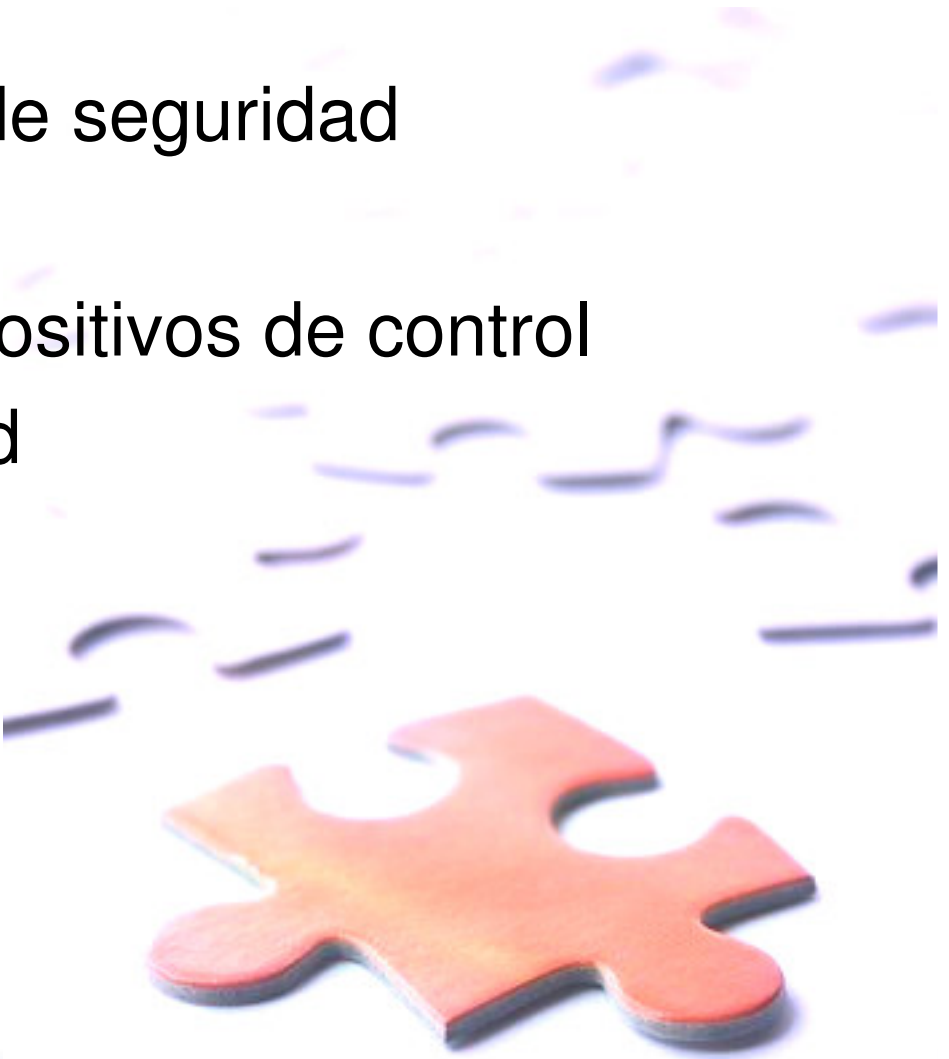
- ✓ Activa
  - Herramientas de escaneo de puertos y vulnerabilidades
- ✓ Pasiva
  - Monitorización con herramientas tipo NetFlow: nfsen/nfdump
  - Capturas de tráfico con *taps* o *span-ports*
  - Revisión de configuraciones
  - Bitácoras (*logs*)
  - Documentación

Criterios o reglas de oro

- ✓ Seguridad en profundidad
- ✓ Simplicidad
- ✓ Biodiversidad
- ✓ Control de acceso
- ✓ Complementariedad de tecnologías
- ✓ Principio de mínimo privilegio
- ✓ Adecuación a las necesidades productivas/riesgo
- ✓ Escalabilidad
- ✓ Redundancia

Procedimiento

- ✓ Política de seguridad
- ✓ Clasificación en niveles de seguridad
- ✓ Diseño
- ✓ Despliegue de red y dispositivos de control
- ✓ Dispositivos de seguridad
- ✓ Documentación
- ✓ Explotación



Qué es más conveniente …

¿Integración o migración?

- ✓ Infraestructuras de proveedor de servicios Internet
  - Red académica y de investigación: Anella Científica
  - Punto Neutro de Internet en Cataluña (CATNIX)
- ✓ Redes de servicio
  - Supercomputación
  - Servicios web
  - Otros
- ✓ Redes de datos y almacenamiento
- ✓ Redes de preproducción y desarrollo
- ✓ Redes de gestión en banda y fuera de banda
- ✓ Red corporativa (x2)
  - Usuarios y invitados
  - Servicios

Medidas de seguridad

- ✓ Nivel 1
  - Enlaces físicos separados
  - Control de *patch-pannels*
  - Dispositivos físicos dedicados
- ✓ Nivel 2
  - Segmentación mediante VLANs, PVLANs
  - Control de acceso por puerto con 802.1x
  - Seguridad de puerto (MACs) y limitación de protocolos
  - Monitorización y control de protocolos de nivel 2-3: DHCP, ARP
- ✓ Nivel 3-4
  - Listas de control de acceso en cortafuegos, encaminadores o sistemas
  - Virtualización con tecnología VRF
- ✓ Nivel 7
  - Control de protocolos a nivel de aplicación
  - Dispositivos *proxy*, cortafuegos de inspección, etc.

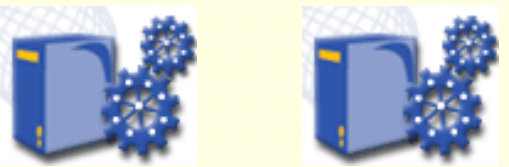
Retos

- ✓ Entornos de preproducción
- ✓ Virtualización de la infraestructura
- ✓ Red de invitados
- ✓ Red inalámbrica
- ✓ Telefonía IP
- ✓ Redes de gestión

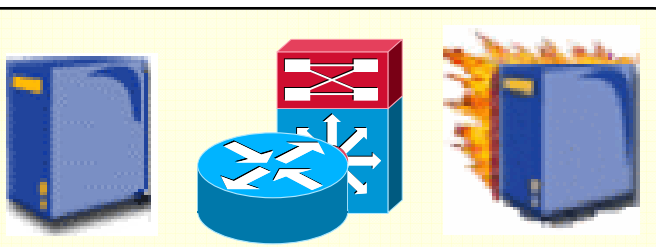
Arquitectura de gestión

Estaciones de gestión

Servidores, consolas o pasarelas de gestión



Sistemas o aplicaciones gestionadas



cfragoso@cesca.cat

http://www.cesca.cat

¡GRACIAS!