ARQUITECTURA DE SEGURIDAD EN LA RED DE LA USC

José A. Pizarro Bedoya
Responsable Unidad de Seguridad

ÁREA DE TECNOLOXÍAS DA INFORMACIÓN E DAS COMUNICACIÓNS

1. INTRODUCCIÓN
2. ANTECEDENTES
3. EVOLUCIÓN DE LA RED DENTRO DE UNA ARQUITECTURA DE SEGURIDAD INTEGRADA
   - PLANTEAMIENTO
   - OBJETIVOS
4. ARQUITECTURA DE SEGURIDAD DE RED EN LA USC
   - EQUIPAMIENTO
   - MÓDULOS DE GESTIÓN DE RED
   - SOLUCIÓN DE RED DE CUARENTENA

COMPARTIR NUESTRA EXPERIENCIA EN LA **IMPLANTACIÓN DE MECANISMOS** QUE PERMITEN UNA **GESTIÓN MÁS EFICIENTE** DE LOS **INCIDENTES DE SEGURIDAD** EN LA RED.

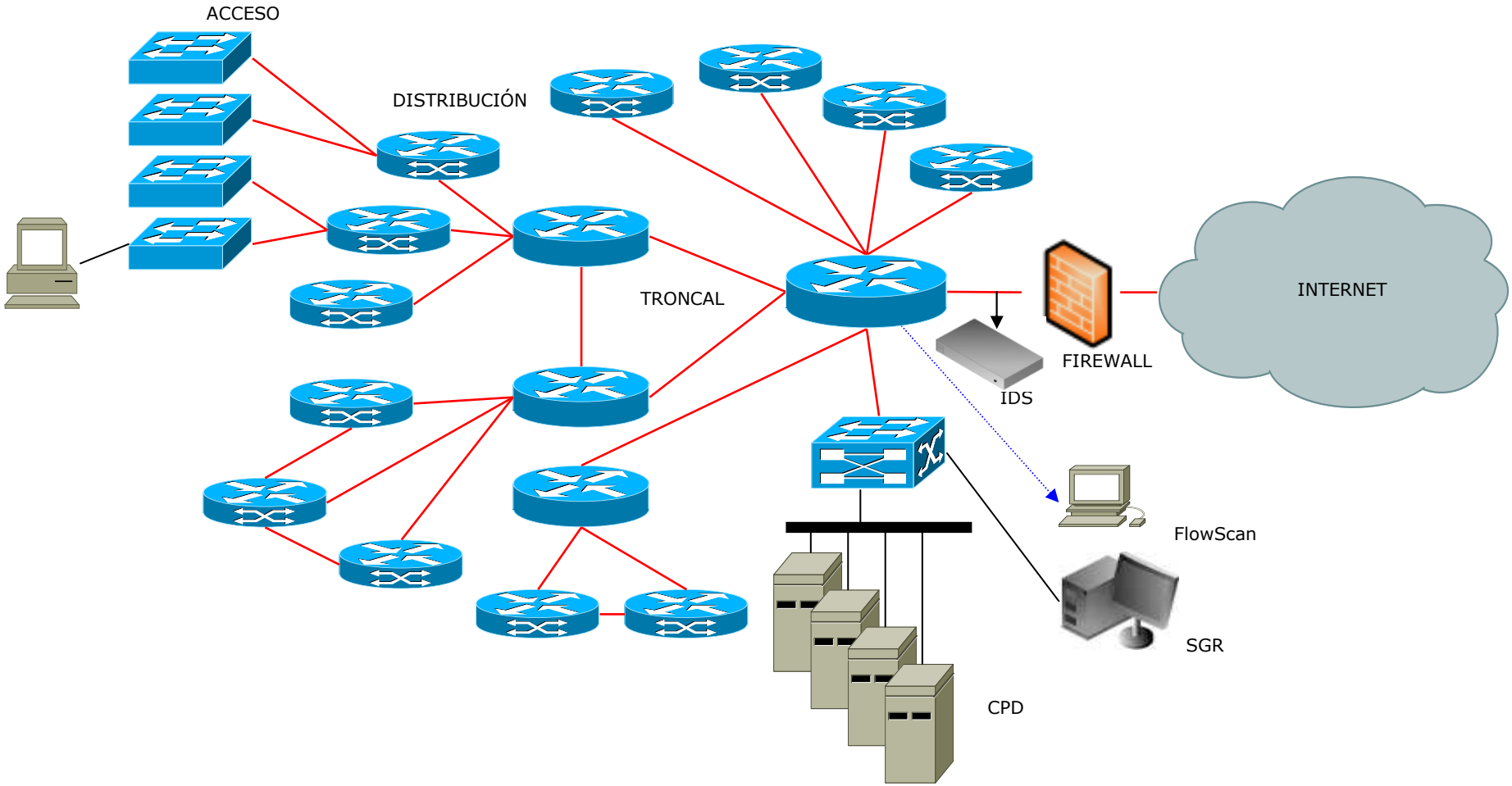
ANTECEDENTES: Red USC 2007.

- Red Gigabit Ethernet en troncal y distribución y Fast Ethernet en acceso:
  - 3 Campus en Santiago, 1 Campus en Lugo.
  - +10.000 puertos de acceso.

- Sistemas de monitorización:
  - Monitorización flujos (Flowscan): analizando los flujos del router principal de la red.
  - MRTG.

- Sistemas de seguridad
  - IDS (Snort) analizando el tráfico intercambiado con el exterior de la red.
  - Firewall perimetral.

Red USC 2007


ACCESO
DISTRIBUCIÓN
TRONCAL
INTERNET
FIREWALL
IDS
FlowScan
SGR
CPD

ANTECEDENTES: Red USC 2007.

Carencias de esta arquitectura:

- No estaba orientada a la seguridad.
- No integraba suficientemente los distintos elementos: red, sensores, herramientas de monitorización.

-> Los incidentes de seguridad y los incumplimientos de la normativa eran difíciles de gestionar y consumían demasiados RRHH.

-> Aplicar una Política de Uso Aceptable era demasiado laborioso.

-> No permitía controlar el acceso.

ANTECEDENTES: Red USC 2007

- Gestión de un incidente:
  - Lectura de logs,
  - Recepción e interpretación de alertas,
  - Interpretación de estadísticas,
  - Actuación remota o in situ.
  - Proceso de decisión a la hora de aplicar régimen sancionador: cortar servicio? duración?

-> Tiempos de respuesta elevados.

- **Conclusión: se necesitan herramientas que automaticen los procesos (en la medida de lo posible).**

PLANTEAMIENTO PARA LA EVOLUCIÓN DE LA RED:

- OBJETIVOS DE CAPACIDAD Y CONECTIVIDAD:
  - Mejorar la capacidad de procesado de los routers y switches.
  - Mejorar velocidad acceso.
  - Incorporar soporte de nuevas funcionalidades.
  - Mejorar la redundancia de la red.

PLANTEAMIENTO PARA LA EVOLUCIÓN DE LA RED:

- OBJETIVOS relacionados con la seguridad:
  - Reducir el tiempo de respuesta y actuación ante incidentes.
  - Reducir los costes de gestión de los incidentes.

  -> Mejorar la eficiencia en la gestión de los incidentes.

  - Permitir controlar el acceso a la red
  - Permitir clasificar a los usuarios por perfiles

  -> Mejorar la eficiencia en la gestión de los usuarios

PLANTEAMIENTO PARA LA EVOLUCIÓN DE LA RED:

- FUNCIONALIDADES requeridas :
  - La red debería de ser capaz de **integrarse** con otros sistemas para tratar de **aislar** en un **tiempo** razonable y de forma **automática** un usuario malicioso o una máquina comprometida.
  - La red de debería de tener capacidad de manejar autenticación 802.1X y perfiles para proporcionar servicios diferenciados por grupos de usuarios.
  - La red debería de permitir "mapear" una Política de Uso Aceptable de las distintas redes (Alumnos, PAS, PDI) de forma sencilla.

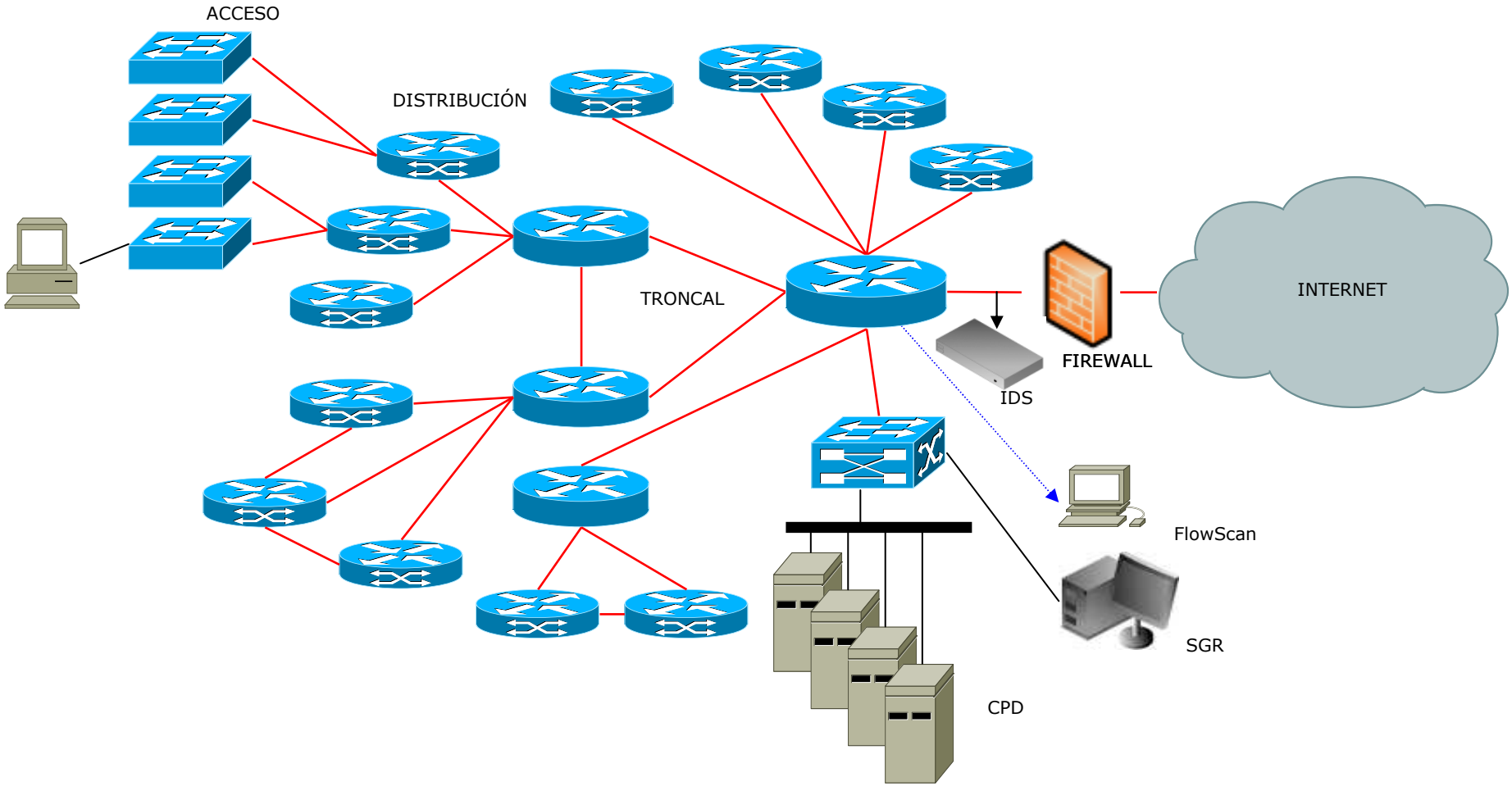
PROYECTOS PARA EVOLUCIONAR LA RED:

- Renovación de firewalls e incorporación de un sistema de recolección de logs específico.

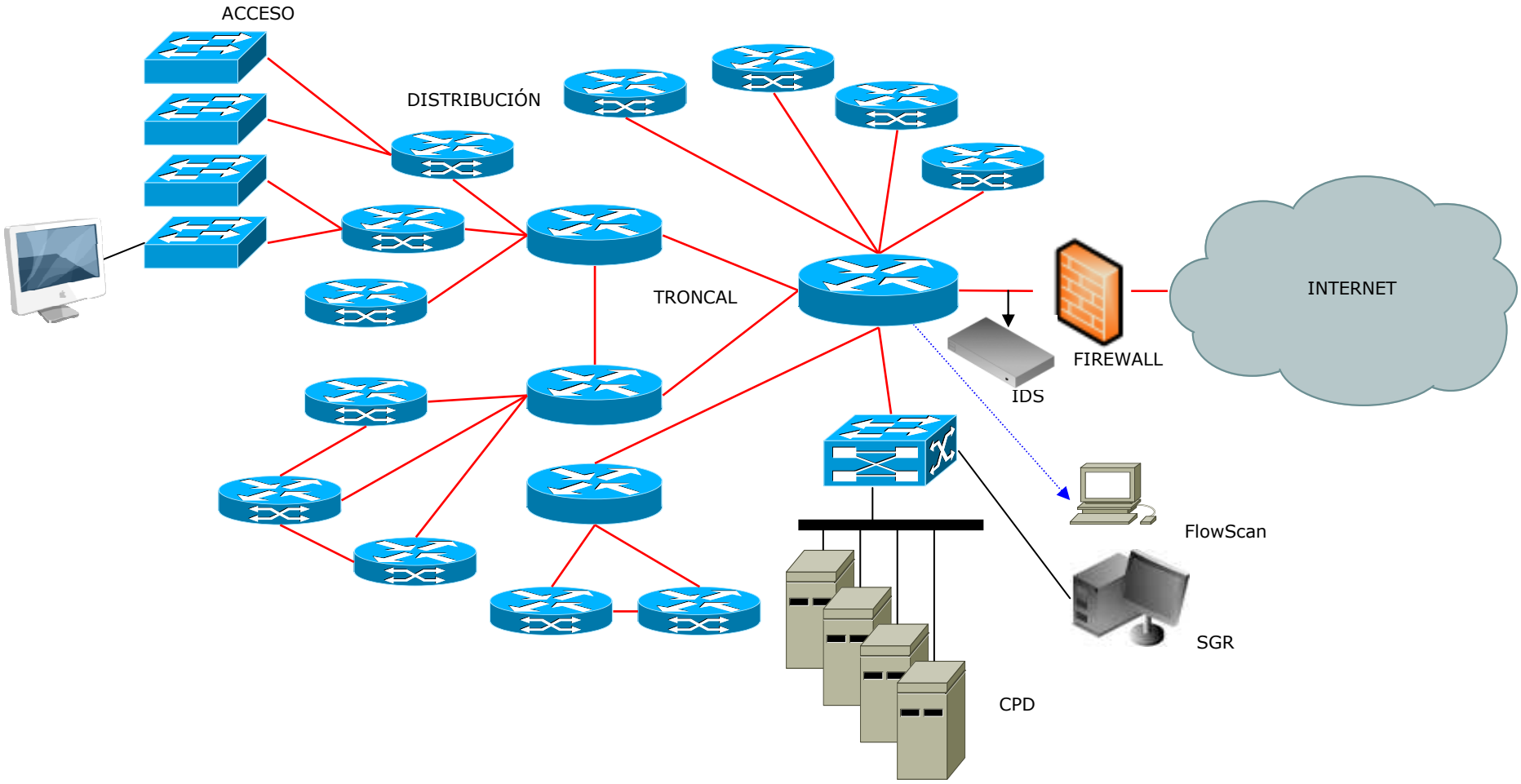
- Renovación del equipamiento de red y plataforma de gestión.

- Incorporación de nuevas herramientas de análisis de uso de red:
  - IPS integrado en firewals,
  - nuevos sensores Snort,
  - Nfsen,

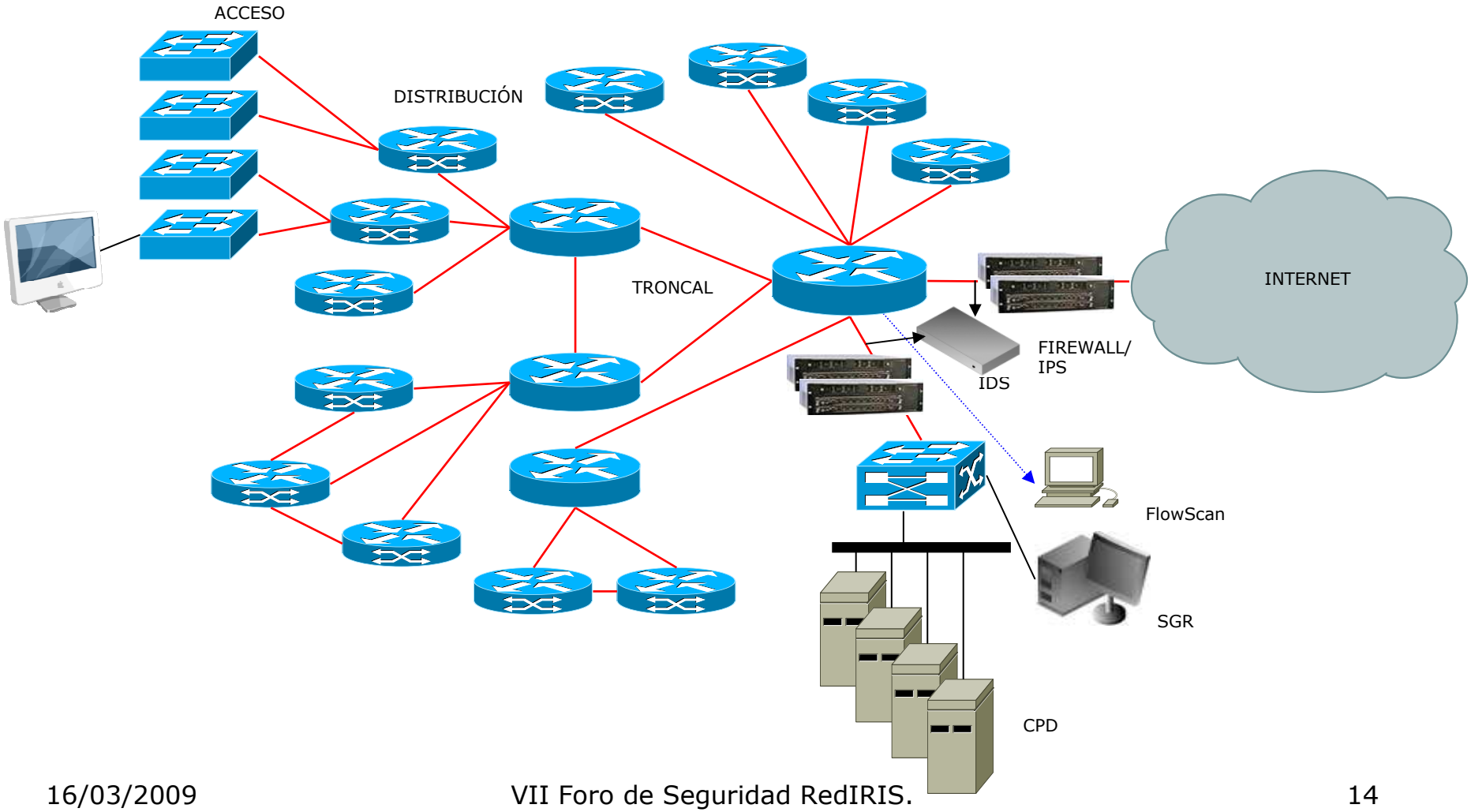
Evolución Red USC



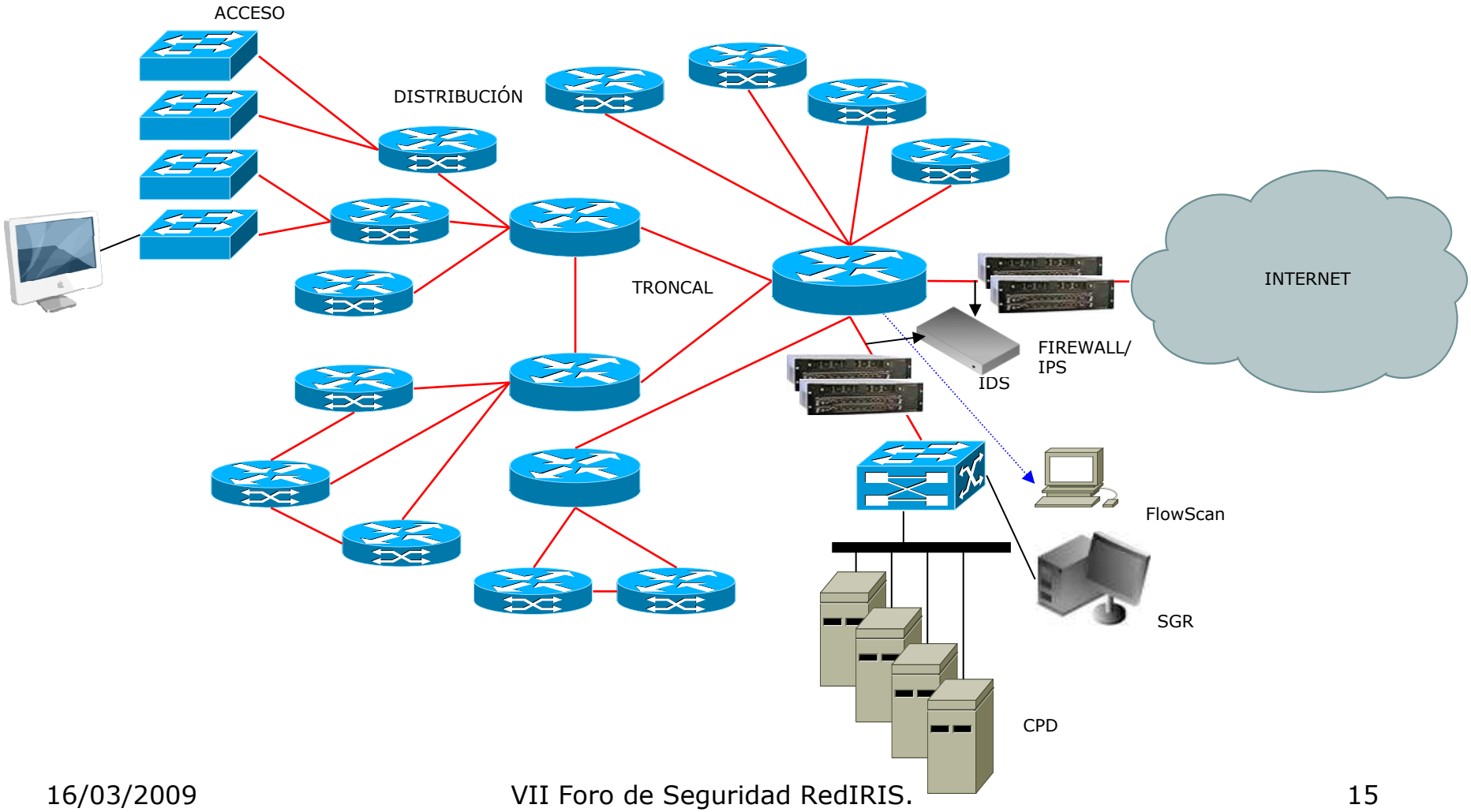
Evolución Red USC



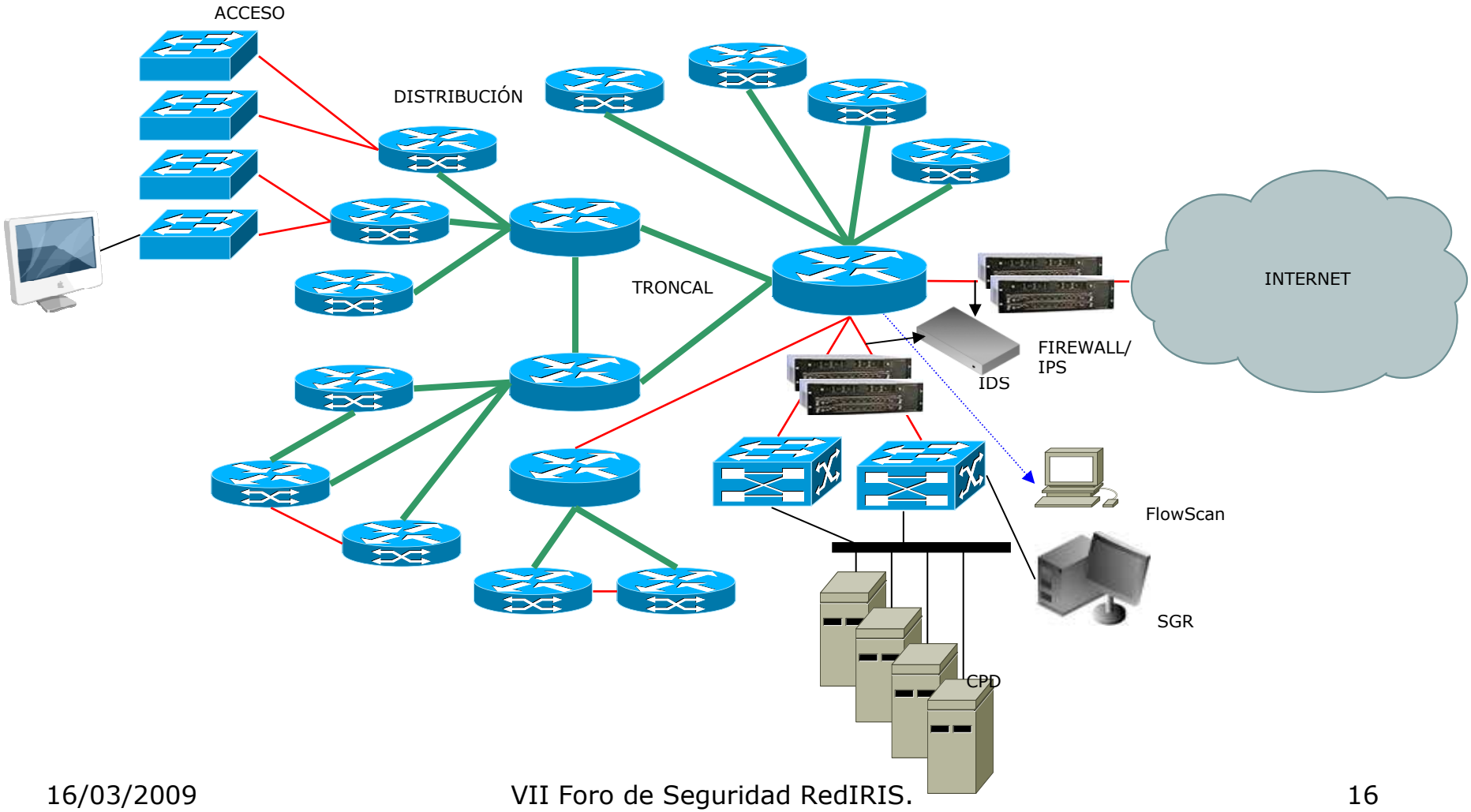
Evolución Red USC



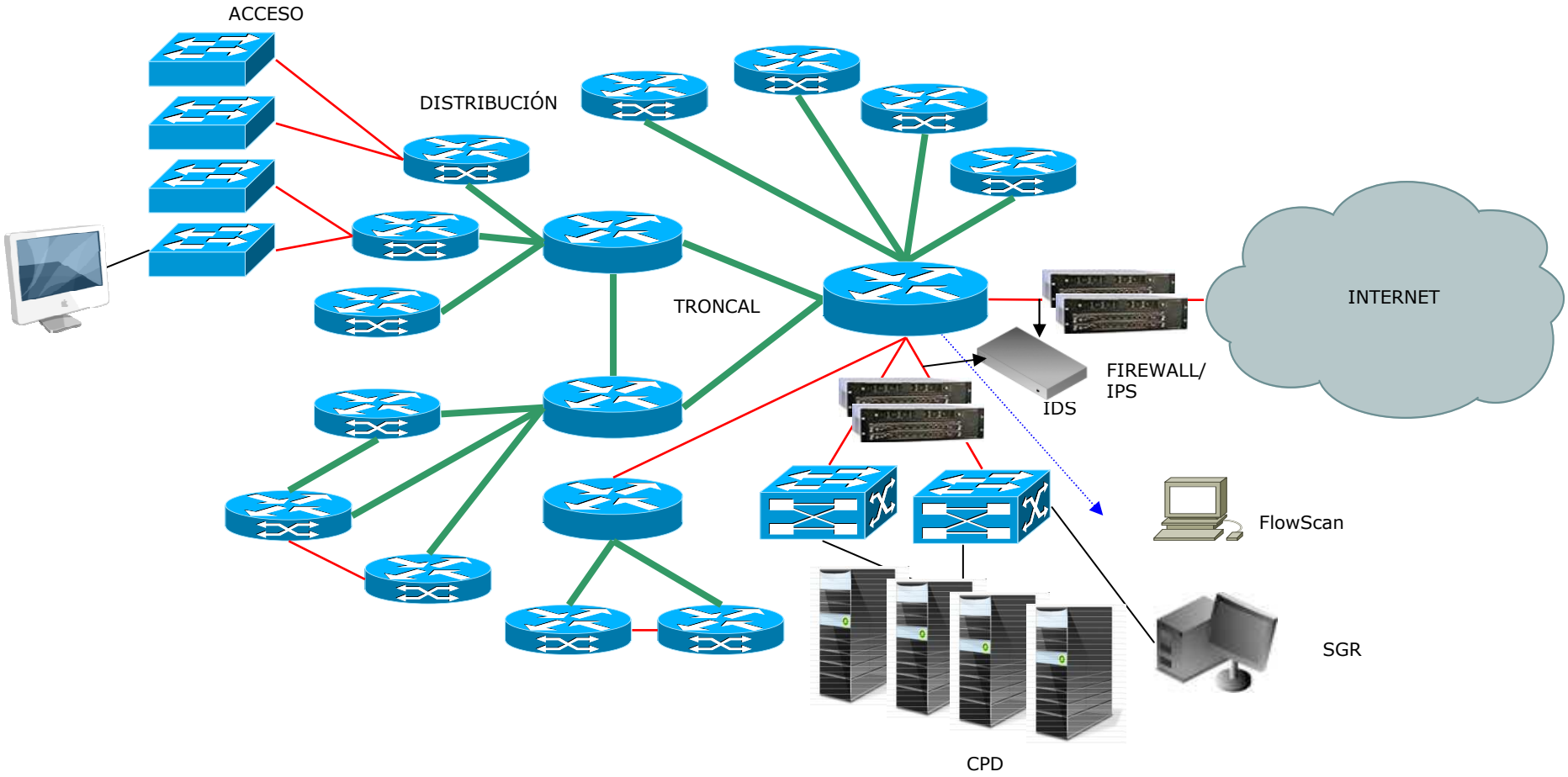
Evolución Red USC



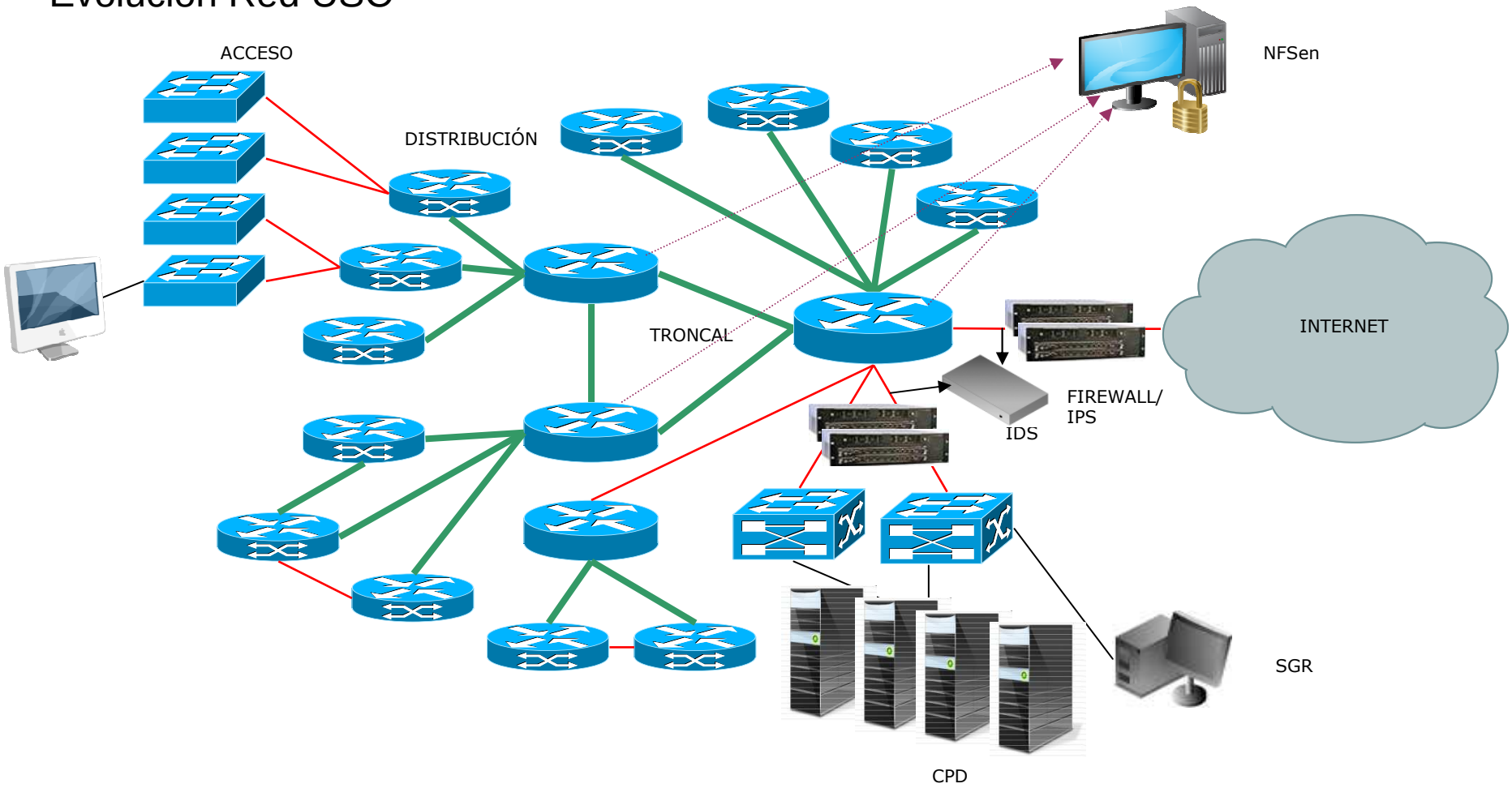
Evolución Red USC



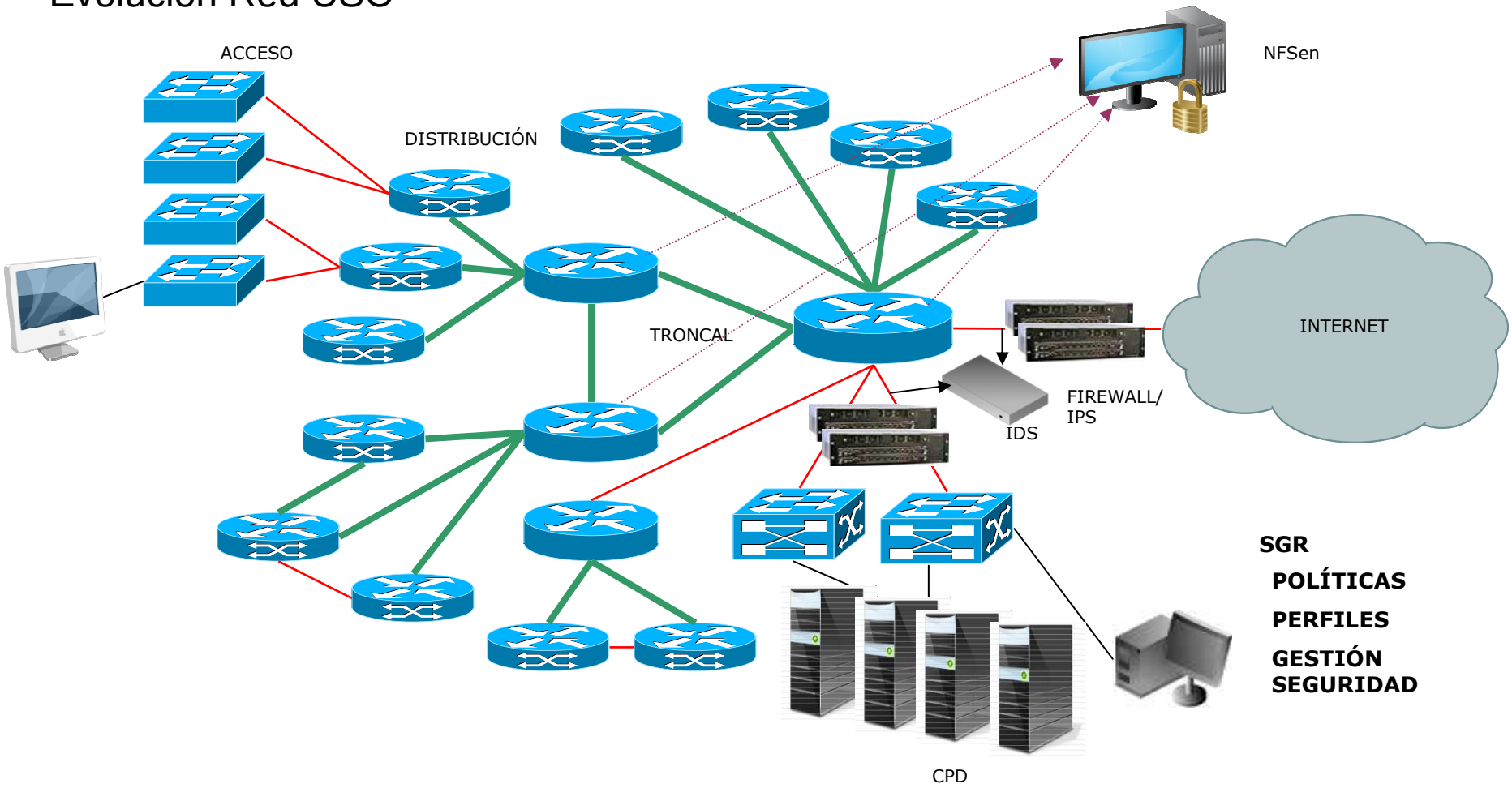
Evolución Red USC



Evolución Red USC



Evolución Red USC



ARQUITECTURA ORIENTADA A LA SEGURIDAD EN LA NUEVA RED USC

- EQUIPAMIENTO Y PLATAFORMA DE GESTIÓN DE RED ENTERASYS.
- FIREWALLS FORTINET.
- IDS Snort.

ARQUITECTURA ORIENTADA A LA SEGURIDAD: PERFILES EN LA LAN

- Implementado por el Módulo de Gestión de Políticas (Policy Manager)
- Qué nos permite hacer un módulo de gestión de políticas?
  - Definir y desplegar políticas en los equipos de la red.

  -> Aplicar a usuarios y/o puertos de red distintos perfiles.

ARQUITECTURA ORIENTADA A LA SEGURIDAD: PERFILES EN LA LAN

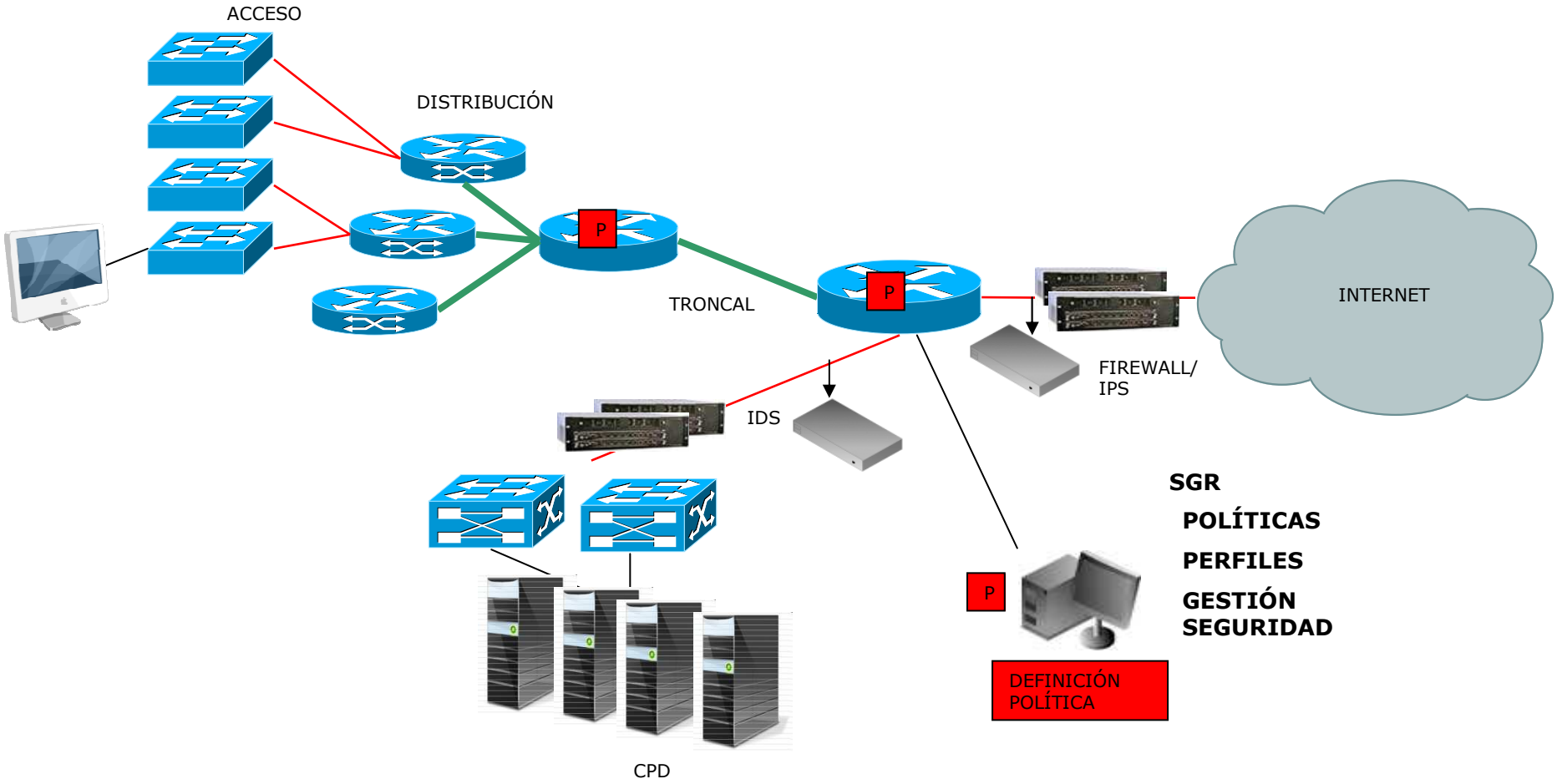
- Definir políticas es definir un conjunto de reglas y aplicarlas a distintos perfiles de uso.
- En la práctica un perfil (role) esta formado por un conjunto de reglas de filtrado y de aplicación de calidad de servicio y Rate Limiting.

- Ejemplo:
  - Perfil: perfil_usuario
  - Reglas:
    - Denegar Protocolos Ilegales = no permitir IPX, no permitir Appletalk
    - Denegar servicios de red: no permitir servir DNS, no permitir servir DHCP.
    - Aplicar CoS 802.1p=3, Rate limit= 20Mbps

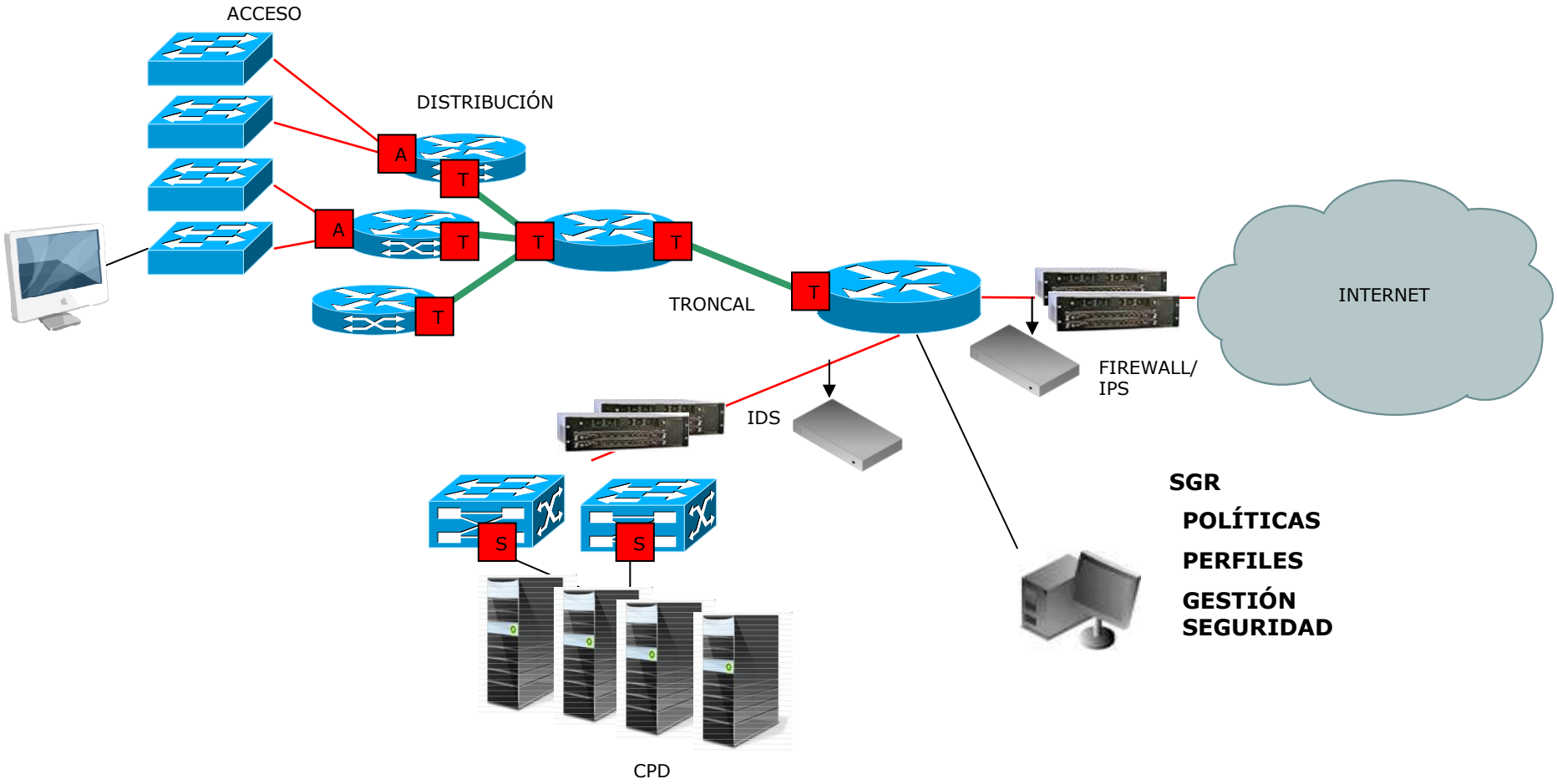
PERFILES EN LA LAN

- Experiencia USC:
  - Hemos definido una Política de uso aceptable de la red y la hemos desplegado en los conmutadores del nivel de distribución y troncal.
  - La política define perfiles estáticos para
    - puertos troncales
    - puertos de usuario
    - puertos servidores corporativos
  - La política contempla la aplicación de un perfil en función del tipo de usuario (experiencia piloto para puestos móviles).
  - Hemos definido una política de cuarentena, cuya aplicación vamos a ver.

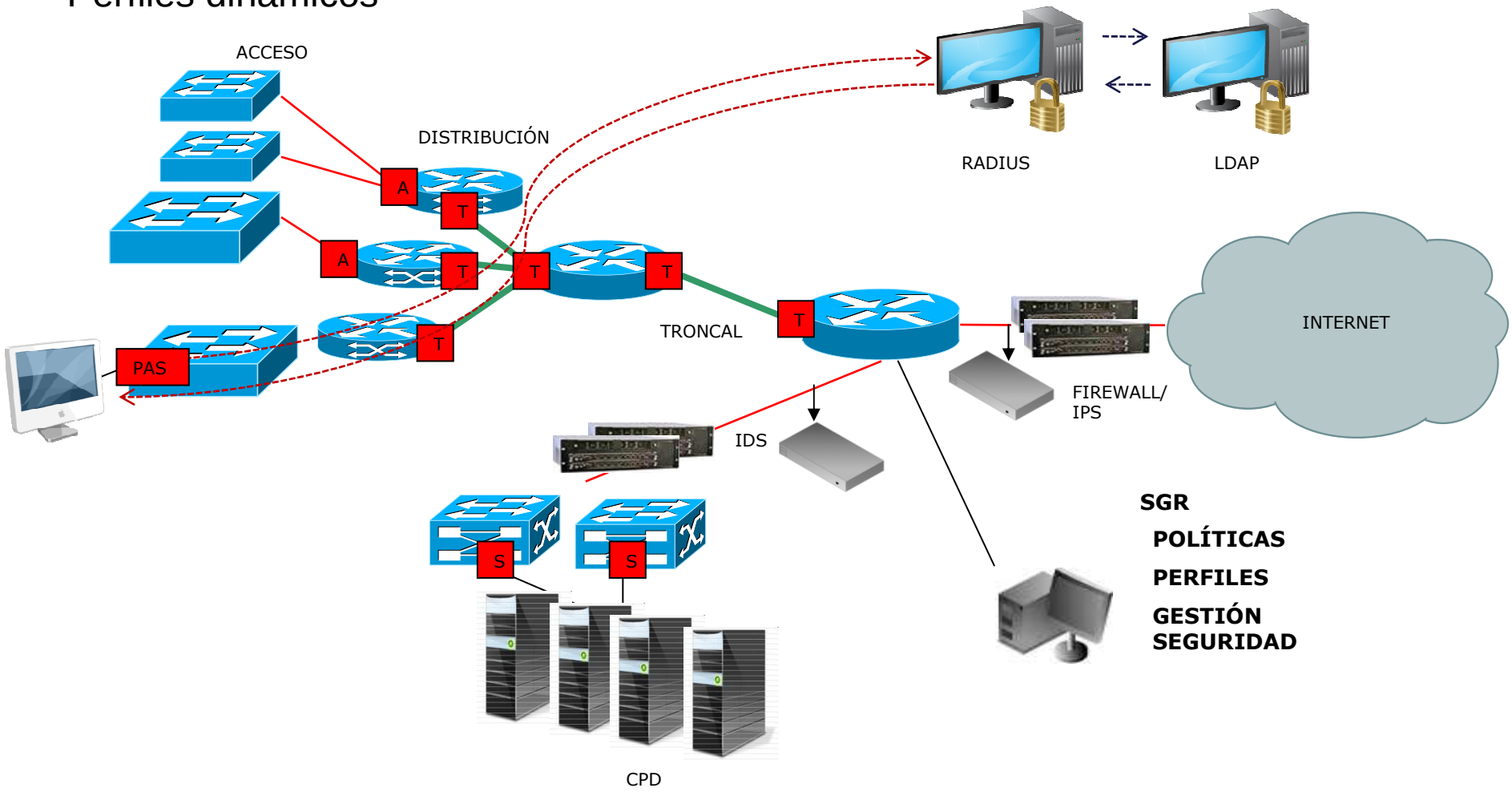
Perfiles estáticos



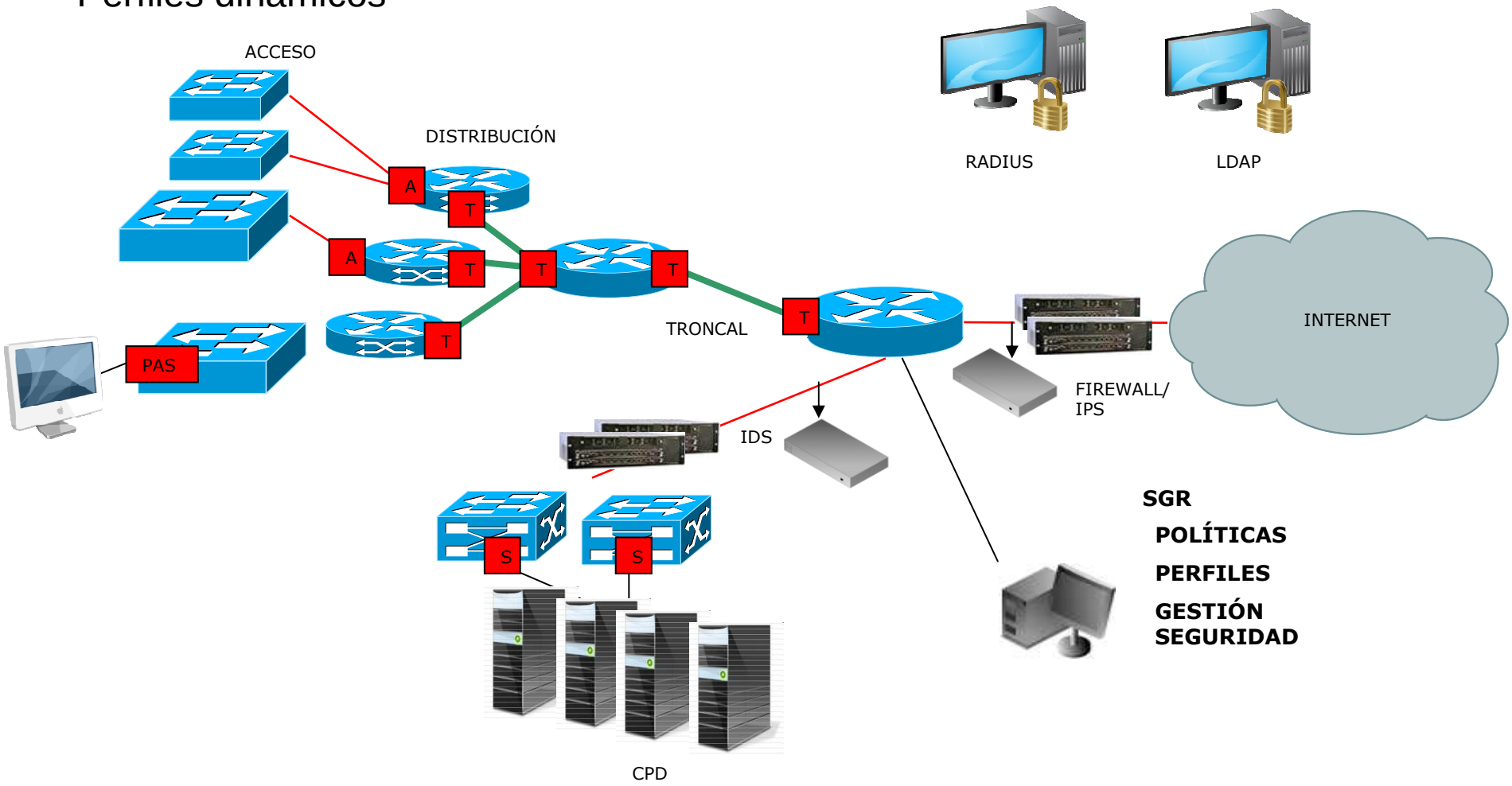
Perfiles estáticos



Perfiles dinamicos



Perfiles dinamicos



GESTION AUTOMATIZADA DE LA SEGURIDAD EN LA LAN

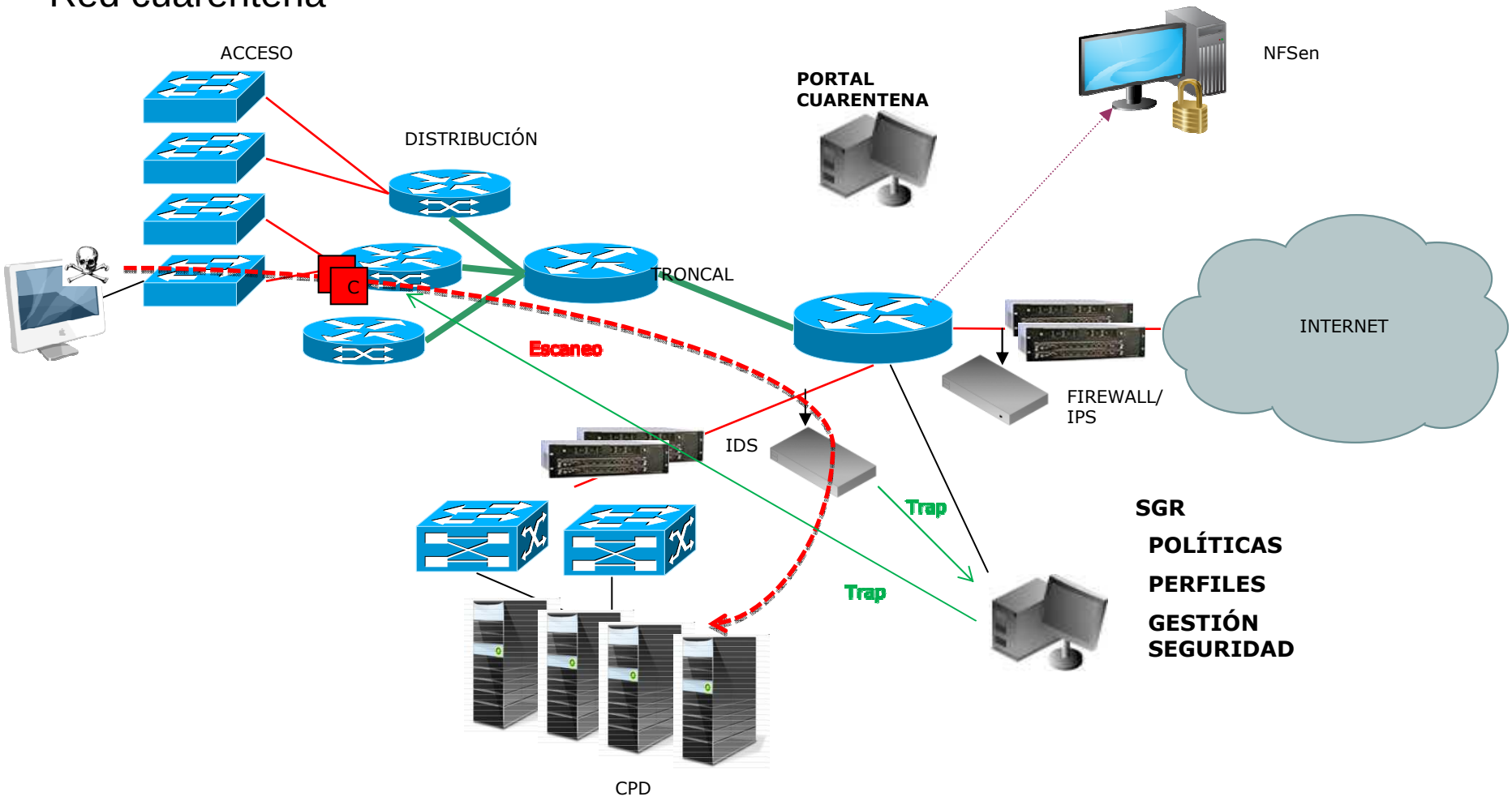
- Implementado por el Módulo ASM de Netsight.
- Se basa en la recepción de alertas procedentes de IPS (u otros equipos) y en la ejecución de una serie de acciones posteriores.
- En función de la categoría de la alerta podemos realizar distintas acciones: Ej: deshabilitar el puerto del usuario, cambiar el perfil a aplicar al usuario.
- El sistema puede funcionar automáticamente o asistido por un operador, que será el que finalmente confirme la acción a realizar.
- Se pueden configurar temporizadores para ejecutar la acción y para el restablecimiento de la situación anterior.
- Se pueden ejecutar scripts asociados a cada acción del ASM. P.ej.: envío de correo/SMS al grupo de seguridad cada vez que un equipo se ponga en cuarentena.

IMPLEMENTACIÓN RED DE CUARENTENA

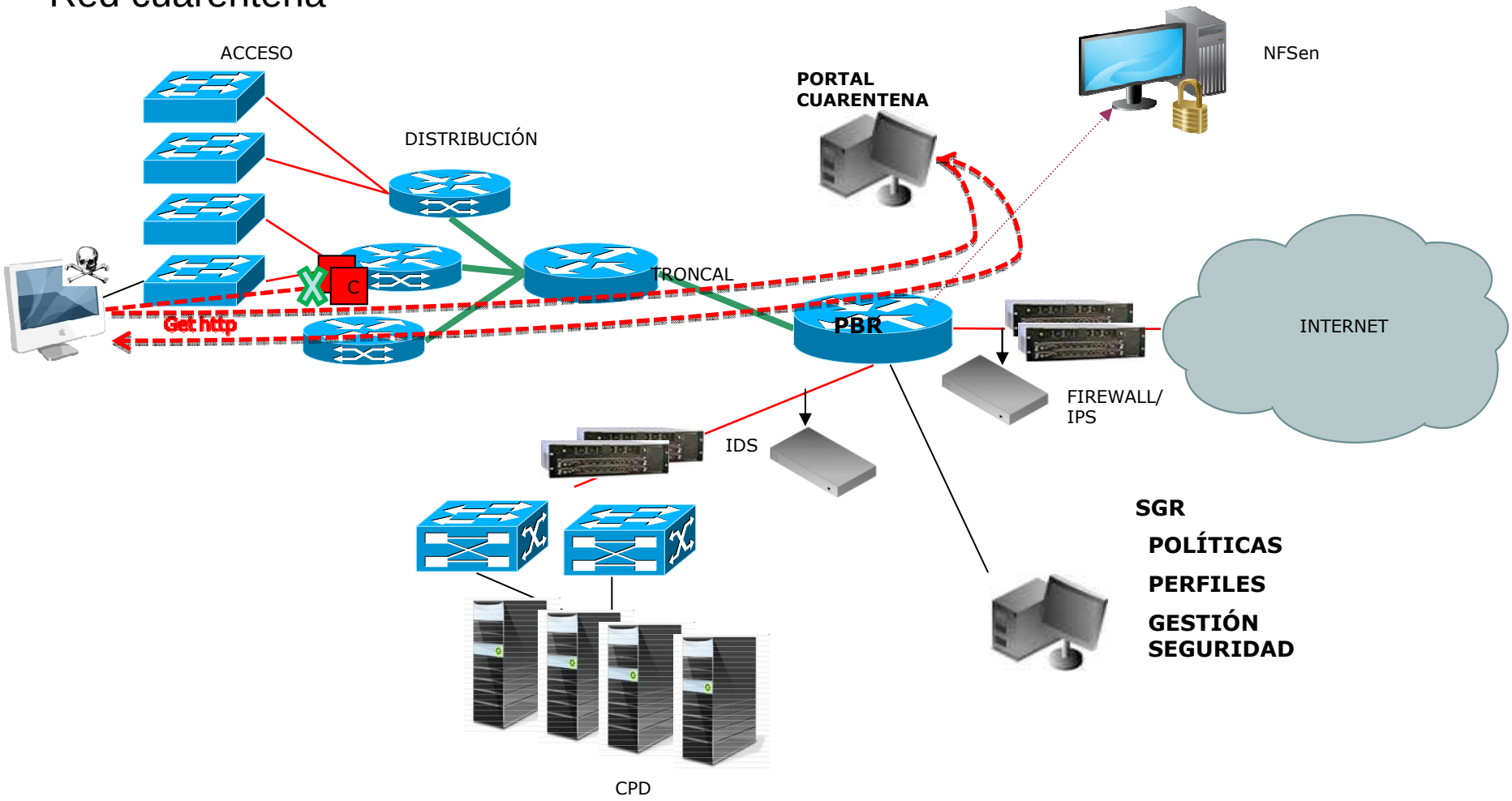
- Objetivo: que el usuario, en caso de ser apartado a la red de cuarentena, tenga acceso a recursos que le permitan reparar el incidente de la forma más autónoma posible.

1. IDS detecta coincidencia en una firma,
2. *Trap* SNMP al ASM,
3. ASM localiza al usuario (MAC),
4. Ejecución acciones,
   - Envío correo al usuario
   - Envío SMS operadores.
   - Cierre puerto.
   - **Aplicación perfil de cuarentena.**

Red cuarentena



Red cuarentena



A FAVOR DE ESTA IMPLEMENTACIÓN

- Se consigue una automatización razonable de la gestión de los incidentes de seguridad.
- Permite desplegar y mantener actualizada la PUA implementada en la red, reflejo de la Política definida.
- Conceptualmente se asemeja a un firewall en el nivel de acceso

DESVENTAJAS DE ESTA IMPLEMENTACIÓN

- Integración con otros IDS distintos del del propio del fabricante.
- Limitaciones filtrado en distribución
- Registro de tráfico bloqueado por políticas

AÚN HAY MUCHO POR HACER …

- NAC
- Integración con otros sistemas: firewalls, IPS, NFSen, correlador de eventos,
- Integración con la WLAN.
- Comunicación bidireccional entre SGR y resto de los sistemas.

CONCLUSIONES

Se pueden automatizar gran parte de las tareas a la hora de gestionar incidentes de seguridad en la red.

Es necesario personalizar mucho las herramientas: monitorización de red, detección de intrusiones, ASM, PM, ...

MUCHAS GRACIAS

joseantonio.pizarro @ usc.es