Segmentación de red en la URV
De la “B” a la “C”.

Antoni Cortés y Jose Oriol Lorenzo
Universitat Rovira i Virgili (URV)

Situación de partida

- La red de la URV nació plana, ya que el tamaño y equipos que teníamos en su momento era lo que más nos convenía
- En 2018 decimos segmentar. Los problemas derivados de una red plana ya eran complicados de gestionar:
  - Bucles en redes de más de 2000 hosts
  - Multicast no controlado (tarjetas Intel y Windows 10)
  - CPU de los conmutadores centrales
  - Spanning Tree (implica tener enlaces de core sin utilizar). No nos planteamos MSTP.
  - Incremento del ancho de banda e impacto en los FW que se necesitan adquirir (y mantener)

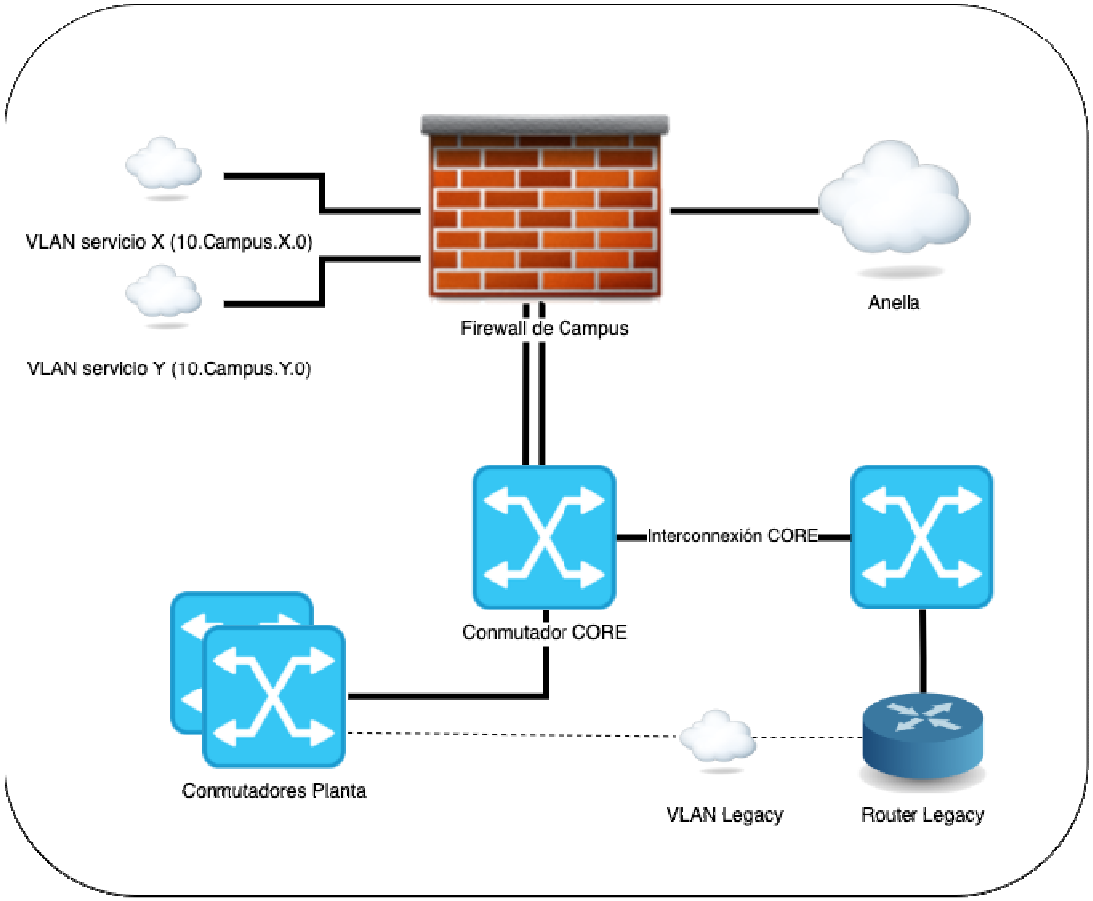
Objetivo

Carta a los reyes…

- Segmentación L3 por campus
  - Más que segmentación por campus, segmentación por servicios….
- Direccionamiento propio para cada campus
- L2 “contenido”
- Salida a internet local
  - Redundada, por supuesto….
- Interconexiones entre campus
  - Redundadas, por supuesto…
  - Pero “seguras” (aka filtradas)
- Gestión centralizada

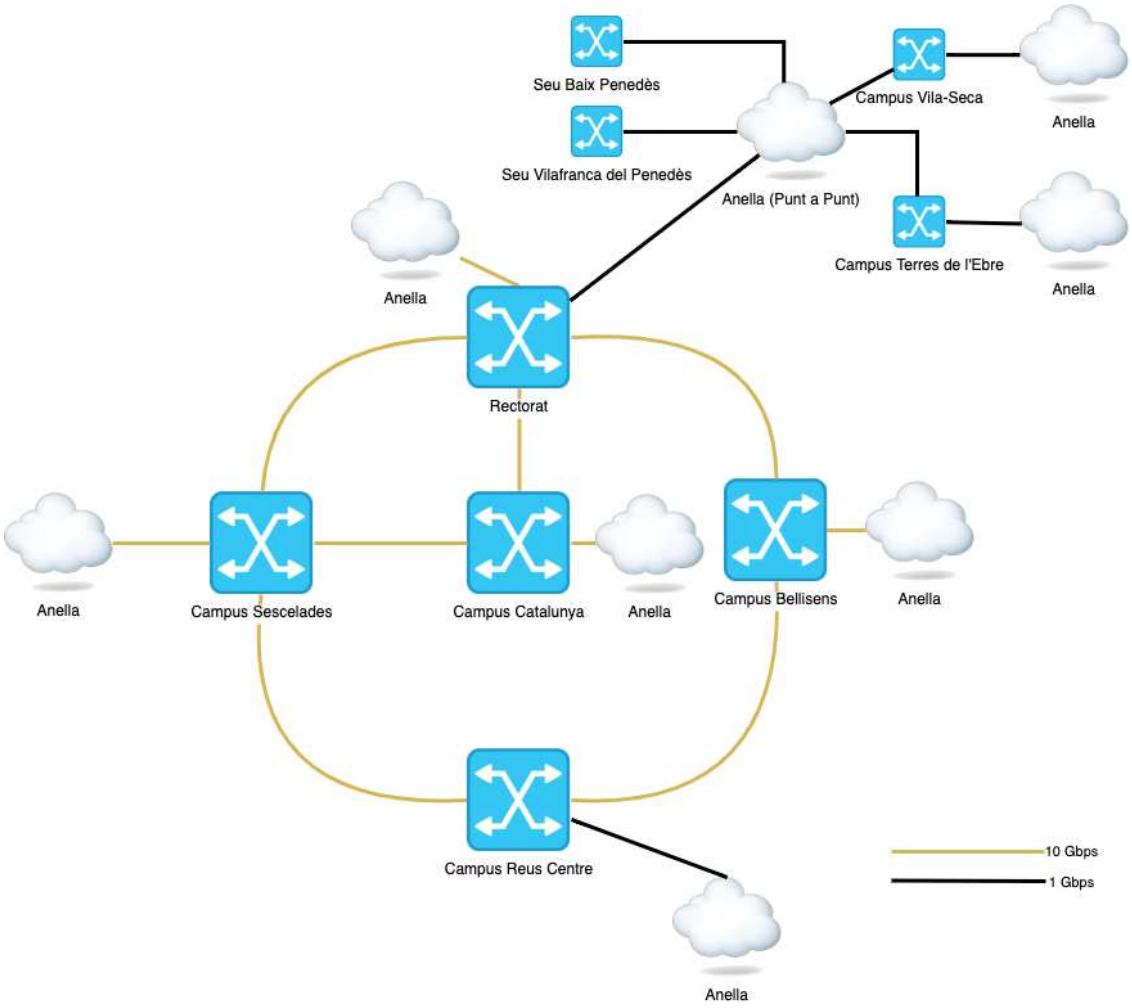
Evolución a estructura por Campus

- Cada campus tiene su FW de core
- Gestiona todo el tráfico del campus (Norte – Sur)
- Podemos aislar hosts de la red (tráfico Este – Oeste)
- Convivimos con el modelo antiguo, así que extendemos las VLANS ”legacy” desde el core de Rectorado donde están los routers “legacy”



Situación actual L1 – L2

- FO dedicada intercampus
- FO Anella por Campus
- VLANs distribuidas por el core, implica tener STP y por tanto hay FO sólo para redundancia
- VLANs también sólo de campus



Modelo de red de Campus - Segmentación

Hola chic@s...
Hoy vamos a ver, como segmentar la red....

Nunca es tan fácil.... y lo sabes

Modelo de red de Campus – Segmentación

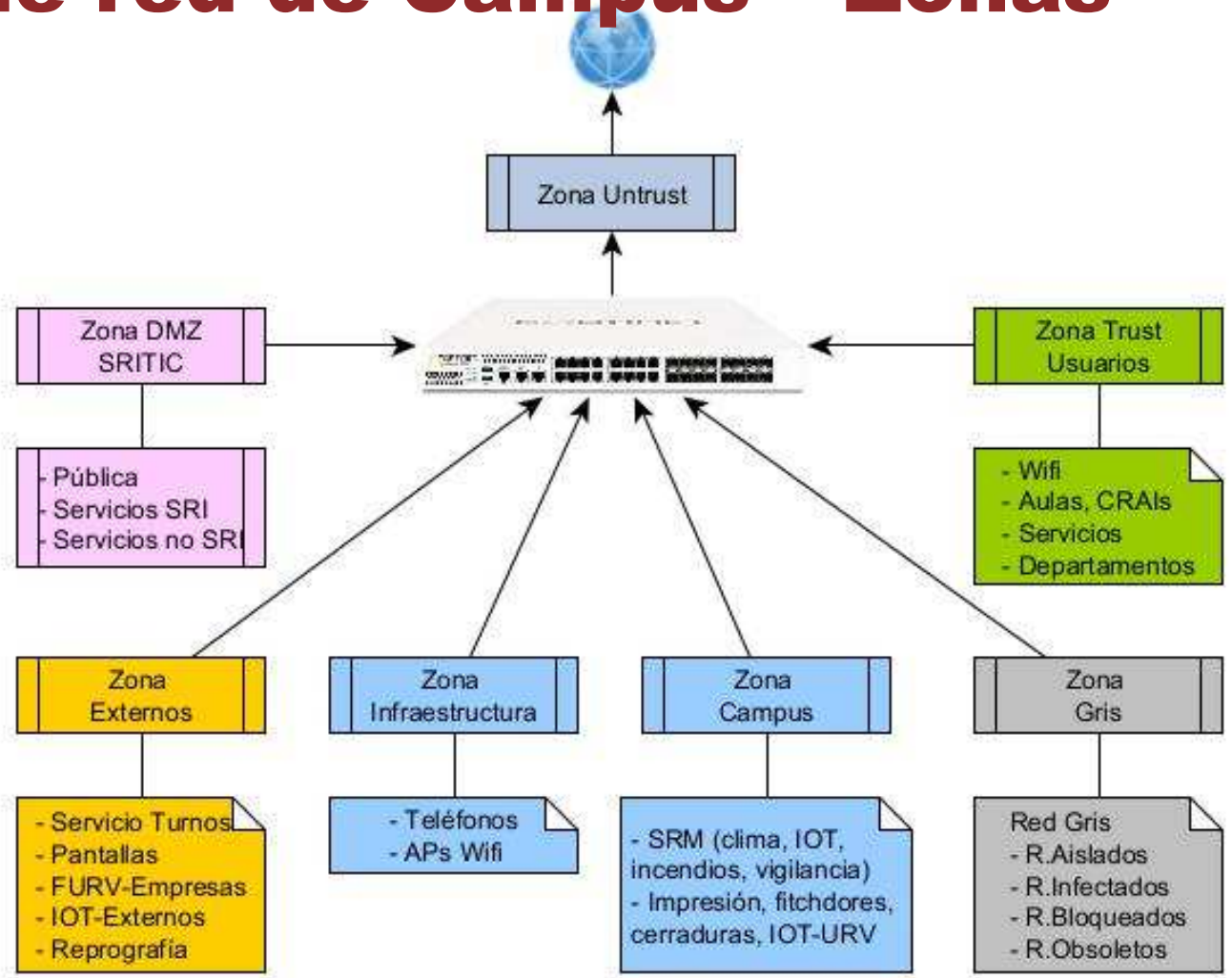
Cómo lo hacemos?

- Segmentación L3 por campus
  - FireWall local en cada campus
  - Interfaz para cada red de servicio
  - Salida a internet redundada eBGP
  - Conexiones entre campus redundadas

Ya ya…. Pero… como lo hacemos?

- Definición de un modelo “teórico” de campus
  - El mismo modelo para campus grandes (miles) y campus pequeños (decenas)
  - Modelo flexible y adaptable a nuevas necesidades

Modelo de red de Campus – Zonas



Modelo de red de Campus – Zonas

- Zonas
  - Agregan interfaces por tipología de clientes
  - Redes similares -> supernetting en **bloques** (lo necesitaremos…)
  - Interfaces -> redes de servicio, /24… /23… /22 según necesidad
  - Bloqueo de tráfico intrazone!!! todo pasa por el FireWall 

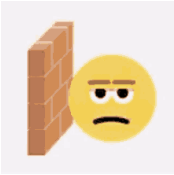
- Definición de redes
  - 10.**Campus**.**Servicio**.0 /24
    - /24 lo más habitual
    - Supernetting /23 /22 por ej. para bloques Wifi
  - "**Servicio**" define a su vez la VLAN correspondiente. (VLAN base + #Servicio)
  - En todos los campus, para el mismo servicio, tenemos la misma red

Modelo de red de Campus – Zonas

- Ejemplo, zona Trust (Usuarios)
  - Bloque trabajadores 10.**CAMPUS**.**32**.0/19 (/24 para las redes)
    - Distintas interfaces, por servicio o servicios agregados (departamento, servicio, oficina)
    - DHCP: Zona baja para direcciones fijas, zona alta para dinámicas
  - Laboratorios y aulas de docencia 10.**CAMPUS**.**64**.0/20
    - Distintas interfaces, por aula / facultad / etc.
  - Bloque Aulas CRAI (bibliotecas) y “libre acceso” 10.**CAMPUS**.**80**.0/20
  - Bloque usuarios WIFI 10. **CAMPUS**. **128**.0/19 (8190 hosts)
    - Wifi Trabajadores (Eduroam URV) 10.**CAMPUS**.**128**.0/21 (2046 hosts)
    - Wifi Eduroam (usuarios no URV) 10.**CAMPUS**.**136**.0/22
    - Wifi Eventos 10.**CAMPUS**.**140**.0/22
    - Wifi Alumnos 10.**CAMPUS**.**144**.0/20 (-> tuvimos que ampliarlo, el modelo lo contempla)

Modelo de red de Campus – Zonas

- El modelo ha resultado ser “resistente”
  - Asignamos redes “pares” a los **servicios 32, 34, 36**… para que sean ampliables de /24 a /23
  - Agregamos servicios poco numerosos en la misma red. Evitamos redes despobladas con pocos usuarios
  - No ocupamos una red más de 50%-60% no queremos tener que partir redes en un futuro próximo. Evitamos redes superpobladas
  - Los bloques asignados son generosos y permiten añadir redes
  - Reservamos bloques libres entre los bloques asignados
- Filtrado en destino
  - Siempre se aplica la política de filtrado en el FW destino
  - Simplificamos políticas
  - Excepción: VPN SSL para usuarios



Interconexión de Campus

- Imatge per canviar model – de interconnexió (neurones, interconnexió)

- Interconnexió de campus (SDWAN, BGP, VPN, etc)

Interconexión de Campus

- Conexión actual (VLANs Punto a Punto): Conexión entre el FW de Rectorat con el FW de cada Campus
- VPN: Todos los FW mantienen túneles con el nodo central (Hub-Spoke). Se establecen túneles a través de Internet
- Evolución a L3: Una vez finalizada la migración los enlaces de CORE sólo tendrán VLANs punto a punto (QinQ para excepciones), con lo que podremos quitar Spanning Tree

Interconexión de Campus

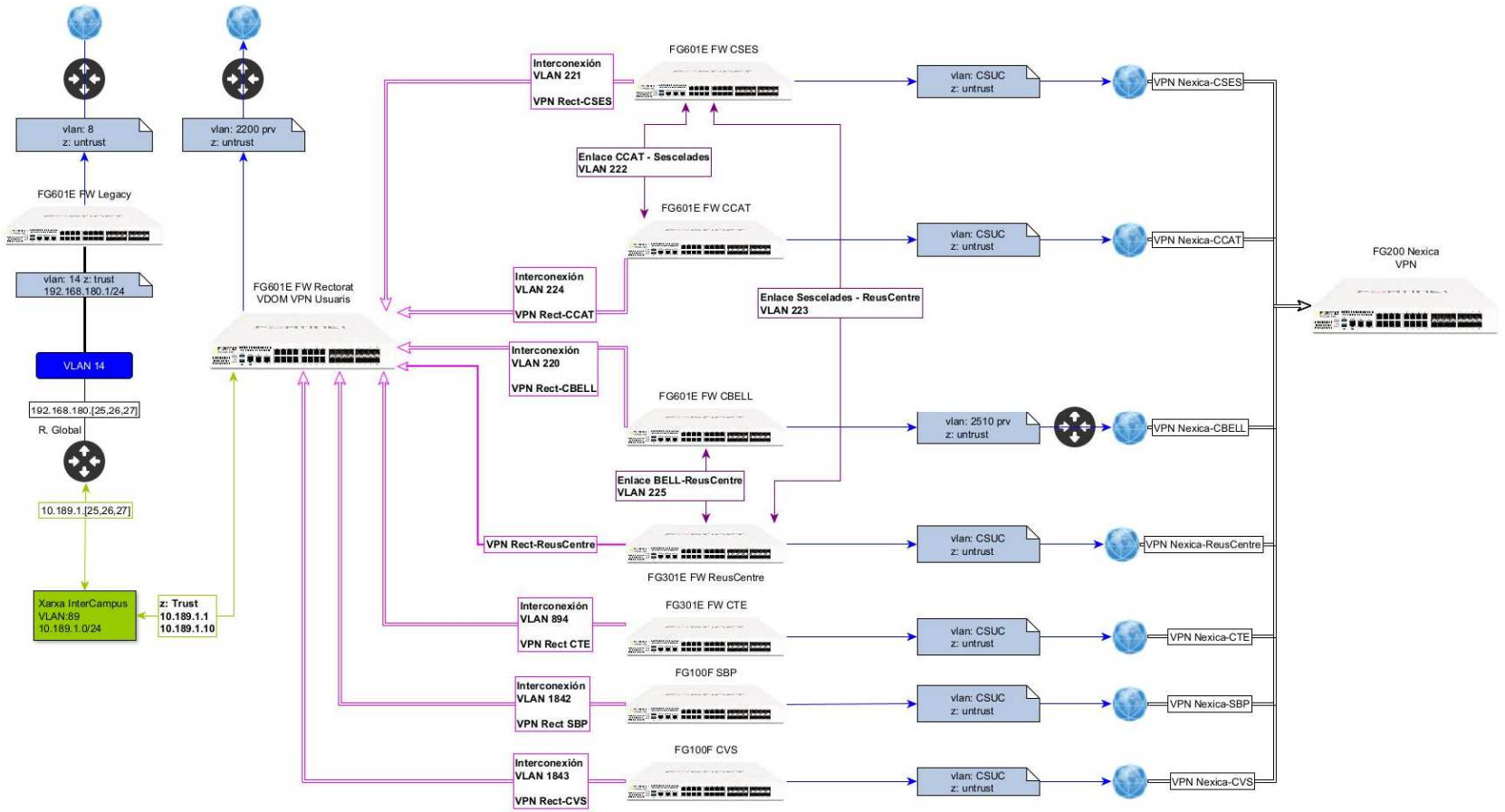
L5-7

L4

L3

L2

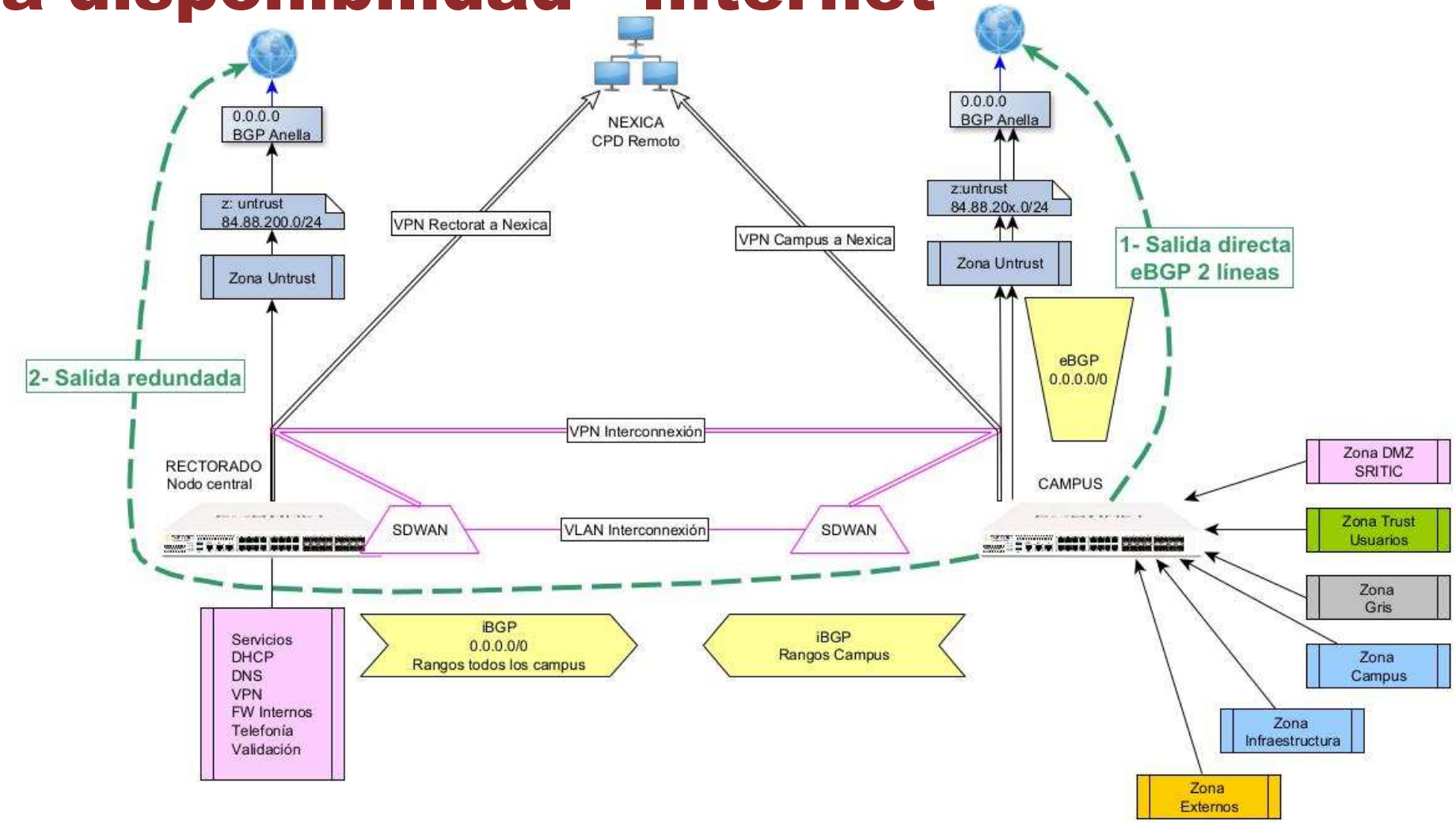
L1



Alta disponibilidad - Internet

- Mantenemos redundancia de acceso a l'Anella
  - eBGP - doble salida
- Mantenemos redundancia entre FW de campus
  - iBGP con el nodo central que publica 0.0.0.0/0
- Los FireWalls
  - Gestionan todo el protocolo BGP
  - Salida directa a internet (inspección L7)
- Nodo central rectorado
  - Aplica a su zona "SD-WAN" permisos de salida comunes (inspección L7)

Alta disponibilidad - Internet



Alta disponibilidad – Recursos internos

- Mantenemos redundancia interna
  - Modelo Hub – Spoke Nodo central -> Rectorado.
  - Entre FW de campus i nodo central. Conexión PaP + conexión IPSEC
  - iBGP con el nodo central -> publica 0.0.0.0/0 + redes de servidores + redes del resto de campus
  - iBGP des de los campus -> publican su rango interno + DMZ públicas locales
- Gestión
  - Los FW se encargan de gestionar todo el protocolo BGP
  - Aprovechando la funcionalidad de SDWAN, podemos utilizar siempre el mejor camino (pérdida, rendimiento, criterios de alto nivel) o agregar
  - Fácil añadir nuevas líneas.

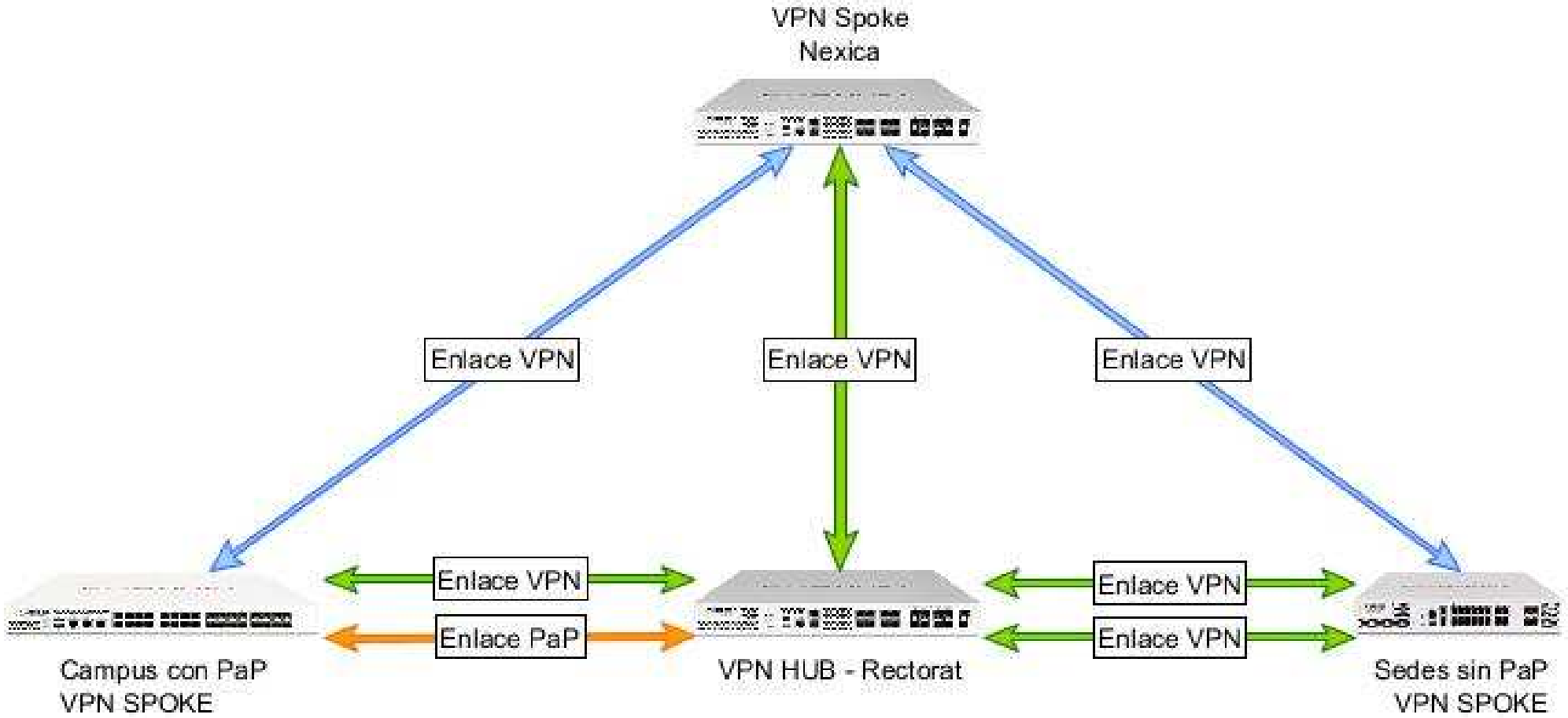
Alta disponibilidad – Recursos internos

- Sencillez
  - No hemos implementado una malla de todos contra todos.

  Hicimos un estudio del tipo de tráfico y diseñamos una solución adaptada. Hay que mantener un equilibrio entre redundancia y sencillez, ya que estas configuraciones son más robustas y más gestionables.
  - Es fácil añadir nuevos campus

  Implica el nodo central y la configuración local de campus (receta)
- Esta alta disponibilidad permite centralizar servicios esenciales DNS, DHCP, telefonía, validación, AD, etc…. Que no se replican en los campus

Alta disponibilidad – Recursos internos



Evolución

- Integración del CPD remoto como un nodo más del Campus (eBGP, VPN y SDWAN)
- Acabar de migrar las redes finales y dejar el core sólo con L3.
- Asignación de red por 802.1X
  - Eso ya es otra historia… pero “el modelo” se ha diseñado pensando en 802.1X

Cómo acabar una segmentación

- Hay dispositivos OT (cable y wifi), cada vez más, difíciles de migrar, no todos soportan DHCP e implica un gran esfuerzo humano.
- No siempre resulta fácil que los administradores de servidores cambien direccionamiento IP (licencias, desconocimiento, etc.).
- En los casos en los que no podamos migrar, utilizaremos técnicas de encapsulado de L2 en L3. No vamos a dejar VLANs ”planas” en la Universidad.
- Es recomendable tener una herramienta de IPAM. Hemos pasado de gestionar unas decenas de VLANs y direccionamientos IP a centenares.
- Todo es fácil hasta que llegamos a las redes de trabajadores
  - Requiere apoyo político y estrategia de comunicación… “vender el proyecto”.

La receta para “el éxito” ??

1. Tener el control de la red.
   - En la URV la gestión de la red está centralizada.
   - Ya venimos de un direccionamiento privado.
2. Buena sinergia Comunicaciones – Seguridad
   - Trabajamos codo con codo.
   - Respetamos las competencias pero nos permitimos intrusismo constructivo.
   - Diseño común, criterio único.
3. Libertad de decisión por parte de la dirección del SRITIC
   - “Los expertos sois vosotros”.

La receta para “el éxito” ??

El equipo….

Comunicaciones

Seguridad

Imposible llevar a cabo el proyecto sin la inestimable ayuda de

- Técnicos de campus y técnicos de docencia.
- El soporte e implantación del diseño del core por parte de nuestro integrador.
- La ayuda y seguimiento continuo del fabricante.

Conclusiones

- El modelo de funcionamiento Comunicaciones – Seguridad por separado está obsoleto? O es que somos los raros?
  - En nuestra Universidad, la buena sintonía entre las áreas de seguridad y comunicaciones han facilitado mucho la evolución.
- Todos los equipos de comunicaciones de la Universidad se gestionan desde el FW, lo que permite tener una visibilidad antes impensable.
  - FW como controlador de los conmutadores
  - FW como controlador del wifi
- Integramos la red cableada, el WIFI y la Seguridad en un “fabric”. Simplifica la gestión e integra toda la información.

Conclusiones (II)

- Qué tiene de nuevo este proyecto?
  - El FW es el nuevo CORE de la red. Gestiona Conmutadores, VLANs, AP's, 802.1X, rutas (iBGP, eBGP), logs, …
  - Gestión de la red desde un FW: Cómo es nuestra experiencia
  - REST API: El soporte de APIs de forma nativa ha simplificado mucho la gestión de la arquitectura. Por ejemplo hemos desarrollado una aplicación para distribuir ACLs (política de uso razonable) a todos los switches de forma centralizada:

    https://github.com/oriollorenzo/FortiSW-PolicyManager