USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

ÁREA DE TECNOLOXÍAS DA INFORMACIÓN E COMUNICACIÓNS (ATIC)

Despliegue de un CPD virtual en Azure, Universidade de Santiago de Compostela

Antonio Pérez Casas,
Responsable da unidade de rede da Área TIC da USC
Xosé Antonio Rubal López,
Responsable de Proxectos Institucionais da USC

AGENDA

- Punto de partida, objetivos y casos de uso
- Descripción de la nueva red
- Despliegue de la red
- Siguientes fases

Punto de partida

- La USC dispone de un CPD local (on-premises) tradicional
- Servicios:
  - Comunes: DNS, identificación, monitorización, copias,...
  - Básicos: almacenamiento, cómputo, bases de datos,...
  - De aplicación: servidores de aplicaciones, web,...
- Orientado fundamentalmente a servicios básicos a alumnado, personal docente y servicios administrativos y de gestión
- Algunos servicios importantes ya están en la nube: Office 365 para toda la comunidad, aplicación de RRHH, etc

Nuevas necesidades

- Introducción de nuevas tecnologías de despliegue de aplicaciones: contenedores, gestores de bases de datos, etc.
- CPD de respaldo
- Nuevas prestaciones para centradas en el servicio a la docencia y la investigación: aulas virtuales, recursos de computación para grupos, etc.
- Opciones: ampliar el CPD o utilizar un proveedor de computación en la nube?

Microsoft Azure

- Elegimos Microsoft Azure por razones:
  - Económicas: condiciones para suscribir un Enterprise Agreement para las universidades
  - Tecnológicas: modelo claro de infraestructura como código
  - Organizativas: personal y recursos para implementar y mantener nuevos servicios
- Primeros casos de uso:
  - Azure Devops para proyectos de desarrollo: gestión de integral del proyecto, repositorios de código y entorno CI/CD
  - Entorno QA implementado como clúster de Kubernetes (AKS)
  - Prototipos de aulas de docencia virtuales (Azure Labs Service)
  - Nuevo sitio web de la USC
  - Despliegue de aplicaciones con necesidades especiales: GIS Esixe

Proyecto CD-USC-Azure

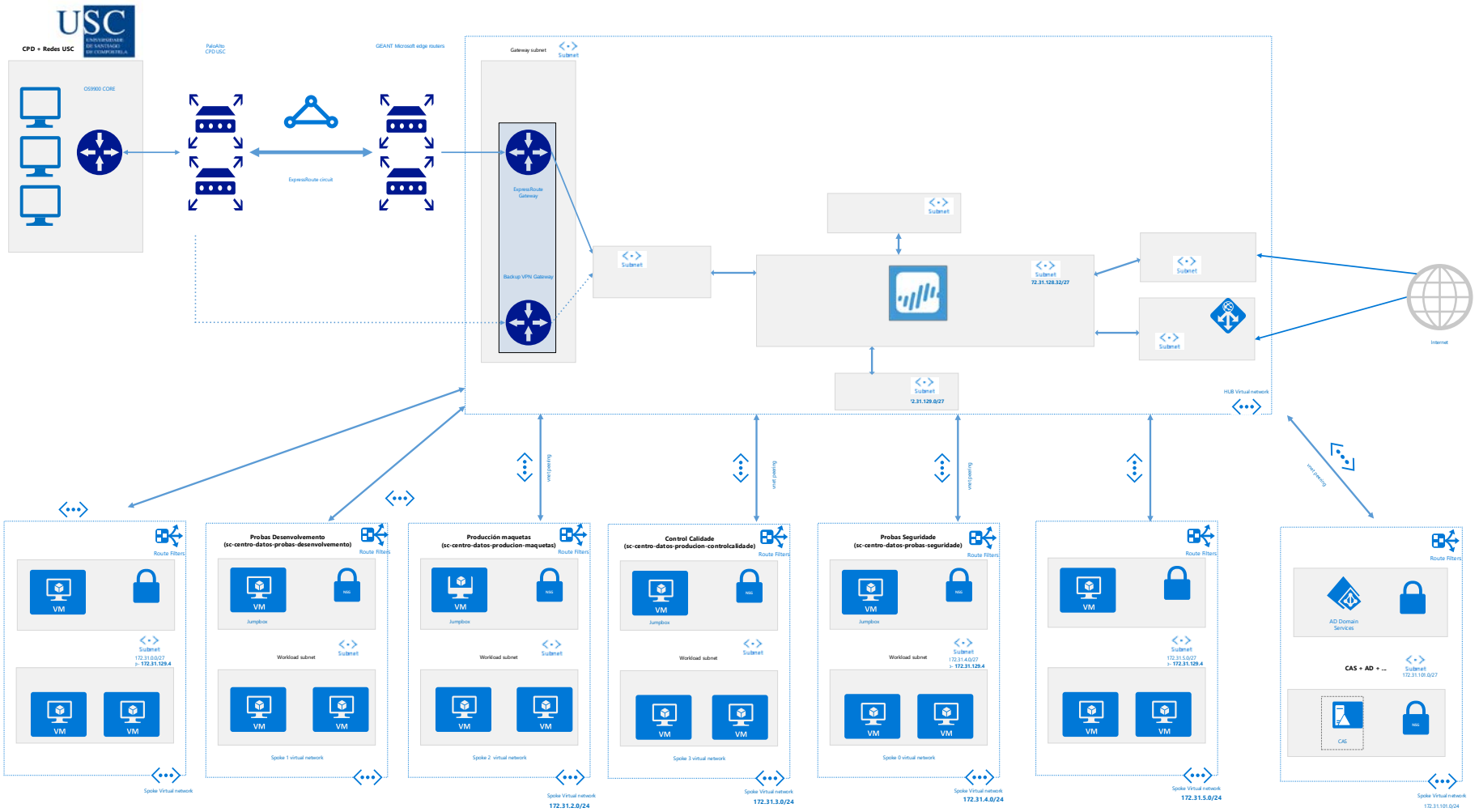
- Objectivo: definición e implementación del Centro de Datos de la USC en Microsoft Azure
- Fases:
  - Formación de los responsables de unidades del área TIC
  - Definición de la arquitectura y prácticas de gobierno
  - Formación de los técnicos de sistemas y desarrollo
  - Implementación y puesta en marcha de la infraestructura básica
  - Despliegue de los casos de uso iniciales

Elementos desplegados en la nube

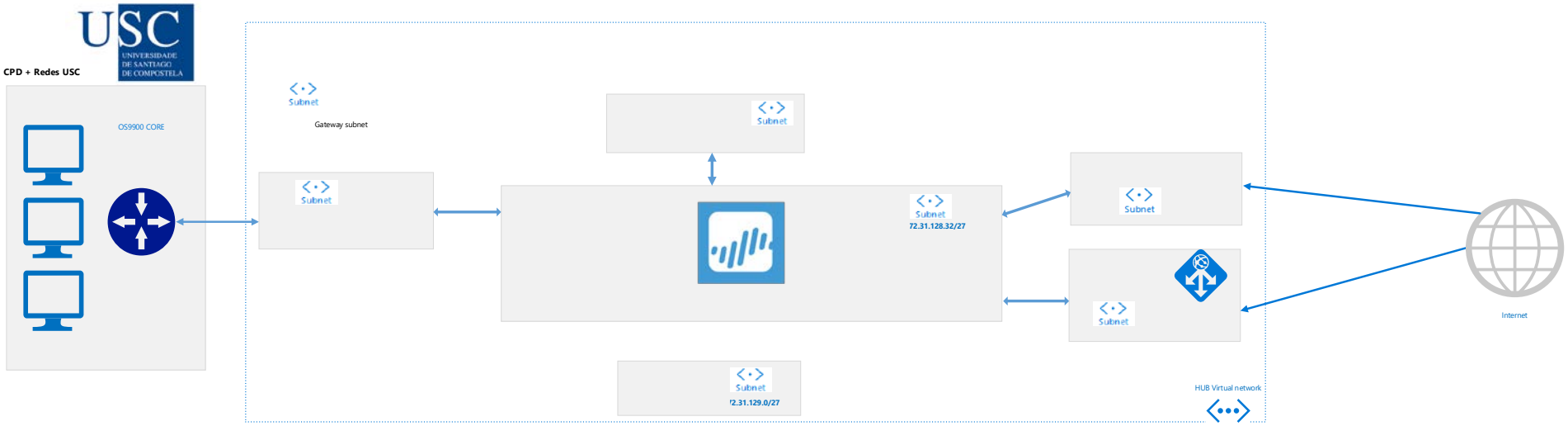
- Nodo central (Hub) con cuatro zonas: Hub centralizado, zona de proyectos, zona de interconexión con CPD local y zona de acceso a internet y Azure Público (SaaS, PaaS)

  - Spoke Hub
  - Spoke recursos compartidos
  - Spokes Proyectos
  - VPN y Express Route
  - Firewall Palo Alto
  - Application Gateway y SNAT
  - Siguientes fases

Esquema general CPD USC en Azure

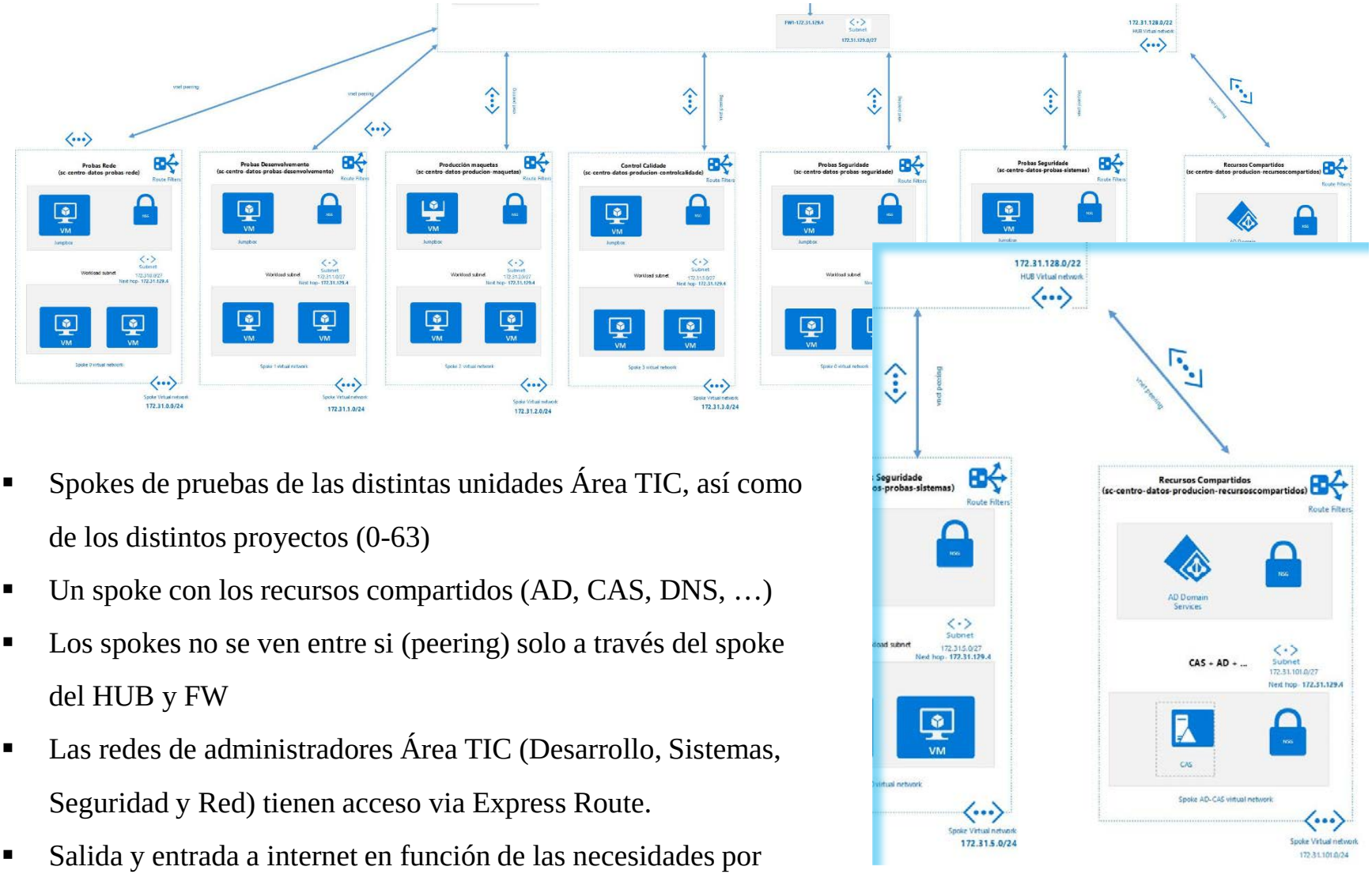


Spoke Hub



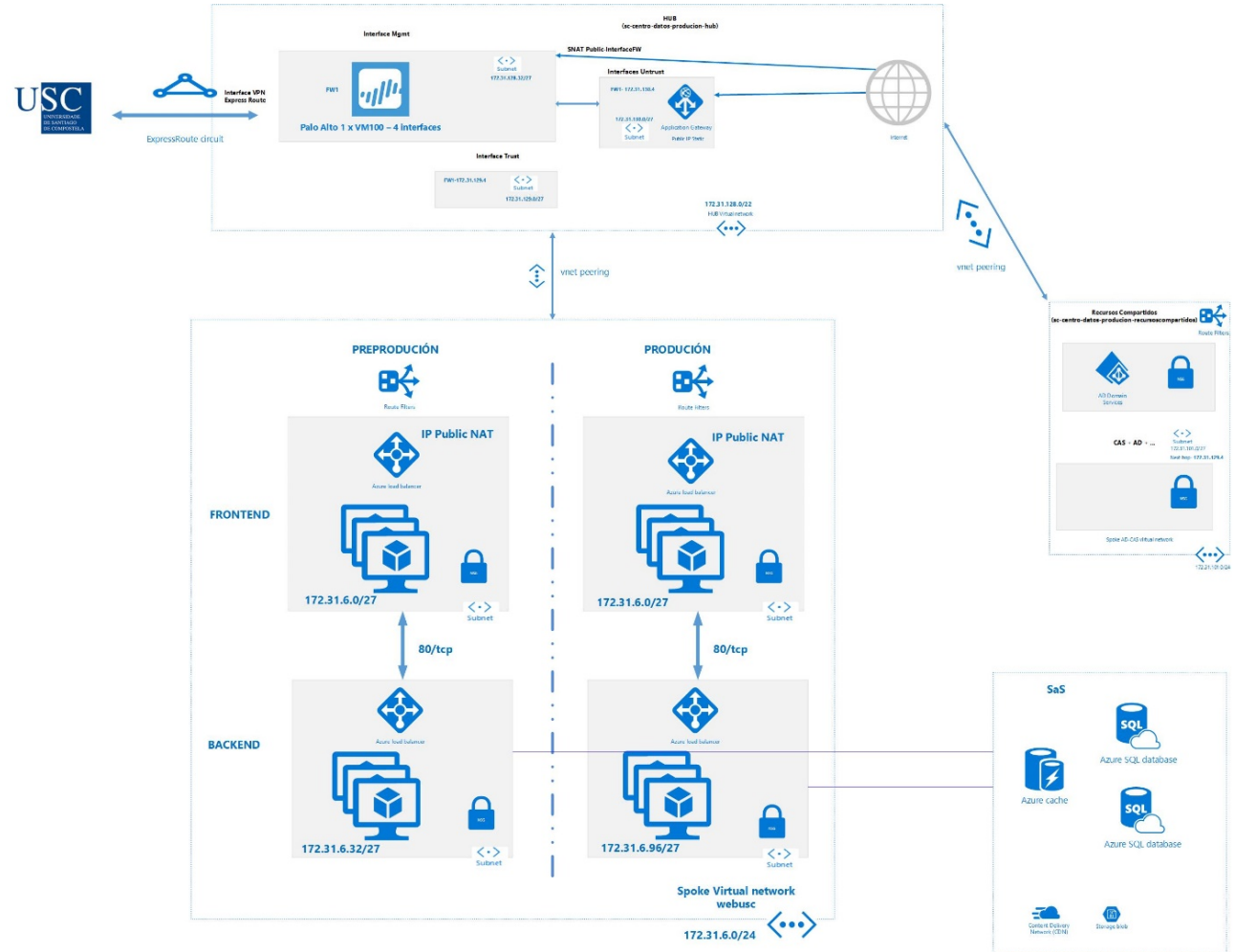
- Elemento principal un NGFW VM-100 de PaloAlto (esta previsto despliegue en HA)
- Zona de interconexión al CPD y red local de la USC con VPN y Express Route
- Una zona confiable (Trust) a los spokes de los diferentes proyectos/servicios)
- Una zona para la salida/entrada a internet y/o direcciones públicas de Azure (Untrust)
- Un interface de gestión do FW (MGMT)
- Direccionamiento amplio /22 y reparto de IP´s por zonas (muy importante prever todas las necesidades futuras)

Spokes de proyectos y servicios



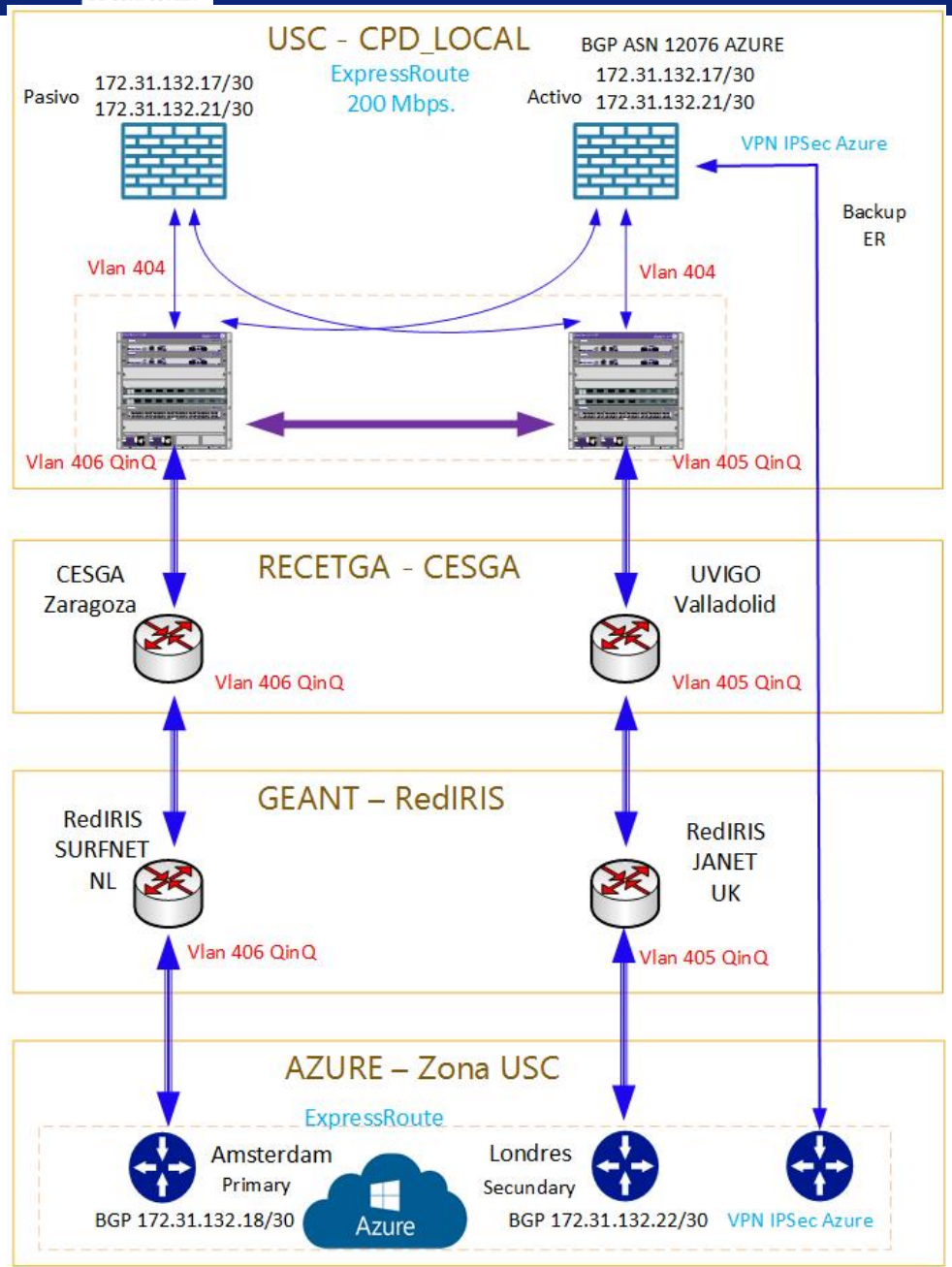
- Spokes de pruebas de las distintas unidades Área TIC, así como de los distintos proyectos (0-63)
- Un spoke con los recursos compartidos (AD, CAS, DNS, …)
- Los spokes no se ven entre si (peering) solo a través del spoke del HUB y FW
- Las redes de administradores Área TIC (Desarrollo, Sistemas, Seguridad y Red) tienen acceso via Express Route.
- Salida y entrada a internet en función de las necesidades por proyecto.

Spoke web-usc



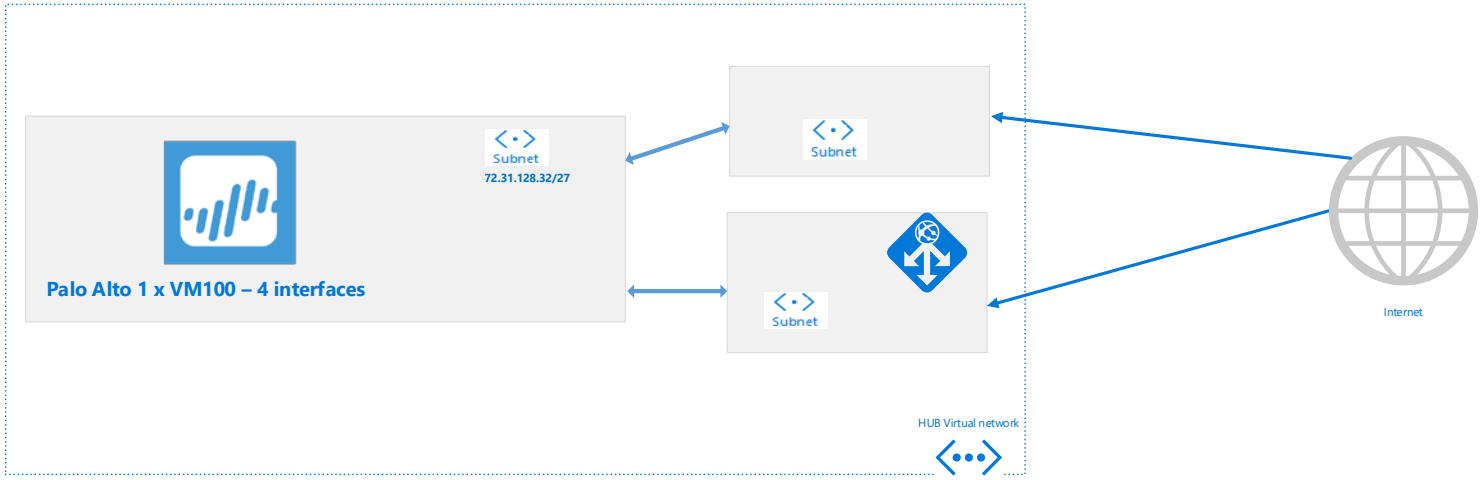
- Nueva web de la USC (4T 2019), realizada en DRUPAL 8
- Zona de preproducción y zona de produción
- Configuración Frontend + Backend
- Balanceadores para escabilidad en función de la demanda
- Acceso a Bases de Datos, Backups y outros servicios de Azure
- Acceso parcial a partes de la web actual en el CPD local de la USC mediante conexión seguras Express Route
- Acceso Microsoft Storage mediante “service endpoints” (config. en la virtual network)

Express Route + VPN IPsec



- Express Route USC-CESGA-REDIRIS-GEANT-AZURE (200 Mbps. redundados)
- Configuración básica QinQ, BGP, puertos cruzados para HA nos FW
- Pruebas de ancho de banda -> 200 Mbps.
- Pruebas de convergencia < 5 seg.
- Monitorización en puerto local de los equipos de Alcate-Lucent OS9900
- Entre 7-14 días de despliegue y pruebas (agradecimiento al CESGA, RedIRIS y GEANT)
- VPN IPsec USC-Internet-AZURE
- Pruebas de convergencia < 15 seg.

Zona Untrust - Internet



- Zona Untrust para interconectar con internet y redes públicas de Azure
- Configurado un Application Gateway de Azure para recoger peticiones http y https
- Configuradas numerosas SNAT para entrada de tráfico de internet al margen del AG
- Debido a las aplicaciones SaaS tuvimos que realizar mas SNAT de los inicialmente previstos
- Confusa la configuración SNAT. Crear IP Pública Azure, crear segunda IP privada Azure en el interface del FW y asociarlas en Azure. En el FW asociar la IP privada del HUB con la IP privada del servidor en el spoke correspondiente.

Elementos Azure network CPD USC

Virtual Network
Spoke
SubNet
Peering

Azure load balancer

Express Route
VPN IPSec

Application Gateway

AD Domain Services

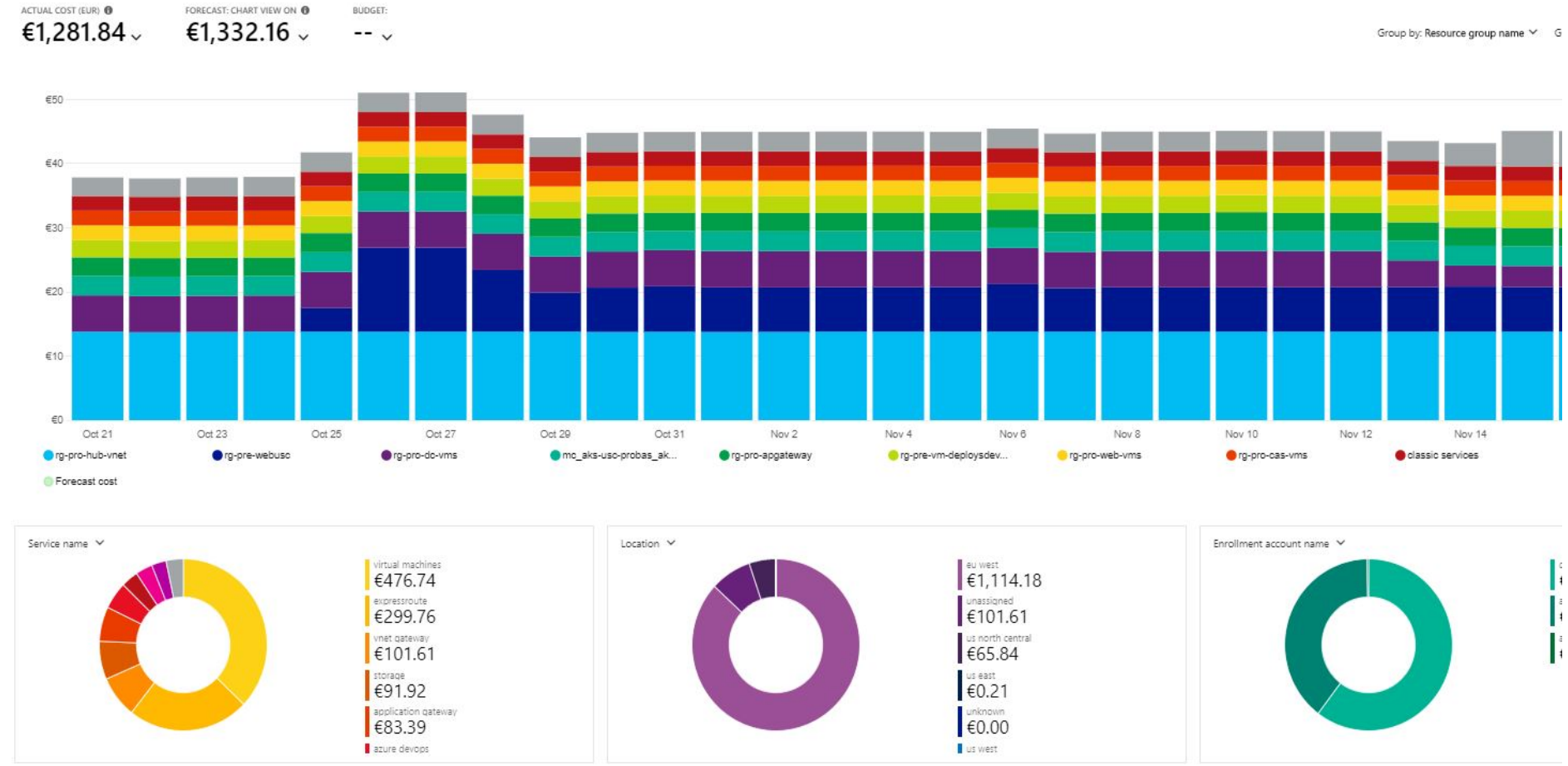
Route Filters
NSG (Network Security Group)

DNS Servers

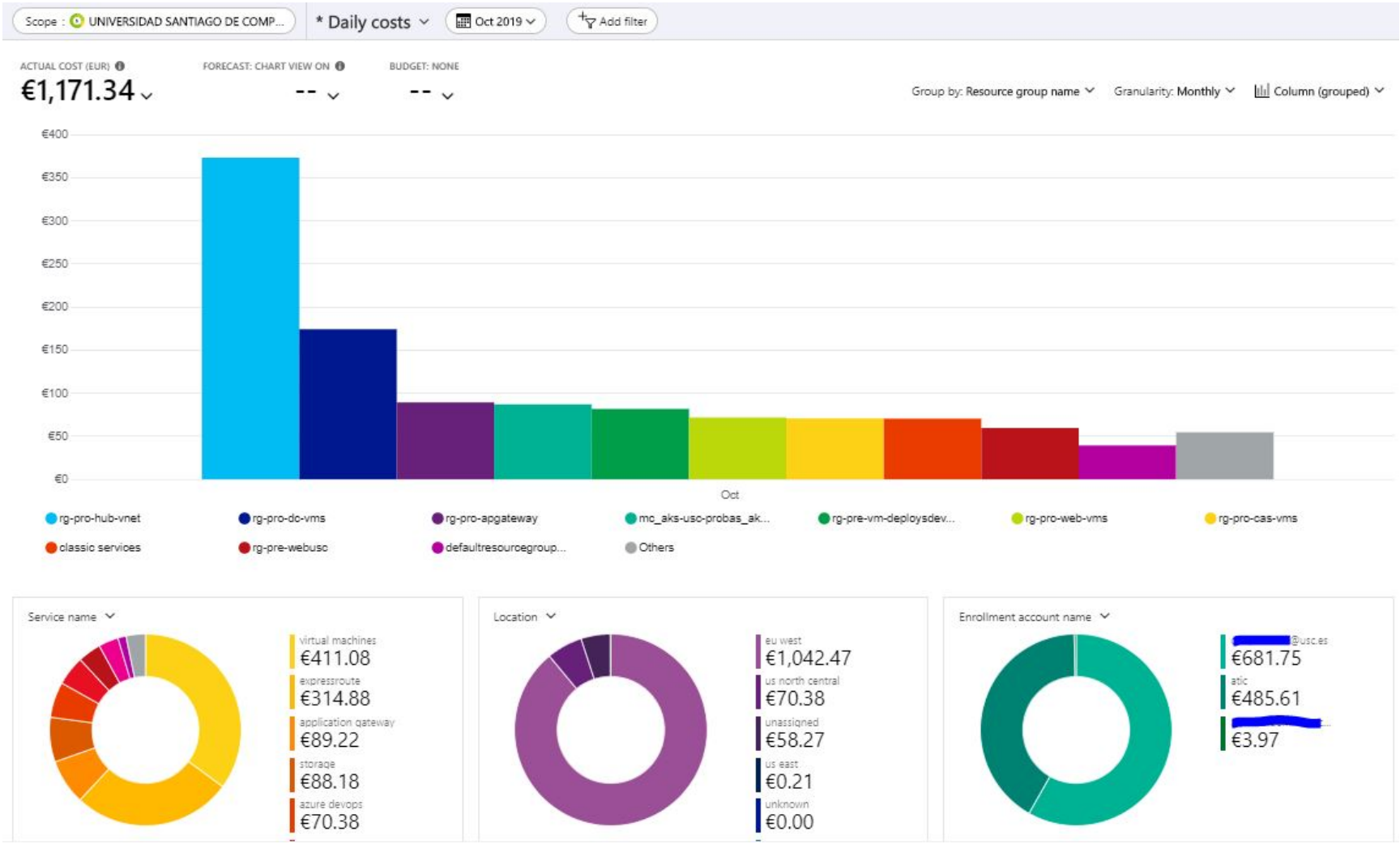
Palo Alto (NFG)

CAS – Control de Acceso

Coste básico CPD USC en Azure



Coste básico CPD USC en Azure



Express Route 314,88 €/mes
Vnet Gateway 58,27 €/mes
Application Gateway 89,22 €/mes
FW PaloAlto VM-100 (subs. 3 años) 120 €/mes

Conclusiones

- Definir inicialmente el posible el escenario completo, posteriormente algunos cambios que en otros entornos son sencillos en este entorno obligan a rehacer varios elementos, planificar direccionamiento IP generoso
- Muy importante la documentación, nomenclatura, procedimientos, … permite distribuir las tareas tanto internamente como externamente pero precisa mucho orden y documentación
- No hay una configuración única, si quieres un CPD IaaS esta puede ser adecuada, pero si tienes mucho SaaS pueden existir otras configuraciones
- Ojo con las direcciones públicas de los servidores si se activan no pasan por el Hub y pierdes el control
- En muchos casos debes permitir el tráfico exterior a las zonas pública de Azure, listados detallados y actualizados periódicamente en: https://docs.microsoft.com/es-es/azure/azure-portal/azure-portal-safelist-urls
- Múltiples soluciones como los services endpoint, simplifican ciertas conexiones con Servicios Azure, pero precisan añadir seguridad adicional en los extremos
- Despliegue muy rápido, todos los elementos a golpe de click

Futuro

- Establecer un modelo de operación para el CD-USC-Azure: contratación y operación por terceros.
- Proyectos a corto plazo:
  - Clúster Kubernetes de producción:
    - Migración de aplicaciones con altas necesidades de disponibilidad
    - Despliegue de nuevas aplicaciones
  - Copias de seguridad del CPD local
  - Entornos de prácticas en la nube
  - Recursos de computación para los grupos de investigación
  - Virtualización del puesto de trabajo
- Evaluar la migración de servicios del CPD local

Muchas gracias,

Antonio Pérez Casas
Responsable da rede de datos Área TIC
antonio.perez.casas@usc.es
Xosé Antonio Rubal López
Responsable de Proxectos Institucionais
xoseantonio.rubal@usc.es