



Captura de trafico en redes industriales para analisis con sondas de OT

Alex Lopez

Iberia Sales



Corporate Overview



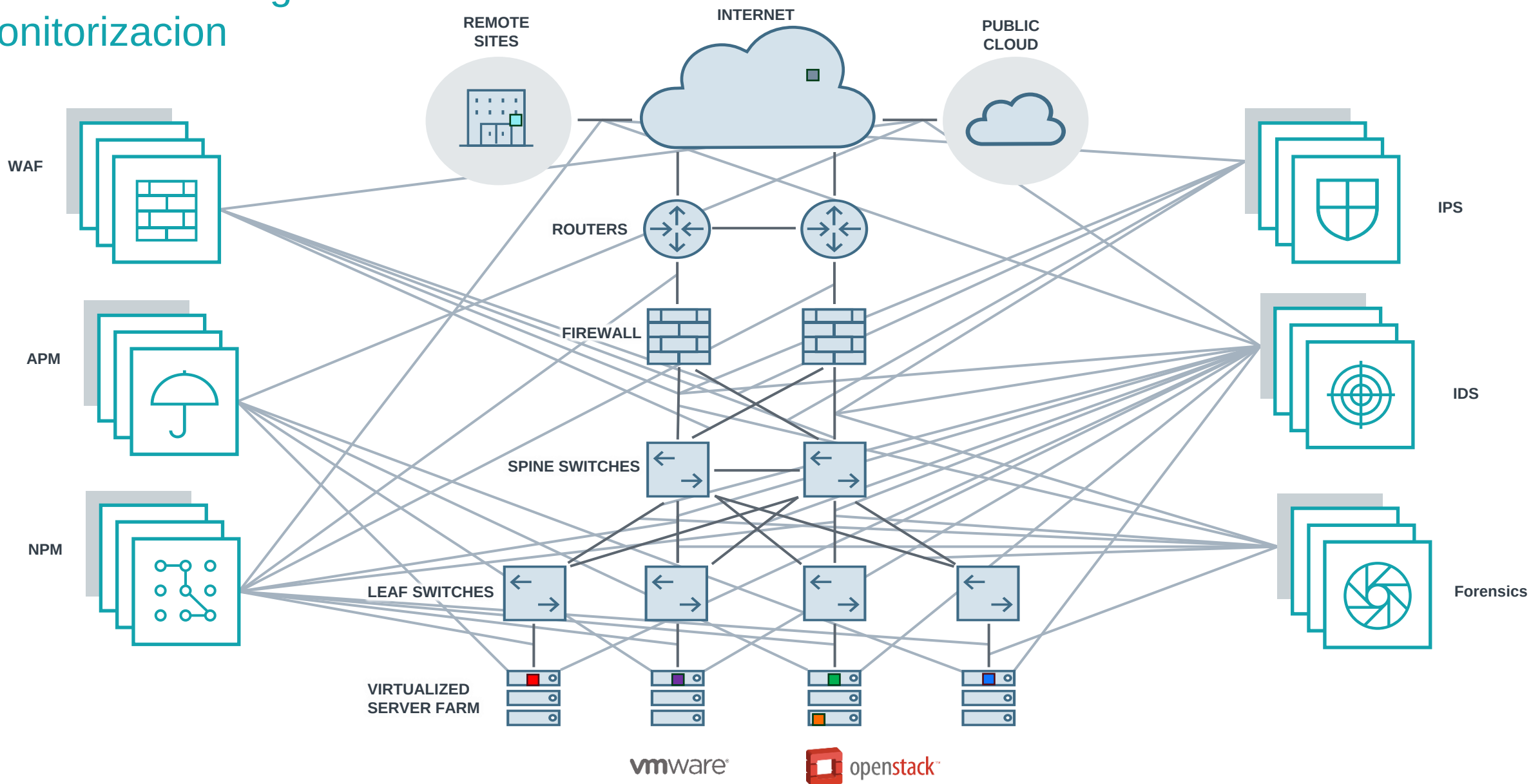
THE ESSENTIAL ELEMENT OF YOUR SECURITY

Gigamon is leading the convergence of networking and security. Our next generation network packet broker helps make threats more visible, deploy resources faster and maximize performance.

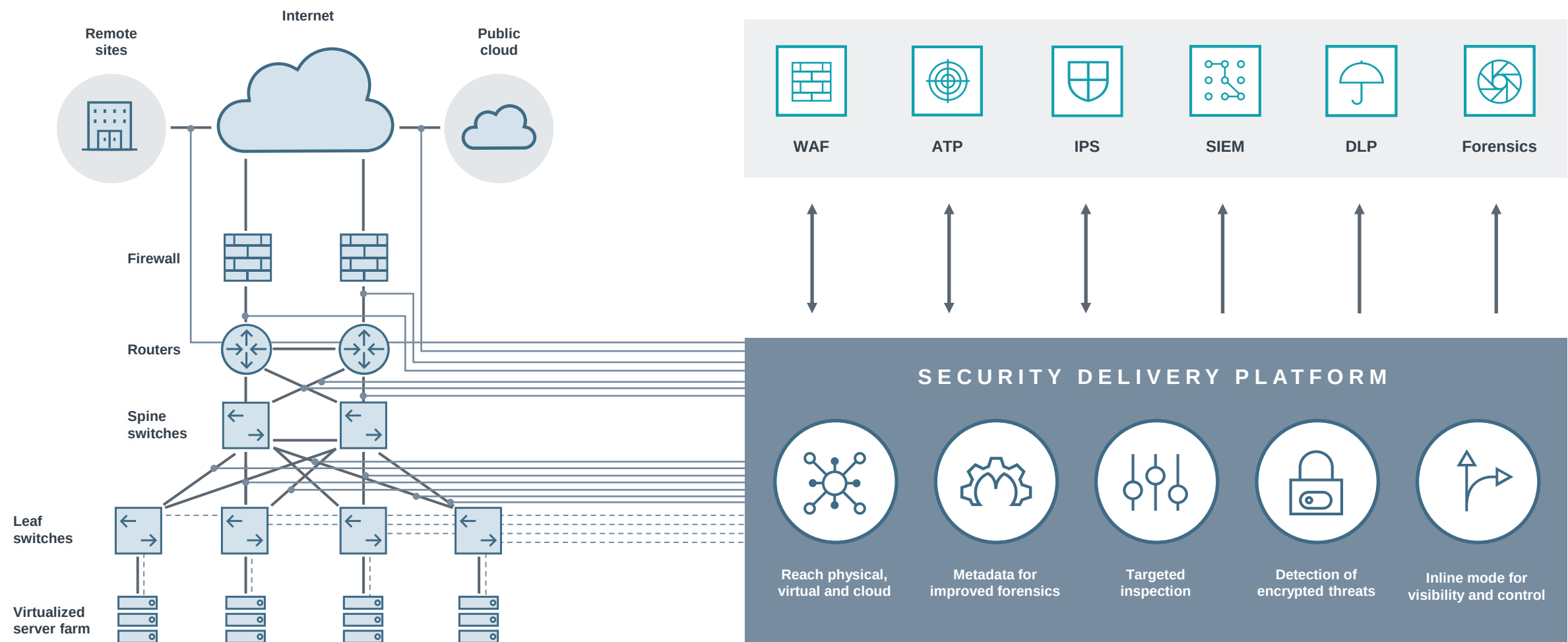
HQ Santa Clara California, USA	FOUNDED 2004	EMPLOYING 1000 employees	SERVING Over 2,800 customers	NAMED Market leader
GLOBAL OFFICES 20 countries	CEO Shane Buckley	PATENTS 51 Global patents issued	VERTICALS Public Sector Financial Services Healthcare Retail Technology Service Providers	

*Fév. 2018 : Informations sur les bureaux, employés et brevets
**T1 2018 : Nombre de clients

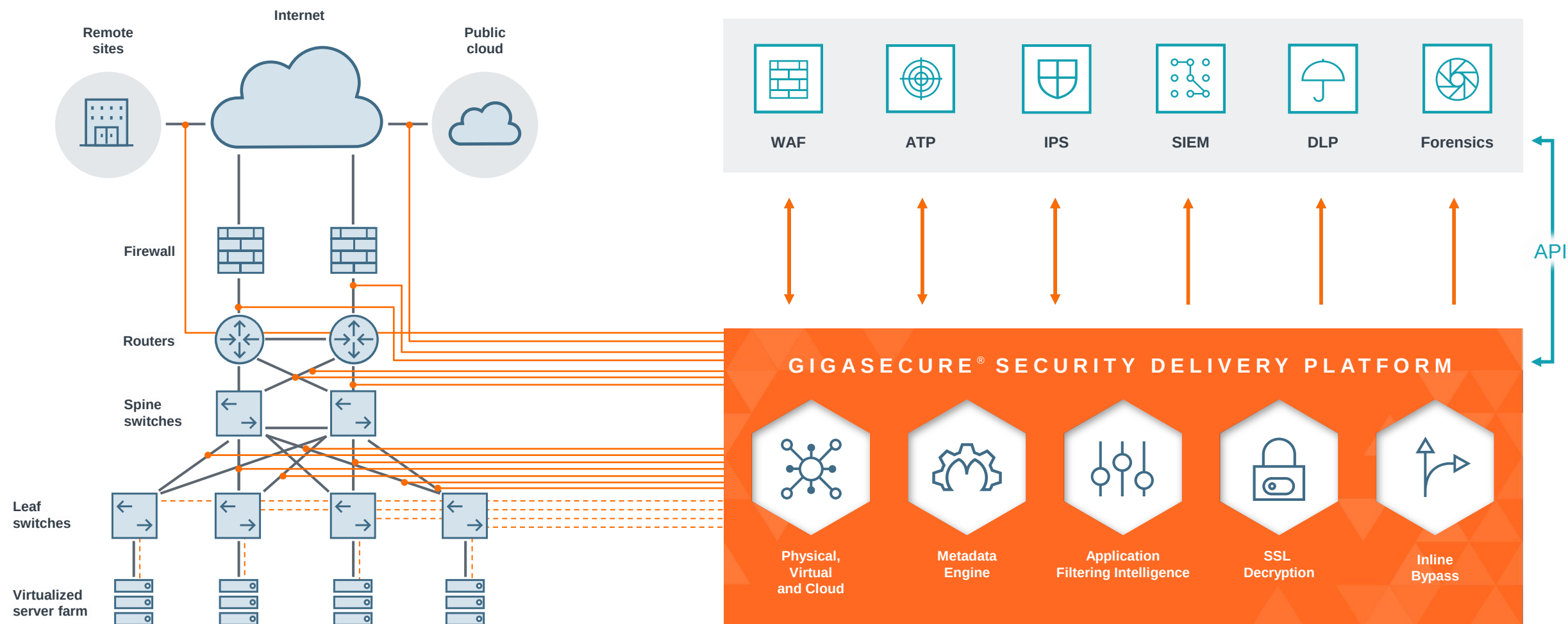
Retos en los despliegues de soluciones de seguridad & Monitorización



Network Packet Brokers



Ingenieria de trafico en los NPBs



Arquitectura Fuera de Banda: TAPs

TAP – Test Access Port

Realizan un copia EXACTA de todo el trafico

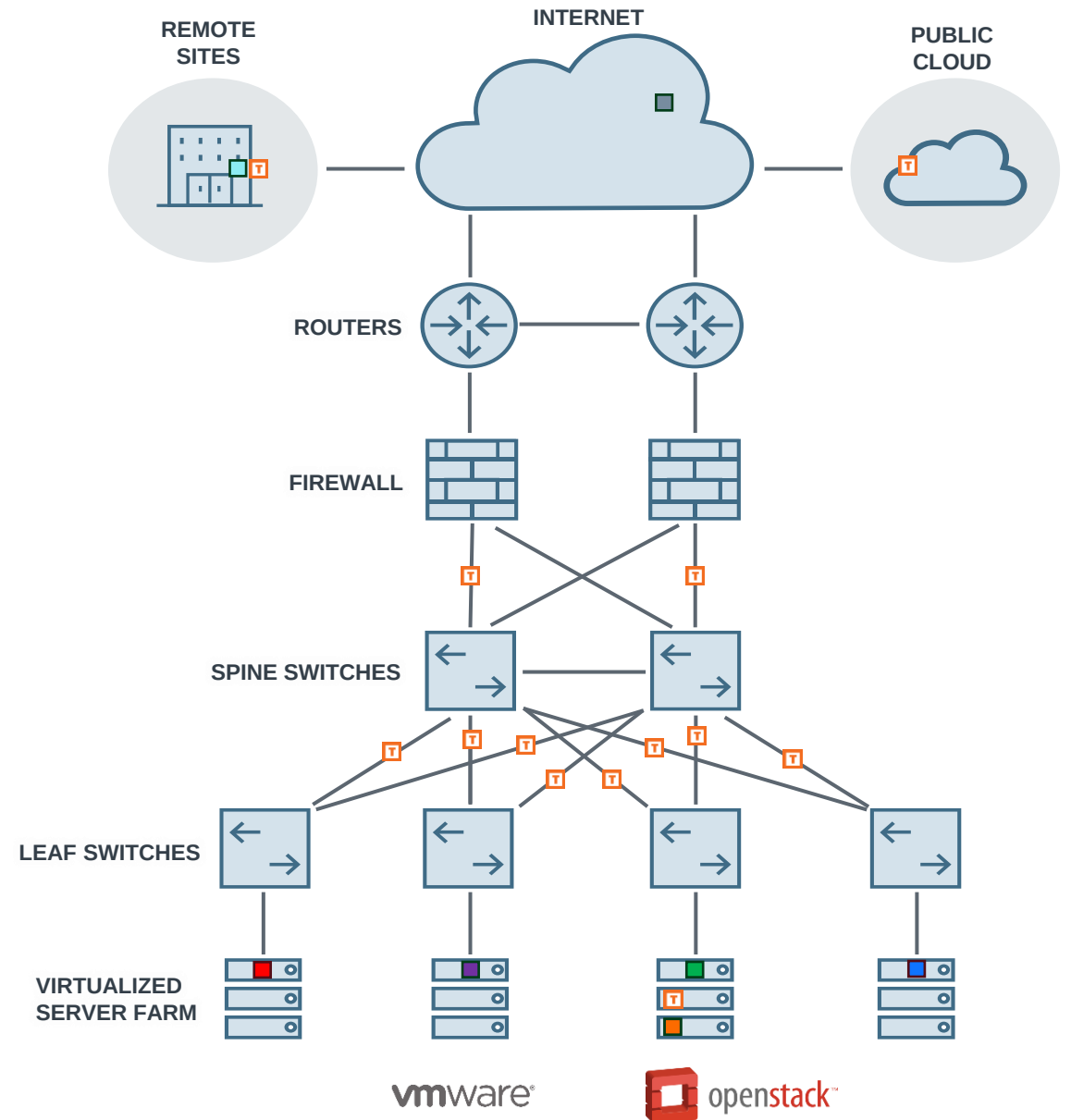
De un enlace de 1Gb bidireccional, sacan 2 enlaces de 1Gb

Fisicos:

- Fibra (1g/10g/25g/40g/100g)
- Cobre

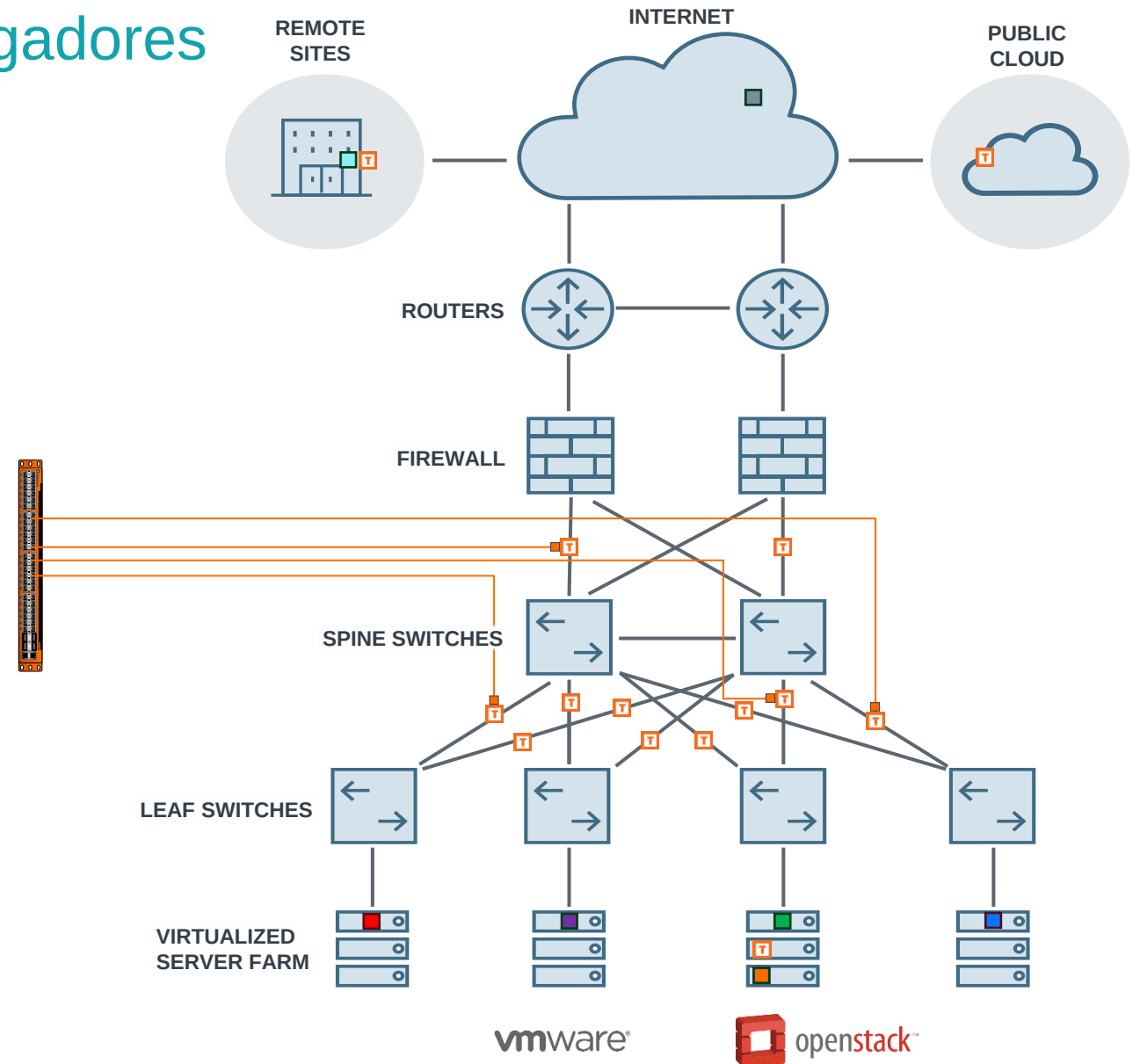
Vituales

- AWS
- Azure
- VMWare
- OpenStack
- Nutanix
- Anycloud (GCP, Oracle..)
- Kubernetes



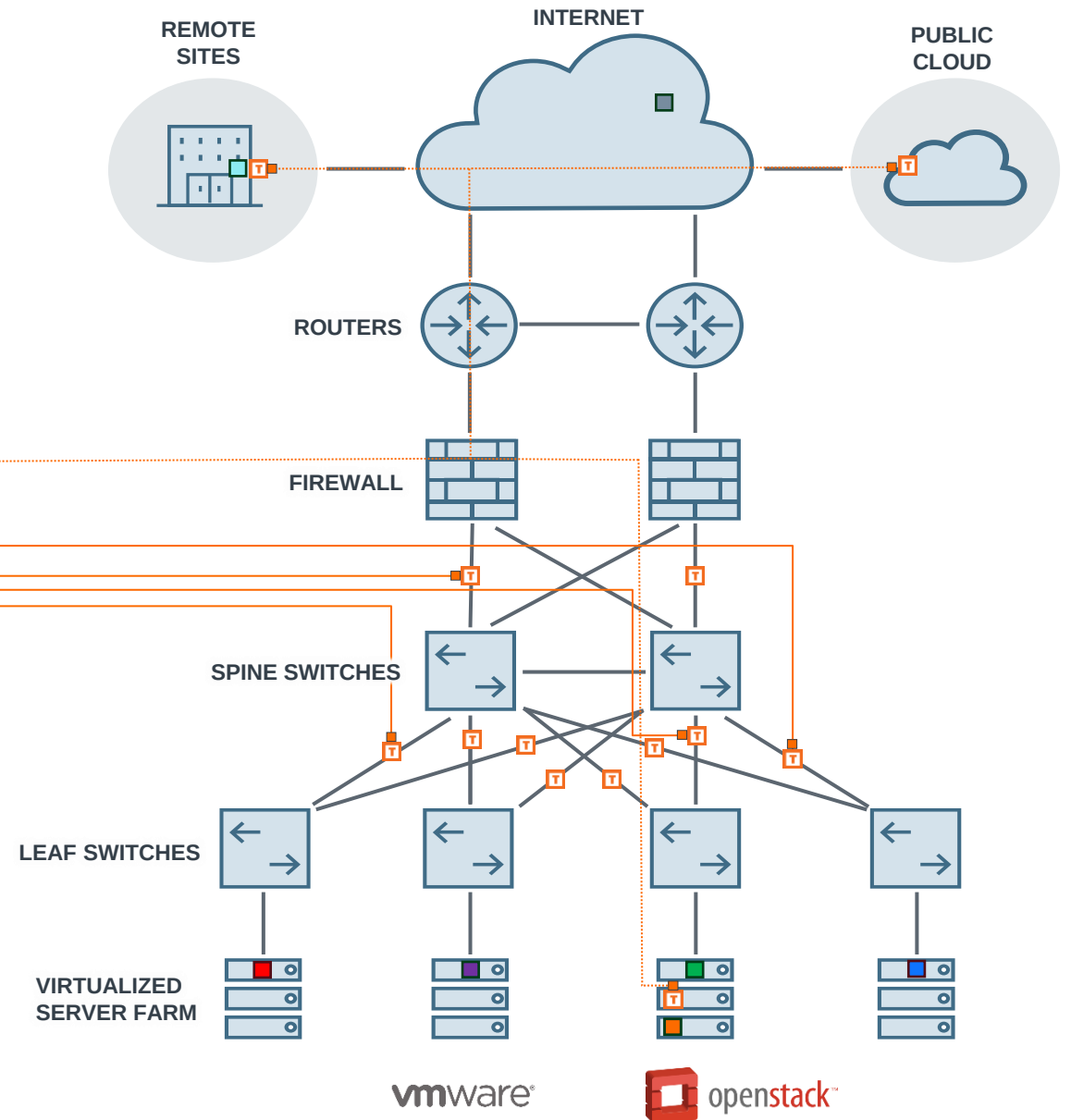
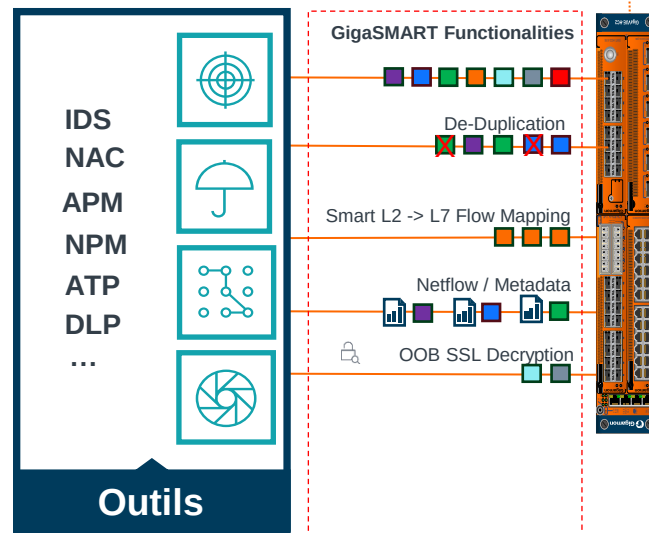
Arquitectura Fuera de Banda: Agregadores

- Agregan enlaces provenientes de los TAPs en otro de mayor capacidad y mayor utilización
- Opciones de 1Gb/10Gb/25Gb/40Gb/100Gb
- Soporte de cualquier tipo de interfaz via sfp/sfp+/qsfp...
- Filtrados L2/3/4
- Desencapsulado
- Terminacion de tuneles



Arquitectura Fuera de Banda: NPBs

- Reciben el trafico de los agregadores y lo entregan a las herramientas de monitorizacion & visibilidad
- Son los equipos encargados de realizar la ingenieria de trafico previa a la entrega a las herramientas:
 - Deduplicacion
 - Filtrado por Aplicacion
 - Cifrado/descifrado de SSL
 - Generacon de Metadatos
 - Eliminacion de cabeceras
 -



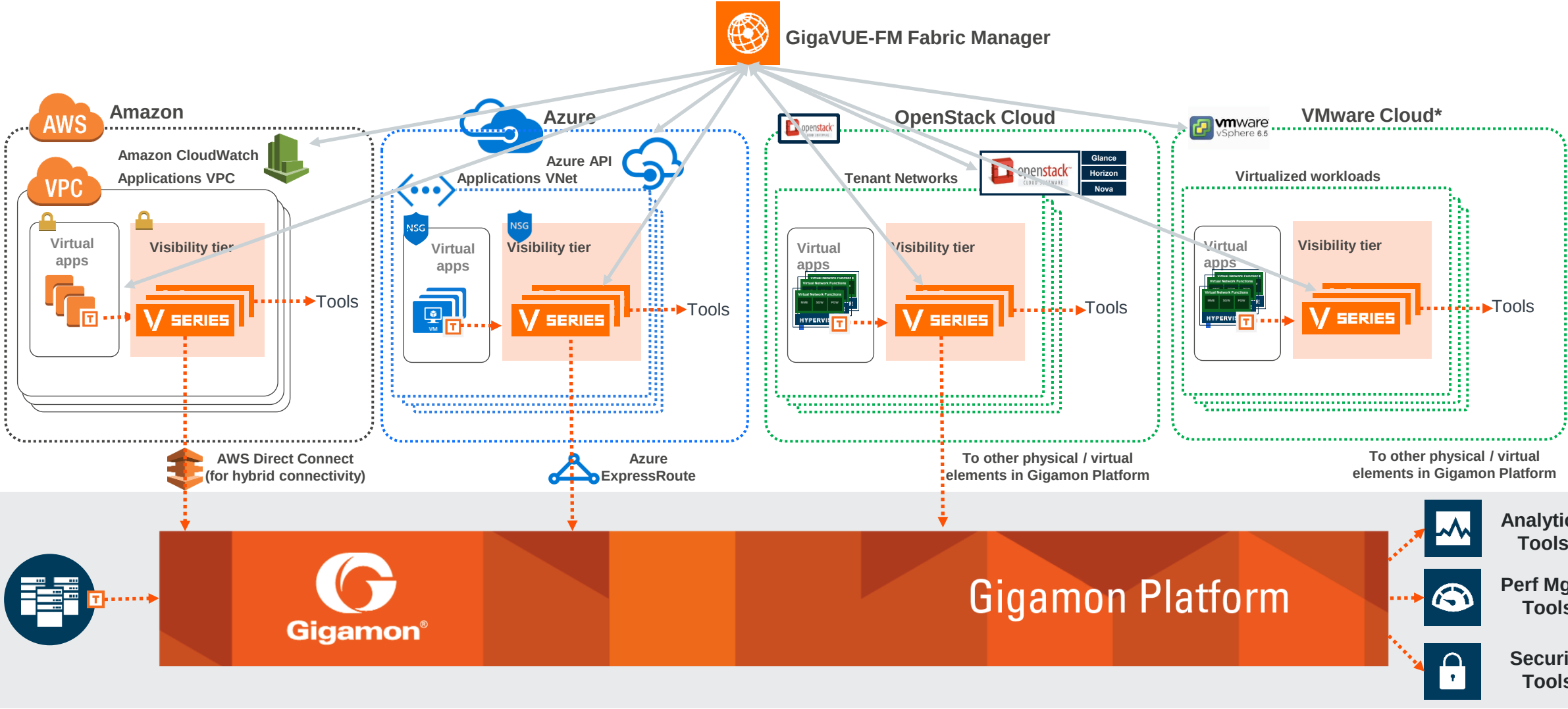
Configuracion para CPD



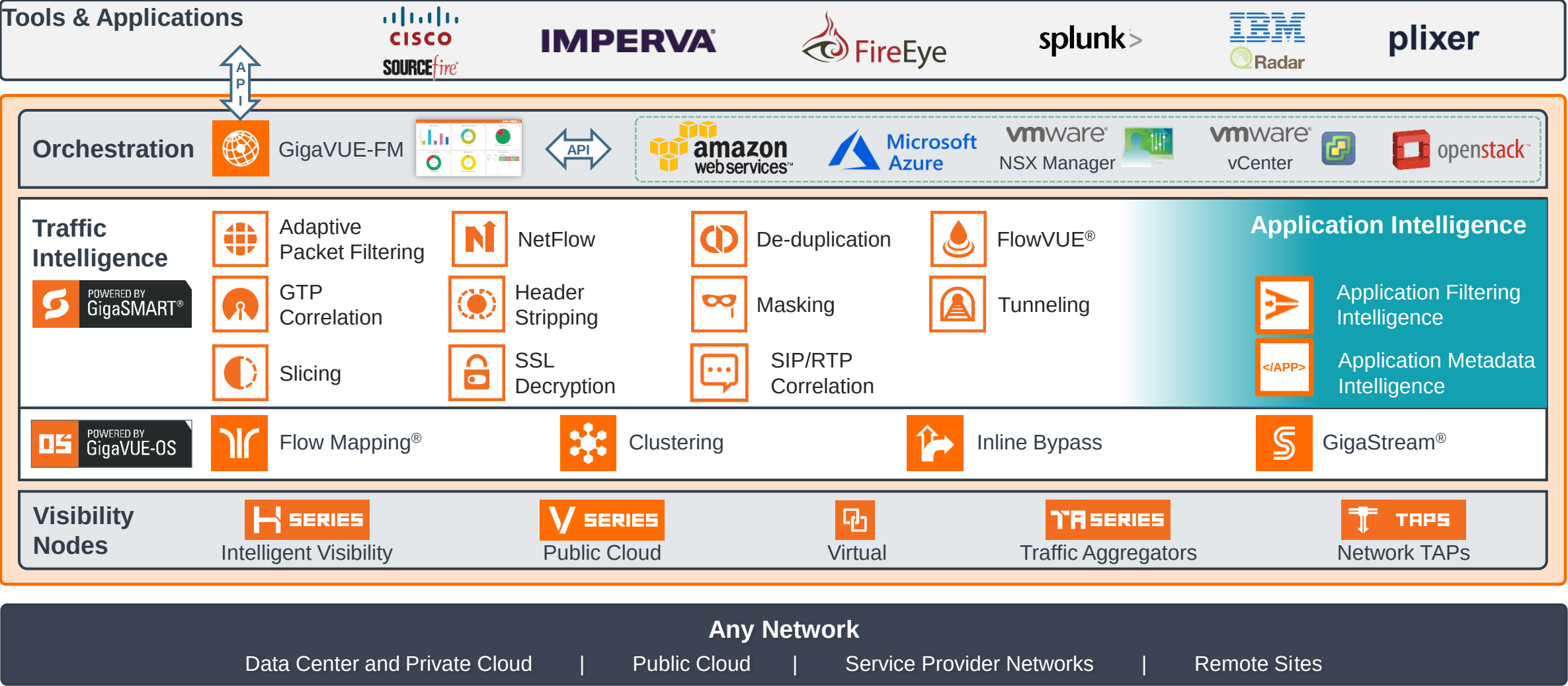
Configuración “mini” para sedes remotas



Arquitectura NPB Virtual



Funcionalidades de ingenieria de trafico

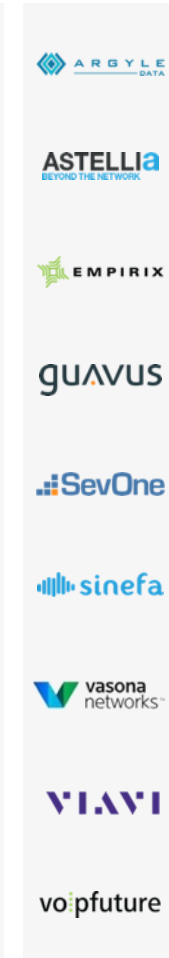


Gigamon Ecosystem Partners

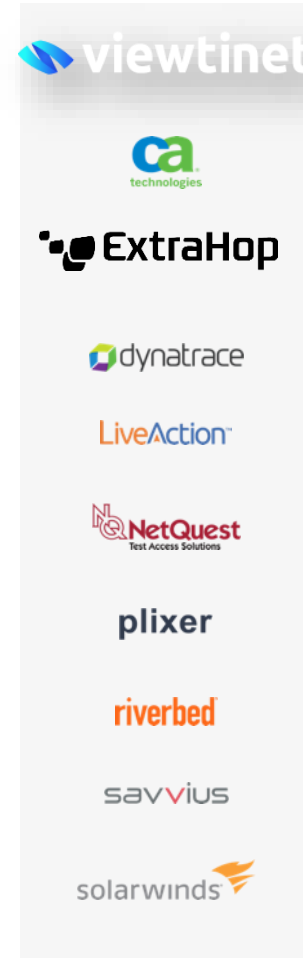
Security and Vulnerability Management



Service Provider



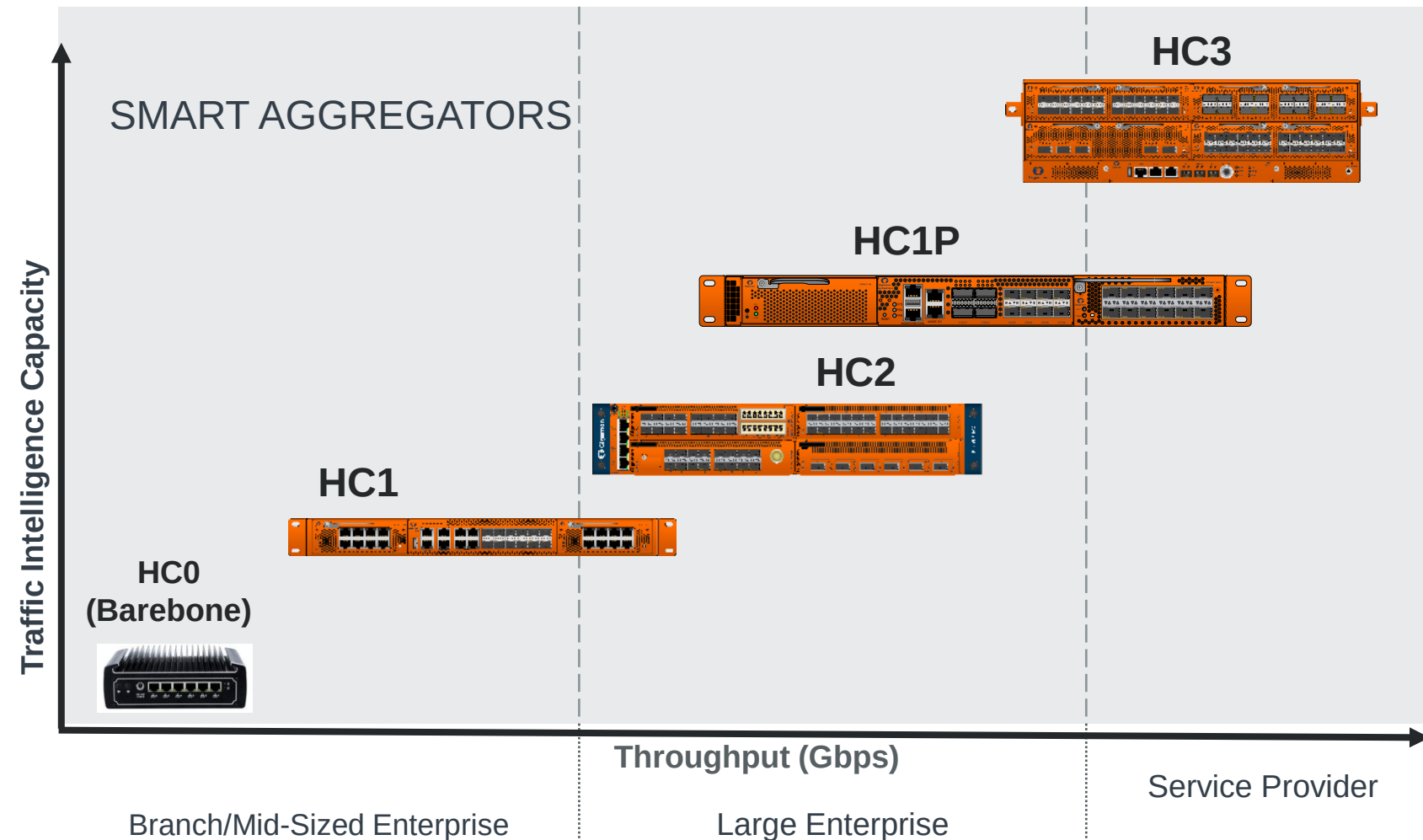
Performance Management



Infra-structure



Portfolio

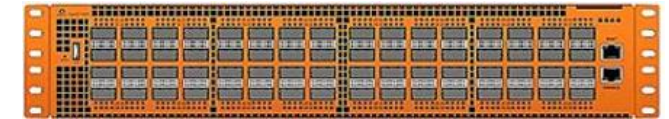


GigaVUE-FM
Appliance or VM

Traffic aggregator



GigaVUE-TA25



GigaVUE-TA200



GigaVUE-TA400

TAP



Serie A



Serie M



Serie G

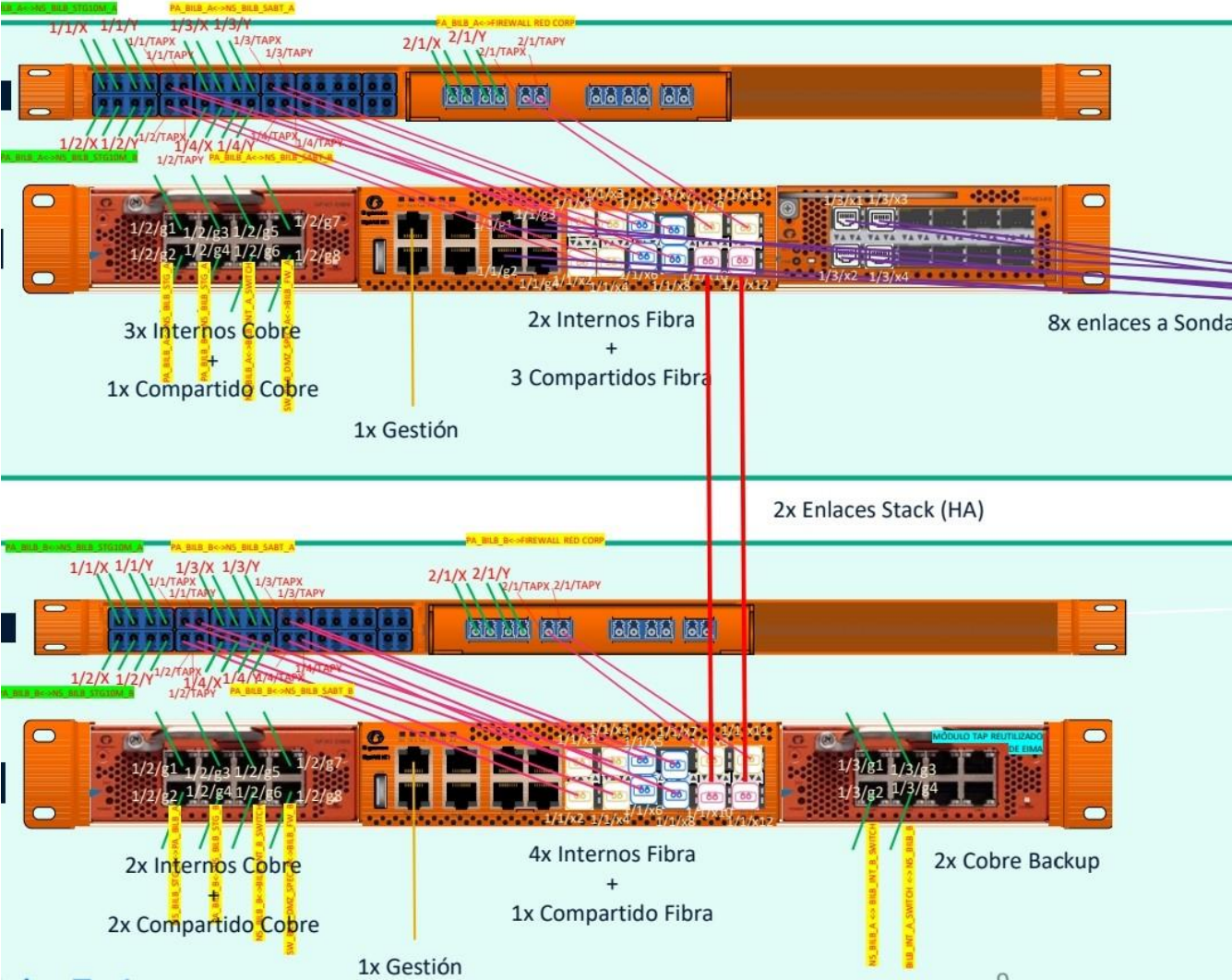


GigaVUE-VSeries



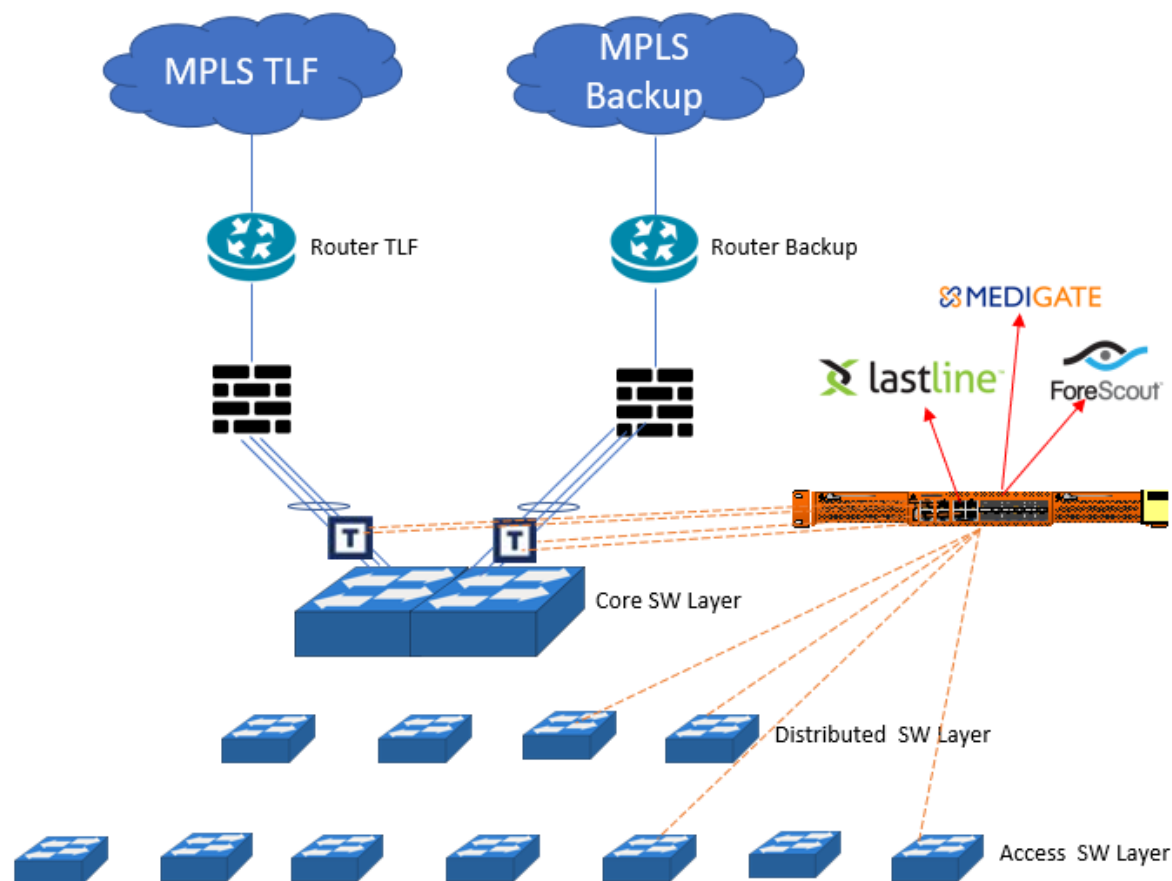
BiDi 40G / 100G Fiber TAP

Algunas referencias (Utility)



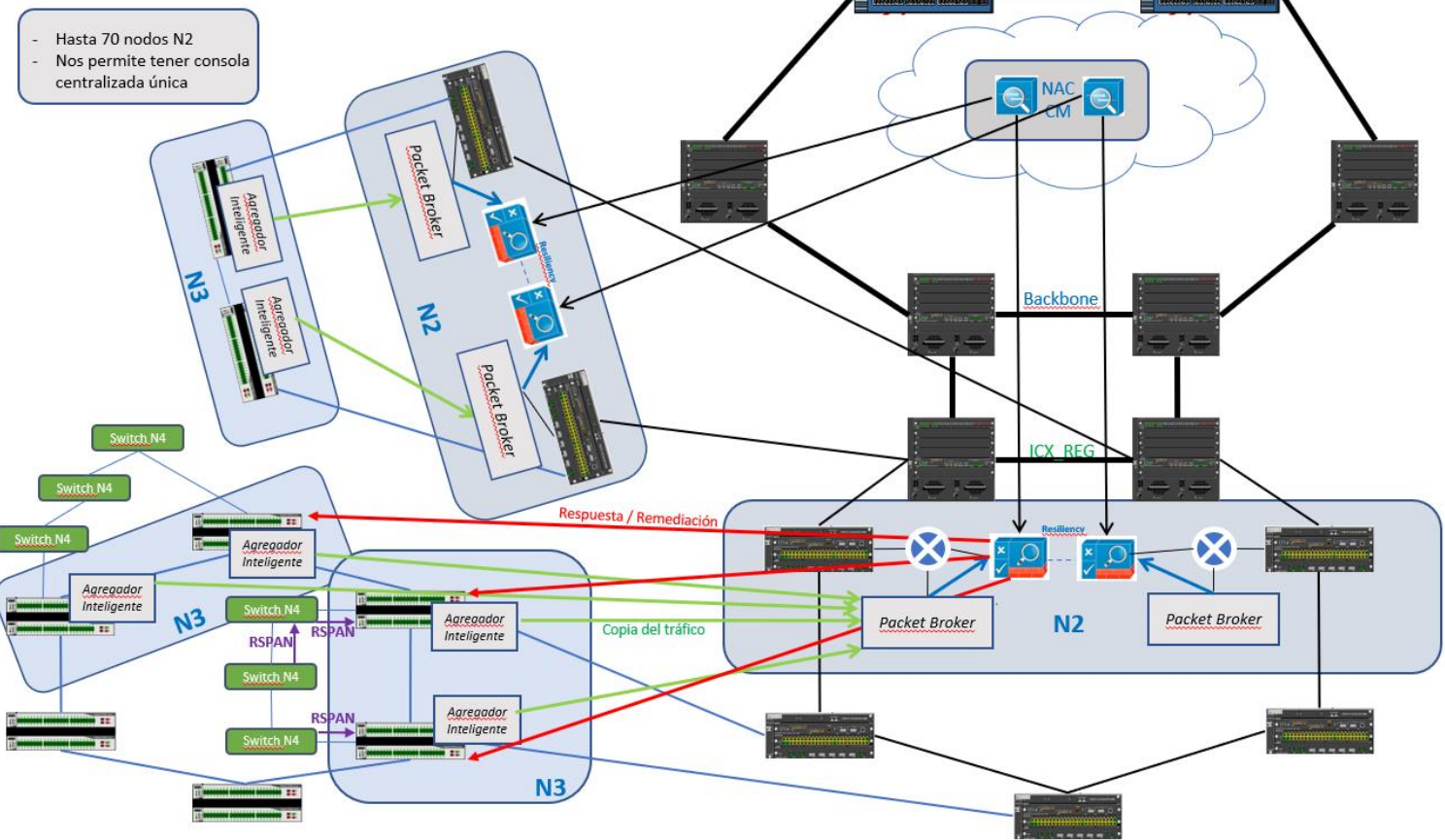
Algunas referencias (hospitales)

Hospital Grande



Algunas referencias (Ferroviario)

Arquitectura distribuida: Escalado



Beneficios de la tecnologia

- Simplificación de la operación

- ▶ Eliminación de ventanas de mantenimiento, simplificación de PoCs, resolución de problemas de asimetría de trafico

- Reducción de los costes en las herramientas de seguridad/monitorización:

- ▶ Filtrado de trafico a enviar, de-duplicación, consolidación de puertos, descifrado de SSL, uso de metadatos, agregación de puertos, recorte de paquetes...

- Extension de la visibilidad y la seguridad a las sedes remotas:

- ▶ Centralización de herramientas, Manipulación de trafico, supresión de cabeceras, tunelización...

- Visibilidad y seguridad en la cloud publica, privada e hibrida:

- ▶ Reaprovechamiento de herramientas

- Cumplimiento de la regulación

- ▶ Enmascarado y difuminación de la información



Preguntas?

alex.lopez@gigamon.com