Captura de Trafico en Cisco ACI

Problema

Muchas organizaciones están desplegando soluciones de Cisco ACI para aprovechar las posibilidades de escalabilidad, alta disponibilidad y orquestación que ofrece esta arquitectura de red. Sin embargo, este esquema representa también numerosos retos de cara a disponer de una visibilidad completa del entorno y poder desplegar herramientas de monitorización y seguridad: los volúmenes de trafico son muy elevados, lo que supone un coste elevadísimo de herramientas si se procesa en su totalidad; el trafico va encapsulado en muchos puntos (VxLAN, QinQ), lo que imposibilidad ser identificado correctamente por las herramientas; tener una visibilidad completa del trafico este-oeste requerirá de combinar captura de trafico en links físicos e infraestructura virtual, que deberá ser consolidado; la arquitectura deberá ser escalable de manera gradual, para ir creciendo en paralelo al despliegue; se deberá poder conectar herramientas en cualquier punto, ofreciendo alta dispobilidad y balanceo de las mismas

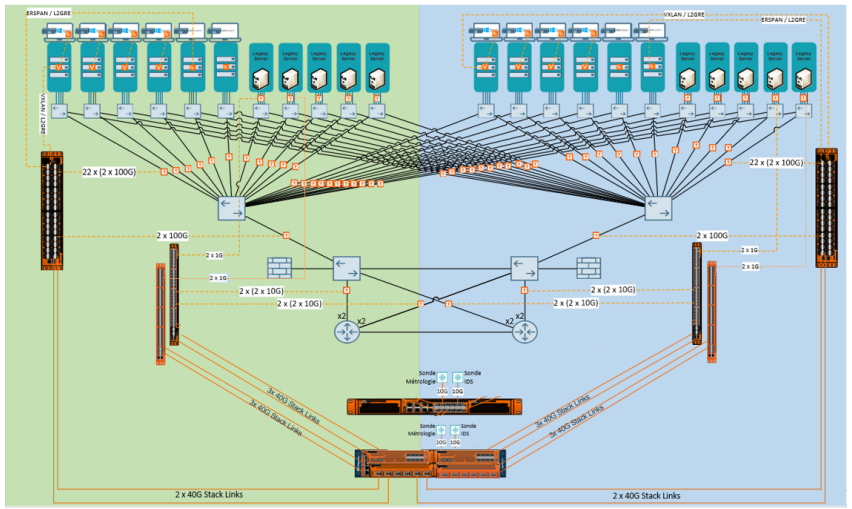
Solución

La arquitectura de Gigamon se puede mapear a la de Cisco en un esquema de Spine&Leaf que permite ir creciendo en paralelo al despliegue de la red ACI y proporcionando alta disponibilidad y balanceo a las herramientas que se conecten.
La solución de Gigamon se adapta a este escenario desplegando distintas opciones para tener visibilidad TOTAL del tráfico:

- ✓ TAPs físicos en aquellos enlaces de red entre capas del Spine&Leaf, con la posibilidad de eliminar los tags VxLan de las NFV a la vez que identificamos cada uno de sus servicios o Bulding Blocks.
- ✓ TAPs Virtuales para las infraestructuras IT desplegadas desde Cisco APIC.
- ✓ Creación de mapas y reglas necesarias en la solución Packet Broker de Gigamon para que cada herramienta de Seguridad y Monitorización reciba el tráfico adecuado.
- ✓ Todo automatizable mediante la API de Gigmaon y su integración con Ansible.

Todo el sistema se comporta como un cluster de recursos compartidos y manejado por un único elemento de gestión, el Fabric Manager, que se puede programar a través de la API para orquestar despliegues automáticos

Esquema



Licencias

Taps
Aggregators
NPB
V-Series
Fabric Manager
Tunneling
Header Stripping
De-deplication
Flow Maps

LINK