Captura de Trafico en SDN

Problema

Muchas organizaciones están desplegando soluciones de SDN para virtualizar tanto la infraestructura IT como la propia red. Estos entornos están basados en soluciones de virtualización OpenStack o Vmware NSX y permiten aprovechar las posibilidades de escalabilidad, alta disponibilidad y orquestación que ofrecen estas tecnologías. 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 disponibilidad y balanceo de las mismas

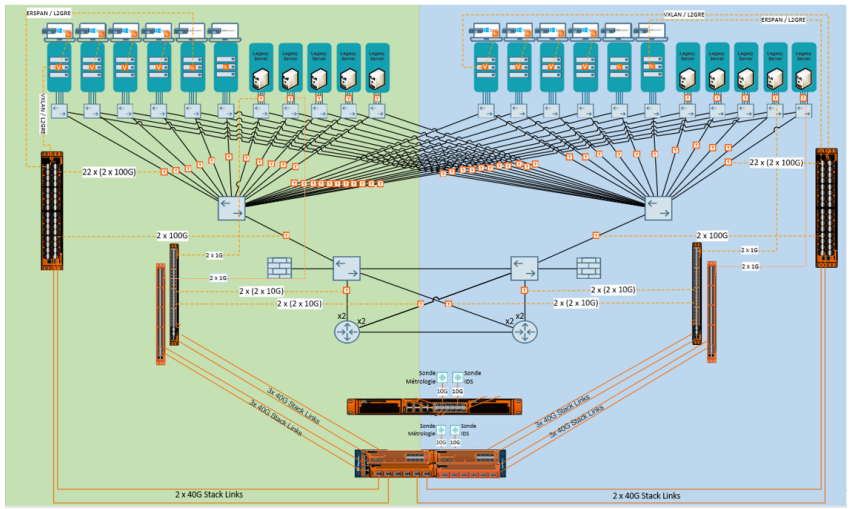
Solución

La arquitectura de Gigamon es compatible con entornos SDN y permite ir desplegándose en paralelo al despliegue de servicios SDN 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 para el tráfico norte-sur con la posibilidad de eliminar los tags VxLan de las SDN a la vez que identificamos cada uno de sus servicios a monitorizar.
- ✓ TAPs Virtuales para el tráfico este-oeste tanto en servicios de red como en infraestructura IT sin necesidad de desplegar agentes en las máquinas virtuales.
- ✓ 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 Gigamon 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