Captura de Trafico en entornos AWS

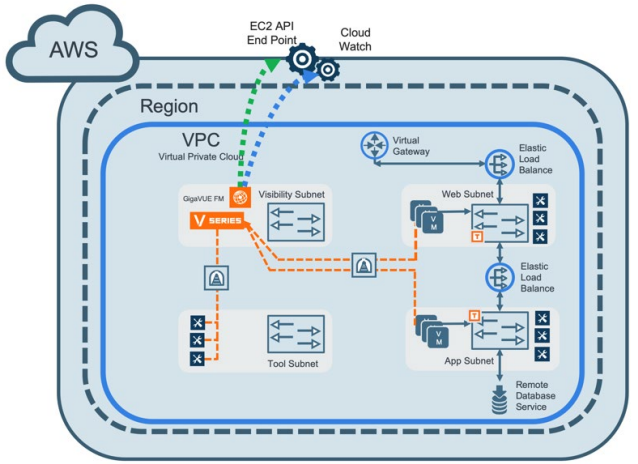
Problema

Cuando los departamentos de Sistemas de las organizaciones inician proyectos de virtualización en la cloud, los departamentos de redes y seguridad se encuentran con un dilema sobre como integrar las políticas de monitorización y seguridad ya desplegadas para la red física en este nuevo entorno. Lo mas habitual es ignorar esta nueva realidad, lo que no tiene ningún sentido mientras va aumentando la parte virtualizada en la cloud. Traer todo el trafico de la Cloud al entorno del datacenter sin filtrar lleva asociados grandes costes, ya que el trafico de subida es gratito, pero no así el de bajada
Crear una VPC especifica de herramientas va a requerir la captura especifica del trafico, tunelizarlo y transportarlo a ese nuevo entorno
Un punto critico de este tipo de soluciones es la orquestación: la solución que se despliegue debe ir automatizada con el orquestador del hipervisor que empleemos, en este caso EC2 API y CloudWatch

Solución

Gigamon dispone de una completa solución para la captura del trafico virtualizado en entornos cloud de AWS
La solución esta totalmente orquestada al conectarse el Fabric Manager a través de la API con EC2 API y CloudWatch
La captura del trafico se puede realizar bien a través del servicio de VPC Traffic Mirroring (https://aws.amazon.com/es/blogs/aws/new-vpc-traffic-mirroring/) o bien a través de Virtual TAPs, gestionados por el G-vTAP controller,
La solución también despliega el SW de Vseries nodes, encargado de realizar las funciones de packet brokering (Filtrado L2-3-4, Netflow, Slicing, Masking, Sampling, de duplicación) y orquestado por el Vseries Controller que permite la escalabilidad a entornos con muchos nodos y máquinas virtuales.
La gestión de túneles VXLan/GRE para poder mover el trafico dentro de la infraestructura de virtualización es totalmente transparente para el usuario

Esquema



Licencias

Fabric Manager
Traffic Visibility for AWS

LINK