

Captura de Trafico en entornos GCP

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 gratuito, pero no así el de bajada

Crear una red específica de herramientas va a requerir la captura específica del trafico, tunelizarlo y transportarlo a ese nuevo entorno

Solución

Gigamon dispone de una solución para la captura del trafico virtualizado en entornos cloud de GCP.

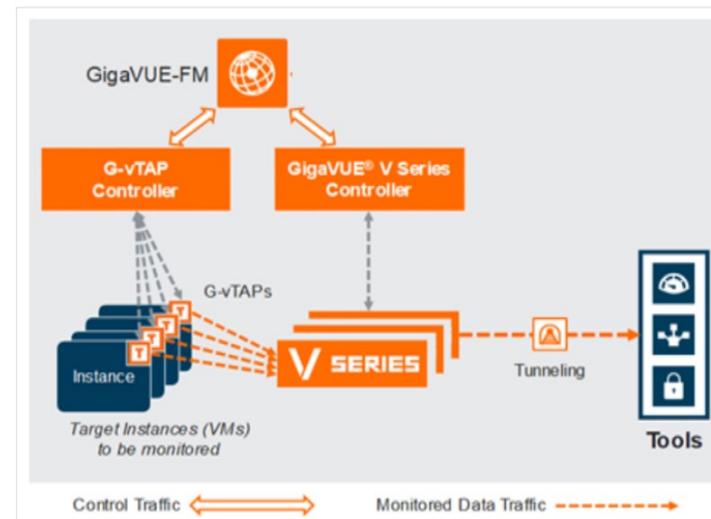
Aun siendo posible la captura del tráfico de cualquier máquina virtual en Google la configuración y administración de la plataforma será manual al no tener aun la integración con la API de Google.

La captura del trafico se realiza a través de Virtual TAPs, gestionados por el G-vTAP controller,

La solución también necesita del despliegue de 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
AnyCloud

[LINK](#)