Captura de Trafico en entornos VMWare

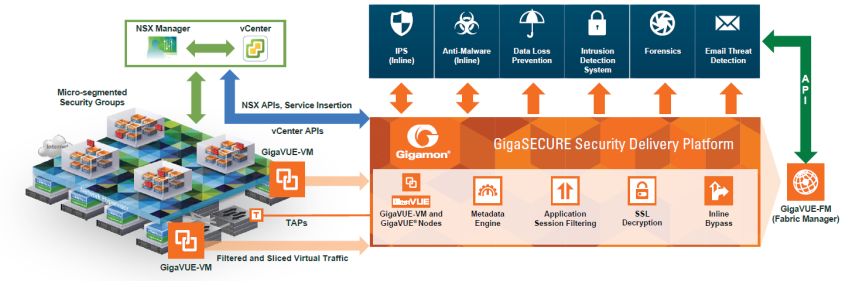
Problema

Cuando los departamentos de Sistemas de las organizaciones inician proyectos de virtualización, 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 de la red. Coger el trafico de los interfaces de salida a la red no resolverá el problema, ya que dejaremos de ver el tráfico este-oeste. Desplegar las mismas herramientas de que ya disponemos para el entorno físico en el virtual supondrá elevados costes, y el problema de sincronizar la información del entorno físico con el virtual
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 Vcenter o NSX-Manager
Por ultimo, para poder sacar el trafico del entorno virtual deberemos tunelizar todo el trafico, preferiblemente de manera automática, y sin interferir con la estrategia de red del propio hipervisor

Solución

Gigamon dispone de una completa solución para la captura del trafico virtualizado en entornos de VMWare, tanto en ESX, como NSX y NSX-T
La solución esta totalmente orquestada al conectarse el Fabric Manager a través de la API con en Vcenter y/o el NSX Manager. De esta manera, el movimiento de maquinas con VMotion es totalmente transparente para el usuario
La solución se basa en el despliegue de una maquina virtual GigaVUE-VM por cada host físico de virtualización, que se conecta directamente al Virtual Distributed Switch de VMWare. Al estar conectado con Vcenter/NSX Manager aprendemos la topología de despliegue de maquinas virtuales automáticamente, lo que nos permite seleccionar el trafico que queremos capturar. Este SW permite realizar filtrados L2-3-4 antes de encapsular y sacar el trafico
El encapsulado del trafico mediante GRE/VXLan/GMIP es transparente para el usuario, que solo debe definir el punto de terminación del túnel mediante su IP, puerto y protocolo

Esquema



Licencias

Fabric Manager
NSX Manager Integration
GigaVUE-VM
Traffic Visibility for NSX-T

LINK