Tunelización para consolidación de Herramientas

Problema

El despliegue de herramientas de monitorización y seguridad se suele disparar cuando nos enfrentamos entornos con gran dispersión geográfica, o en entornos de virtualización o cloud. Esto se debe a que los puntos de captura de trafico no son fácilmente transportables hasta un punto central donde vamos a poder unificarlos, abaratando así el despliegue de la herramienta y simplificando la ingeniería de la solución
El despliegue de sondas locales o virtuales en el punto de origen dela captura no arregla el problema, ya que el propio trafico de control que estas sondas generan debe ser enviado de igual manera a la consola central de administración, por lo que nos volvemos a encontrar con el mismo problema de consolidación de trafico
Las principales barreras técnicas que nos encontramos para poder realizar ese transporte son atravesar infraestructuras virtualizadas sobre las que no podemos mover el trafico transparentemente, ya que colisionarían con los propios servicios de enrutado del hipervisor en cuestión, y el problema equivalente cuando tenemos que atravesar redes enrutadas para la centralización del trafico de sedes dispersas. Igualmente la fragmentación de paquetes puede ser un reto si el receptor del trafico no es capaz de reensamblar los paquetes truncados

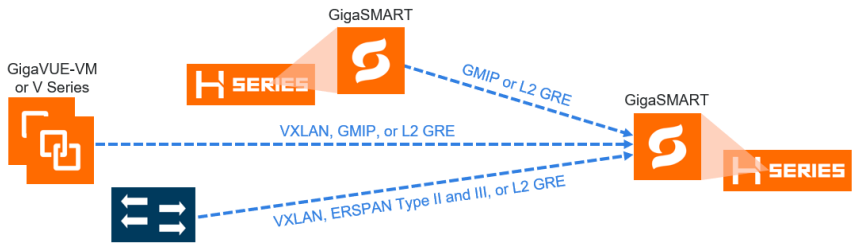
Solución

Los servicios avanzados que proporciona la tarjeta Gigasmart de la plataforma Gigamon tienen soporte de tunelización, tanto para el encapsulado del trafico en origen como para el desencapsulado en destino, y tanto en IPv4 como en IPv6.
Esto nos va a permitir tener visibilidad del trafico este-oeste en los entornos de virtualización, así como atravesar redes enrutadas para consolidar trafico de captura en un punto centralizado
Los protocolos soportados de túneles aseguran la viabilidad del transporte para todos los escenarios posibles:

- VxLAN, GMIP y L2GRE para entornos virtualizados, que aseguraran el transporte del trafico al poder escoger un protocolo diferente al que utilice el propio hipervisor y así no colisionar con la estrategia de direccionamiento de este
- VxLAN, ERSPAN (tipo II y tipo III) y L2GRE para atravesar redes enrutadas capturando trafico de cualquier dispositivo capaz de generar este tipo de túneles
- GMIP para iniciar y terminar túneles entre dispositivos de Gigamon, bien desde taps virtuales, bien desde tarjetas Gigasmart

En la fase de desencapsulado el servicio de tunelización de Gigamon es capaz de reensamblar los paquetes que hayan sido fragmentados

Esquema



Licencias

Tunneling
Advance tunneling

LINK