Aumento de capacidad de Colectoras Mediante truncado avanzado

Problema

Muchas de las herramientas que empleamos de seguridad, monitorización de trafico o grabadoras para análisis forénsicos, solo emplean las cabeceras de los paquetes de cara a realizar sus funciones. De esta manera nos encontramos que enviamos paquetes de hasta 1500 bytes a un equipo que solo va a necesitar los primeros 80, con el consiguiente aumento de coste de almacenamiento, o lo que es equivalente, reducción de la capacidad de almacenamiento, y con el malgasto de proceso de computo en el equipo para que tenga que extraer las cabeceras de los paquetes
En otras ocasiones, hay equipos que con recibir los primeros paquetes de una sesión ya van a poder realizar la función de reconocimiento de aplicación y toma de decisiones que requieren, por lo que contribuir enviando el resto de l sesión no va a hacer mas que malgastar recursos de almacenamiento y proceso
Hay incluso escenarios donde queremos enviar información a equipos colectores que por motivos legales o de compliance no pueden almacenar información contenida en los payloads de los paquetes, por lo que debemos eliminar esta información y guardar únicamente las cabeceras

Solución

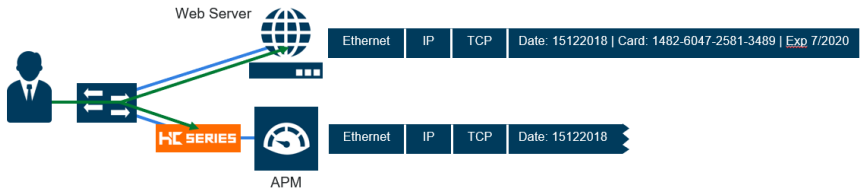
Las funcionalidades de Slicing de la suite de Gigamon resuelven esta problemática.

Por un lado podemos recortar los paquetes a partir de la posición que configuremos en el paquete, de tal manera que el resto se descarta y no alcanza al equipo colector. Para poder realizar correctamente estadísticas se incluirá un campo con el tamaño original del paquete, y se recalculara el CRC

De una manera mas sofisticada, podemos configurar que se envíen los primeros X paquetes de cada sesión, y los posteriores ser descartados, recortados o enviados, según deseemos que se reciba el trafico

La solución de Slicing se puede combinar con la de masking para dar mayor flexibilidad en el cumplimiento del compliance interno o con el marco legal

Esquema



Licencia

Slicing
Advanced Flow Slicing

LINK