Generación de Syslog enriquecidos para SIEM

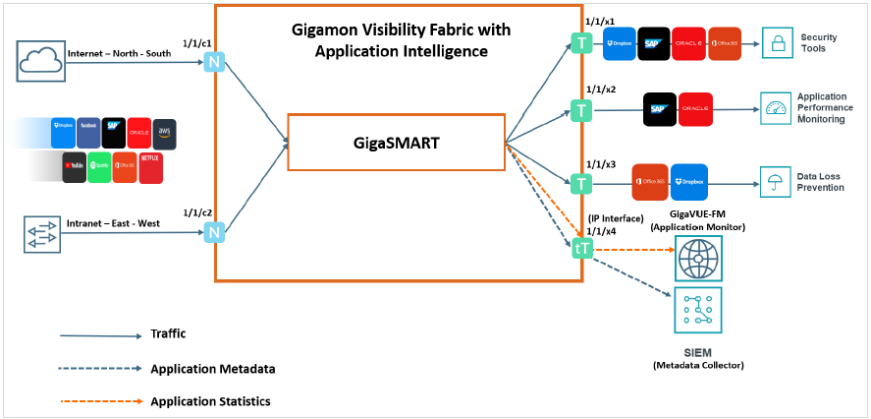
Problema

Las herramientas de seguridad y monitorización acostumbran a ser dimensionadas por el ancho de banda que reciben, y por tanto tener soluciones de identificación de aplicación que nos permitan filtrar que trafico va a recibir cada herramienta son cruciales para controlar los costes de despliegue de nuestra estrategia de visibilidad y seguridad. Pero realizar un filtro binario sobre cada aplicación puede no ser suficiente para cumplir con nuestras políticas de seguridad, así que es necesario tener alguna estrategia adicional para enviar información a nuestras tools suficiente para identificar que esta pasando en la red, pero reduciendo al máximo el ancho de banda que vamos a enviar. Típicamente queremos poder generar datos de datos, esto es, Syslog Adicionalmente es importante tener algún mecanismo que nos permita automatizar ese envío de información, de tal manera que si por ejemplo estamos enviando esos datos a un SIEM, podamos comunicar automáticamente la estructura de Syslog que se este transfiriendo
De igual manera la transferencia de Syslog debe ser flexible y soportar diferentes formatos que se adapten al exporter que va a recibir los datos

Solución

EL modulo de reconocimiento de aplicaciones de la tarjeta Gigasmart Application Filtering Intelligence incluye un modulo adicional de generación de Syslog llamado Application Metadata Intelligence (AMI).
En la actualidad AMI es capaz de generar mas de 5800 campos sobre las 3200 aplicaciones reconocidas mediante un interfaz grafico muy intuitivo
Los Syslog se pueden generar tanto en formato Netflow como en formato CEF de cara a adecuarnos a la herramienta que va a recibirlos
Gracias a la extensa red de partners que posee Gigamon, tenemos integraciones nativas con fabricantes de SIEM (Qradar, Slunk) a través de la API de la plataforma de gestión Fabric Manager, de manera que podemos automatizar el traspaso del formato de Syslog enviados

Esquema



Licencia

Application Metadata Intelligence

LINK