Inserción dinámica de equipos de seguridad en línea

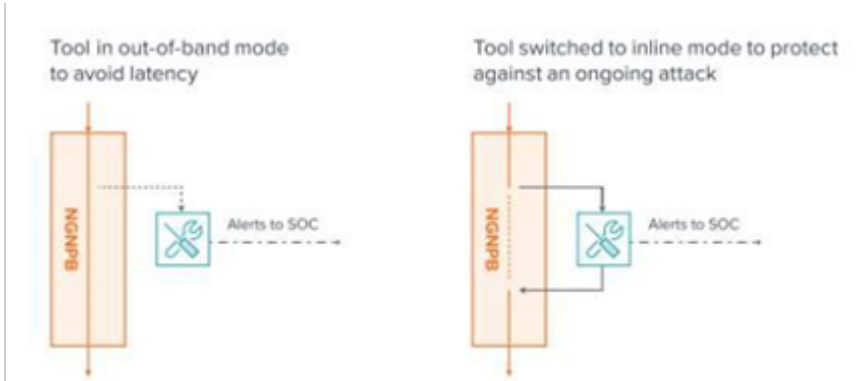
Problema

El despliegue de herramientas de seguridad en línea, como pueden ser los IPS, WAF o DDoS, puede ser conflictivo en muchas ocasiones debido a los retardos en la línea que pueden introducir, el aumento de riesgo en la continuidad del negocio al haber introducido mas equipos en línea o los riesgos para el negocio derivados de configuraciones erróneas de la sonda que puedan afectar a todo el trafico que pasa por ellas
Adicionalmente forzar a que tenga que pasar todo el trafico de la línea por estos equipos de seguridad va a obligar a tener que sobredimensionarlas, con el consiguiente sobrecoste económico que esto va a suponer, cuando en realidad podrían ser dimensionados correctamente si solo el trafico susceptible de ser malicioso acabase atravesándolas
A todo esto hemos de sumar la problemática de proporcionar alta disponibilidad a estos equipos tan críticos, debido a las asimetrías de trafico, diferentes capacidades de las sondas

Solución

Todos los equipos de seguridad tienen modos fuera de banda, también llamados de monitor, por los que están analizando el trafico basados en una copia del mismo son necesidad de estar en línea.
Gracias a la integración que podemos realizar entre la sonda de seguridad y el Network Packet Broker de Gigamon a través de la API programable del Fabric Manager vamos a ser capaces de redirigir el trafico a la propia sonda que ha detectado el ataque fuera de línea de manera dinámica para que pase a estar en linea. Además, con la capacidad de aplicar filtros específicos a nivel 2/3/4 una vez detectado el ataque, tenemos la posibilidad de limitar el trafico que se dirige a la sonda una vez esta en línea de cara a dimensionarla de una manera mas racional, con el consiguiente ahorro en costes
Una vez mitigado el ataque, o bien pasado un tiempo prudencial, podemos automáticamente revertir la situación y volver a colocar la sonda fuera de línea en modo monitor
Estas capacidades de inserción dinámica se suman a las habilidades del NPB de resolver los problemas de proporcionar alta disponibilidad y escalabilidad a estas sondas

Esquema



Load Balancing
Flow Mapping
Fabric Manager
Inline Bypass
Bypass HW

LINK