Despliegues Activo-Activo de equipos de seguridad

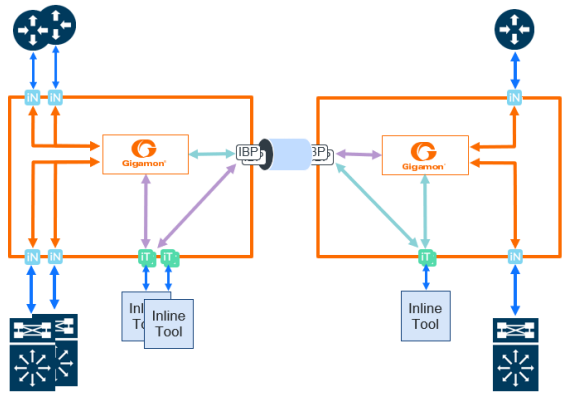
Problema

Por cuestiones de redundancia, es muy habitual comprar todas las herramientas de seguridad en clusters para asegurar que la caída de un equipo no compromete la arquitectura de defensa. Pero es también muy habitual desplegar estas herramientas en arquitecturas activo pasivo, con el despilfarro que supone haber comprado un equipo de seguridad, con su correspondiente OPEX, y no estar disfrutando de el.
Esto se debe a la complejidad de desplegar las herramientas en activo-activo por causa de los problemas de la asimetría del trafico. Al ser el propio internet asimétrico, no podemos asegurar que el trafico generado por en equipo acabe en el otro equipo, por lo que el primero no ve que haya respuesta, y el segundo desconoce que hacer con el trafico que le ha llegado
Si hablamos de trafico cifrado, el problema resulta mas evidente

Solución

La simetrización del trafico en los despliegues activo-activo resulta trivial con la infraestructura de NPB de Gigamon. Colocando NPBs delante de los equipos de seguridad, podemos balancear las sesiones asegurando que cada equipo recibe una parte proporcional del tráfico pero manteniendo la sesión completa siendo válido para el análisis de las herramientas statefull.
De esta manera podemos realizar despliegues activo-activo sin introducir complejidad en la arquitectura de la red

Esquema



Licencia

Flow Mapping
Load Balancing
Bypass HW
Inline Bypass

LINK