# Centralización y descongestión de IDS

## Problema

Las herramientas de Intrusion Detection System (IDS) resultan muy efectivas para la detección de ataques en base a análisis de firmas y de comportamiento del trafico, pero su despliegue supone un importante reto cuando nuestra infraestructura esta muy dispersa geográficamente. Desplegar sondas en cada una de las localizaciones de la organización no resulta viable por los coste que supondría en inversión ni por la complejidad que introduciría en su gestión
Adicionalmente estas herramientas se dimensionan por el ancho de banda que reciben, y se ven muy perjudicadas en su rendimiento cuando reciben trafico cifrado

## Solución

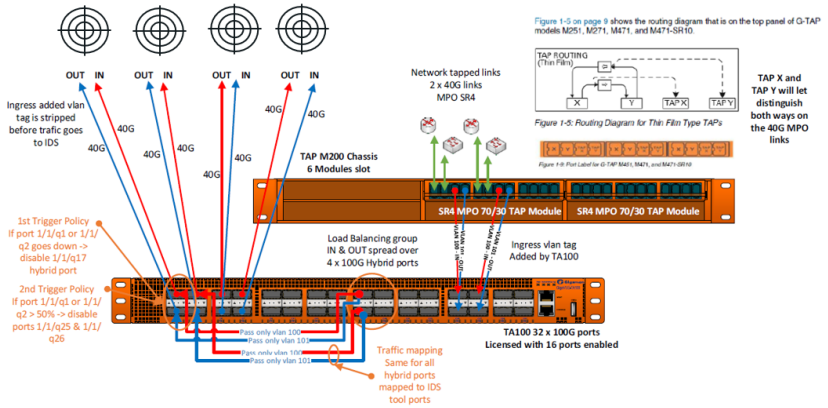
De cara a racionalizar los costes de despliegue de sondas IDS, las soluciones de NPB de Gigamon ofrecen diversas alternativas
Para reducir el ancho de banda que se envía al IDS

- Reducción del trafico enviado a la sonda en base a filtros L2-3-4-7
- Empleo de Advance Slicing para enviar los primeros paquetes de cada sesión, descartando el resto de la sesión cuando no sea relevante para la seguridad
- Descifrado de SSL previo al envío a la sonda

Para centralizar el trafico en sondas centrales

- Obtención de copias del trafico relevante mediante TAPs en sedes remotas para transporte a la sede central y consolidación en sondas centralizadas
- Filtrado del trafico en origen cuando el ancho de banda en transporte esta limitado, tunelizando el trafico hasta el punto central

## Esquema




## Licencia

Flow Mapping
Load Balancing
Tunneling
Application Filter
Intelligence
Advance Slicing
SSL Decryption

LINK