Descongestión y centralización de Trafico en Despliegues de NAC

Problema

Las soluciones de NAC se están convirtiendo en una requisito cada vez mas imprescindibles en la política de seguridad de cualquier organización, especialmente potenciadas por la corriente de Zero Trust lanzada por Google. Las soluciones mas modernas ofrecen muy buena granularidad en las políticas a implementar en el control del acceso a la red, pero para ello necesitan tener una copia del trafico, especialmente para poder identificar el dispositivo que se quiere conectar a la red, basándose en el comportamiento del trafico que generan. Una de las grandes frustraciones que se producen en los despliegues de NAC entre los departamentos de redes y de seguridad se genera al poner el proyecto en producción: mientras que realizar un piloto en una zona acotada resulta muy sencillo y nada disruptivo, al poner la solución completa producción el trafico en la red se duplica de golpe al necesitar el NAC de una copia completa del trafico de la red para poder identificar dispositivos, que acaba comprometiendo la estabilidad de la red

En escenarios de despliegue que involucren sedes remotas, donde los anchos de banda son aun mas escasos, el problema es mucho mas grave, ya que la congestión de red va a suponer incomunicar las delegaciones. Igualmente la generación de la copia del trafico genera problemas, ya que si se emplean técnicas de port mirror/Span no se esta copiando realmente el trafico y sin embargo se están consumiendo gran cantidad de recursos en los switches/routers/firewalls donde se están haciendo la copia

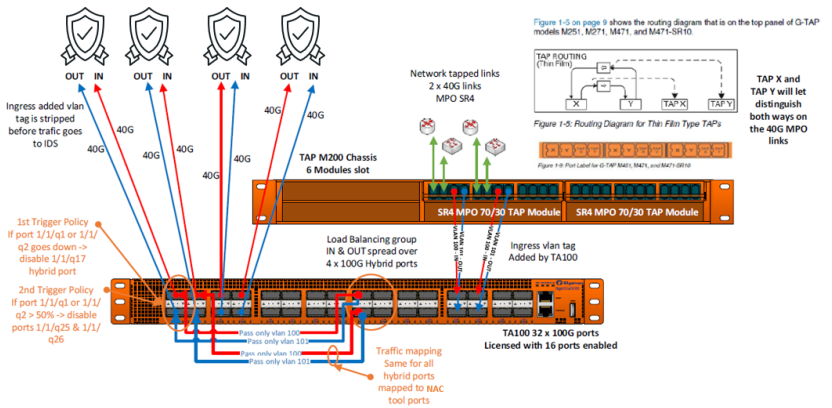
Solución

Gracias a las soluciones de NPBs de Gigamon, es posible desplegar una solución de NAC sin comprometer la estabilidad de la red y proporcionando al NAC una copia real del trafico total de la red. Típicamente en las sedes centrales vamos a desplegar TAPs (pasivos y/o activos) para obtener una copia real del trafico. Esas copias podrán ser agregadas y filtradas gracias a agregadores y/o packet brokers, para crear una red paralela de transporte hasta la consola central del NAC son necesidad de utilizar la red de producción, y por tanto son comprometer su capacidad.

En los despliegues de sedes remotas el empleo de técnicas avanzadas de reducción del ancho de banda (filtros avanzados, deduplicacion de trafico, truncado de paquetes…) nos va a segurar que el ancho de banda que se remita al nodo central sea el minomo necesario para el correcto funcionamiento del NAC, asegurando asi las comunicaciones con las sedes remotas

El hecho de emplear TAPs para realizar las copias evita igualmente malgastar los recursos de memoria y CPU de los equipos de red

Esquema



Licencias

Flow Mapping
De duplicación
Slicing
Adcanced Slicing

LINK