Conexión de Sondas del CCN

Problema

Las organizaciones publicas que despliegan sondas del CCN (SAT-SARA, Carmen, Marta..) se enfrentan siempre al dilema de donde conectar las sondas.: mientras que la sonda dispone de unos puertos limitados de unas características determinadas (fibra, cobre, 1g, 10g..) los puntos de captura idóneos de trafico con muchos mas, y con gran dispersión de medios y velocidades.
Peor aun, si queremos tener visibilidad del trafico este-oeste en las infraestructuras virtualizadas, no tenemos solución posible.
Y aun mas, si de alguna manera consiguiésemos tener acceso a todos esos puntos de captura, el trafico que enviaríamos al a sonda la desbordaría totalmente inutilizando la solución
Para colmo, si el trafico va cifrado, perdemos cualquier tipo de visibilidad sobre esos datos

Solución

La suite completa de Gigamon ayuda a poder desplegar las sondas del CCN de una manera optima:

- Podemos capturar el trafico mediante mirror/SPAN o idealmente Taps y cambiar las velocidades y medios de los puertos para adecuarlos a los disponibles de la sonda
- De cara a no saturar la sonda, podemos aplicar filtros L2-3-4-7 previos a la entrega del trafico
- el trafico SSL, tanto de entrada como de salida, y con clave segura o no segura, puede ser abierto antes de ser enviado a la sonda
- El trafico este-oeste de las infraestructuras virtuales puede ser capturado, consolidado con el proveniente de la red física, y enviado el mismo equipo.

Esquema


CCN-STIC-105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación

7.3.3 FAMILIA: CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

GigaVUE (HD8, HD4, HC3, HC2, HC1)

Versión	version 5.1.01
Familia	Captura, Monitorización y Análisis de Tráfico
Fabricante	Gigamon
Categoría	ENS ALTO
Fecha Inclusión	01/11/2019
Revisión de Validez	31/05/2020

Descripción

Network Packet Brokers HC/HD Series. Network Packet Brokers de alto rendimiento con soporte de puertos 1g/10g/25g/40g/100g en fibra multimodo o/y monomodo y 100m/1000m/10g en cobre y funcionalidades de filtrado de trafico L2-3-4-7 con motor de DPI, generación de Netflow/IPFix/Metadatos, Cifrado/Descifrado de SSL/TLS (incluyendo protocolos RSA, DHE, ECC, y PFS), Terminación de túneles (GRE, VXLAN, ERSPAN, GMIP), Truncado de paquetes, Eliminación de cabeceras, Enmascarado, De-Duplicación, Clustering, Balanceo, Captura de tráfico para entornos virtuales (VMWare ESX/NSX, Openstack, Kubernetes, AWS, GCP, Azure, Nutanix), simetrización de tráfico para arquitectura HA, Inline Bypass con Heartbeat positivo y negativo, Cambio de medio y velocidad, Bypass HW, TAPsintegrados.

Observaciones

Procedimiento de empleo seguro pendiente de publicación

Licencia

Flow Mapping
Application Intelligence
De-duplication
Advanced Slicing
SSL Decryptoin
vTAPs
Tunneling
Header stripping

LINK