Connessione di Sonde del CCN

Problema

Le organizzazioni pubbliche che distribuiscono sonde del CCN (SAT-SARA, Carmen, Marta...) devono sempre affrontare il problema di dove collegarle: mentre la sonda dispone di alcune porte limitate da caratteristiche determinate (fibra, rame, 1g, 10g...) i punti di cattura idonei del traffico possono averne molte di più, con grande dispersione di mezzi e velocità.
Peggio ancora, se si desidera avere visibilità del traffico est-ovest sulle infrastrutture virtualizzate, non esistono soluzioni.
Inoltre, se in qualche modo si riesce ad avere accesso a tutti questi punti di cattura, il traffico inviato alla sonda sarà eccessivo, rendendo inutile la soluzione.
Per giunta, se il traffico viene crittografato, si perde qualsiasi tipo di visibilità su questi dati.

Soluzione

La suite completa di Gigamon aiuta a distribuire le sonde del CCN in modo ottimale:

- E' possibile catturare il traffico mediante mirror/SPAN o idealmente Tap e modificare le velocità e i mezzi delle porte per adeguarle a quelle disponibili della sonda
- Per non saturare la sonda, si possono applicare filtri L2- 3-4-7 prima della trasmissione del traffico
- Il traffico SSL, sia in ingresso che in uscita, e con chiave di sicurezza o meno, può essere aperto prima di essere inviato alla sonda
- Il traffico est-ovest delle infrastrutture virtuali può essere catturato, consolidato con quello che proviene dalla rete fisica, e inviato allo stesso dispositivo.

Schema


CCN-STIC-105

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 tráfico 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

Licenza

Flow Mapping
Application Intelligence
De-duplication
Advanced Slicing
SSL Decryption
vTAP
Tunneling
Header stripping

LINK