Riduzione dei costi degli strumenti di sicurezza

Problema

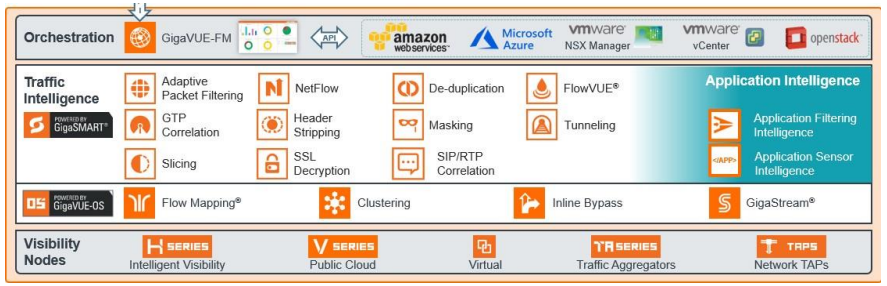
Gli strumenti di sicurezza sono decisamente fondamentali per potere implementare le politiche definite dal CISO dell'organizzazione per difendere le informazioni attive dell'impresa. Purtroppo, il numero di tecnologie di sicurezza tende ad avvicinarsi al numero di vettori di attacco esistenti, che non smette di aumentare, per cui il CISO si deve confrontare sempre di più col problema di come distribuire il proprio budget, spesso esiguo, per potere acquisire strumenti che hanno un CAPEX elevato e, peggio ancora, un OPEX ancora maggiore, normalmente associato a firme aggiornate e che comportano un altro costo elevatissimo in termini di risorse umane per la gestione dei dispositivi. Per questo è fondamentale poter ridurre il costo di questi strumenti per disporre di un budget che consenta di realizzare questo delicato equilibrio.
Il parametro principale in base al quale di solito vengono dimensionati tali strumenti è sempre il volume di traffico che dovranno gestire, che insieme alla necessaria ampiezza del perimetro di rete da mettere in sicurezza determina sempre costi elevati di implementazione. Poter ridurre la larghezza di banda che lo strumento dovrà gestire, oltre a semplificare per quanto possibile l'architettura di distribuzione, farà sì che il progetto sia più vantaggioso dal punto di vista economico.

Soluzione

La combinazione di soluzioni di tutta la suite di Gigamon permetterà non solo di semplificare le distribuzioni degli strumenti di monitoraggio, estendendo paradossalmente la visibilità delle sedi in remoto e degli ambienti di visualizzazione, ma determinerà sempre un significativo risparmio nel tool di monitoraggio utilizzato.
Le tecniche di riduzione dei costi sono numerose, ma volendo elencare le principali:

- Filtraggio del traffico a livello L2-3-4-7
- Generazione di metadati, che riduce notevolmente il volume di traffico che sarà processato
- Taglio dei pacchetti, per inviare al tool solo le intestazioni necessarie per l'analisi
- Taglio avanzato dei pacchetti, affinché siano trasmessi solo i primi pacchetti di una sessione, spesso sufficienti all'analisi
- Deduplicazione del traffico per trasmettere solo una volta una copia di tutto il traffico che circola sulla rete
- Decodifica SSL per evitare questo pesante compito agli strumenti
- Tunnellizzazione, affinché si possa applicare uno strumento centralizzato a una rete geograficamente distribuita

Schema



Licenza

Flow Mapping
Suite Gigasmart

LINK