Centralizzazione e decongestione IDS

Problema

Gli strumenti di Intrusion Detection System (IDS) risultano molto efficaci per la rilevazione di attacchi in base ad analisi delle firme e del comportamento del traffico, ma la loro distribuzione costituisce una sfida significativa quando l'infrastruttura è molto dispersa geograficamente. Distribuire sonde su ciascuna delle sedi dell'organizzazione non risulta fattibile a causa dei costi che comporterebbe in termini di investimenti e della complessità che introdurrebbe nella sua gestione.
Inoltre questi strumenti sono dimensionati in base alla larghezza di banda che ricevono e la loro resa è molto compromessa quando ricevono traffico crittografato.

Soluzione

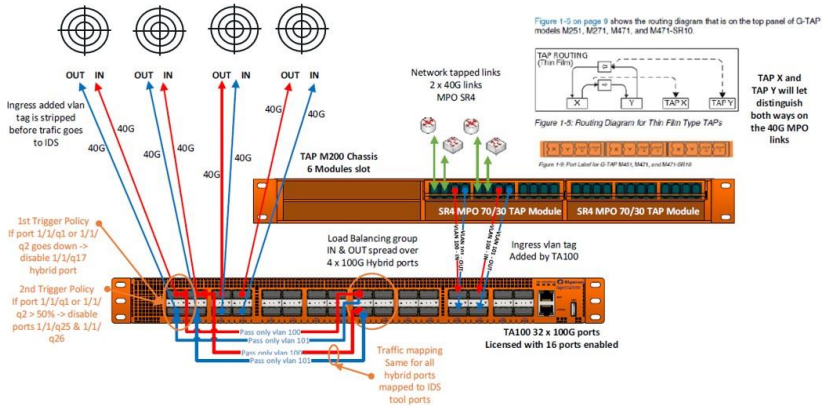
Per razionalizzare i costi di distribuzione di sonde IDS, le soluzioni NPB di Gigamon offrono diverse alternative.
Per ridurre la larghezza di banda che viene inviata all'IDS:

- Riduzione del traffico inviato alla sonda in base a filtri L2-3-4-7
- Impiego di Advance Slicing per inviare i primi pacchetti di ogni sessione, scartando il resto della sessione quando non è rilevante ai fini della sicurezza
- Decodifica SSL prima della trasmissione alla sonda

Per centralizzare il traffico su sonde centralizzate:

- Ottenimento di copie del traffico di interesse tramite TAP nelle sedi in remoto per trasporto alla sede centrale e consolidamento in sonde centralizzate
- Filtraggio del traffico all'origine quando la larghezza di banda nel trasporto è limitata, tunnellizzando il traffico fino al punto centrale

Schema



Licenza

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

LINK