

Distribuzione attivo/attivo di dispositivi di sicurezza

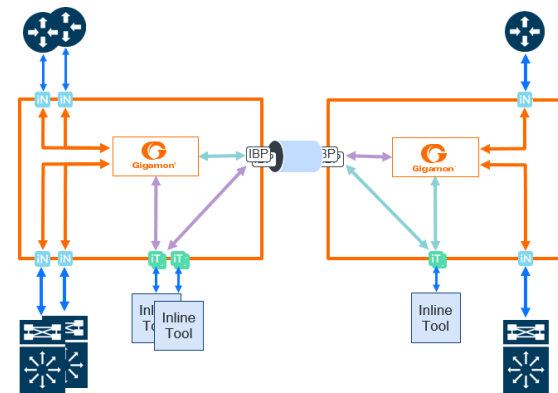
Problema

Per questioni di ridondanza è molto comune acquistare tutti gli strumenti di sicurezza in cluster per garantire che un eventuale guasto su un dispositivo non comprometta l'architettura di protezione. Tuttavia è molto comune anche distribuire questi strumenti in architetture attivo/passivo, con lo spreco che comporta l'aver acquistato un dispositivo di sicurezza, col corrispondente OPEX, e non utilizzarlo. Ciò è dovuto alla complessità di distribuire gli strumenti in attivo/passivo a causa dei problemi di non bilanciamento del traffico. Essendo internet non bilanciato, non si può garantire che il traffico generato da un dispositivo arrivi all'altro dispositivo, per cui il primo non vede alcuna risposta e il secondo non sa cosa fare del traffico che gli è arrivato. Se si parla di traffico crittografato, il problema è ancora più evidente

Soluzione

Il bilanciamento del traffico nelle distribuzioni attivo/attivo risulta perfetto con l'infrastruttura NPB di Gigamon. Mettendo NPB davanti agli strumenti di sicurezza, è possibile bilanciare le sessioni assicurando che ogni dispositivo riceva una parte proporzionale di traffico, mantenendo però la sessione completa valida per le analisi degli strumenti statefull. In questo modo è possibile realizzare distribuzioni attivo/attivo senza introdurre elementi di complessità nell'architettura della rete.

Schema



Licenza

Flow Mapping
Load Balancing
Bypass HW
Inline Bypass

[LINK](#)