

Connessione di Sonde di sicurezza OT

Problema

Le organizzazioni industriali che si preoccupano di distribuire soluzioni di sicurezza industriale (OT) si scontrano col problema di come poter consolidare il traffico proveniente dai punti di cattura, molto numerosi e dispersi geograficamente, in un punto centrale a cui applicare tutta l'intelligenza. Realizzare un pilota in un unico luogo risulta semplice, ma la distribuzione reale su tutta la rete di solito è molto complessa. Il problema principale di solito è la rete di trasporto che si utilizza, spesso con tecnologie a basso flusso e flessibilità, come PDH o SDH. Distribuire molte sonde lungo tutta la rete non risolve il problema, dal momento che anche se riduce la quantità di informazioni da trasmettere dal momento che le sonde generano i metadati necessari per l'analisi delle informazioni, non si risolve il problema di dovere trasportare queste informazioni fino alla console centrale di gestione. Un altro problema tipico è quello che riguarda la cattura di dati in sé. Anche se questi dispositivi industriali gestiscono livelli di traffico molto piccoli, non risulta semplice poterli copiare all'origine, dal momento che i dispositivi di comunicazione impiegati in questo ambiente non hanno queste capacità.

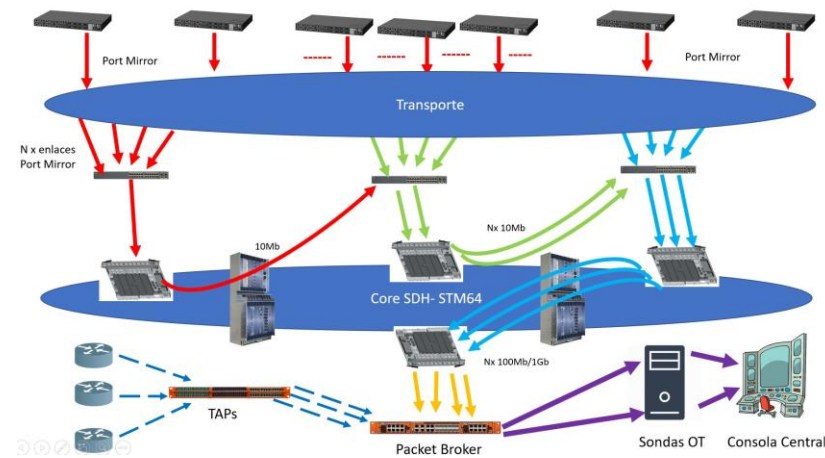
Soluzione

Uno dei grandi vantaggi delle tecnologie di Network Packet Brokers di Gigamon è quello di potere consolidare il traffico che proviene da molti punti di origine diversi per consolidarlo in un punto centrale e abilitare così gli strumenti di visibilità e sicurezza.

Nel caso di dispositivi di sicurezza OT si sarà in grado di realizzare questo compito in diversi modi:

- Quando non è possibile generare la copia del traffico tramite dispositivo di comunicazione, le soluzioni TAP si fanno carico di estrarre la copia letterale del traffico, consentendo di trasmetterla al punto centrale tramite la rete di trasporto
- Quando si impiegano dispositivi intermedi per incapsulare il traffico e trasmetterlo tramite RESPAN al punto centrale, il packet broker centrale può de-incapsulare il traffico interessato e unirlo al traffico proveniente dal datacenter principale
- Se si ha la necessità di realizzare aggregazioni intermedie di traffico per ridurre la larghezza di banda da trasmettere, di solito per limitazioni della capacità della rete di trasporto, i dispositivi aggregatori possono svolgere questa funzione

Schema



Licenza

Application Filtering
Intelligence
Application metadata
Intelligence
Flow Mapping
Tunneling

[LINK](#)