Decongestione del traffico in distribuzioni NAC

Problema

Le soluzioni NAC stanno diventando un requisito sempre più imprescindibile nella politica di sicurezza di qualsiasi organizzazione, potenziate in particolare dal modello di flusso ZeroTrust lanciato da Google. Le soluzioni più moderne offrono un'eccellente granularità nelle politiche da implementare per il controllo di accesso alla rete, ma, per farlo, devono conservare una copia del traffico, soprattutto per potere identificare il dispositivo che desidera connettersi alla rete, in base al comportamento del traffico che generano. Una delle grandi frustrazioni che nascono nell'applicazione di NAC tra i dipartimenti di rete e di sicurezza nasce quando si inserisce il progetto in produzione: mentre realizzare un progetto pilota in un'area limitata risulta più semplice e per nulla problematico, quando si inserisce la soluzione completa nella produzione, il traffico nella rete raddoppia improvvisamente, richiedendo al NAC una copia completa del traffico di rete per poter individuare i dispositivi e questo finisce per compromettere la stabilità della rete.
In contesti di applicazione che coinvolgano sedi remote, in cui le larghezze di banda sono ancora più scarse, il problema è molto più grave, perché la congestione della rete arriva a provocare la mancata comunicazione dalle diverse sorgenti. Anche la generazione della copia del traffico causa problemi, dal momento che, se si impiegano tecniche di port mirror/Span, non si sta copiando effettivamente il traffico e in compenso si consumano grandi quantità di risorse su switch/router/firewall di cui si sta facendo la copia.

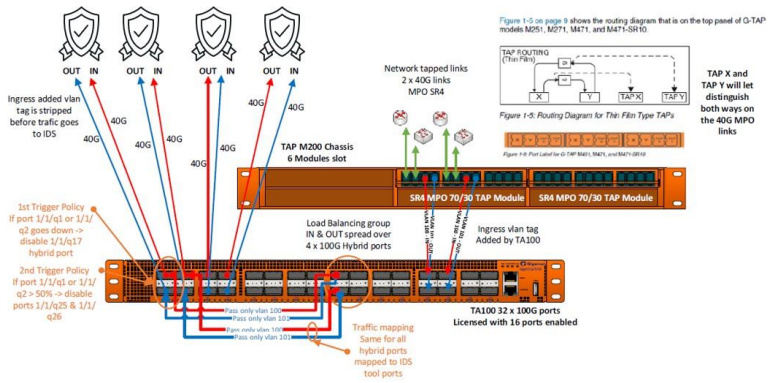
Soluzione

Grazie alle soluzioni NPB di Gigamon è possibile applicare una soluzione NAC senza compromettere la stabilità della rete e garantendo al NAC una copia effettiva del traffico totale della rete. Di solito nelle sedi centrali applichiamo TAP (passivi e/o attivi) per ottenere una copia effettiva del traffico. Queste copie potranno essere aggregate e filtrate grazie ad aggregatori e/o packet broker, per creare una rete parallela di trasporto fino alla console centrale del NAC senza bisogno di utilizzare la rete di produzione e quindi senza comprometterne la capacità.

Nelle applicazioni a sedi in remoto l'impiego di tecniche avanzate di riduzione della larghezza di banda (filtri avanzati, deduplicazione del traffico, troncamento pacchetti...) assicura che la larghezza di banda trasmessa al nodo centrale sia il minimo necessario per il corretto funzionamento del NAC, garantendo così le comunicazioni con le sedi in remoto.

Il fatto di impiegare TAP per realizzare le copie evita contemporaneamente di sprecare risorse di memoria e CPU dei dispositivi di rete.

Schema



Licenze

Flow Mapping
De duplicación
Slicing
Advanced Slicing

LINK