Cattura di traffico in ambienti Kubernetes

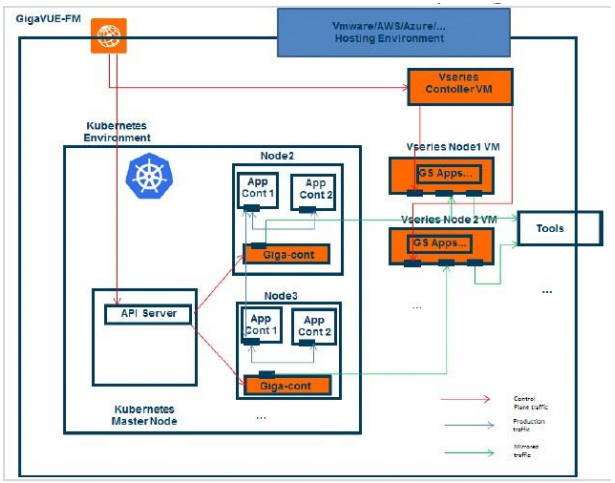
Problema

Quando i dipartimenti Sistemi delle aziende avviano i progetti di virtualizzazione, i dipartimenti di rete e sicurezza devono affrontare il grave problema di come integrare in questo nuovo ambiente le politiche di monitoraggio e sicurezza già messe in atto tramite rete fisica. La cosa più comune è ignorare questa nuova realtà, ma questo non ha alcun senso, dal momento che la parte virtualizzata della rete continua ad aumentare. Tenere sotto controllo il traffico delle interfacce di ingresso alla rete non risolverà il problema, dal momento che non vedremo comunque il traffico est-ovest. Applicare gli stessi strumenti di cui disponiamo già in ambiente fisico in quello virtuale comporterà costi elevati e il problema di sincronizzare le informazioni dell'ambiente fisico e di quello virtuale.
Un punto critico di questo tipo di soluzioni è l'orchestrazione: la soluzione che viene applicata deve essere automatizzata con lo strumento orchestratore dell'hipervisor utilizzato, in questo caso Kubernetes.
Infine, per poter rimuovere il traffico dall'ambiente virtuale dovremo tunnellizzare tutto il traffico, preferibilmente in modo automatico, e senza interferire con la strategia di rete del proprio controller Containers.

Soluzione

Gigamon dispone di una soluzione completa per la cattura di traffico virtualizzato in ambienti Containers.
La soluzione è completamente orchestrata al momento della connessione del Fabric Manager tramite l'API col servizio Kubernetes.
La soluzione si basa sull'applicazione di container connessi alla funzione di rete dell'ambiente, che supporta attualmente Calico e Flannel.
Il traffico catturato viene indirizzato tramite i tunnel GRE/VXLan verso il SW Vseries nodes, incaricato di realizzare le funzioni di packet brockering (Filtro L2-3-4, Netflow, Slicing, Masking, Sampling, di duplicazione) e orchestrato dal Vseries Controller, che permette la scalabilità verso ambienti con molti nodi e macchine virtuali.
La gestione dei tunnel GRE/VXLan per poter mobilizzare il traffico all'interno dell'infrastruttura di virtualizzazione è totalmente trasparente per l'utente.

Schema



Licenze

Fabric Manager
Traffic Visibility
for Containers

LINK