Cattura di traffico in ambienti VMWare

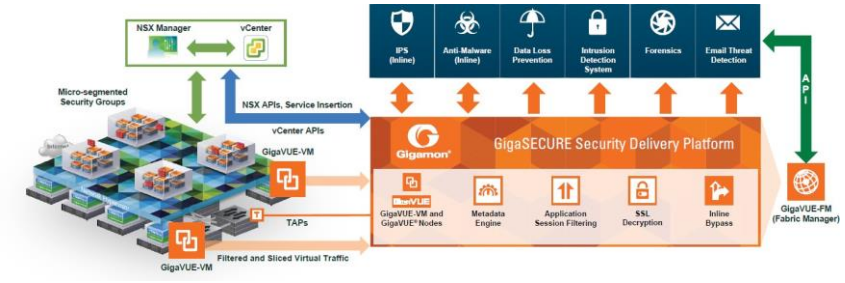
Problema

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 Vcenter o NSX-Manager.
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 hypervisor.

Soluzione

Gigamon dispone di una soluzione completa per la cattura di traffico virtualizzato in ambienti VMWare, sia in ESX che in NSX e NSX-T.
La soluzione è completamente orchestrata al momento della connessione del Fabric Manager tramite l'API con Vcenter e/o NSX Manager. In questo modo, il movimento delle macchine con VMotion è completamente trasparente per l'utente.
La soluzione si basa sull'impiego di una macchina virtuale GigaVUE-VM per ogni host fisico di virtualizzazione, che si connette direttamente al Virtual Distributed Switch di VMWare. Grazie alla connessione con Vcenter/NSX Manager individuiamo automaticamente la topologia di distribuzione della macchine virtuali, e questo ci permette di selezionare il traffico che desideriamo catturare. Questo SW permette di applicare i filtri L2-3-4 prima di incapsulare e rimuovere il traffico.
L'incapsulamento del traffico tramite GRE/VXLan/GMIP è trasparente per l'utente, che deve solo definire il punto terminale del tunnel tramite il suo IP, la porta e il protocollo.

Schema



Licenze

Fabric Manager
NSX Manager
Integration
GigaVUE-VM
Traffic Visibility
for NSX-T

LINK