

Cattura di traffico in ambienti AWS

Problema

Quando i dipartimenti Sistemi delle aziende avviano i progetti di virtualizzazione in cloud, 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 in cloud continua ad aumentare. Portare tutto il traffico del Cloud nell'ambiente del datacenter senza applicare filtri comporta notevoli costi associati, dal momento che il traffico in entrata è gratuito, ma non quello in uscita.

Creare una VPC specifica di strumenti richiede la cattura specifica del traffico, la tunnelizzazione e il trasporto dello stesso in questo nuovo ambiente.

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 EC2 API e CloudWatch.

Soluzione

Gigamon dispone di una soluzione completa per la cattura di traffico virtualizzato in ambienti cloud AWS.

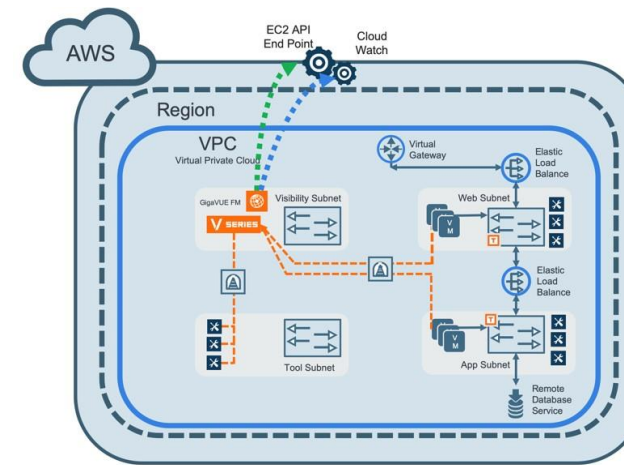
La soluzione è completamente orchestrata al momento della connessione del Fabric Manager tramite l'API con EC2 API e CloudWatch.

La cattura del traffico può anche essere realizzata tramite il servizio VPC Traffic Mirroring (<https://aws.amazon.com/es/blogs/aws/new-vpc-traffic-mirroring/>) o attraverso Virtual TAP, amministrati dal controller G-vTAP,

La soluzione impiega inoltre il SW di Vseries nodes, col compito 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 VXLAN/GRE per poter mobilizzare il traffico all'interno dell'infrastruttura di virtualizzazione è totalmente trasparente per l'utente.

Schema



Licenze

Fabric Manager
Traffic Visibility for AWS

LINK