Capture du trafic en environnement AWS

Enjeu

Lorsque les équipes informatiques lancent des projets de virtualisation cloud, les équipes réseau et sécurité sont confrontées à un défi : intégrer à ce nouvel environnement les politiques de surveillance et de sécurité déjà déployées sur le réseau physique. Beaucoup se contentent d'ignorer le problème... mais l'infrastructure du cloud ne cesse de s'étendre. Acheminer tout le trafic du cloud vers le datacenter, sans filtrage, implique des coûts importants, puisque le trafic en amont est gratuit, mais pas celui en aval.

La création d'un réseau spécifique Amazon Virtual Private Cloud nécessite de capturer le trafic de manière sélective, de le tunneliser et de le transporter vers le nouvel environnement.

L'orchestration est, quant á elle, essentielle : la solution déployée doit fonctionner de manière automatisée avec l'orchestrateur d'hyperviseur utilisé, en l'occurrence l'API EC2 et CloudWatch.

Solution

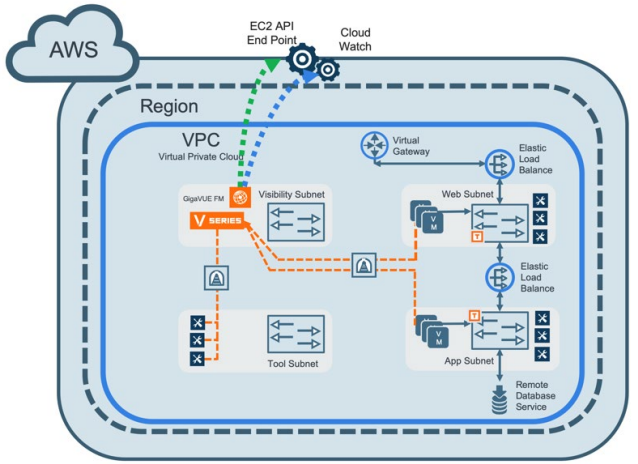
Gigamon dispose d'une solution complète permettant de capturer le trafic virtualisé en environnement AWS cloud. Cette solution est entièrement pilotée par le gestionnaire Fabric Manager via l'API EC2 et CloudWatch.

La capture du trafic est réalisée soit via le service VPC Traffic Mirroring (.https://aws.amazon.com/es/blogs/aws/new-vpc-traffic-mirroring/), soit par des TAP virtuels gérés par le contrôleur G-vTAP.

La solution s'appuie sur le déploiement de logiciels de nœuds nVseries pour les fonctions de Packet Brokering (filtrage L2-3-4, Netflow, Slicing, Masking, Sampling, Déduplication). Ces logiciels sont pilotés par le contrôleur Vseries qui permet d'évoluer vers des environnements plus complexes, comportant de nombreux nœuds et machines virtuelles.

La gestion des tunnels VXLan/GRE pour le transfert du trafic dans l'infrastructure de virtualisation est totalement invisible pour l'utilisateur.

Architecture



Licences

Fabric Manager

Traffic Visibility for AWS

LIEN