Gestion du trafic Nord Sud dans un environnement de secours Cloud

Architecture Cloud et Réseaux · https://preview.nuabee.fr/documents/gestion-trafic-firewall-nord-sud/

Dans un contexte de déclenchement d'un Plan de Reprise d'Activité (PRA), la gestion du trafic réseau dit ***nord-sud*** (c'est-à-dire les flux entrants et sortants entre les utilisateurs, les systèmes externes ou partenaires et l'environnement Cloud de secours) est une étape cruciale afin de garantir le niveau de sécurité et de disponibilité adéquat.

Nuabee a la capacité de s'adapter à des contraintes techniques et organisationnelles des clients. Cet article présente de manière synthétique les **deux options de firewall** proposées par Nuabee pour répondre à ces besoins.

Option 1 : firewall natif Cloud via Security Groups et ACL

La première option repose exclusivement sur les **mécanismes de sécurité natifs du Cloud T Cloud Public (anciennement Open Telekom Cloud)**, à savoir :

- le routage réseau standard,
- les *Security Groups*,
- les *Access Control Lists (ACL)*.

Cette approche permet de définir des règles de filtrage directement au niveau des ressources Cloud (instances, sous-réseaux, réseaux). ***Les Security Groups agissent comme des firewalls distribués, appliquant des règles de manière fine et dynamique, tandis que les ACL permettent un contrôle plus global des flux au niveau réseau.***

Les **groupes de sécurité** agissent comme des pare-feu virtuels qui contrôlent le trafic réseau à destination et en provenance des instances. Ces groupes permettent de définir des règles de trafic basées sur des critères spécifiques :

- **Règles d'entrée et de sortie** : Les règles d'entrée spécifient le trafic autorisé à entrer dans une instance, tandis que les règles de sortie contrôlent le trafic sortant. Par exemple, une règle d'entrée peut autoriser uniquement le trafic HTTP (port 80) et HTTPS (port 443) à partir de certaines adresses IP.

- **Filtrage par IP et port** : Les administrateurs peuvent restreindre l'accès à certaines plages d'adresses IP ou à des ports spécifiques, ce qui permet de limiter les points d'entrée potentiels aux seules adresses ou services nécessaires.
- **Stateless vs Stateful** : Les groupes de sécurité sont généralement stateful, ce qui signifie que les réponses au trafic autorisé sont automatiquement autorisées, simplifiant ainsi la gestion des règles.

Cette solution est particulièrement adaptée au déploiement rapide et simple d'une solution de pare-feu. Elle offre un bon niveau de sécurité et couvre la plupart des besoins sans nécessiter le déploiement ou la gestion d'équipements supplémentaires, tout en s'intégrant pleinement aux services de T Cloud Public.

La configuration classique d'un firewall "on-prem" ne fonctionne pas exactement comme celle dans le Cloud, puisqu'il y a une différnte dans l'architecture/la segmentation reseau. La façon même de gérer le trafic change dans le cloud (règles sur les VMs plutôt que le Firewall) entrainant une application des règles différente mais offrant le même niveau de sécurité tout en essayant de simplifier au maximum le réseau (regroupement de VLANs, etc...).

Option 2 : appliance de sécurité du client intégrée au cloud

La deuxième option s'adresse aux clients disposant déjà de leur **propre appliance de sécurité** (physique ou virtuelle) et souhaitant pouvoir l'utiliser dans l'environnement cloud de secours.

Attention : L'appliance doit être compatible cloud et doit être disponible au format KVM.

Le but est souvent d'interconnecter les sites distants au site de PRA (IPSec, SDWAN, ...) ou encore d'utiliser le client VPN SSL/IPsec du firewall (client VPN déployé sur les poste de travail) pour la reconnexion des utilisateurs nomades.

Dans ce cas, Nuabee accompagne l'intégration de l'appliance dans le Cloud. Nuabee met à disposition cette appliance pour que le client (ou son prestatire) puisse effectuer la configuration des flux réseau et du routage (et si besoin l'interconnexion avec les environnements existants).

La configuration d'un firewall "on-prem" ne fonctionne pas exactement comme celle dans le Cloud, puisqu'on n'a pas la même architecture/segmentation reseaux. Il est donc nécessaire d'adapter la configuration du firewall au contexte du Cloud. La façon même de gérer le trafic changant dans le cloud (règles sur les VMs plutôt que le Firewall).

Elle est particulièrement pertinente pour les organisations soumises à des contraintes spécifiques (de type tunnel avec certificats) ou utilisant de fonctionnalités avancées de leurs équipements de

sécurité (IDS/IPS). La gestion classique du routeur s'effectuant plutôt via les mécanismes natifs du cloud.

Attention : Cette option nécessite, la plupart du temps, d'une licence supplémentaire pour cette appliance. Le client est amené à se rapprocher de son revendeur afin de se fournir cette licence, Nuabee ne le faisant pas.

Une approche adaptée à chaque besoin

Plutôt que de proposer une solution unique, Nuabee privilégie une approche pragmatique et adaptée au besoin du client. Le choix entre firewall natif Cloud ou appliance spécifique dépend donc :

- Du niveau de sécurité attendu.
- Des contraintes techniques.
- De l'architecture existante.
- Des fonctionnalités indispensables.
- De la politique de sécurité en place.

Dans tous les cas, Nuabee s'appuie sur son expertise Cloud et sécurité pour concevoir une gestion du trafic nord-sud cohérente, sécurisée et alignée avec les besoins métiers de ses clients.