Gestion du trafic et de la sécurité dans le Cloud

Architecture Cloud et Réseaux · https://preview.nuabee.fr/documents/gestion-du-trafic-et-de-la-securite-dans-le-cloud/

Introduction

Cet article s'adresse à ceux qui souhaitent comprendre comment fonctionne la gestion du trafic réseau et de la sécurité dans le Cloud, notamment dans le cadre d'un Plan de Reprise d'Activité (PRA) by Nuabee. Il aidera à choisir entre conserver votre Appliance de sécurité actuelle ou utiliser les solutions natives du Cloud combinées aux services Nuabee.

Cloud vs On-Premise : quelles différences pour votre infrastructure réseau ?

L'approche On-Premise classique

Dans un environnement On-Premise, l'appliance de sécurité est au cœur de la gestion des flux réseau, de la sécurité et de la segmentation de l'infrastructure.

L'approche Cloud : le SDN (Software Defined Networking)

Le Cloud repose sur une couche logicielle appelée **SDN (Software Defined Networking)**, imposée par le fournisseur Cloud. Cette couche remplace l'appliance de sécurité physique et offre des fonctionnalités équivalentes :

- **Security Groups** : autorisent ou refusent le trafic au niveau de chaque machine virtuelle.
- **ACL (Access Control Lists) ou Firewall** : gèrent les communications au niveau des sous-réseaux (équivalent des VLAN On-Premise).

Un article dédié explique ces fonctionnalités

Point clé : la couche SDN du Cloud ne peut pas être remplacée par une appliance de sécurité tierce. Elle constitue le socle de sécurité obligatoire de l'infrastructure Cloud.

Faut-il déployer une appliance de sécurité dans le Cloud ?

Nuabee peut instancier une machine virtuelle à partir d'une image fournie par vos soins, pour reproduire votre appliance de sécurité dans le Cloud.

Cas d'usage pertinents

- Rester dans une logique fermée **SD-WAN** déjà déployée en On-Premise.
- Conserver le **VPN actuel** utilisé On-Premise pour des raisons de compatibilité (ex : SD-WAN, IPSEC propriétaires) ou de politique interne.
- Utiliser des fonctionnalités avancées de sécurité (Exemple: IDS/IPS)

Aspects financiers à anticiper

- **Coûts supplémentaires dans le Cloud** : consommation de ressources (CPU, RAM, stockage) en fonction du gabarit de l'appliance et de son mode de déploiement (permanent ou à la demande).
- **Seconde licence souvent nécessaire** : la licence On-Premise ne couvre généralement pas l'instance Cloud. Nuabee ne fournit pas cette licence, il faudra donc se rapprocher d'un revendeur pour l'obtenir.

Limites techniques à prendre en compte

- Disponibilité d'une **image virtuelle adaptée** au Cloud Provider (format KVM) **obligatoire**.
- **Nombre d'interfaces réseau** :Selon le nombre d'interfaces nécessaire, un impact fort sur le gabarit avec des interfaces réseaux supplémentaires est à prévoir afin de répliquer la topologie réseau (8 maximum). Cela peut également amener à faire des regroupements réseau.
- **Import de la configuration On-Premise** : la couche SDN du Cloud est non-compatible avec une architecture On-Premise (voir section « Cloud vs On-Premise »), ce qui **nécessite d'adapter** la configuration spécifiquement pour le Cloud.
- **Maintenance supplémentaire** : A chaque évolution de configuration On-Premise, il peut êter nécessaire d'effectuer une mise à jour en parallèle sur l'appliance Cloud.

Recommandation Nuabee

Dans la majorité des cas, il n’est pas recommandé de déployer une appliance de sécurité virtuelle dans le Cloud. Les solutions natives du Cloud, combinées aux services Nuabee, offrent une meilleure flexibilité, des coûts maîtrisés et une maintenance simplifiée.

Les solutions proposées par Nuabee

Atelier topologie réseau

Lors de l’avant-vente, de l’onboarding ou en amont d’un test de reconnexion, Nuabee organise des ateliers dédiés pour :

1. Qualifier les spécificités de votre réseau.
2. Comprendre votre infrastructure et sa segmentation actuelle.
3. Proposer une architecture Cloud adaptée à votre PRA et à vos contraintes métier.

Ces ateliers permettent de concevoir une solution sur-mesure, alignée avec vos besoins réels.

Les différents services de reconnexion pour votre PRA

Afin de reconnecter les utilisateurs et les sites lors d’un PRA, Nuabee peut proposer les solutions suivantes :

- VPN SSL utilisateurs VPN pensé pour être compatible avec la fonctionnalité native de Windows, simple à déployer et à gérer.

Plus de détail

- Tunnel(s) IPsec site-à-site : pour reconnecter vos sites distants

Plus de détail

Vous souhaitez tout de même déployer une appliance virtuelle ?

Si la conservation de votre appliance de sécurité reste nécessaire pour votre organisation, Nuabee peut vous accompagner.

À prévoir :

- Des ateliers de reconnexion supplémentaires pour concevoir l’architecture.
- Une mise en œuvre spécifique, adaptée à vos besoins et à votre appliance.

Chaque projet étant unique, nos équipes vous accompagnent pour définir la solution la plus adaptée à votre contexte.