Les groupes de sécurité et ACL/Firewall dans le Cloud

Architecture sécurité · https://nuabee.fr/documents/les-groupes-de-securite-et-acl-dans-le-cloud/

Le besoin des clients

Dans un contexte de PRA Nuabee, le Client dispose d'un espace de secours dans le Cloud T Cloud Public (anciennement Open Telekom Cloud) qui lui est dédié, entièrement inaccessible depuis l'extérieur (bulle de confiance) que l'on appelle tenant.

Cet article explique l'articulation entre les concepts de tenant (ou projet) et les solutions de sécurité complémentaire qui existent au travers des groupes de sécurité et des ACL/Firewall.

Principes d'architecture tenant et VPC

Chaque espace de secours d'un client est hébergé dans un tenant dédié. Un tenant est un concept utilisé pour regrouper des ressources (VM, subnets, utilisateurs, ...) au sein d'un environnement cloud OpenStack qui permet une meilleure organisation, une isolation des ressources et un contrôle d'accès au sein de l'infrastructure cloud.

A l'intérieur d'un tenant, il est possible d'avoir plusieurs VPC. Le service Virtual Private Cloud (VPC) permet de fournir des réseaux virtuels logiquement isolés, configurables et gérables pour les serveurs (ECS), ce qui améliore la sécurité des ressources dans le système Cloud et simplifie le déploiement du réseau.

Security Groups : quelle utilisation ?

Un groupe de sécurité contient une ou plusieurs règles de sécurité :

- Les règles s'appliquent soit en entrée, soit en sortie
- Permet d'autoriser des paquets TCP/UDP/ICMP depuis ou vers un CIDR ou un autre Security group

- Par défaut, une machine peut recevoir des paquets des autres machines d’un même groupe de sécurité et envoyer des paquets vers n’importe où.

Le peering Inter VPC

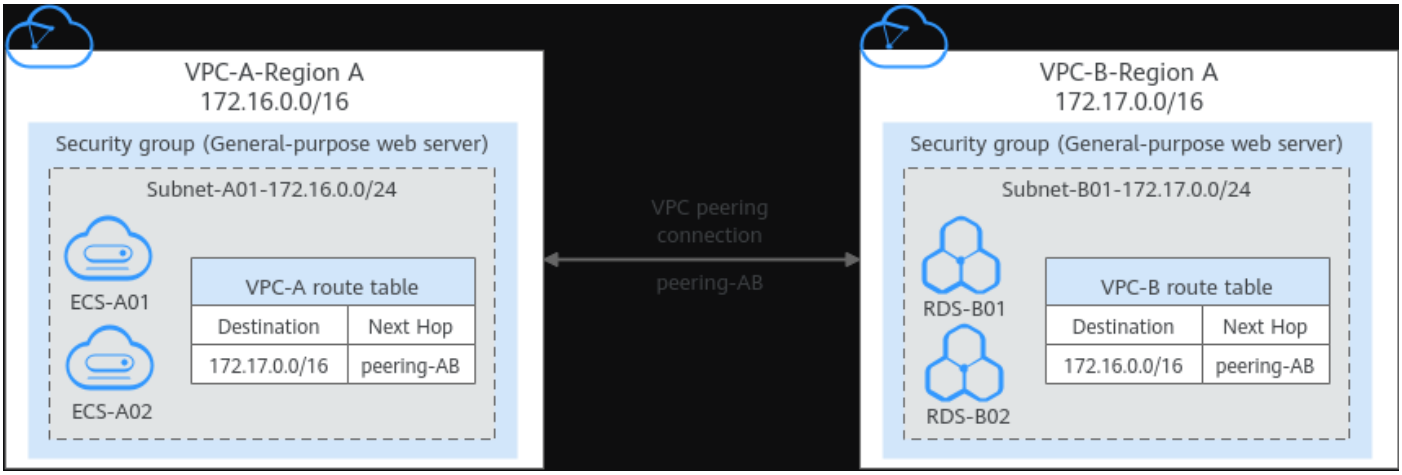
Le peering VPC est une fonction qui permet de relier deux VPC dans T Cloud Public Fonctionne entre des VPC locaux (dans un même tenant) et distants (entre différent tenant)

- dans les 2 cas le montage du peering doit être accepté formellement de chaque côté

Un appairage de VPC est accompagné de règle de routage qui indiquent quels CIDR peuvent traverser l’appairage.

Elles doivent être entrées des deux côtés si on souhaite une connexion bidirectionnelle

- Une architecture multi-peering peut permettre la centralisation de multiples flux.



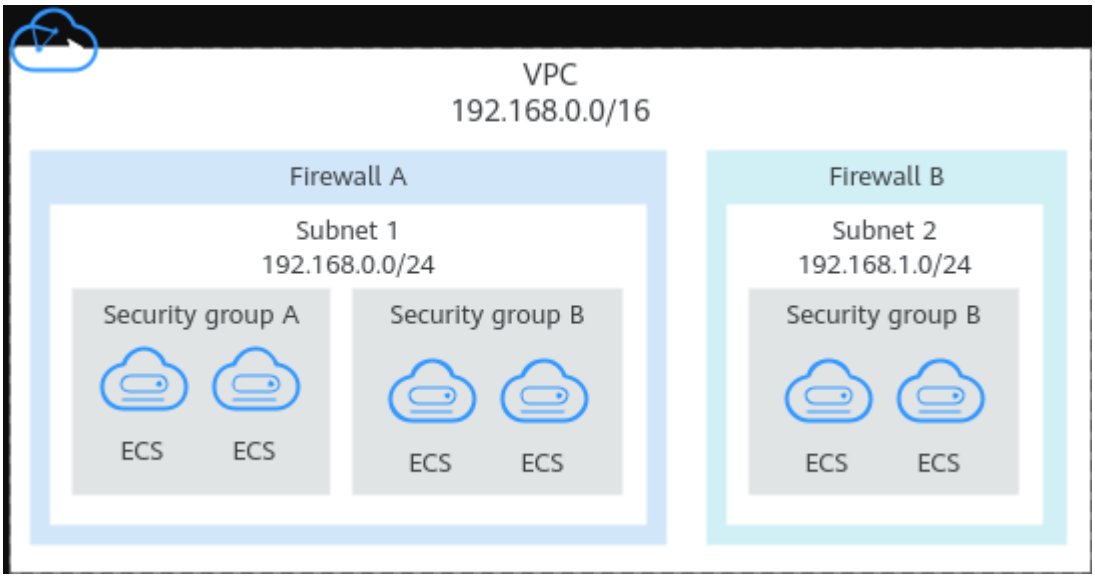
Les principes d’un ACL/Firewall dans un VPC

Les ACL/Firewall réseau (liste de contrôle d’accès) sont une couche de sécurité facultative d’un VPC qui :

- Fait office de pare-feu pour le contrôle du trafic entrant et sortant d’un ou plusieurs sous-réseaux.

Les listes ACL/Firewall réseau utilisent des règles similaires aux groupes de sécurité afin d’ajouter une couche de sécurité supplémentaire à un VPC.

- Permet une seconde couche de sécurité au dessus des groupes de sécurité pour limiter globalement des flux



Les ACL/Firewall viennent en complément des groupes de sécurité (security groups).

- Par exemple pour bloquer globalement des CIDR entiers sans avoir à paramétrer chaque machine
- Pour autoriser uniquement les IP d'une entreprise à accéder à des services cloud, notamment dans le cas d'un environnement SI Cloud

Elles permettent d'appliquer des règles globales de sécurité au niveau d'un réseau entier.

Dans le cas de la communication entre des machines dans le Cloud, via du peering par exemple, les ACL/Firewall permettent de gérer plus finement le trafic autorisé dans le cadre peering inter-VPC

ACL/Firewall réseau versus Groupe de Sécurité

Groupe de sécurité	ACL réseau
Fonctionne au niveau instance (première couche de défense)	Fonctionne au niveau sous-réseau (seconde couche de défense)
S'applique à une instance uniquement si quelqu'un indique le groupe de sécurité lors du lancement de l'instance, ou associe ultérieurement le groupe de sécurité à l'instance	S'applique automatiquement à toutes les instances des sous-réseaux auxquels il est associé (couche de défense de secours, de sorte que vous n'avez pas à compter sur quelqu'un qui indique le groupe de sécurité)
Permet uniquement de spécifier des IP Source **OU** destination (règle d'entrée ou de sortie)	Permet de spécifier des IP source **ET** de destination

Est avec état (stateful) : le trafic de retour est automatiquement autorisé, sauf si explicitement interdit.	
Nous évaluons toutes les règles avant de décider si le trafic doit être autorisé	Nous traitons les règles par ordre numérique pour décider si le trafic doit être autorisé