Service de VPN IPsec – VPNaaS

Architecture Cloud et Réseaux · https://preview.nuabee.fr/documents/service-de-vpn-vpnaas/

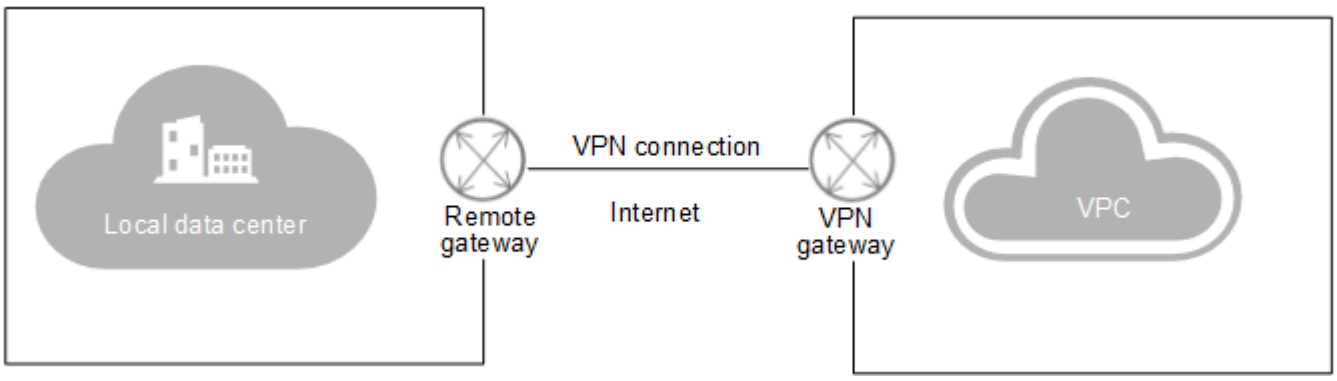
Virtual Private Network

Un réseau privé virtuel (VPN) établit un tunnel de communication chiffré, basé sur Internet, entre un utilisateur et un Cloud privé virtuel (VPC).

Par défaut, les serveurs (ECS) d'un VPC ne peuvent pas communiquer avec le datacenter client ou le réseau privé de ce dernier. Pour permettre la communication entre eux, il faut utiliser un VPN qui se compose d'une passerelle VPN et d'une ou plusieurs connexions VPN.

La fonctionnalité de VPN as a Service du VPC permet de créer à la demande des VPN IPSec sur Internet pour chiffrer le trafic depuis le VPC vers le End Point IPsec de son choix. Il est alors possible d'établir des connexions sécurisées entre les infrastructures client et le Cloud T Cloud Public.

Avec le VPN, il est donc possible de connecter à un VPC et d'accéder aux ressources qui s'y trouvent (serveurs, Gateway, …) depuis les différents sites client.

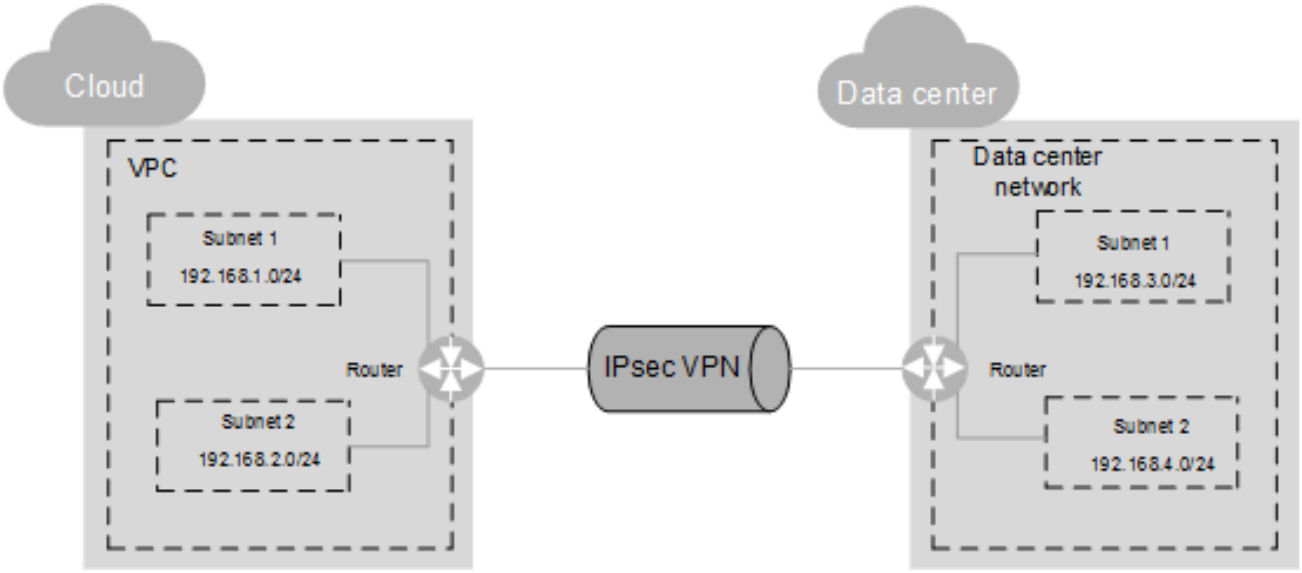


Une passerelle VPN fournit une sortie Internet pour un VPC et travaille avec la passerelle distante dans le datacenter local.

VPN IPsec

Actuellement, les VPN site à site et les VPN en étoile sont pris en charge. Il est nécessaire de configurer des VPN dans le datacenter client et dans le VPC du tenant client dans le cloud T Cloud

Public pour établir la connexion VPN IPsec.



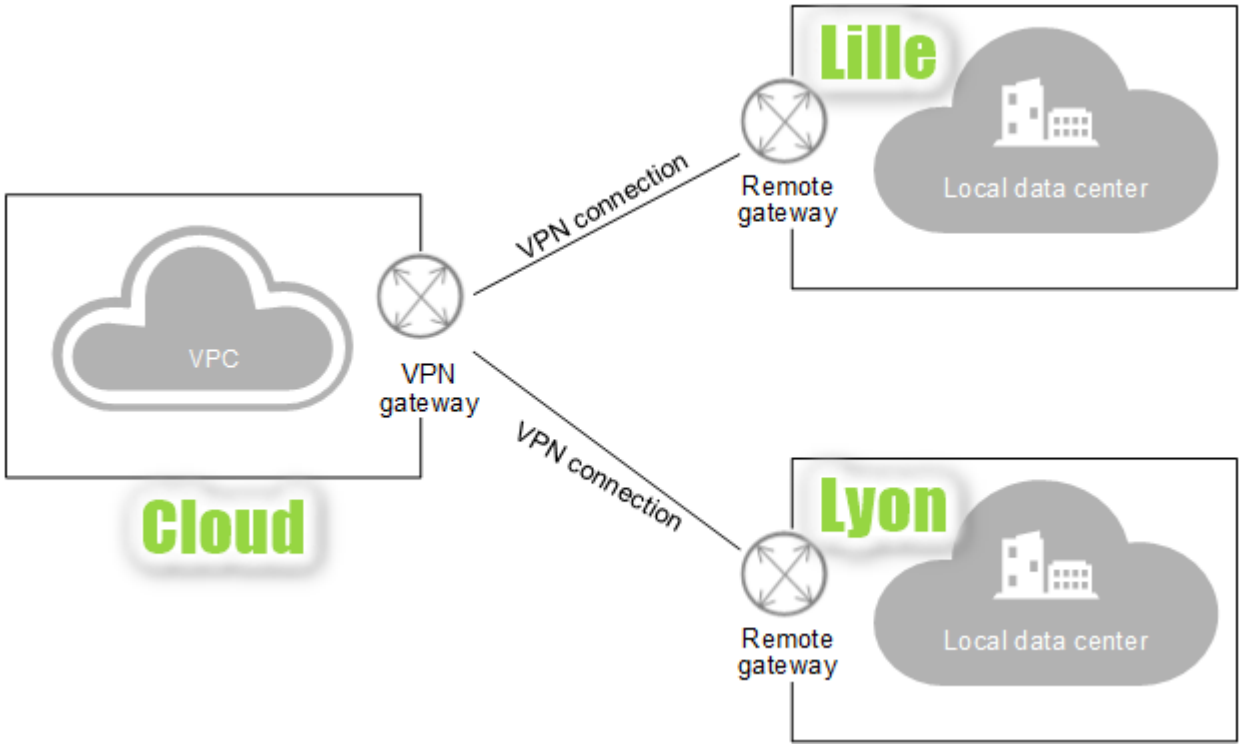
Pour que le VPN IPsec fonctionne, ils doivent utiliser les mêmes configurations de stratégie IKE et IPsec.

Protocole	Description	Contrainte
RFC 2409	Définit le protocole IKE, qui négocie et vérifie les informations clés pour protéger les VPN.	• Utiliser la clé pré-partagée (PSK) accord entre homologues IKE. • Utilise le mode principal pour la
RFC 4301	Définit l'architecture IPsec, les services de sécurité offerts par IPsec et la collaboration entre les composants.	Utiliser le tunnel IPsec pour configur VPN.

Connexion VPN d'un site vers plusieurs sites

Il est possible de configurer un VPN pour connecter plusieurs sites locaux à un seul VPC Cloud. Par défaut, un VPC peut disposer d'un maximum de cinq VPN IPsec mais il est possible d'augmenter le quota.

Dans ce cas, les blocs CIDR du sous-réseau de chaque site impliqué dans la connexion VPN ne peuvent pas se chevaucher.



Le bloc CIDR d'un sous-réseau peut être identique au bloc CIDR du VPC (pour un seul sous-réseau dans le VPC) ou à un sous-ensemble (pour plusieurs sous-réseaux dans le VPC).

Les blocs CIDR suivants sont pris en charge :

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255