IPsec VPN Service (VPNaaS)

Cloud and Network Architecture · https://nuabee.com/documents/ipsec-vpn-service-for-drp/

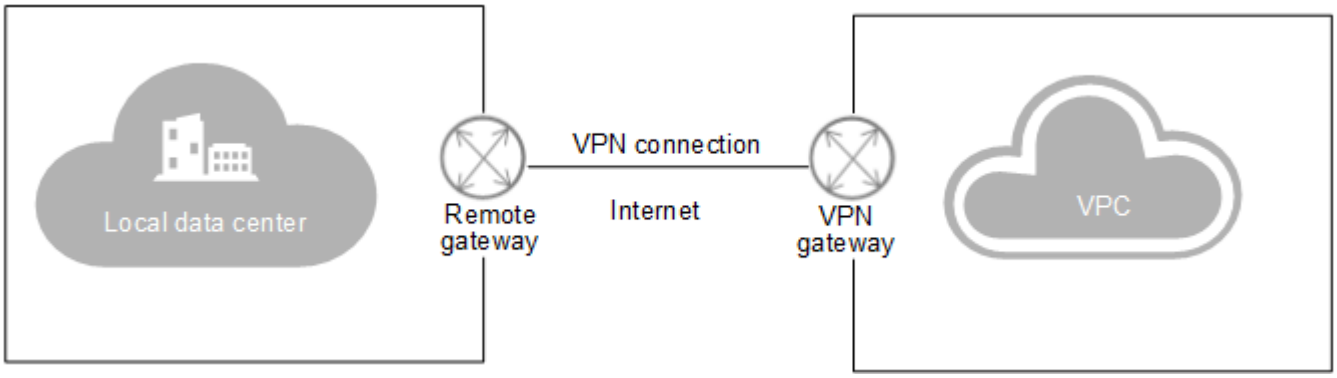
Virtual Private Network

A virtual private network (VPN) establishes an encrypted communication tunnel, based on the Internet, between a user and a virtual private cloud (VPC).

By default, servers (ECS) in a VPC cannot communicate with the customer's data center or private network. To enable communication between them, you must use a VPN, which consists of a VPN gateway and one or more VPN connections.

The VPC's VPN as a Service feature allows you to create on-demand IPSec VPNs over the internet to encrypt traffic from the VPC to the IPSec endpoint of your choice. This makes it possible to establish secure connections between customer infrastructures and the OTC Cloud.

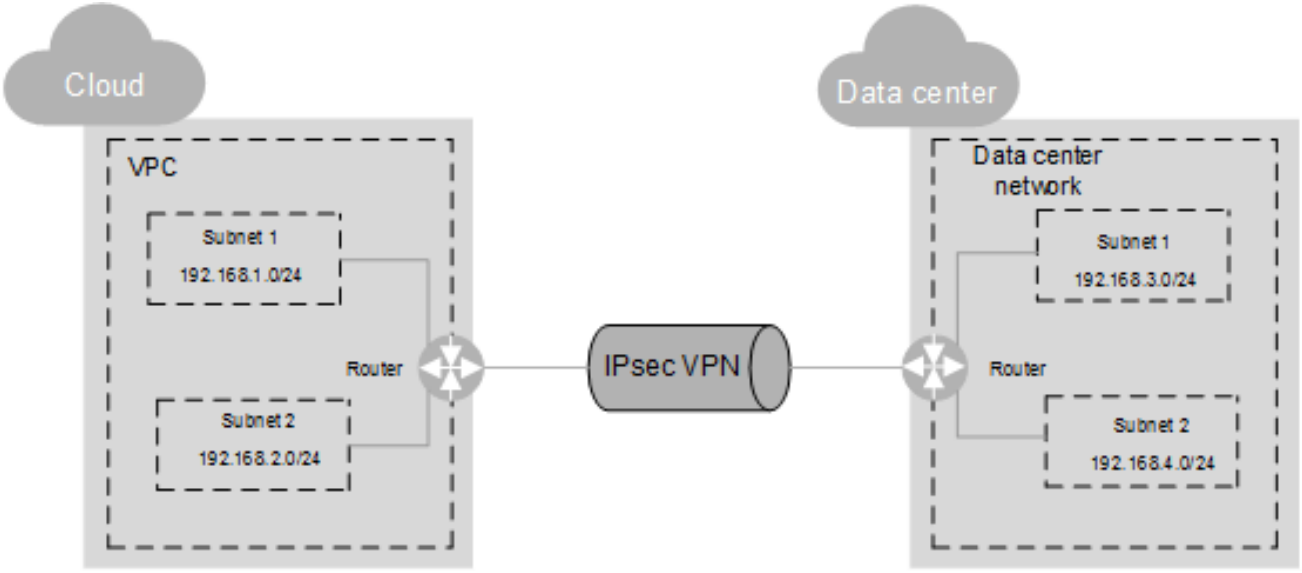
With VPN, it is therefore possible to connect to a VPC and access the resources located there (servers, gateways, etc.) from different client sites.



A VPN gateway provides an Internet exit for a VPC and works with the remote gateway in the local data center.

VPN IPsec

Currently, site-to-site VPNs and star VPNs are supported. It is necessary to configure VPNs in the customer data center and in the customer tenant's VPC in the OTC cloud to establish the IPsec VPN connection.



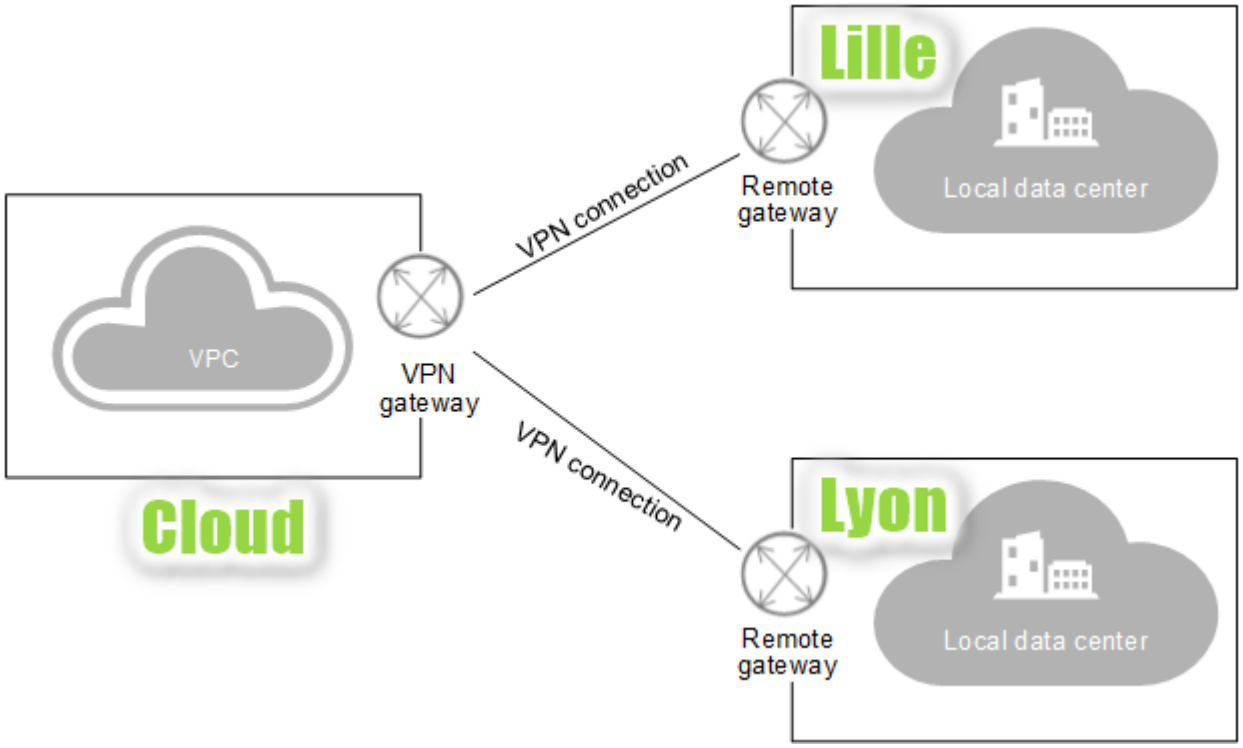
For the IPsec VPN to work, they must use the same IKE and IPsec policy configurations.

Protocol	Description	Constraint
RFC 2409	Defines the IKE protocol, which negotiates and verifies key information to protect VPNs.	• Use the pre-shared key (PS agreement between IKE pe • Use the main mode for trad
RFC 4301	Defines the IPsec architecture, the security services offered by IPsec, and the collaboration between components.	Use the IPsec tunnel to set up a

VPN connection from one site to multiple sites

It is possible to configure a VPN to connect multiple local sites to a single Cloud VPC. By default, a VPC can have a maximum of five IPsec VPNs, but it is possible to increase this quota.

In this case, the CIDR blocks of the subnet of each site involved in the VPN connection cannot overlap.



The CIDR block of a subnet can be identical to the CIDR block of the VPC (for a single subnet in the VPC) or to a subset (for multiple subnets in the VPC).

The following CIDR blocks are supported:

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