# IPsec VPN service – VPNaaS

Cloud and Network Architecture · https://nuabee.com/documents/service-de-vpn-vpnaas/

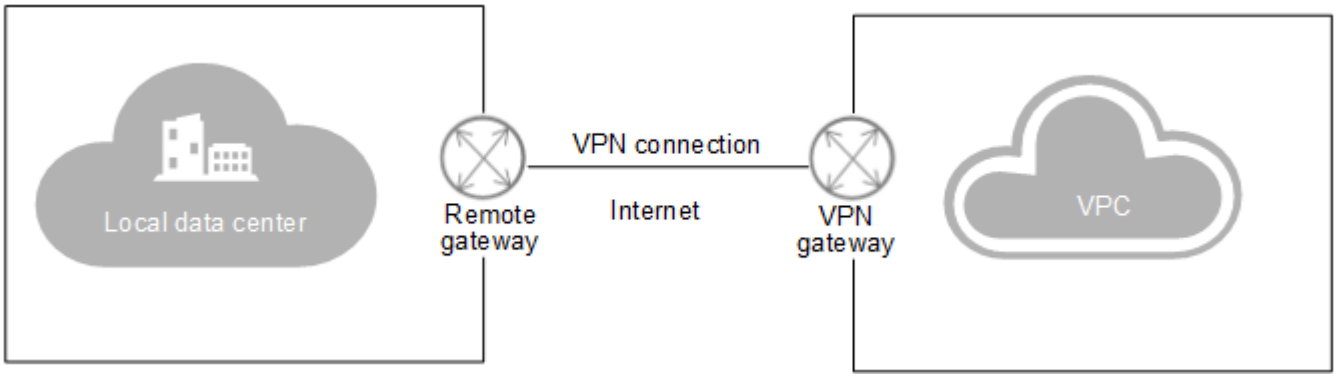
## Virtual Private Network

A Virtual Private Network (VPN) establishes an encrypted, Internet-based communication tunnel between a user and a Virtual Private Cloud (VPC).

By default, the servers (ECS) of a VPC cannot communicate with the customer's datacenter or private network. To enable communication between them, a VPN must be used, consisting of a VPN gateway and one or more VPN connections.

The VPC's VPN as a Service feature enables IPSec VPNs to be created on demand over the Internet, encrypting traffic from the VPC to the IPsec End Point of choice. Secure connections can then be established between customer infrastructures and the OTC Cloud.

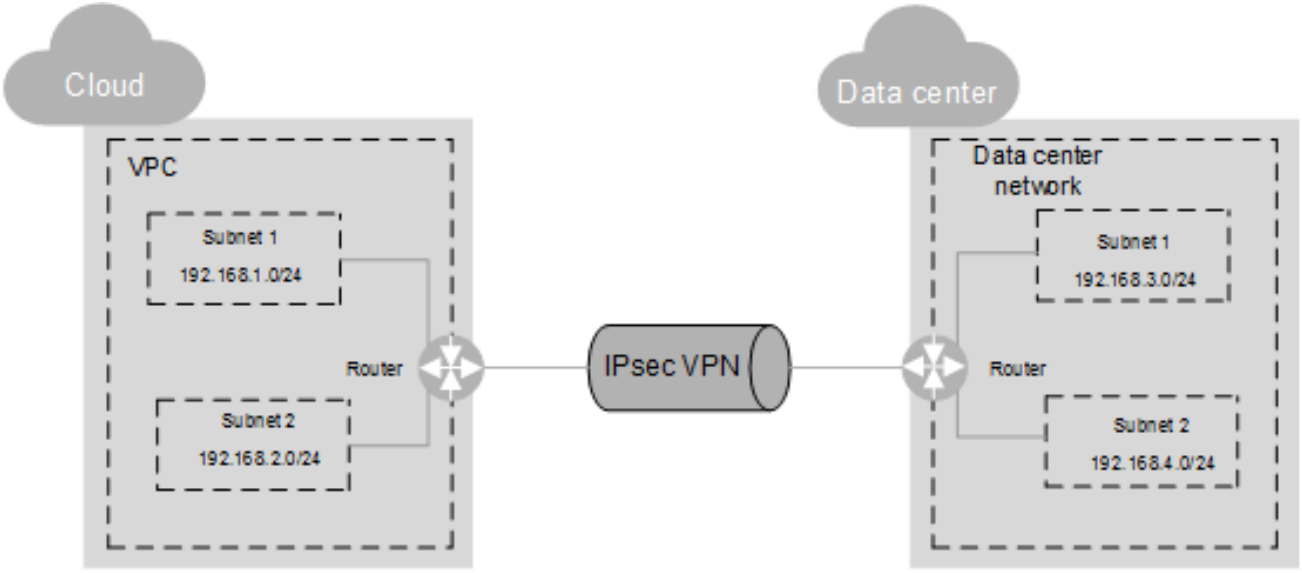
With VPN, it is therefore possible to connect to a VPC and access its resources (servers, gateway, etc.) from different customer sites.




A VPN gateway provides an Internet outlet for a VPC and works with the remote gateway in the local datacenter.

## IPsec VPN

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



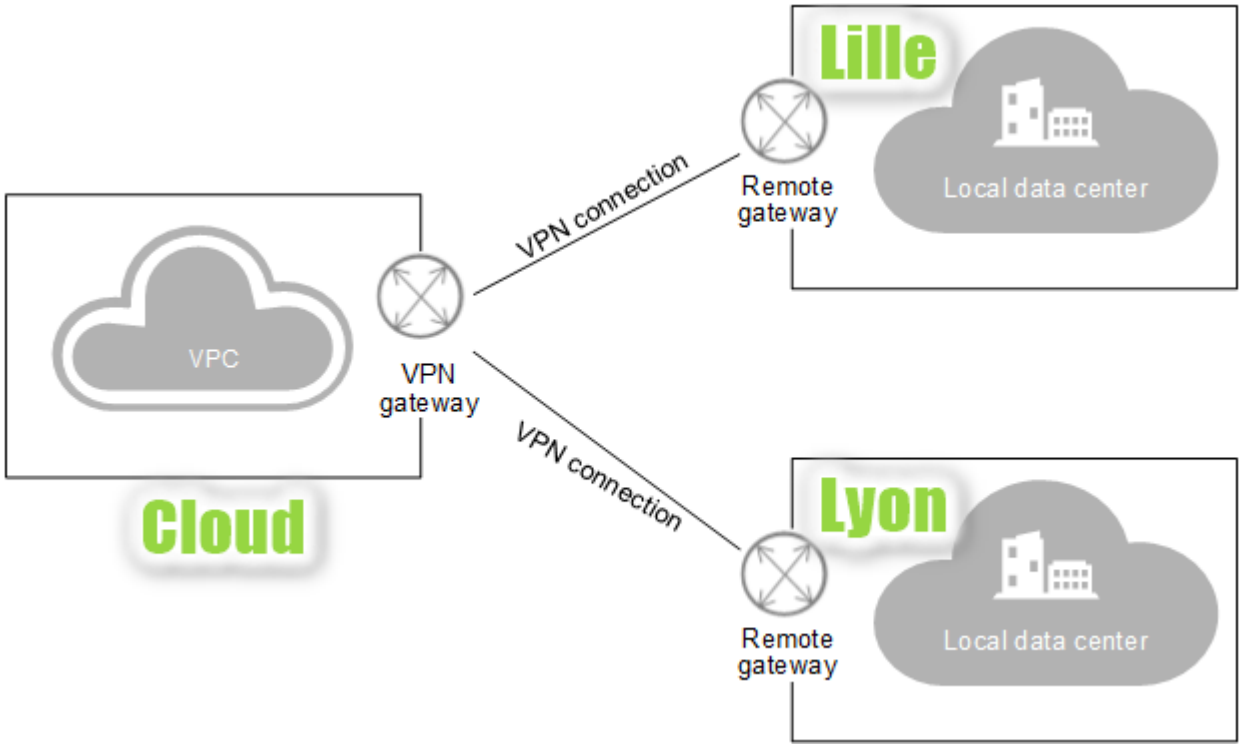

For the IPsec VPN to work, they must use the same IKE and IPsec policy configurations.

| Protocol | Description | Constraint |
| --- | --- | --- |
| RFC 2409 | Defines the IKE protocol, which negotiates and verifies key information to protect VPNs. | • Use the pre-shared key (PSK) to reach agreement between IKE peers.<br>• Use main mode for negotiation. |
| 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. |

## VPN connection from one site to multiple sites

A VPN can be configured 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 the quota.

In this case, the subnet CIDR blocks of each site involved in the VPN connection may not 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 several 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