Virtual Private Network

Service Overview

Issue 01
Date 2020-05-30
Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.
## Contents

1 Virtual Private Network
2 IPsec VPN
3 Application Scenarios
4 Usage Restrictions
5 Reference Standards and Protocols
6 VPN and Other Services
7 Billing
8 Region and AZ
A Virtual Private Network (VPN) establishes an encrypted, Internet-based communications tunnel between a user and a Virtual Private Cloud (VPC). With VPN, you can connect to a VPC and access service resources in it.

By default, ECSs in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN.

A VPN consists of a VPN gateway and one or more VPN connections. A VPN gateway provides an Internet egress for a VPC and works together with the remote gateway in the local data center. A VPN connection uses the Internet-based encryption technology to connect the VPN gateway and the remote gateway to enable communication between the local data center and VPC. The VPN connection allows you to quickly build secure hybrid cloud environment. Figure 1-1 shows the VPN networking.

**Figure 1-1** VPN networking

---

**VPN Gateway**

A VPN gateway is an egress gateway of a VPC. With a VPN gateway, you can create a secure, reliable, and encrypted connection between a VPC and the corporate data center or between a VPC and another VPC in another region.

The VPN gateway works together with the remote gateway in the local data center. Each local data center must have a remote gateway, and each VPC must have a VPN gateway. The VPN service allows you to set up point-to-point VPN connections or VPN connections from one point to multiple points. A VPN gateway can connect to one or more remote gateways. Figure 1-2 shows the VPN gateway.
**Figure 1-2** VPN gateway

![VPN gateway diagram]

**VPN Connection**

A VPN connection uses the Internet-based IPsec encryption technology to establish a secure and reliable communications tunnel between a VPN gateway and the remote gateway in a local data center. Currently, only IPsec VPN connections are supported.

A VPN connection uses the IKE and IPsec protocols to encrypt transmitted data, ensuring data security and reliability. A VPN connection transmits data over the Internet, which ensures low costs.
The Internet Protocol Security (IPsec) VPN is an encrypted tunneling technology that uses encrypted security services to establish confidential and secure communication tunnels between different networks.

In Figure 2-1, a VPC has two subnets: 192.168.1.0/24 and 192.168.2.0/24. On your router deployed in your physical data center, you also have two subnets: 192.168.3.0/24 and 192.168.4.0/24. You can use VPN to enable subnets in your VPC to communicate with those in your data center.

Currently, the site-to-site VPN and hub-spoke VPN are supported. You need to set up VPNs in both your data center and the VPC to establish the VPN connection.

Ensure that the VPN in your VPC and that in your data center use the same Internet Key Exchange (IKE) and IPsec policy configurations. Your device complies with IPsec standards and protocols.
3 Application Scenarios

With the VPN between the VPC and your traditional data center, you can easily use the ECSs and block storage resources provided by the cloud platform. Applications can be migrated to the cloud and additional web servers can be deployed to increase the computing capacity on a network. In this way, a hybrid cloud is built, which reduces IT O&M costs and protects enterprise core data from being leaked.

The VPN service allows you to set up site-to-site VPN connections or VPN connections from one site to multiple sites.

Site-to-site VPN connection

You can set up a VPN to connect a local data center to a VPC, thus building a hybrid cloud. Figure 3-1 shows a site-to-site VPN connection.

![Figure 3-1 Site-to-site VPN connection](image)

VPN connection from one site to multiple sites

You can also set up a VPN to connect multiple local data centers to a VPC, thus building a hybrid cloud. Figure 3-2 shows a VPN connection from one site to multiple sites.

NOTE

The subnet CIDR blocks of each site involved in the VPN connection cannot overlap.
**Figure 3-2** VPN connection from one site to multiple sites

![Diagram of VPN connection from one site to multiple sites]
Observe the following constraints when using the VPN service:

- A maximum of two VPN gateways can be created in each account by default.
- A maximum of 12 VPN connections can be created in each account by default.

Before purchasing VPN gateways, check your remaining quota. If the quota has been reached, submit a service ticket to request for quota increase.
The following standards and protocols are associated with the IPsec VPN:

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and its use with IPsec
- RFC 3625: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2) Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4322: Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4359: The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2)
- RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2)
## Table 6-1 Related services

<table>
<thead>
<tr>
<th>Related Operation</th>
<th>Related Service</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only after a VPC is created, services in the local data center can be migrated to the cloud through a VPN.</td>
<td>VPC</td>
<td>Creating a VPC</td>
</tr>
<tr>
<td>With the VPC service, you can create security groups, define security group rules, and add ECSs in the VPC to the security groups, improving ECS access security.</td>
<td>VPC</td>
<td>Creating a Security Group</td>
</tr>
<tr>
<td>A NAT gateway enables servers in a local data center to access the Internet or provides services that are accessible from the Internet.</td>
<td>NAT Gateway</td>
<td>Using SNAT and DNAT Rules to Enable Inter-Cloud High-Speed Internet Access</td>
</tr>
</tbody>
</table>
HUAWEI CLOUD VPN uses pay-per-use billing. You pay only for what you use, for as long as you need it. No complex forecasts and budgets are required. You can buy one or more VPN connections and will be billed based on the number of used VPN connections and usage duration.

**Billing Items**

<table>
<thead>
<tr>
<th>Billing Option</th>
<th>Item 1</th>
<th>Item 2</th>
<th>Billing Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billed by bandwidth</td>
<td>VPN gateway bandwidth</td>
<td>VPN connection</td>
<td>Total price = VPN gateway bandwidth price + VPN connection price</td>
</tr>
<tr>
<td>Billed by traffic</td>
<td>Public network traffic</td>
<td>VPN connection</td>
<td>Total price = Public network traffic price + VPN connection price</td>
</tr>
</tbody>
</table>

For details, see *Product Pricing Details*.

**Billing Modes**

- **Pay-per-Use**
  - **Billed by bandwidth**
  
  The billing cycle is one hour and the generated price varies according to the bandwidth size. The total price includes the gateway bandwidth price and the price of the VPN connection created with the VPN gateway. When you create another connection for the gateway, only the price of this created connection will be billed.
  
  Total price = VPN gateway bandwidth price + VPN connection price

  Your purchased VPN gateway bandwidth is in the outbound direction, that is, the bandwidth from a VPC to a customer data center.
a. If the purchased bandwidth is no more than 100 Mbit/s, the bandwidth in the inbound direction is limited to 100 Mbit/s.

b. If the purchased bandwidth is more than 100 Mbit/s, the bandwidth in the inbound direction is the same as that of the purchased bandwidth.

For example, if your selected bandwidth is 50 Mbit/s, you use the VPN gateway for 5 hours, and then delete it, you will be billed for 5 hours based on the 50 Mbit/s bandwidth. Note: Even if you do not transmit data during those five hours, you will still be billed for the bandwidth.

- **Billed by traffic**
  The traffic price incurred each hour will be collected and the billing unit is 1 GB. If less than 1 GB is used, the price varies (Total price = Used traffic/1 GB x Price of 1 GB traffic). In this case, modifying the bandwidth size does not change the public network traffic price per GB. Only traffic in the outbound direction is collected.
  
  Total price = Public network traffic price + VPN connection price

### Renewal

For details, see [Renewal Management](#).

### Expiration and Overdue Payment

For details, see [Service Suspension and Resource Release](#) and [Payment and Repayment](#).
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

Figure 8-1 shows the relationship between regions and AZs.

Figure 8-1 Regions and AZs

HUawei Cloud provides services in many regions around the world. Select a region and AZ based on requirements. For more information, see HUAWEI CLOUD Global Regions.
Selecting a Region

When selecting a region, consider the following factors:

- **Location**
  It is recommended that you select the closest region for low network latency and quick access. Regions within the Chinese mainland provide the same infrastructure, BGP network quality, as well as resource operations and configurations. Therefore, if your target users are on the Chinese mainland, you do not need to consider the network latency differences when selecting a region.
  - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **AP-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If your target users are in Africa, select the **AF-Johannesburg** region.
  - If your target users are in Europe, select the **EU-Paris** region.
  - If your target users are in Latin America, select the **LA-Santiago** region.

  **NOTE**
  The **LA-Santiago** region is located in Chile.

- **Resource price**
  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.