VPN Connections

Product Documentation

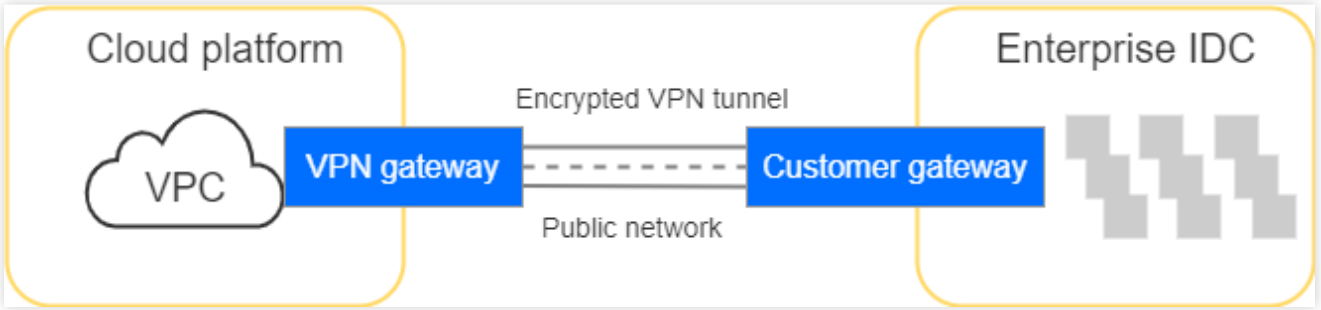
Contents

VPN Connections 3
- Product Introduction 3
  - VPN Connection Overview 3
  - Product Composition 5
    - IPsec VPN 5
    - SSL VPN 9
  - Product Features 10
  - Limits 11
  - Related products 14
- Purchase Guide 15
  - Billing Overview 15
  - Purchase Method 17
- Quick Start 19
  - Creating an IPsec VPN Connection 19
    - Overview 19
    - Step 1: Creating a VPN Gateway 21
    - Step 2: Creating a Customer Gateway 23
    - Step 3: Creating a VPN Channel 24
    - Step 4: Local Gateway Configuration 27
    - Step 5: Configuring a Routing Table 28
    - Step 6: Activating a VPN Channel 29
  - Creating an SSL VPN Connection 30
- Operation Guide 34
  - Operation Overview 34
  - Viewing Monitoring Data 35
  - Setting Alarms 36
  - Modifying VPN Tunnel Configuration 37
  - VPN Gateway 38
  - VPN Tunnel 41
  - Customer Gateway 44
  - SSL Server 46
  - SSL Client 49
- FAQs 51
  - Concepts 51
  - Function category 55
- Glossary 58

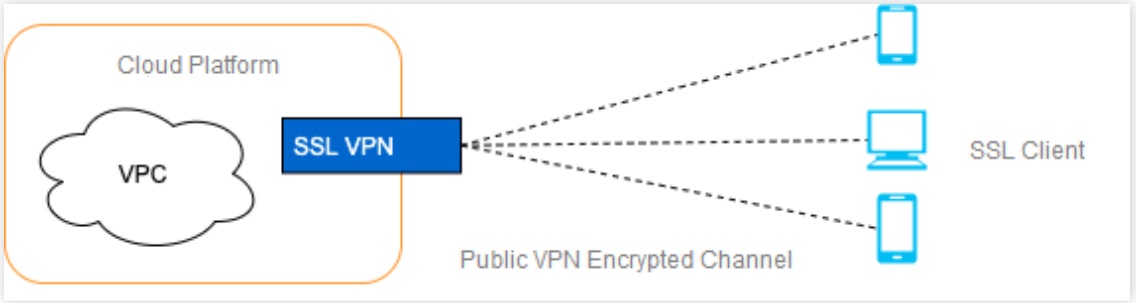
Product Introduction
VPN Connection Overview

A VPN connection is a way to achieve remote access through an encrypted public network channel. VPN gateway is an important part of VPN connection. There are two types of VPN gateways:

- IPsec VPN Gateway: Mainly realizes site-to-site interconnection. For example, when IDC is connected to a VPC, after a VPN connection is established, you only need to configure the relevant routing policies in the routing table to achieve communication.
- VPN gateway: An IPsec VPN gateway created in the VPC.
- Customer Gateway: A logical object that records the public IP address of the IPsec VPN gateway on the IDC side (the IDC side must have a fixed public IP).
- VPN Channel: An encrypted IPsec VPN channel connecting the VPN gateway and the customer gateway. Each VPN gateway can establish multiple VPN channels, and each VPN channel can connect to a local IDC.



- SSL VPN Gateway: Mainly realizes point-to-point interconnection. For example, you can access the VPN server through any browser with built-in SSL to access the VPC. As shown in the figure below, an SSL VPN connection is divided into the following components.
- VPN Gateway: SSL VPN gateway created in the VPC.
- SSL Server: The service module in the VPN gateway used to provide SSL services, mainly implementing the encapsulation and decapsulation of data packets.
- SSL Client: Any browser with built-in SSL can be used as an SSL client to access.


Cloud Platform
VPC
SSL VPN
SSL Client
Public VPN Encrypted Channel

Product Composition
IPsec VPN

VPN connections support IPsec VPN and SSL VPN connections. This section introduces the components of the two connection methods.

IPsec VPN

An IPsec VPN connection consists of three components: VPN gateway, customer gateway, and VPN channel.

VPN Gateway

A VPN gateway is an egress gateway for VPC to establish a VPN connection. It is used with the customer gateway (the IPsec VPN service gateway on the IDC side) to establish secure and reliable encrypted network communication between the cloud platform's VPC and the external IDC. The VPN gateway, underpinned by software virtualization, adopts a dual-server hot standby policy. If one of the servers fails, it will automatically switch to the other, ensuring normal business operations.

The VPN gateway bandwidth limit includes the following options: 5 Mbps, 10 Mbps, 20 Mbps, 50 Mbps, 100 Mbps.

Customer Gateway

The customer gateway is a logical object used to record the public IP of the IPsec VPN gateway on the IDC side (the IDC side must have a fixed public IP). It needs to be used in conjunction with the VPN gateway. One VPN gateway can establish encrypted VPN network channels with multiple customer gateways.

VPN Tunnel

After the VPN gateway and customer gateway are established, you can establish a VPN channel for encrypted communication between the VPC and the external IDC. This VPN channel supports IPsec encryption protocol and can meet the needs of most VPN connections.
The VPN channel runs in the operator's public network. Network congestion and jitter in the public network can affect the quality of the VPN network. If your business is sensitive to latency and jitter, you are recommended to connect with VPC via a Direct Connect line. For more details, see Direct Connect Service.

Establish VPN channel

When it implements IPsec, the VPN channel in the cloud platform uses the IKE (Internet Key Exchange) protocol to establish a session. IKE has a set of self-protection mechanisms that can safely authenticate identities, distribute keys, and establish IPSec sessions on insecure networks.

- Basic Configuration
- SPD (Security Policy Database) policy

- IKE Configuration (optional)
- IPsec Configuration (optional)
  The following section introduces the basic information, SPD policy, IKE configuration (optional) and IPsec configuration (optional) in detail.

Basic Configuration

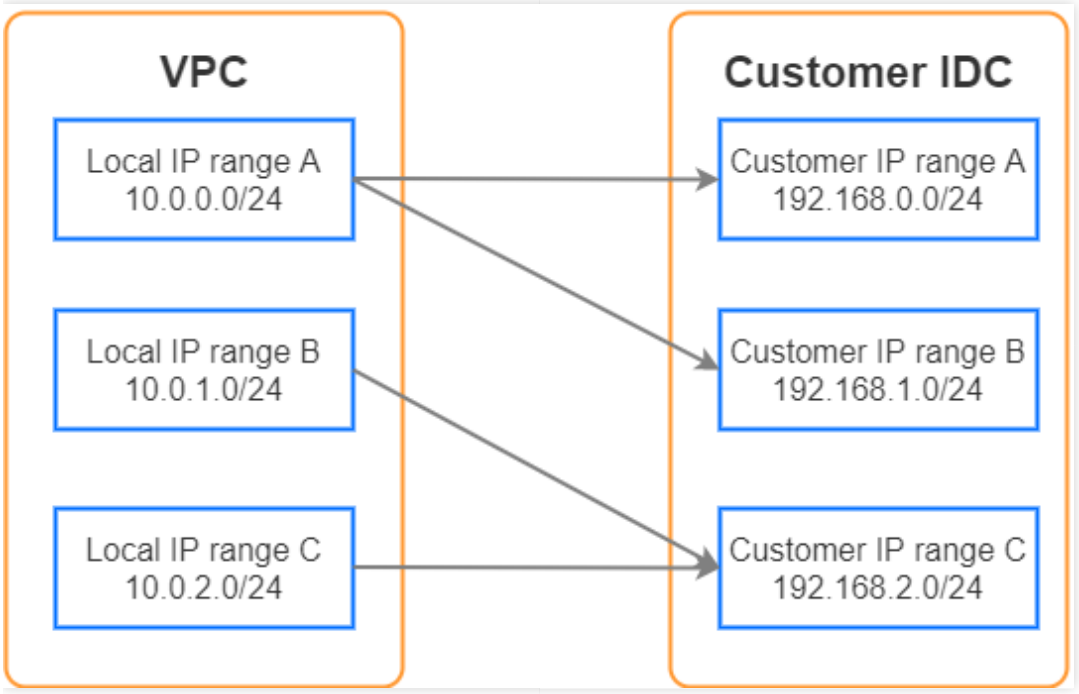
The basic configuration mainly includes basic information such as VPN channel name, region, VPC, VPN gateway, and customer gateway.

SPD Policy

The SPD (Security Policy Database) policy consists of a series of SPD rules, which are used to specify which IP ranges in the VPC can communicate with which IP ranges in the IDC. Each SPD rule includes a local IP range CIDR and at least one peer IP range CIDR. A local IP range CIDR and a peer IP range CIDR form a set of matching relationships. There can be multiple sets of matching relationships under one SPD rule.

> Note:
>
> The matching relationships of the rules in all channels under the same VPN gateway cannot overlap, that is, in a group of matching relationships, the local IP range and the remote IP range cannot overlap at the same time.

Example:
As shown in the figure below, the following SPD rules already exist under a VPN gateway:



- SPD Rule 1: The local IP range is 10.0.0.0/24, and the peer IP ranges are 192.168.0.0/24 and 192.168.1.0/24. There are two sets of matching relationship.

- SPD Rule 2: The local IP range is 10.0.1.0/24, and the peer IP range is 192.168.2.0/24. There is one set of matching relationship.
- SPD Rule 3: The local IP range is 10.0.2.0/24, and the peer IP range is 192.168.2.0/24. There is one set of matching relationship.

  Their matching relationships are:
- 10.0.0.0/24-----192.168.0.0/24
- 10.0.0.0/24-----192.168.1.0/24
- 10.0.1.0/24-----192.168.2.0/24
- 10.0.2.0/24-----192.168.2.0/24

  These four sets of matching relationships cannot overlap with each other, that is, their local IP ranges and remote IP ranges cannot overlap at the same time.
- If a new matching relationship of 10.0.0.0/24-----192.168.1.0/24 is added, the SPD rule cannot be added because it overlaps with an existing matching relationship.
- If a new matching relationship of 10.0.1.0/24-----192.168.1.0/24 is added and it does not overlap with the existing three matching relationships, then the SPD rule can be added.

IKE configuration

Configuration Items	Description
Version	IKE V1
Identity Authentication Method	Default Pre-shared Key
Authentication Algorithm	Identity authentication algorithm and it supports MD5 and SHA1.
Negotiation Mode	Supports main (main mode) and aggressive (aggressive mode). The difference between the two is that aggressive mode can send more information with fewer packets and establish connections quickly, but it exposes the security gateway's identity in a clear manner. When using aggressive mode, configuration parameters such as Diffie-Hellman and PFS cannot be negotiated and require compatible configurations on both ends
Local ID	Supports IP and FQDN (Fully Qualified Domain Name)
Customer ID	Supports IP and FQDN
DH group	Specifies the DH group used when exchanging IKE keys. The security of the key exchange increases with the size of the DH group, but the exchange time also increases. - Group1: DH group using the 768-bit Modular Exponential (MODP) algorithm.

Configuration Items	Description
	- Group2: DH group using the 1024-bit MODP algorithm. - Group5: DH group using the 1536-bit MODP algorithm. - Group14: DH group using the 2048-bit MODP algorithm, does not support dynamic VPN implementation of this option. - Group24: DH group using the 2048-bit MODP algorithm with a 256-bit prime order subgroup, does not support group VPN implementation of this option.
IKE SA Lifetime	Unit: Seconds. Sets the SA lifetime for IKE security proposals. Before the set SA lifetime expires, another SA is negotiated to replace the old SA. The old SA will continue to be used until the new SA is negotiated. Once the new SA is established, it will be used immediately, and the old SA will be automatically cleared after its lifetime expires.

IPsec configuration

Configuration Items	Description
Encryption Algorithm	Supports 3DES, AES-128, AES-192, AES-256, DES.
Authentication Algorithm	Supports MD5 and SHA1.
Message Encapsulation Mode	Tunnel
Security Protocol	ESP
PFS	Supports disable, dh-group2, dh-group5, and dh-group14.
IPsec SA lifetime(s)	Unit: Seconds
IPsec SA lifetime(KB)	Unit: KB

SSL VPN

SSL VPN

An SSL VPN connection consists of three parts: a VPN gateway, an SSL server, and an SSL client.
How it works: With an SSL VPN gateway instance created in the VPC, the VPN gateway is configured on the SSL server, and then an SSL client corresponding to the SSL server is created to implement communication between the SSL client and the VPC.

VPN Gateway

The VPN gateway is the egress gateway for the VPC to establish a VPN connection. The client communicates with the VPC through SSL VPN.

SSL Server

The SSL server is a service module in the VPN gateway that provides SSL services. It primarily encapsulates and decapsulates data packets. Therefore, in the VPN gateway, it is necessary to configure the SSL server for the local IP range, client IP range, and communication protocol, port, and algorithm.

SSL Client

The SSL client is connected through OpenVPN, which creates an SSL client and provides the client configuration file and certificate download feature. Two-way authentication is needed between the client and the server. Only an authenticated client can establish a communication connection with the server.
You can access RIO through any browser with built-in SSL as an SSL client. The client operating system supports Windows, MAC, and Linux (mainstream versions).

Product Features

Remote Communication

Remote communication to VPC can be established through VPN connection. For example, site-to-site communication between IDC and VPC can be established through IPsec VPN; point-to-point communication between client and VPC can be established through SSL VPN. For specific implementation methods, see Quick Start.

Traffic Alarms

You can set custom traffic alarms for VPN connections. When the metric value exceeds a certain threshold, an alarm is automatically triggered. The alarm message is sent via email and SMS to help you get an early warning of risks. Monitoring and alarm services are free of charge and can help you quickly locate problems when they occur. Set the alarm policy. For details, see Setting Alarm.

Metric Monitoring

The VPN gateway supports data monitoring, and the monitoring items mainly include public network outbound bandwidth, public network inbound bandwidth, outbound packet volume, and inbound packet volume. Through real-time monitoring of various metrics, you can get timely updates of product running status and ensure stable product running.

Limits

IPsec VPN Usage Limitations

When you use an IPsec VPN connection, you need to pay attention to the following:

- After the VPN parameters are configured, you need to add a routing policy pointing to the VPN gateway in the subnet-associated routing table, and the network request from the CVM in the subnet to access the peer IP range is transmitted to the customer gateway through the VPN channel.
- After the routing table is configured, you need to ping the IP in the peer IP range from the CVM in the VPC to activate the VPN channel.
- The stability of VPN connections depends on the quality of the operator's public network.
- The resource limits are as follows:

Resources	Limit (pcs)	can request for high quota
Number of VPN gateways per VPC	10	No
Number of customer gateways in the same region	20	No
Number of VPN channels supported by the same customer gateway	10	No
Number of VPN channels that can be created on the same VPN gateway	20	No
Number of SPDs per VPN channel	10	No
Number of peer IP ranges supported by each SPD	50	No

> Note:
>
> - The number of VPN tunnels supported by the same customer gateway is an account-level Quota .

- Only one VPN tunnel can be established between the same customer gateway and a VPN gateway within a VPC.

The customer gateway does not support the following IP addresses:

- All 0s, all 255s, or a multicast address starting with 224.

- Loopback Address: 127.xxx/8 .
- An IP in which the host bits are all 0 or all 1, for example:
- For example, in the A category, an IP starting with 1 - 126 is 1 - 126.0.0.0 and 1 - 126.255.255.255 .
- For example, in the B category, an IP starting with 128 - 191 is 128 - 191.x.0.0 and 128 - 191.x.255.255 .
- For example, in the C category, an IP starting with 192 - 223 is: 192 - 223.xx0 and 192 - 223.xx255 .
- Internal Service Address: 169.254.xx/16 .

SSL VPN usage limitations

SSL Client Constraints:

- The SSL VPN client uses the open source OpenVPN for docking, and users need to download OpenVPN themselves.
- The SSL VPN client must support Windows, Mac, and Linux (mainstream versions) systems.
- The client and server must perform two-way certificate authentication. The client's certificate and key are requested for and downloaded from the cloud, and the configuration file is provided for download.
- The client certificate SNI is the SSL VPN instance ID (SSL VPN client instance ID).
  SSL Server Constraints:
- The server must perform two-way certificate authentication. The root certificate and server certificate are valid for 10 years, and the client certificate is valid for 3 years.
- Only one client IP address pool can be configured.
- Can access one VPC-side CIDR.
- The maximum number of connections, supporting 5, 10, 20, 50, 20, and 100.
  SSL VPN Gateway Constraints:

- The client communicates with the VM in the VPC through the SSL VPN gateway. Currently, SSL VPN only connects to the OpenVPN client.
- EIP opens UDP port 1194 to provide SSL VPN services.
- When different users use the same certificate and key to communicate with the SSL VPN gateway, only one user can establish an SSL VPN connection with the SSL VPN gateway at the same time. If two users keep trying to establish a connection, neither of them can establish a connection.

Related products

For information about VPN connection related products, see the following table:

Product Name	Relationship with VPN connection
VPC	VPN connection is a way to connect your peer IDC and VPC through a public network encrypted channel.
DC	If your business is sensitive to latency and jitter, you are recommended to connect with the VPC through Direct Connect.
Routing table	You need to add a routing policy pointing to the IPsec VPN gateway in the routing table associated with the subnet so that network requests can be transmitted to the customer gateway through the VPN channel.

Purchase Guide
Billing Overview

An IPsec VPN connection consists of three parts: a VPN channel, a customer gateway, and a VPN gateway. This document introduces the billing details of each part.

VPN Tunnel

The VPN channel is free for users.

Customer Gateway

The customer gateway is free for users.

VPN Gateway

The VPN gateway supports traffic-based postpaid billing, including two parts of fees: Traffic fees and gateway fees generated by accessing the public network (calculated by the hour).

Gateway Inquiry

You can select different bandwidth specifications on the VPN gateway purchase page to learn about the corresponding gateway fees.

Create VPN Gateway

Gateway Name *

You can enter 60 more characters

Region: luzon

Network *: vpc-5odtk24l (test-vpc-01 | ...

Bandwidth Limitation: 5M | 10M | 20M | 50M | 100M | 200M | 500M | 1000M

bps

VPN Type *: IPsec VPN | SSL VPN

Carrier *: BGP

Billing Method: Bill-by-Traffic

Total Price(Before discount): 0.1 PHP/hr(Gateway Fee) | 0.1 PHP/GB(Traffic Fee)

Total Price(After discount): 0.1 PHP/hr (Gateway Fee) | 0.1 PHP/GB (Traffic Fee)

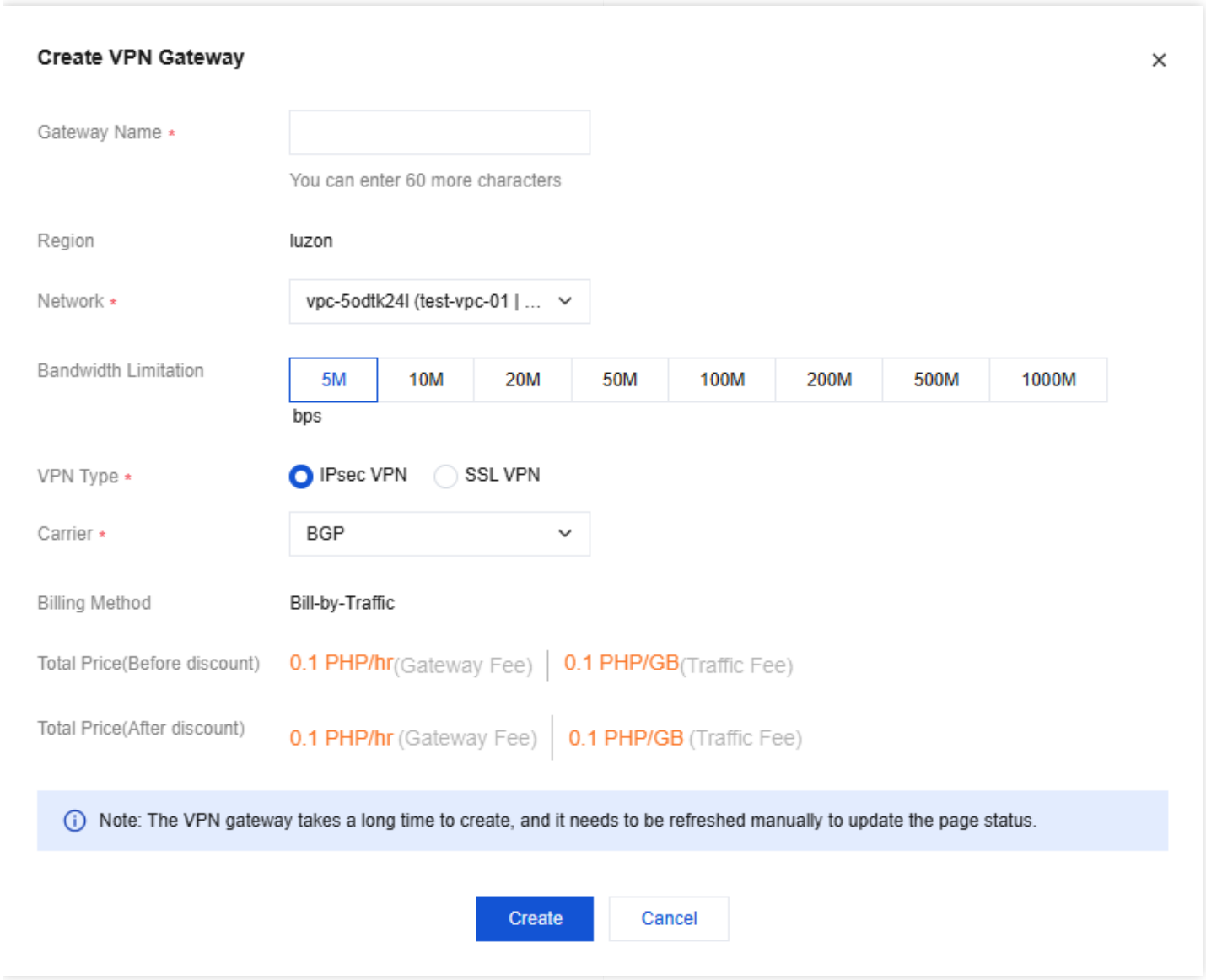
Note: The VPN gateway takes a long time to create, and it needs to be refreshed manually to update the page status.

Create | Cancel

Purchase Method

Below are the specific steps for purchasing VPN.

1. Log in to the cloud platform and choose Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to go to the VPC console.
2. In the directory on the left side, choose VPN Connection > VPN Gateway to go to the VPN Gateway management interface.
3. Select a region and click Create.
4. In the pop-up dialog box, configure the following parameters and click Create.
    - Gateway Name: Enter the VPN gateway name, which should not exceed 60 characters.
    - Network: Select the VPC network to which the VPN gateway belongs as needed.
    - VPN Type: IPSec and SSL are supported.
    - Max. Bandwidth: Select the bandwidth limit of the VPN gateway as needed.
    - Billing Method: Currently, only traffic-based billing is supported. This billing method is suitable for scenarios with significant bandwidth fluctuations.



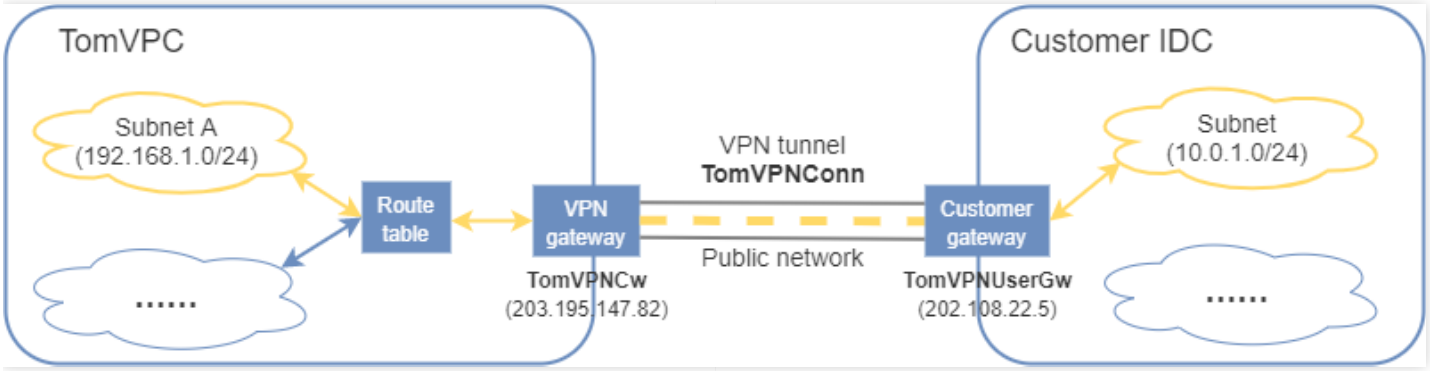
> Note:
>
> VPN gateways with bandwidth above 100 Mbps should use DPDK hosts. If the option for bandwidth above 100 Mbps is not displayed on the Purchase page, contact the cloud platform's technical support personnel for assistance.

Quick Start
Creating an IPsec VPN Connection
Overview

You need to implement several steps to make the IPsec VPN connection effective, and then you can perform full self-configuration of IPsec VPN in the console. An example is given below.

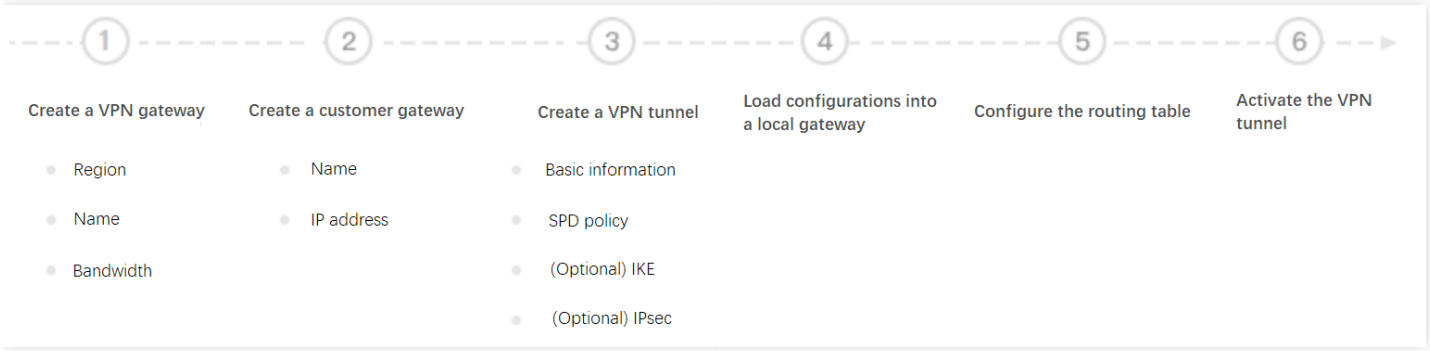
Example

Use an IPsec VPN to establish the connectivity between subnet A (192.168.1.0/24) in your VPC (TomVPC) in City 1 and the subnet (10.0.1.0/24) in your IDC. Assume the public IP address of the VPN gateway in your IDC is 202.108.22.5 .



Step Description

The VPN Connections activation flowchart is shown below.



For detailed instructions, please refer to:

- Step 1: Creating a VPN Gateway
- Step 2: Creating a Customer Gateway
- Step 3: Creating a VPN Channel
- Step 4: Local Gateway Configuration
- Step 5: Configuring a Routing Table
- Step 6: Activate the VPN Tunnel

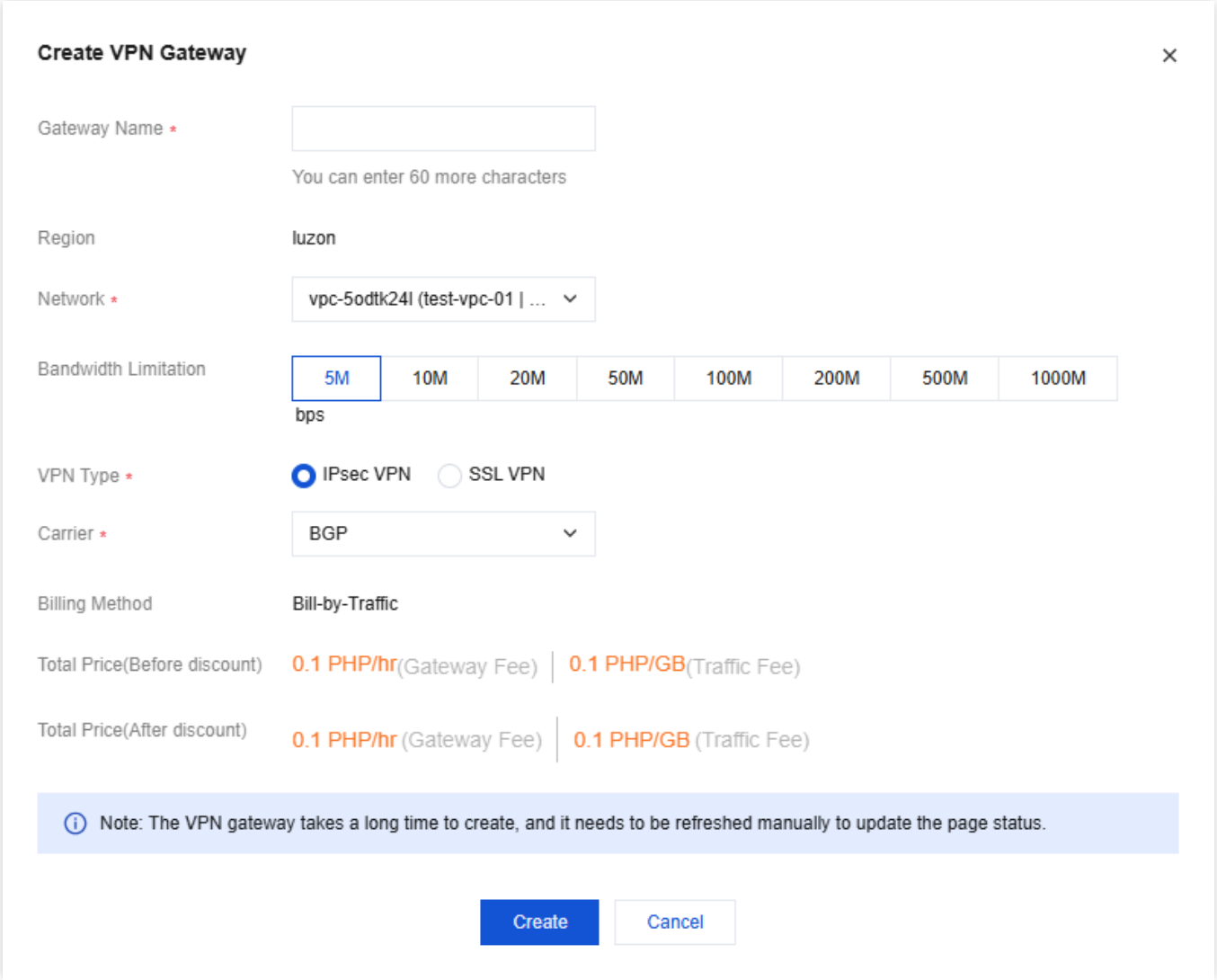
Step 1: Creating a VPN Gateway

1. Log in to the cloud platform and choose Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to go to the VPC console.

2. In the directory on the left side, choose VPN Connection > VPN Gateway to go to the VPN Gateway management interface.

3. Select a region and click Create. > Note: If Create is grayed out and No Virtual Private Cloud Available is displayed when you move your mouse pointer over it, before creating a VPN gateway.

4. In the pop-up Create VPN Gateway dialog box, fill in the VPN gateway name (such as TomVPNGw), select the network it belongs to and bandwidth limit, select IPsec VPN as the VPN type, and select the Carrier.



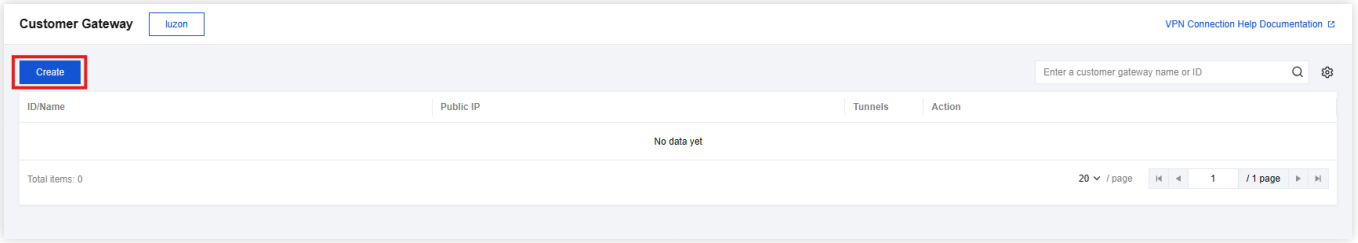
5. After setting the parameters, click Create. The system will allocate a public network IP address such as 203.195.147.82 to the created VPN gateway.

> Note:
>
> VPN gateways with bandwidth above 100 Mbps should use DPDK hosts. If the option for bandwidth above 100 Mbps is not displayed on the Purchase page, contact the cloud platform's technical support personnel for assistance.

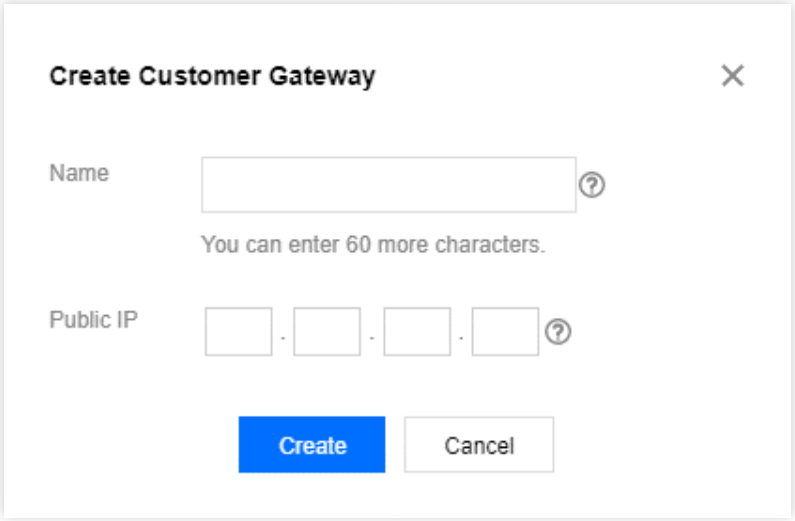
Step 2: Creating a Customer Gateway

Before creating a VPN channel, you need to create a customer gateway:

1. Log in to the cloud platform and select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the Virtual Private Cloud console.
2. In the directory on the left, click VPN Connection > Customer Gateway to enter the Customer Gateway interface.
3. Select a region, and click Create.



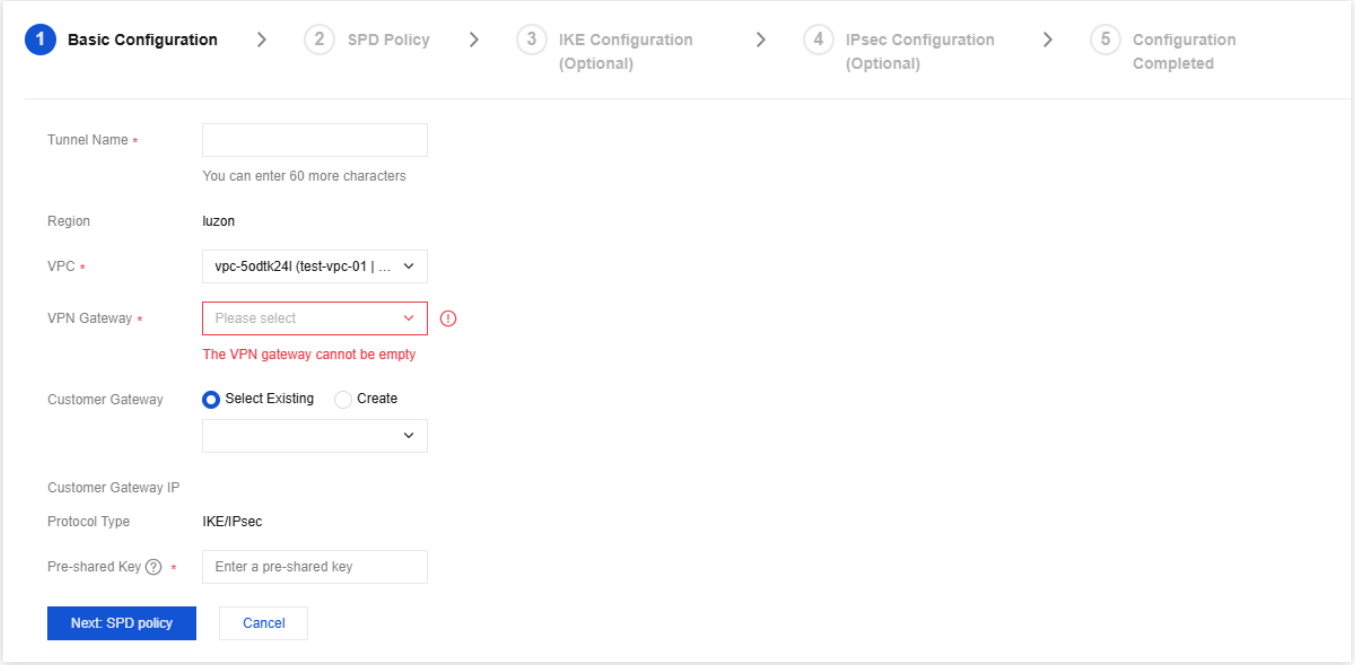
4. Fill in the customer gateway name (for example, TomVPNUserGw) and the public network IP of the IDC VPN gateway, for example, 202.108.22.5 .



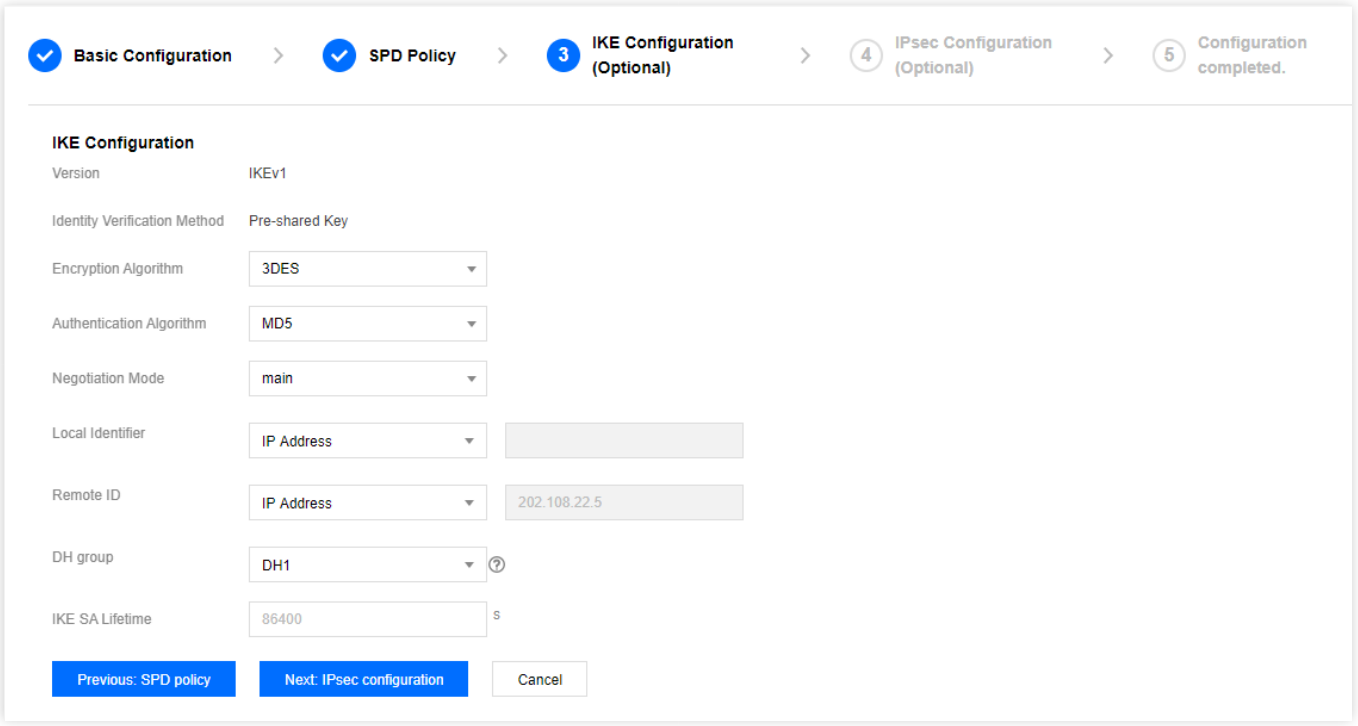
5. Click Create.

Step 3: Creating a VPN Channel

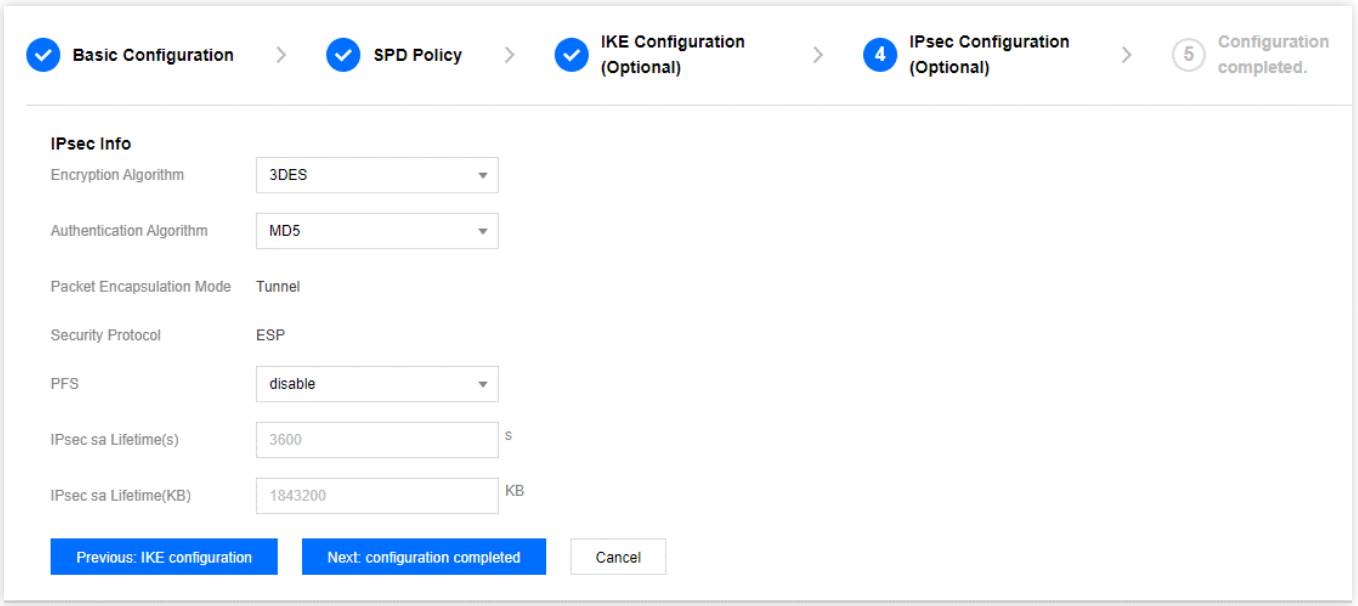
1. Log in to the cloud platform and select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the Virtual Private Cloud console.
2. In the directory on the left, click VPN Connection > VPN Tunnel to enter the VPN Tunnel interface.
3. Select a region and Virtual Private Cloud, and click Create.
4. Enter the channel name (for example, TomVPNConn), select TomVPNGw as the VPN gateway and TomVPNUserGw as the customer gateway, and enter the pre-shared key (for example, 123456), and click Next: SPD Policy.



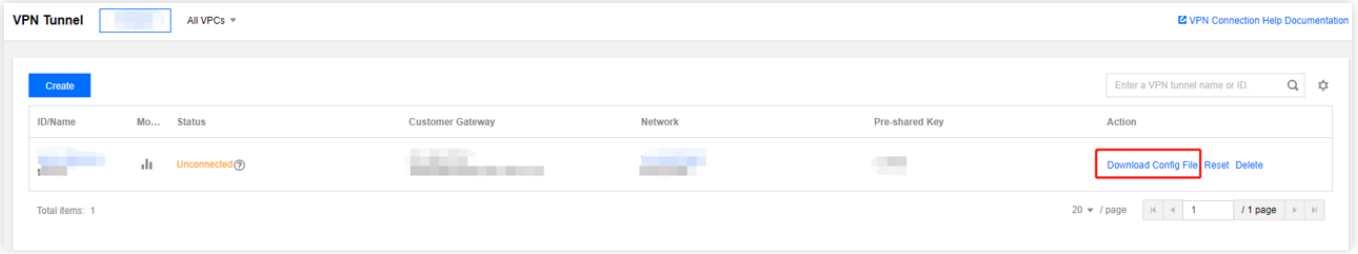
5. Enter the SPD policy to match the local IP range with the customer IP rang. In this example, the local IP range is the IP range 192.168.1.0/24 of subnet A, and the customer IP range is 10.0.1.0/24 . Click Next: IKE Configuration.
6. (Optional) Configure IKE parameters. If advanced configuration is not required, click Next: IPsec Configuration.



7. (Optional) Configure IPsec parameters. If no configuration is required, click Next: Complete Configuration.



8. After successful creation, return to the VPN channel list page, click Download Configuration File to download the file.



Step 4: Local Gateway Configuration

After the first three steps are completed, the configuration of the VPN gateway and VPN channel on the cloud has been completed. You need to continue to configure the VPN channel information on the other side on the "local gateway".

- Connect the Cloud Platform and Local Data Center
  The local gateway is a network device with VPN feature, which is usually a data center egress router or firewall. You can configure VPN on this network device to configure the local gateway.

  > Note: configurations may vary depending on the manufacturer of the network device. Perform configuration based on the actual condition of your network device.

- Connect Different Cloud Platforms
  The local gateway is another VPN gateway deployed in your cloud platform VPC on the other side. You can repeat Steps 1-3 on the other VPN gateway to configure the local gateway.

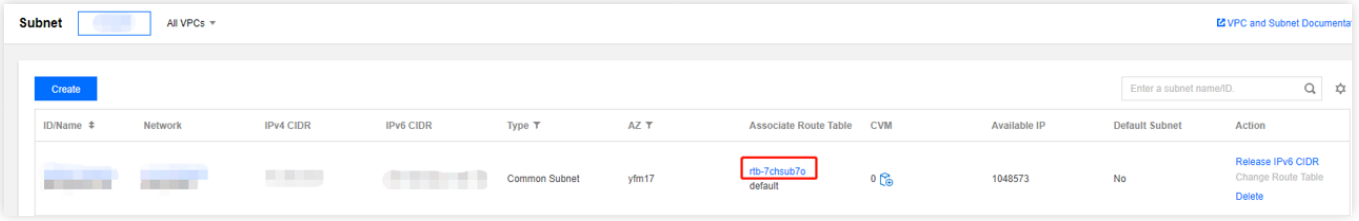
- Connect the Cloud Platform and Other Public Clouds
  The local gateway is the VPN gateway on your destination public cloud. You need to operate on the VPN gateway on the destination public cloud to configure the local gateway. For the configuration method, refer to the documentation on the destination public cloud.

  > Note:
  >
  > - All three methods above require that the VPN configuration on your local gateway is consistent with the information of the VPN channel configured in Step 3; otherwise, your VPN tunnel cannot be connected normally.
  > - The configuration information of the VPN channel on the cloud platform can be viewed from the console. You can also complete the configuration by downloading the configuration file and loading it into the IPsec VPN gateway in the local data center.

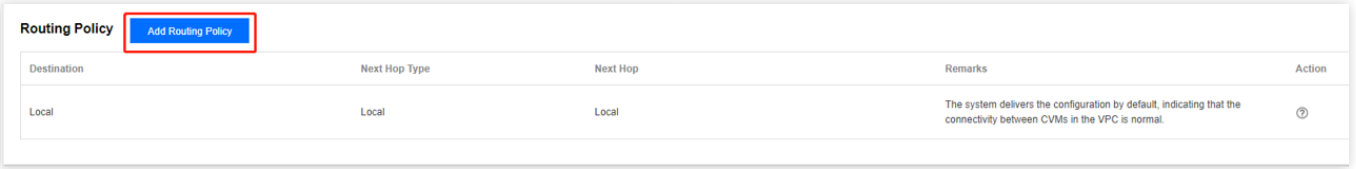
Step 5: Configuring a Routing Table

As of Step 4, we have successfully configured a VPN channel, but we still need to configure a routing table to route the traffic in subnet A to the VPN gateway so that the IP range in subnet A can communicate with the IP range in the IDC.

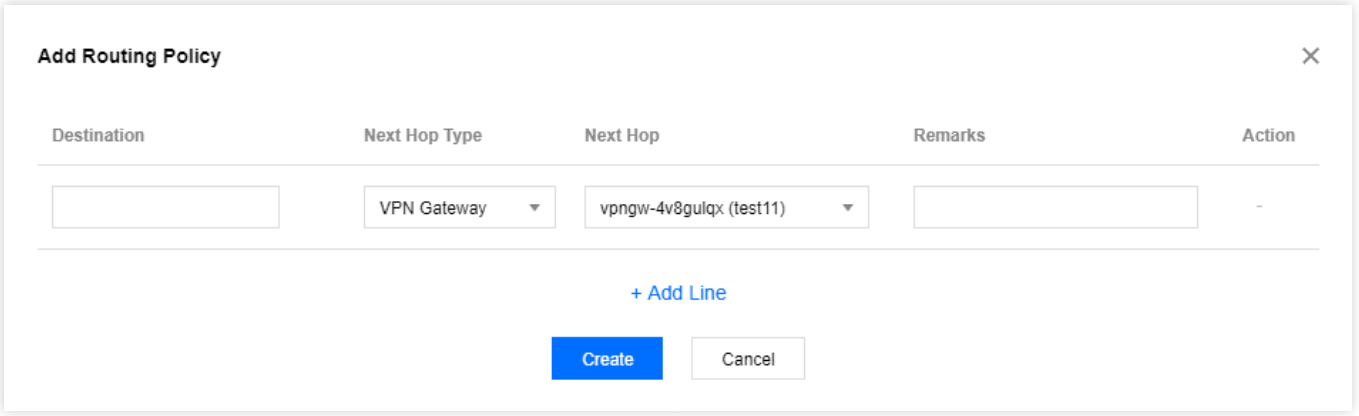
1. Log in to the Virtual Private Cloud (VPC) console.
2. In the directory on the left, click Subnet and select a region and Virtual Private Cloud, for example, City 1 and TomVPC . Click the routing table ID associated with subnet A to enter the details page.



3. You can click Add Routing Policy.



4. In the pop-up box, enter the destination IP range (10.0.1.0/24), select VPN Gateway for the next hop type, and select the VPN gateway you just created for the next hop TomVPNGw , click OK.



> Note: If your local gateway is a VPN gateway deployed on the cloud platform VPC on the other side, repeat the above steps to configure routing for the local gateway.

Step 6: Activating a VPN Channel

1. Use the Cloud Virtual Machine in the VPC to ping the IP in the customer IP range to activate a VPN channel.
   For example: Use TomVPC Cloud Virtual Machine in Subnet A to ping 10.0.1.1 .

Creating an SSL VPN Connection

Scenarios

Access VPC remotely through the SSL VPN connection.

Operation Steps

Step 1: Creating an SSL VPN Gateway

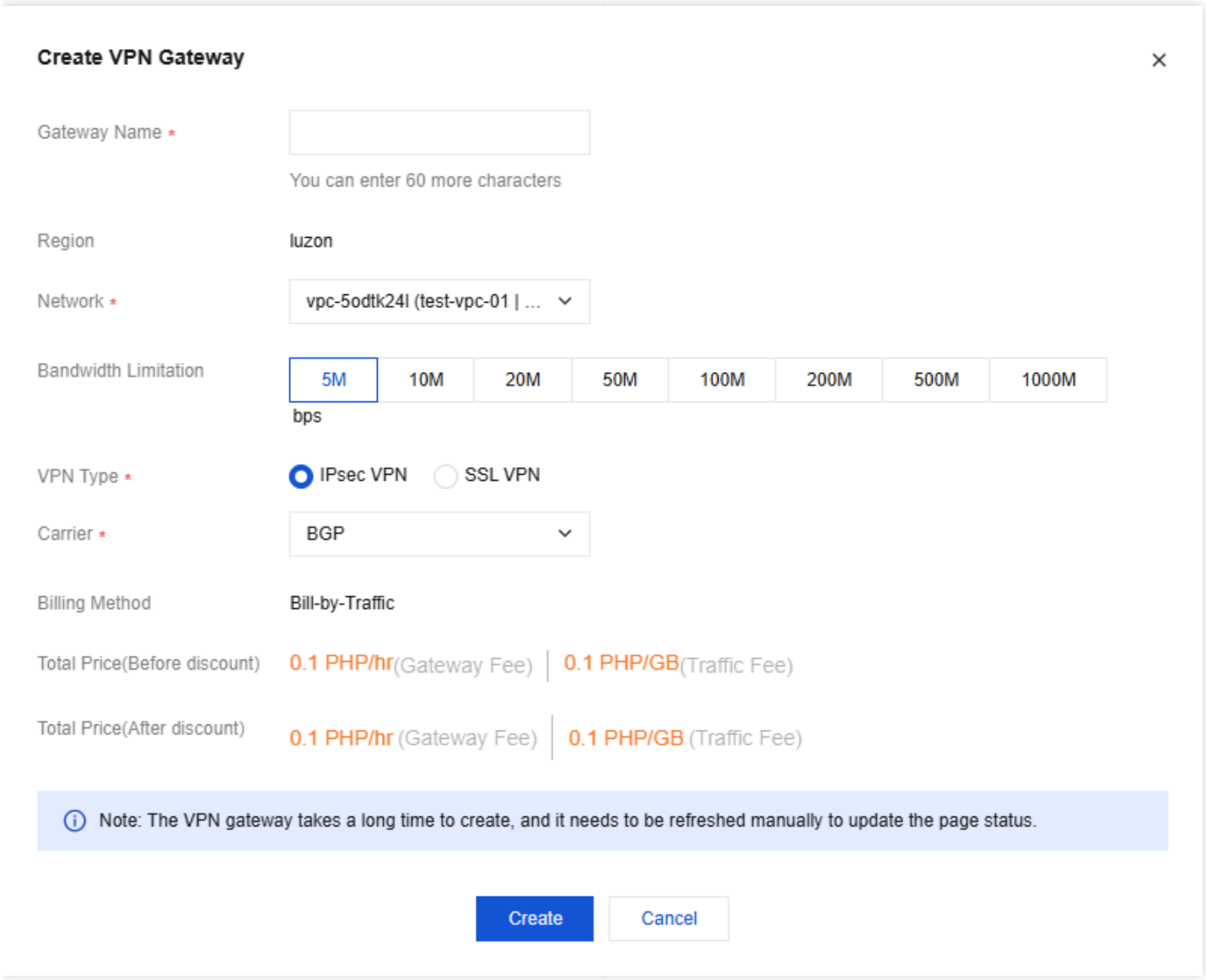
1. Log in to the cloud platform and choose Cloud Products > Cloud Computing & Networking > Private Network to go to the VPC console.

2. In the directory on the left side, choose VPN Connection > VPN Gateway to go to the VPN Gateway management interface.

3. Select a region and click New.

   > Note:
   >
   > If Create is grayed out and No Virtual Private Cloud Available is displayed when you move your mouse pointer over it, create a VPC before creating a VPN gateway.

4. Fill in the VPN gateway name (such as TomVPNGw), select the network to which it belongs (such as TomVPC) and bandwidth limit, select SSL VPN as the VPN type, and click Create. After a VPN gateway is created, the system randomly allocates a public network IP address such as 203.195.147.82 .

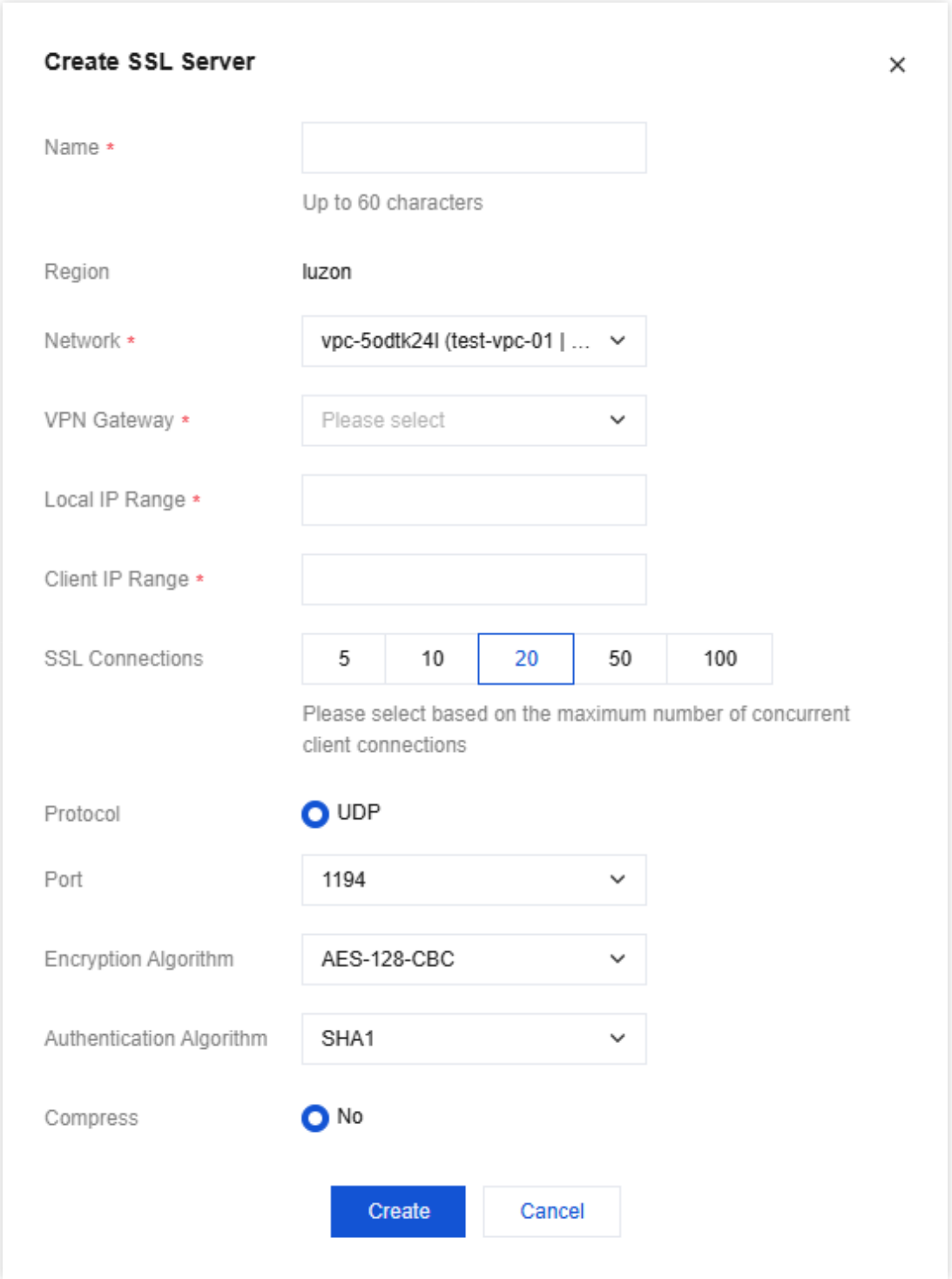


> Note:
>
> VPN gateways with bandwidth above 100 Mbps should use DPDK hosts. If the option for bandwidth above 100 Mbps is not displayed on the Purchase page, contact the cloud platform's technical support personnel for assistance.

Step 2: Creating an SSL Server

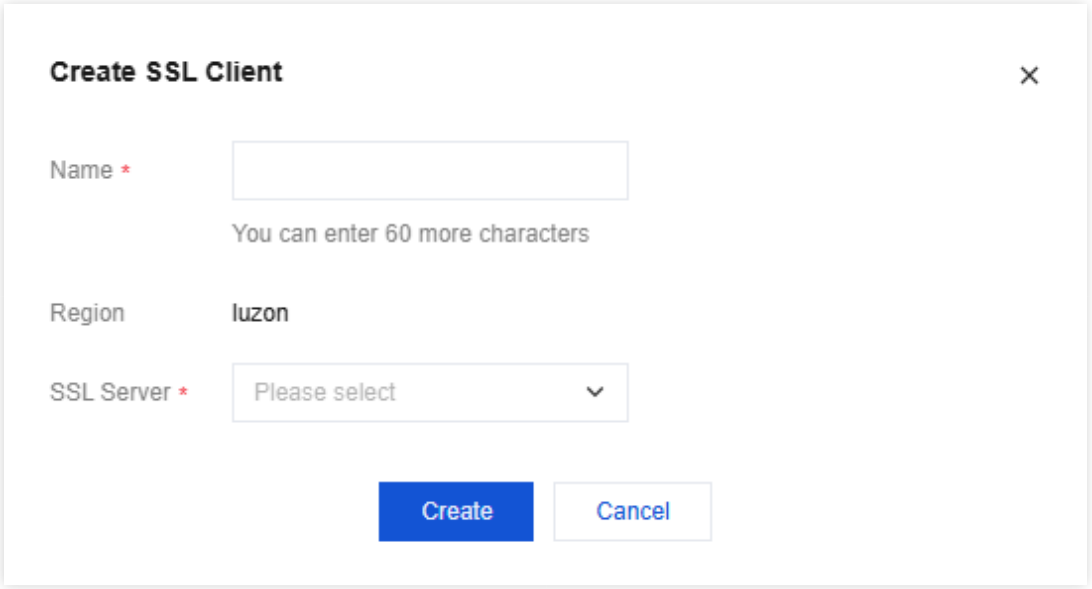
1. Click SSL Server to go to the SSL Server interface.
2. Click Create, configure parameters in the pop-up Create SSL Server dialog box, and click Create.
   Parameter description:
   - Network: Select a VPC to create a VPN connection.
   - VPN Gateway: Select the SSL VPN gateway created in Step 1.
   - Local IP Range: Fill in the local IP range of the server. The IP range should be within the VPC CIDR range.

- Client IP Range: Fill in the client IP range. Only private address segments 10, 172, and 192 are supported. The mask range is 16-24, which cannot overlap with the VPC IP range.
- Number of SSL Connections: Select the number of SSL connections.
- The protocol, port, encryption algorithm, authentication algorithm, and compression parameter values are shown in the figure and cannot be modified for the moment.



Step 3: Creating an SSL Client

1. Click SSL Client to go to the SSL Client interface.
2. Click Create, fill in the name of the SSL client in the pop-up Create SSL Client dialog box, select the SSL server created in Step 6, and click Create.



3. Click Download Configuration. The certificate is used to verify identity with the server.

> Note:
>
> The user uses the certificate and key to establish a connection with the VPN gateway. The user verifies the server certificate, and the server verifies the user certificate. After the verification passes, the server allocates an IP address from the client IP address pool to the user. This IP address is used to communicate with the VM in the VPC.

Step 4: Configuring Routing

1. Configure a routing policy in the VPC, with the destination address being the client IP address pool and the next hop being the SSL VPN gateway.

Feature Verification

Access the service in the VPC through the client browser. If you can access it normally, it means that the configuration is correct. If the access is abnormal, check and record the configuration information and contact technical support personnel in time.

Operation Guide
Operation Overview

This section provides a guide to using the VPN console, which allows you to create and manage VPN-related operations. When you use a VPN connection, you can refer to this section to learn about VPN gateway creation, console-related features, and operation guide.

- If you need to create an IPsec VPN connection, refer to the operation guide for VPN gateways, customer gateways, and VPN channels.
- If you need to create an SSL VPN connection, refer to the operation guide for VPN gateways, SSL servers, and SSL clients.

Common Operations

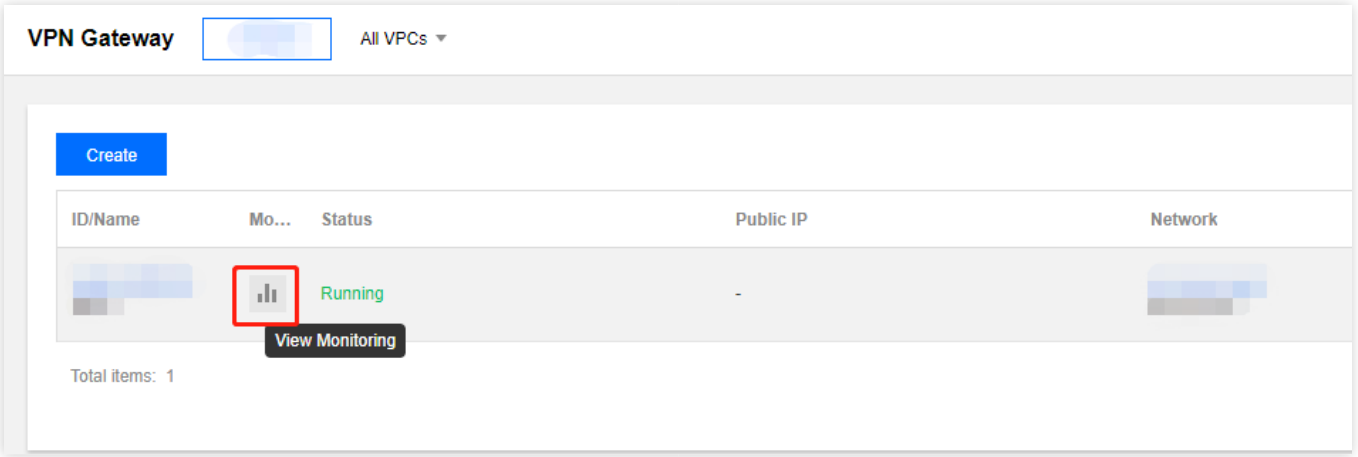
- Viewing Monitoring Data
- Setting Alarms
- Modifying VPN Channel Configuration

Viewing Monitoring Data

The VPN channel and VPN gateway provide the feature of viewing monitoring data.

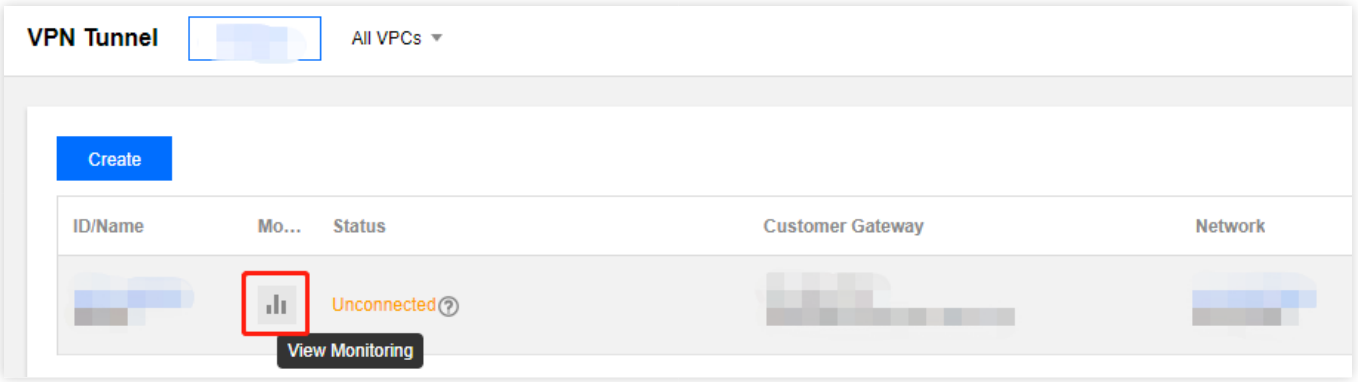
VPN Gateway

1. Log in to the Virtual Private Cloud (VPC) console.
2. Click VPN Connection > VPN Gateway in the left navigation bar.
3. Select a region and Virtual Private Cloud, and click the VPN gateway monitoring icon you want to view in the list to view the monitoring data.



VPN Tunnel

1. Log in to the Virtual Private Cloud (VPC) console.
2. Click VPN Connection > VPN Tunnel in the left navigation bar.
3. Select a region and Virtual Private Cloud, and click the VPN channel monitoring icon you want to view in the list to view the monitoring data.



Setting Alarms

The VPN channel provides alarm feature:

1. Log in to the cloud platform, select Cloud Services > Management and Audit > Cloud Monitoring to enter the Cloud Monitoring interface.

2. In the directory on the left, select Alarm Configuration > Alarm Policy to enter the alarm policy configuration page, and click Add.

3. Enter the name of alarm policy, select Virtual Private Cloud > VPN Tunnel as the policy type, select the alarm object, set the alarm policy, select the alarm receiving group and alarm channel, and click Finish. You can view the set alarm policy in the alarm policy list.

4. Viewing an Alarm Message
   When an alarm condition is triggered, you will receive an alarm through the selected alarm channel (SMS/email/message center), or you can click Alarm History in the left directory to view it.

Modifying VPN Tunnel Configuration

1. Log in to the Virtual Private Cloud (VPC) console.

2. In the directory on the left, click VPN Connection > VPN Tunnel to enter the management page.

3. Click the ID of the VPN channel to be modified to enter the details page.

4. Modify basic information and SPD policy on the Basic Information page.

5. Click the Advanced Configuration tab to modify IKE and IPsec configurations.

VPN Gateway

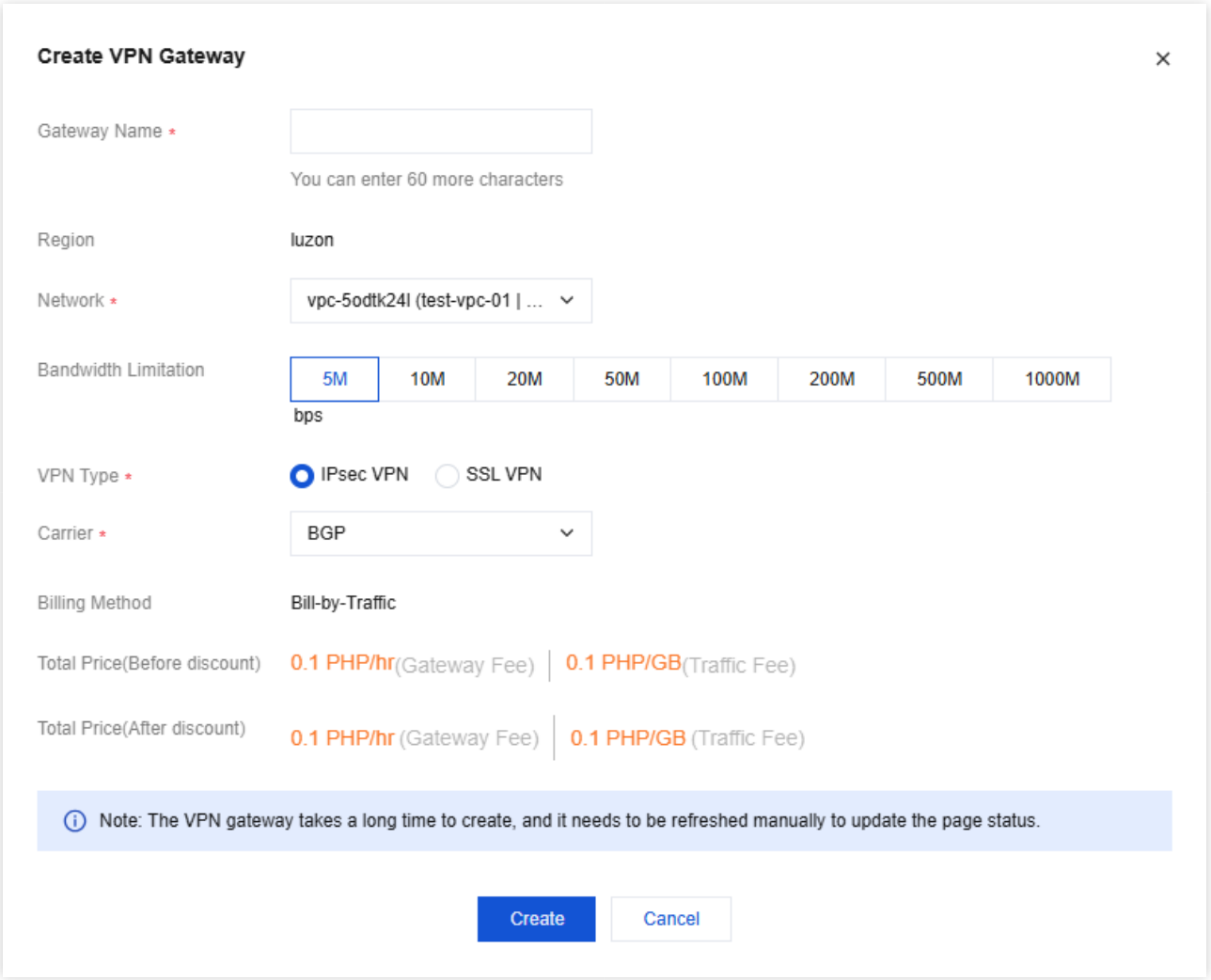
Creating a VPN Gateway

Overview

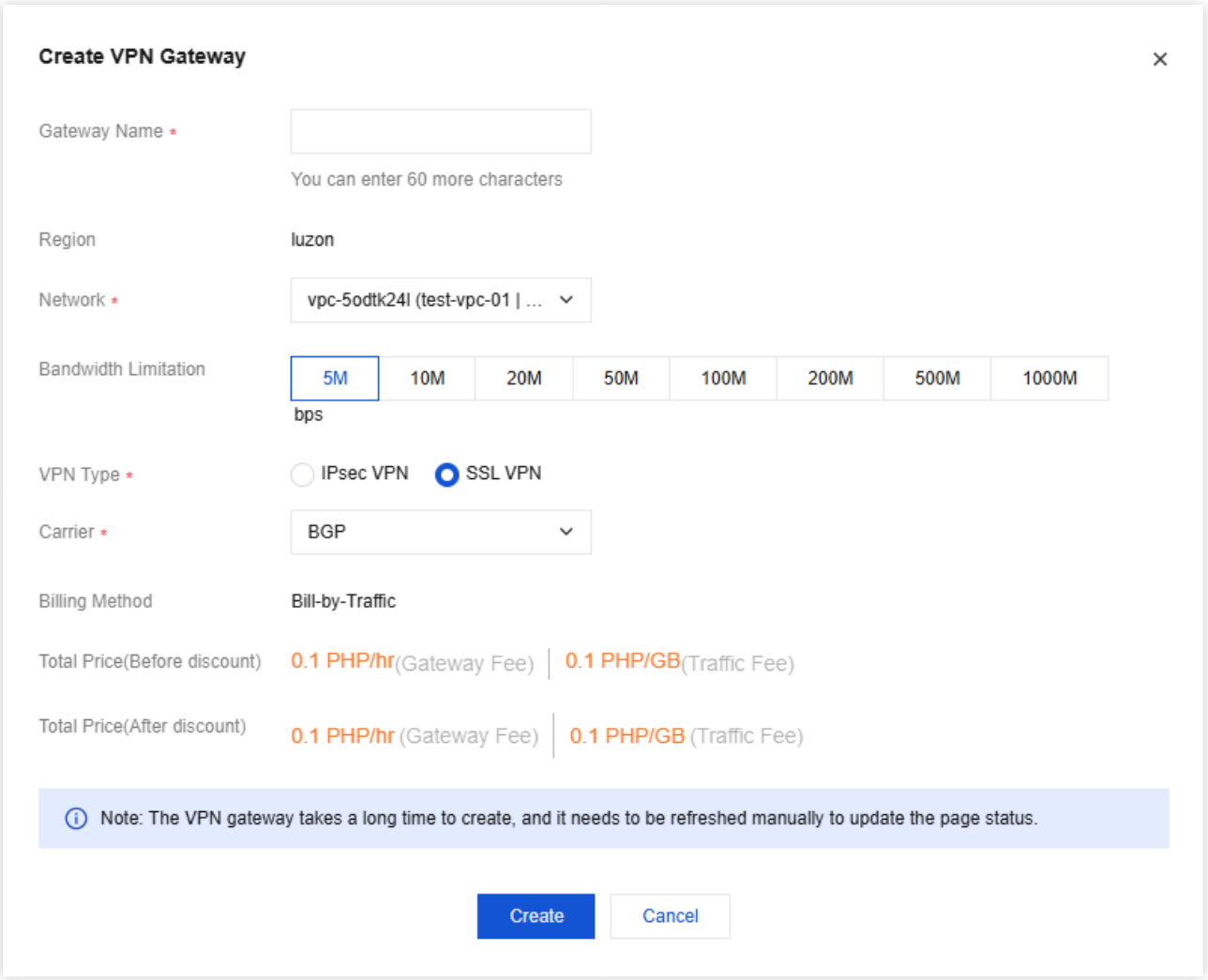
The VPN gateway is an important part of a VPN connection. This section mainly introduces how to create a VPN gateway through the console.

Directions

1. Log in to the Virtual Private Cloud VPC console, select VPN Connection > VPN Gateway in the left navigation bar to enter the VPN gateway management interface.
2. Click Create and the Create VPN Gateway dialog box pops up.
3. Set parameters according to the gateway type.
   - IPsec VPN



   - SSL VPN



Parameter description:

- Gateway name: Customize the gateway name.
- Network: Select the Virtual Private Cloud to which the VPN gateway belongs.
- Bandwidth limit: The system supports bandwidths of 5M, 10M, 20M, 50M, and 100M. Select a bandwidth as needed.
- VPN type: Select IPsec VPN or SSL VPN.
- Operator: This parameter is displayed only when VPN Type is IPsec VPN. Select an operator as needed.

4. With gateway parameters set, click Create to start task creation. When the Status column displays Running, the creation is successful.

Querying a VPN Gateway

Operational Scenario

The VPN Gateway management interface displays all created VPN gateways. You can view gateway details and monitoring information by entering a specific gateway. The system also supports quick search by VPN gateway name or ID.

Directions

1. Enter the VPN Gateway management interface to query all VPN gateway information, one gateway instance per entry.
2. Click the gateway ID to enter the Basic Information interface and query details and routing policy of the gateway.
3. Click the Monitoring tab. The interface will display the gateway's metric information, including External outbound bandwidth, Public Network Inbound Bandwidth, Packet Outbound Quantity, and Incoming Packet Volume. You can also enter the metric display interface through the VPN Gateway interface.  .
   Field description:
   - Real-time: You can view current metrics.
   - Recent 24 hours: You can view metrics of the past 24 hours.
   - Recent 7 days: You can view metrics of the past 7 days.
   - Select date: You can customize the time period of querying metrics.
   - Data comparison: You can view the comparison of real-time data at two moments.
   -  : The method of displaying metrics can be changed.
4. Click the upper right  to set the display parameters of the interface.
5. Enter the VPN gateway name or ID in the search box at the upper right to quickly search for gateway instances.

Deleting a VPN Gateway

Operational Scenario

You can delete VPN gateway instances that have not established a connection. Gateway instances that are in preparation or have already established VPN connections cannot be deleted.

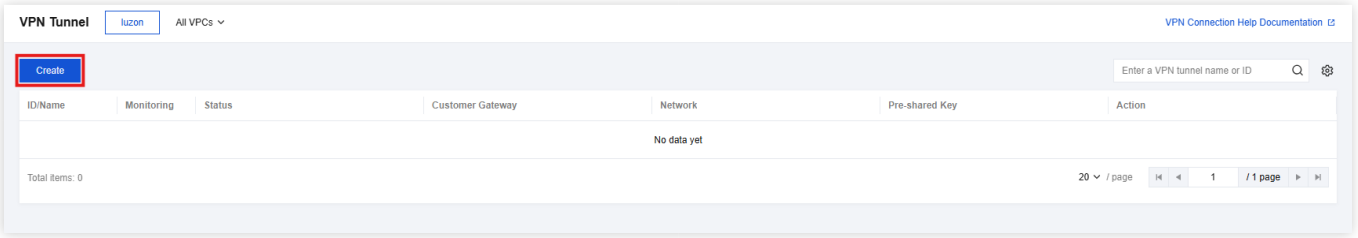
Directions

1. On the VPN Gateway management page, click Delete on the right side of the gateway instance to be deleted.
2. In the pop-up Confirmation dialog box, click OK to complete the deletion operation.

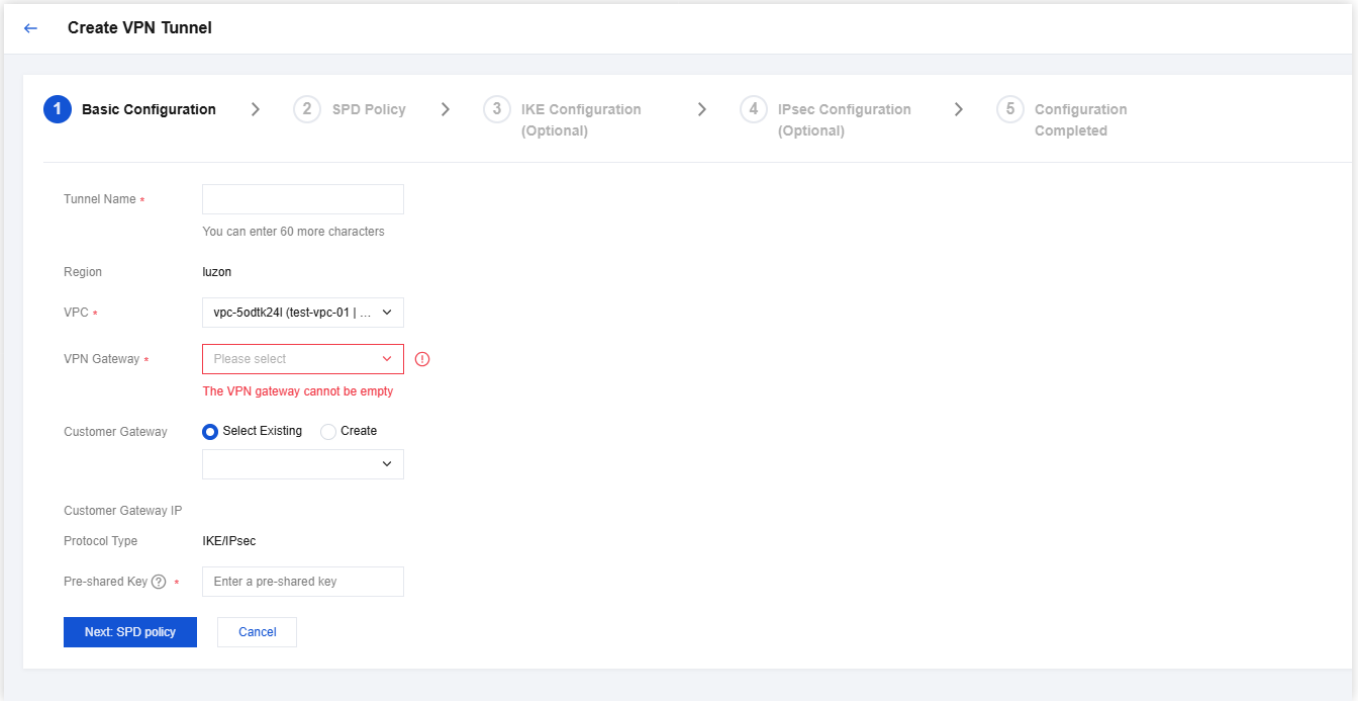
VPN Tunnel

Creating VPN Tunnel

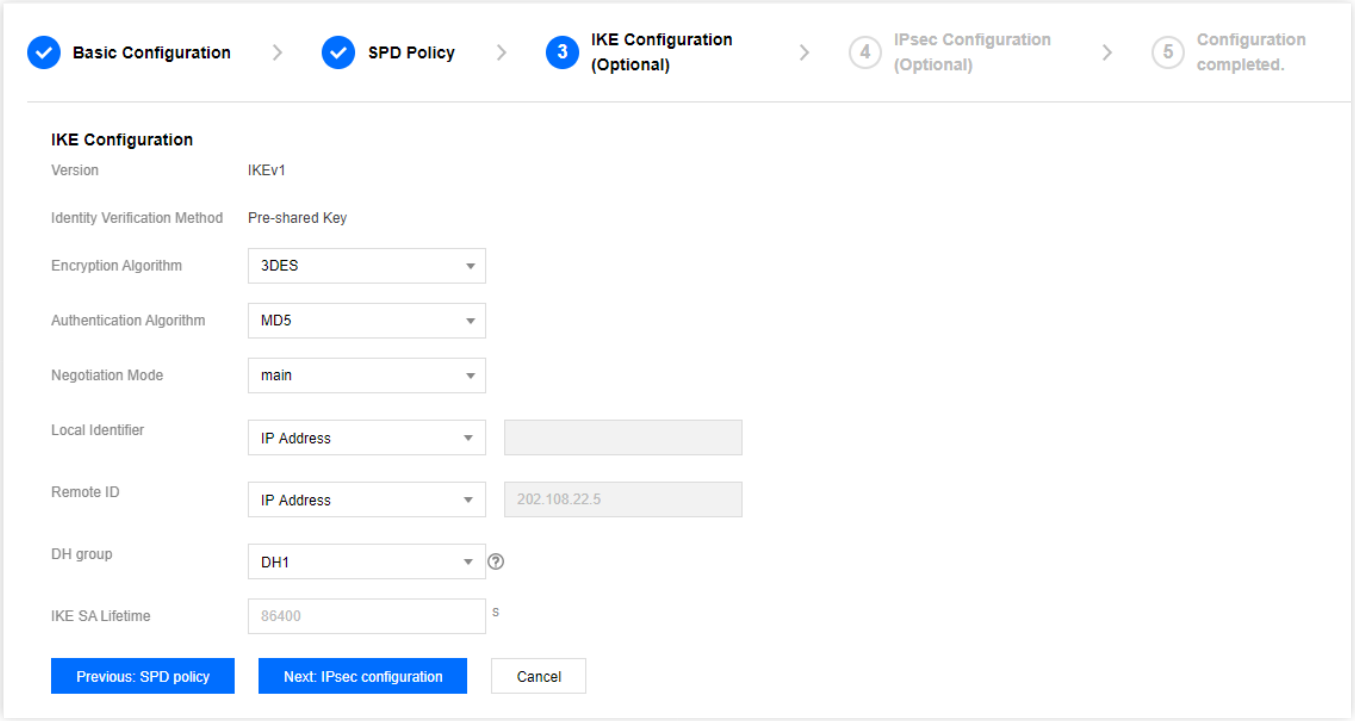
1. Log in to the cloud platform and select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the Virtual Private Cloud console.
2. In the directory on the left, click VPN Connection > VPN Tunnel to enter the VPN Channel interface.
3. Select a region and Virtual Private Cloud, and click Create.



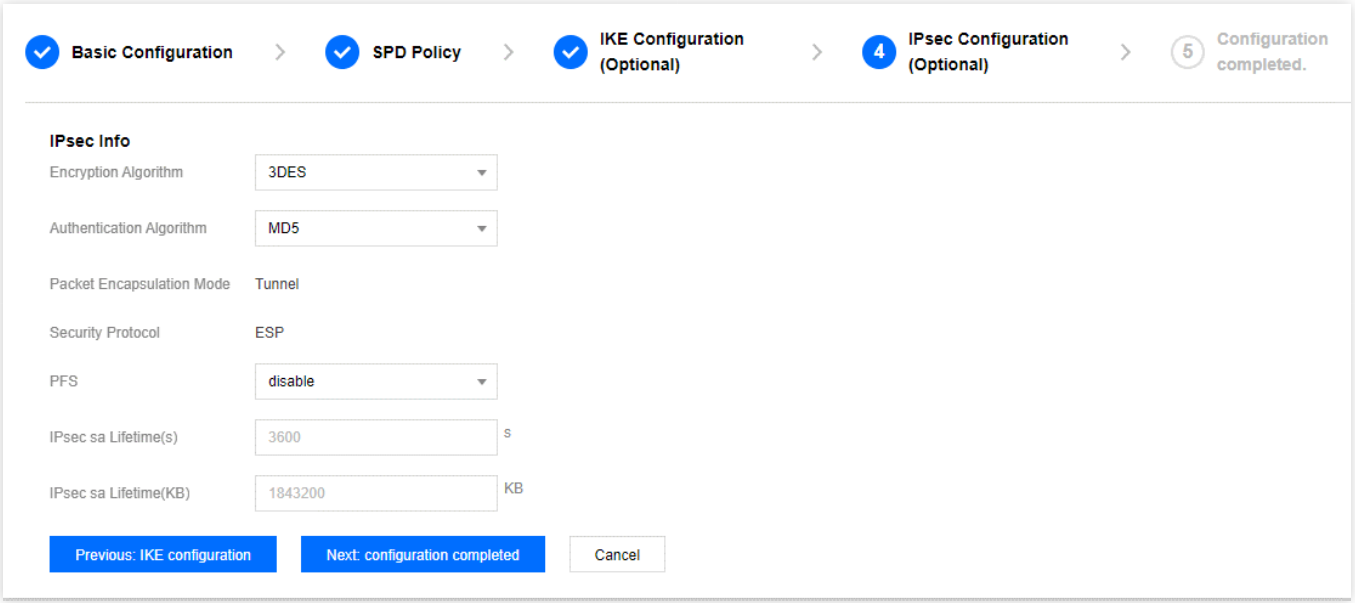
4. Enter the tunnel name (for example, TomVPNConn), select TomVPNGw as the VPN gateway and TomVPNUserGw as the customer gateway, enter the pre-shared key (for example, 123456), and click Next: SPD Policy.



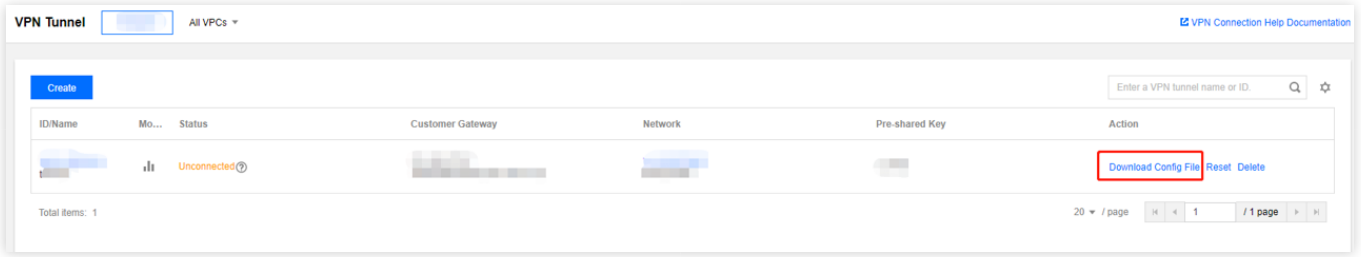
5. Enter the SPD policy to match the local IP range with the customer IP rang. In this example, the local IP range is the IP range 192.168.1.0/24 of subnet A, and the customer IP range is 10.0.1.0/24. Click Next: IKE Configuration.
6. (Optional) Configure IKE parameters. If advanced configuration is not required, click Next: IPsec Configuration.



7. (Optional) Configure IPsec parameters. If no configuration is required, click Next: Complete Configuration. After it is created, return to the VPN channel list page, click Download Configuration File to download the file.



8. After successful creation, return to the VPN channel list page, click Download Configuration File to download the file.



Querying a VPN Channel

The VPN channel management interface displays all created VPN channels. Entering a specific channel allows you to view gateway details and monitoring information. The system also supports quick search by VPN channel name or ID.

1. Enter the VPN Channel management interface.
   The channel list displays all VPN channel information, one channel instance per entry.
2. Query the VPN channel in the search box in the upper right corner of the channel list.
3. (Optional) Click Display Column Settings next to the search box to set the channel parameters to be displayed.
4. Click the Channel ID to enter the Basic Information interface and view channel details.
5. Click the Monitor tab, and the interface will display the metrics of the network channel, including the public network outbound bandwidth, public network inbound bandwidth, outbound packet volume, and inbound packet volume. You can also view it by clicking the monitoring icon on the VPN Tunnel interface.

Deleting a VPN Channel

You can delete VPN channels that are no longer used from the tunnel list.

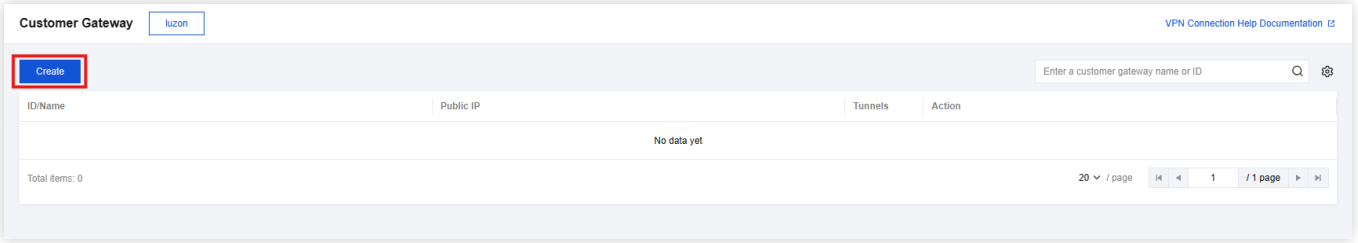
1. Enter the VPN Channel management interface.
2. Find the VPN channel to be deleted in the channel list, and then click Delete in the Operation column.
3. Click OK in the Confirm Deletion dialog box.

Customer Gateway

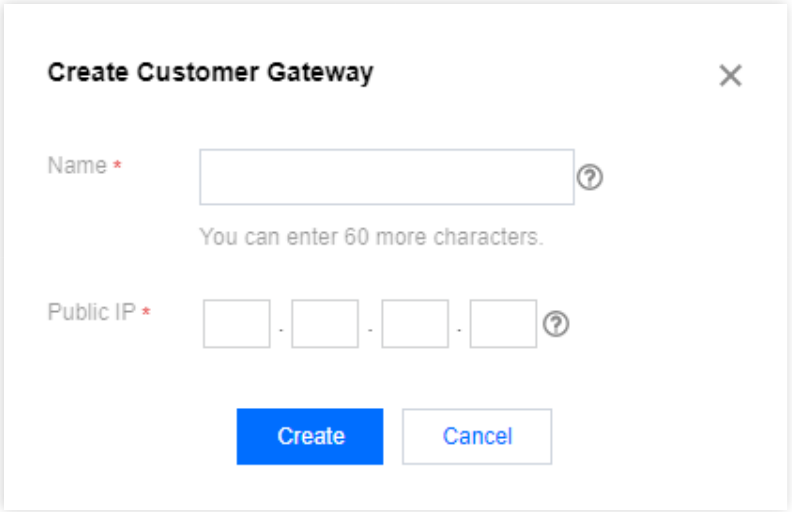
Creating a Customer Gateway

Before creating a VPN channel, you need to create a customer gateway:

1. Log in to the cloud platform and select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the Virtual Private Cloud console.
2. In the directory on the left, click VPN Connection > Customer Gateway to enter the Customer Gateway interface.
3. Select a region, and click Create.



4. Fill in the customer gateway name (for example, TomVPNUserGw) and the public network IP of the IDC VPN gateway, for example, 202.108.22.5.



5. Click Create.

Querying a Customer Gateway

Supports quick search by customer gateway name or ID.

1. Enter the Customer Gateway management interface.
   The channel list shows all customer gateway information.
2. Query the customer gateway in the search box in the upper right corner of the channel list.
3. (Optional) Click Display Column Settings next to the search box to set the customer gateway parameters to be displayed.
4. Click the customer gateway ID to enter the Basic Information interface and query details of the customer gateway.

Deleting a Customer Gateway

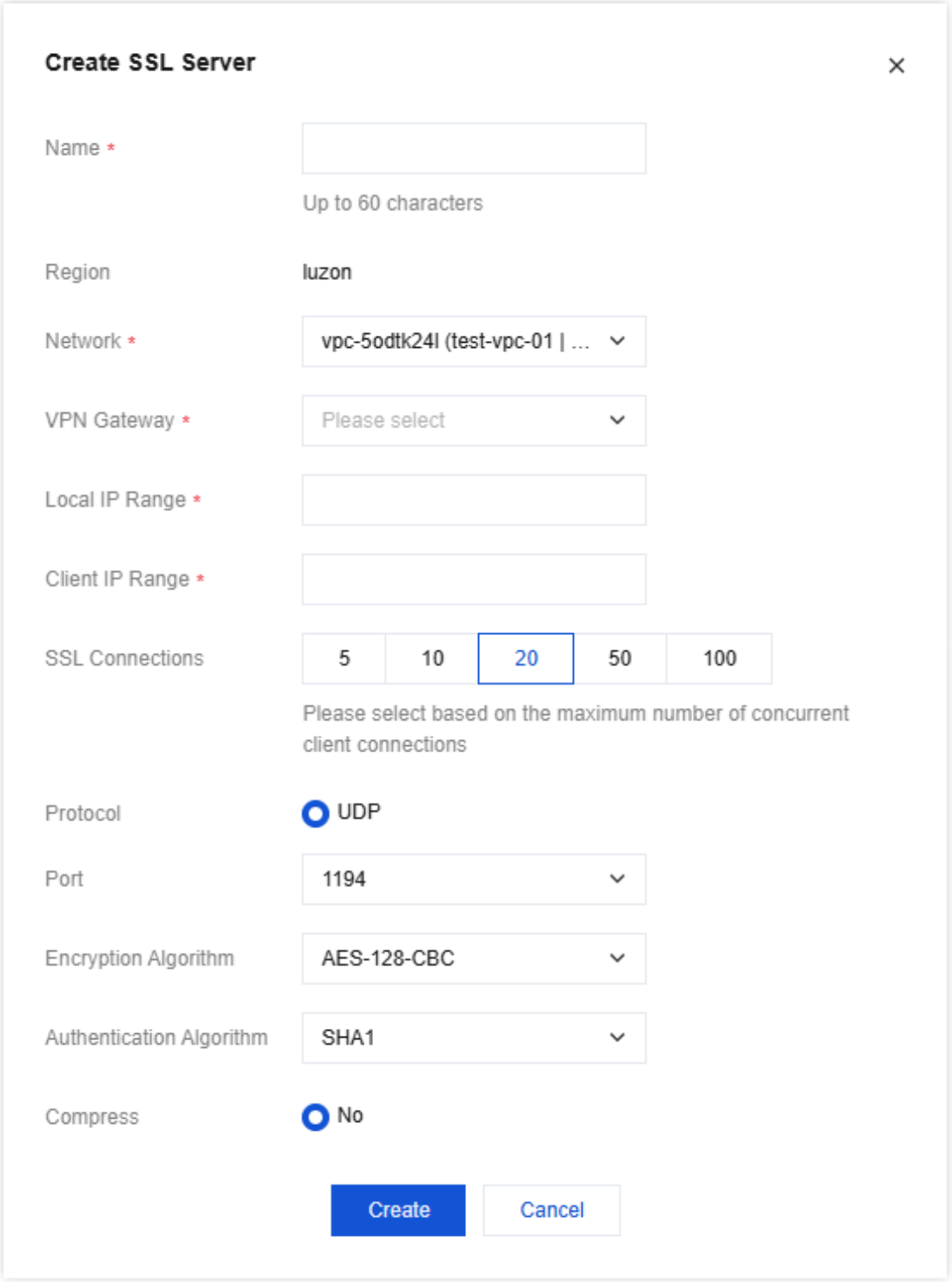
For customer gateways that are no longer in use, you can delete them from the customer gateway list.

1. Enter the Customer Gateway management interface.
2. Find the customer gateway to be deleted in the channel list, and then click Delete in the Operation column.
3. Click OK in the Confirm Deletion dialog box.

SSL Server

Creating an SSL Server

1. Click SSL Server to enter the SSL server interface.
2. Click Create, configure parameters in the pop-up Create SSL Server dialog box, and click Create.



Parameter Description

- Network: Select a Virtual Private Cloud to create the VPN connection.
- VPN gateway: Select the SSL VPN Gateway created in Step 4.
- Local IP range: Fill in the local IP range of the server. The IP range must be within the Virtual Private Cloud CIDR range.
- Client IP range: Fill in the client IP range. Only private address segments 10, 172, and 192 are supported. The mask range is 16-24, which cannot overlap with the VPC IP range.
- Number of SSL connections: Select the number of SSL connections.

- The protocol, port, encryption algorithm, authentication algorithm, and compression parameter values are shown in the figure and cannot be modified for the moment.

Querying an SSL server

Supports fast search by SSL server name or ID.

1. Enter the SSL Server management interface.
   The channel list shows all SSL server information.
2. In the upper right corner of the SSL server list, use the search box to query SSL servers.
3. (Optional) Click Display Column Settings next to the search box to set the SSL server parameters to be displayed.
4. Click the SSL server ID to enter the Basic Information interface and query details of the SSL server.

Deleting an SSL server

You can delete the SSL servers that are no longer used from the list.

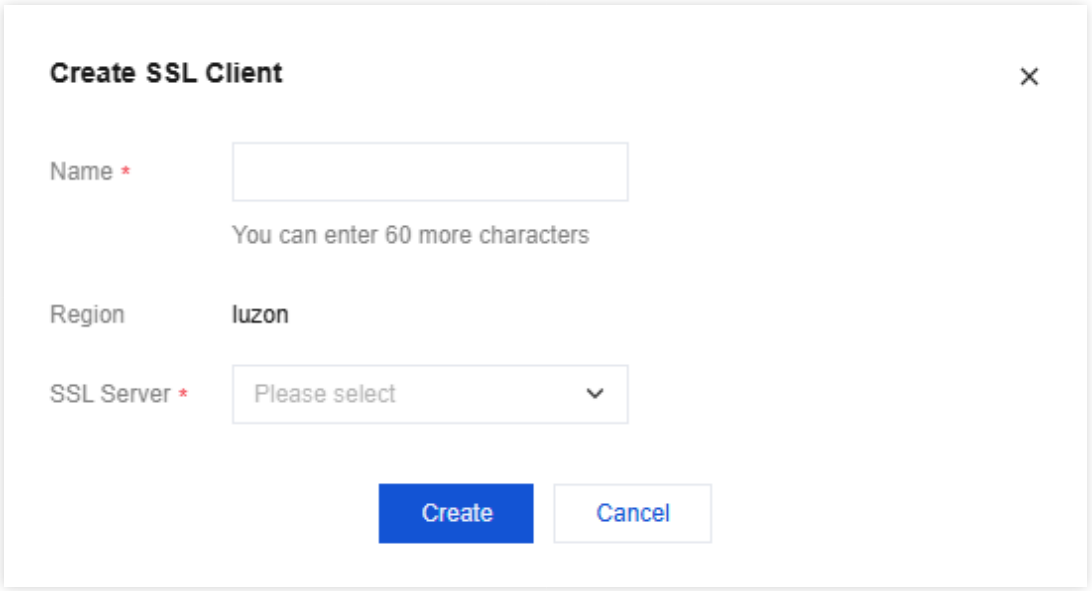
1. Enter the SSL Server management interface.
2. Find the SSL server to be deleted in the SSL server list, and then click Delete in the Operation column.
3. Click OK in the Confirm Deletion dialog box.

SSL Client

Creating an SSL Client

1. Click SSL Client to enter the SSL client interface.

2. Click New, fill in the SSL client name in the New SSL Client dialog box, select the SSL Server created in step 6, and then click Create.



3. Click Download Configuration. The certificate is used to verify the identity with the server.

   The user establishes a connection with the VPN Gateway using a certificate and key. The user side verifies the server certificate, and the server verifies the client certificate. After verification, the server allocates an IP from the Client IP Address Pool to the user. This IP is used for communication with the VPC-internal VM.

Querying an SSL Client

Supports fast search by SSL client name or ID.

1. Enter the SSL Client management interface.
   The channel list shows all SSL client information.

2. In the upper right corner of the SSL client list, use the search box to query SSL clients.
3. (Optional) Click Display Column Settings next to the search box to set the SSL client parameters to be displayed.
4. Click the SSL client ID to enter the Basic Information interface and query details of the SSL client.

Deleting an SSL Client

You can delete SSL clients that are no longer used from the list.

1. Enter the SSL Client management interface.
2. Find the SSL client to be deleted in the SSL client list, and then click Delete in the Operation column.
3. Click OK in the Confirm Deletion dialog box.

FAQs
Concepts

What Is a VPN Connection?

A VPN connection is a way to connect the user's customer IDC to the VPC through a public network encrypted channel. For details, see Product Overview.

What Is a VPN Channel?

After the VPN gateway and customer gateway are established, a VPN channel can be established for encrypted communication between the VPC and the external IDC. For details, see Product Overview.

What Is a VPN Gateway?

A VPN gateway is an egress gateway for VPC to establish a VPN connection. It is used with the customer gateway (IPsec VPN service gateway on the IDC side) to establish secure and reliable encrypted network communication between the cloud platform's VPC and external IDCs. The cloud platform's VPN gateway, underpinned by software virtualization, adopts a dual-server hot standby policy. If one of the servers fails, it will automatically switch to the other, ensuring normal business operations.

A VPN gateway provides eight bandwidth limits: 5 Mbps, 10 Mbps, 20 Mbps, 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, and 1,000 Mbps.

What Is an IPsec VPN?

An IPsec VPN is a way to connect the user's IDC to the VPC through a public network encrypted channel. The cloud platform's VPC IPsec VPN access comprises the following components:

- VPN gateway: The VPN gateway is the IPsec VPN gateway of the VPC. It is used with the customer gateway (IPsec VPN service gateway on the user IDC side) to establish secure and reliable encrypted network communication between the VPC and the user's IDC.
- Customer gateway: The customer gateway refers to the mapping of the IPsec VPN service gateway of the user's IDC in the VPC. It needs to be used together with the VPN gateway. A VPN gateway can be used with multiple customer gateways to establish encrypted VPN network channels.
- VPN channel: It is an encrypted public network IPsec VPN channel. After the VPN gateway and customer gateway are established, a VPN channel can be established for encrypted communication between the VPC and the user's IDC.

What Are the Constraints on VPN Use?

During VPN use, you need to comply with the constraints on the VPN connection and the customer gateway IP address. For details, see Usage Constraints.

How Many VPN Gateways and VPN Channels Can Be Created?

Different resources have different creation quantity limits. For details, see Resource Quota Details Within VPC. If you need a higher quota, fill in the Ticket Application.

Can a VPC Be Connected to Multiple IDCs Through VPN Connections?

Yes. Currently, the VPC can establish VPN gateways and multiple VPN channels on each VPN gateway. Each VPN channel can connect to a local IDC.

Can Communication Between VPCs Be Achieved Through VPN Connections?

Yes. Users need to purchase VPN gateways and configure VPN channels and customer gateways for each of the two VPCs, but the configuration is complicated. VPCs can be interconnected through Peering Connection (PC).

How Is the Quality of the Network Between the VPC and IDC Connected Through VPN Ensured?

- The VPN connection between the VPC and the IDC is transmitted through a public network. Therefore, the overall network quality depends on the quality of the public network. When the public network has latency, packet loss, or jitter, the VPN connection will be affected. If you need more stable communication, it is recommended to use the Direct Connect (DC) service.
- The cloud platform provides 24-hour monitoring for your VPN gateways, issuing alarms for any exceptions. In emergencies, Ops personnel will intervene. Users can also monitor the traffic status of VPN gateways and channels in real time via the console. If any exceptions are found, contact us promptly.

What Is the Difference Between DC and IPSec VPN?

- IPsec VPN uses a public network and the IPsec protocol to establish an encrypted network connection between the user's IDC and VPC. VPN gateways can be purchased, validated, and configured in a few minutes. However, VPN connections may be interrupted by Internet jitter, congestion, and other public network quality issues. IPsec VPN features fast deployment and high cost performance, suitable for users whose business does not require high network connection quality.
- DC, a user-dedicated network connection solution, requires a long time for deployment, but can provide high-quality and highly reliable network connection services. It is suitable for users whose business requires high network quality and security.
  The specific differences between the two schemes are shown in the following table:

Strength	DC	IPsec VPN
Stable	DC provides reliable and guaranteed	Since the IPsec VPN network

Strength	DC	IPsec VPN
network latency	network latency. The connection network is based on a dedicated line. Users can use the fixed routing configuration to avoid the unstable latency caused by congestion or fault-triggered detours.	connection is based on the Internet, routing may be detoured due to linkage congestion during network peak hours, resulting in unstable latency.
Highly reliable disaster recovery connection	DC involves deploying connection devices and network forwarding devices in a distributed and clustered manner, with full-linkage high-reliability configuration. They support dual-line connection with protection and can meet users' high requirements of higher than 99.95% availability.	The IPsec VPN gateway adopts a dual-server hot standby configuration, which has high reliability at the gateway layer. However, due to the unreliable Internet network linkage, it cannot guarantee dedicated line-level network reliability.
Supporting large bandwidth	DC allows a single line to support a maximum bandwidth connection of 10 Gbps. In addition, multiple 10 Gbps linkages can be connected for network load balancing. In theory, the bandwidth supported has no limit.	A single IPsec VPN gateway supports a maximum bandwidth limit of 100 Mbps. The VPC supports configuring multiple VPN gateways, which can support VPN connections with a bandwidth of greater than 100 Mbps.
High security	DC allows the network linkage to be dedicated to users, with no risk of data leakage, ensuring high security and meeting the high network connection requirements of the finance, government, and enterprise sectors.	IPsec VPN network transmission is based on the pre-shared key encryption of the IKE protocol, which can meet most requirements for network transmission security.
Supporting network address translation	DC supports configuring network address translation services on the gateway, IP mapping at both ends of the dedicated line, and IP port mapping at the VPC end, thus perfectly resolving address conflicts when multiple third-party networks are interconnected.	Not supported.

Why Do the Two Ends Have No Traffic or Fail to be Pinged When a VPN Channel Has Been Connected?

Troubleshoot the SPD policy (interesting traffic), routing table, and security group sequentially to see whether they are configured properly:

1. Troubleshoot the SPD policy configuration at both ends.

Check whether the interesting traffic on both sides of the VPN channel is set properly. If your VPN traffic passes through a NAT device, prevent the traffic accessing the cloud platform from being matched by NAT and not reaching the VPN channel, which will cause unavailability of activation traffic and the inability to activate the VPN channel.

2. Troubleshoot the routing configuration at both ends.
   Ensure that a routing policy has been created in the route table for routing to your customer's private network and that the route is pointed to the VPN gateway.
3. Troubleshoot the security policy configuration at both ends.

- The outbound policy of the CVM security group allows active access to the customer IP range, and the inbound policy of the security group allows the customer IP range to actively access your CVM.
- The security policy of your customer's VPN gateway has enabled mutual access between your private network server and CVM.
- Check for security restrictions between your customer's private network server and VPN device.
- Check whether the VPC subnet is bound to the network ACL. If it is, open the corresponding access IP range.
  If the problem remains unresolved after the inspection, submit a work ticket to contact us.

Can I Access the Internet Through a VPN Connection?

No. The cloud platform's VPN product provides services according to relevant national policies and regulations. The VPN gateway only provides the feature of accessing the VPC, and does not provide the feature of accessing the Internet.

Function category

How is VPN gateway implemented and what is its availability?

- A VPN gateway is implemented through network feature virtualization (NFV), which adopts a dual-machine hot standby policy. When a single machine fails, it automatically switches so as not to affect the normal running of the business.
- The VPN channel runs in a public network. Problems such as congestion, jitter, and delay in the public network will affect the quality of the VPN network. If the business has a low tolerance for network transmission delay and jitter, it is recommended to use direct connect.

What to do if a VPN channel is not connected?

The configuration process of VPN channel connectivity requires that the negotiation information on both ends is consistent before a connection can be successfully established. You need to check the consistency of the configuration on both ends in turn. The recommended inspection ideas are as follows:

> Note:
>
> - The VPN channel cannot be established if any parameter is inconsistent.
> - The default VPN configurations of different manufacturers' equipment and cloud platform service providers vary.

1. Check the first phase IKE configuration information.
   Check whether all the parameters required for the first phase, such as the IKE version No., ID authentication method, encryption algorithm, authentication algorithm, negotiation mode, both end identifiers, DH group, and IKE sa lifetime, are consistent. If there are any inconsistencies, modify them and try again.

IKE Configuration Items	Default Configuration	Other Optional Configurations
IKE	IKEv1	-
Identity Authentication Method	Pre-shared Key	-
Encryption Algorithm	3DES	AES-128, AES-192, AES-256, and DES
Authentication Algorithm	MD5	SHA1

IKE Configuration Items	Default Configuration	Other Optional Configurations
Negotiation Mode	main	aggressive
Local ID	IP Address (defaults to the public network IP address of the VPN gateway on the cloud platform)	FQDN
Customer ID	IP Address (defaults to the public network IP address of the customer VPN gateway)	FQDN
DH group	DH1	DH2,DH5,DH14,DH24
IKE SA Lifetime	86400s	Supporting customization

2. Check the Phase 2 IPsec configuration information
   Check whether all parameters required for the second phase, such as the encryption algorithm, authentication method, message encapsulation mode, security protocol, PFS, and IPsec SA generation cycle, are consistent at both ends. If there are any inconsistencies, modify them and try again.
   Converge Cloud The default configuration of the second phase IPsec parameters of the VPN gateway is:

IPsec Configuration Items	Default Configuration	Other Optional Configurations
Encryption Algorithm	AES-128	AES-128, AES-192, AES-256, and DES
Authentication Algorithm	MD5	SHA1
Message Encapsulation Mode	Tunnel	-
Security Protocol	ESP	-
PFS	disable	dh-group1,dh-group2,dh-group5,dh-group14,dh-group24
IPsec sa Lifetime	3600s	Supporting customization
IPsec sa Lifetime	1843200KB	Supporting customization

Why are the monitoring data displayed by the VPN gateway and VPN channel sometimes inconsistent?

Currently, there are differences in the data collection locations and reporting intervals for VPN gateways and VPN channels. The statistical granularity for VPN gateways is 1 minute, while the statistical granularity for VPN channels is 10 seconds, that is, the statistical granularities are inconsistent. Therefore, when data are aggregated on the monitoring page, the displayed data of the VPN gateway and the VPN channel will be inconsistent.

How to configure VPN?

IPsec VPN can be fully self-configured in the console. For details, see Quick Start.

How to create a VPN gateway?

Users can go to the Virtual Private Cloud (VPC) console to create a VPN gateway. For details, see Creating VPN Gateway.

How to create a VPN channel?

Users can go to the Virtual Private Cloud (VPC) console to create a VPN channel. For details, see Creating VPN Channel.

How to view VPN connection monitoring data?

Users can enter the Virtual Private Cloud (VPC) console to view VPN connection monitoring data. For details, see Viewing Monitoring Data.

How to set up VPN connection alarms?

Users can go to the Virtual Private Cloud (VPC) console to set up VPN connection alarms. For details, see Setting Alarms.

How to modify VPN channel configuration?

Users can enter the Virtual Private Cloud (VPC) console to modify the VPN channel configuration. For details, see Modifying VPN Channel Configuration.

Glossary

Customer Gateway

The customer gateway refers to the mapping of the IPsec VPN service gateway of your IDC in the Virtual Private Cloud. The customer gateway needs to be used together with the VPN gateway. One VPN gateway can establish encrypted VPN network channels with multiple customer gateways.

IPsec VPN

IPsec VPN (Internet Protocol Security VPN) is a way to connect your IDC and the Virtual Private Cloud through a public network encrypted channel.

Routing table

Routing table contains a series of routing policies that are used to define the network traffic direction of each subnet in the Virtual Private Cloud.

Routing Policy

Routing policy is a rule for the path that network traffic follows. Each routing policy contains three parameters:

1. Destination: Description of the destination IP range. The destination cannot be the IP range in the Virtual Private Cloud where the routing table is located.
2. Next hop type: The next hop type of the Virtual Private Cloud supports a series of types such as "public network gateway", "VPN gateway", and "direct connect gateway". You need to create such a gateway first; otherwise, you cannot pull this next hop type.
3. Next hop: It specifies the next hop gateway to which the subnet traffic associated with this routing table will be forwarded.

Virtual Private Cloud

VPC creates an independent network space on the cloud platform, very similar to the traditional network you operate in your data center. However, hosted in the cloud platform's VPC are your cloud services, including: Cloud servers, CLB, Cloud Database, and other cloud service resources. You don't need to worry about purchasing and operating network equipment; you can custom define IP ranges, IP addresses, routing policies, etc. through software. Not only can you flexibly access the Internet via Elastic IP, NAT Gateway, and Public Gateway, but you can also connect your VPC with your data center through VPN / DC. At the same time, the cloud platform VPC's PCGW service can help you easily achieve global service unification and two-location three-center disaster recovery. Additionally, the security groups and network ACLs within the cloud platform VPC can meet your network security needs in multiple dimensions and comprehensively.

VPN Gateway

VPN gateway is an IPsec VPN gateway for the Virtual Private Cloud, which is used together with the customer gateway (IPsec VPN service gateway on your IDC side) to establish secure and reliable encrypted network communication between the Virtual Private Cloud and your IDC.

VPN Tunnel

VPN Tunnel is an encrypted public network IPsec VPN tunnel. After the VPN gateway and customer gateway are established, a VPN tunnel can be established for encrypted communication between the Virtual Private Cloud and your IDC.

Connection

A connection is the physical line connection between a cloud platform and a local data center. A connection can establish dedicated tunnels with direct connect gateways in multiple regions.

Subnet

Subnet is a flexible division of Virtual Private Cloud IP ranges. Applications and services can be deployed in different subnets, and multi-layer web applications can be hosted securely and flexibly in the cloud platform VPC.

Direct Connect

Direct connect is a method for quickly connecting the english-NFV and local data centers. You can use a connection to connect to cloud {{conf.title}computing resources in multiple regions at once, achieving flexible and reliable hybrid cloud deployment.

Dedicated tunnel

A dedicated tunnel is a network link division of a connection. Users can create dedicated tunnels connected to different direct connect gateways to interconnect local data centers with multiple Virtual Private Clouds.

Direct Connect Gateway

A direct connect gateway is a direct connect traffic entrance to the Virtual Private Cloud, which can connect multiple dedicated tunnels and interconnect with multiple local data centers.