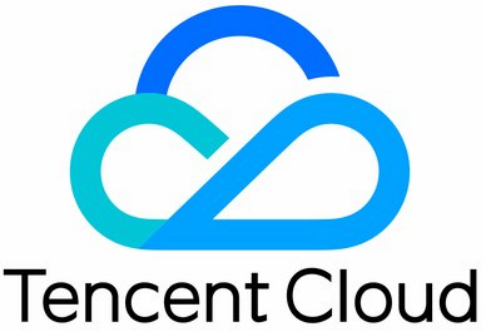
VPN Connections

FAQs



Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

FAQs
Concept category

Last updated: 2024-09-26 10:43:57

What is IPsec VPN?

IPsec VPN is a way to connect user IDCs and VPCs through an encrypted channel over the public network. Tencent Cloud VPC IPsec VPN connection consists of the following components:

- **VPN Gateway**: It is an IPsec VPN gateway for the Virtual Private Cloud, which is used together with the customer gateway (IPsec VPN service gateway on the user IDC side) to establish secure and reliable encrypted network communication between the Virtual Private Cloud and the user IDC.
- **Customer Gateway**: The customer gateway refers to the mapping of the IPsec VPN service gateway of the user 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.
- **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 Virtual Private Cloud and the user IDC.

Can a VPC be connected to multiple IDCs through VPN connections?

Yes, currently the Virtual Private Cloud can establish VPN gateways and establish multiple VPN channels on each VPN gateway. Each VPN channel can connect to a local IDC.

What is the difference between Direct Connect and IPSec VPN connection?

- IPsec VPN connections use a public network and the IPsec protocol to establish an encrypted network connection between the user's data center and the Virtual Private Cloud. 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. When the user's business does not require high network connection quality, it is a fast deployment and cost-effective option.
- Direct connect provides a user-dedicated network connection solution. It takes a long time to build, but can provide high-quality and highly reliable network connection services. When the user's business requires high network quality and security, this solution can be selected for deployment.

The specific differences between the two are shown in the following table:

Strengths	Direct Connect	IPsec VPN
Stable Network Delay	The network latency is reliable and limited to a low level. The connection network is based on a DC. You can use a fixed routing configuration to avoid the latency and instability caused by congestion or fault-triggered detours.	The network connection is based on the Internet. When the network link is blocked during peak hours, it may cause routing detours and unstable latency.
Highly Reliable Disaster Recovery Connect	Both connection devices and network forwarding devices are deployed in a distributed and clustered manner, with full-link high-reliability configuration, supporting dual-line connection with protection, meeting your stringent requirements for availability above 99.95%.	It adopts a dual-machine hot backup configuration, which has high reliability at the gateway layer. However, due to the unreliable Internet network link, it cannot guarantee dedicated line-level network reliability.
Supporting Large Bandwidth	A single line supports a maximum bandwidth connection of 10 Gbps, and can also allow connection with multiple 10 Gbps links for network CLB, with no theoretical upper limit.	A single gateway supports a maximum bandwidth of 3 Gbps. VPC supports multiple VPN gateway configurations, and by configuring multiple VPN gateways, it can support VPN access beyond 3 Gbps.
High Security	The network link is dedicated to users, with no risk of data leakage, ensuring high security and meeting the stringent network connection requirements of the finance, government, and enterprise sectors.	Network transmission is based on the pre-shared key encryption of the IKE protocol, which can meet most network transmission security requirements.
Supporting Network Address Translation	It supports configuring network address translation services on the gateway, enabling IP mapping at both ends of the DC and IP port mapping at the VPC end, thus resolving address conflicts when	Not support.

	multiple networks are interconnected.	

What are the constraints on using a VPN?

When using VPN, 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.

How to assure the network quality between the Virtual Private Cloud and IDC connected through VPN?

- VPN Connections between VPC and IDC are transmitted over the public network. Therefore, the overall network quality depends on the quality of the public network. When the public network experiences latency, packet loss, or jitter, VPN Connections will be affected accordingly. If you need more stable communication quality, it is recommended to use DC service.
- Tencent Cloud provides 24-hour monitoring for your VPN gateways and reports alarms for abnormal situations. Operations personnel are available for emergencies. You can also monitor the traffic status of VPN gateways and channels in the console in real time. If any exceptions occur, please promptly contact us.

Can I access the Internet through a VPN connection?

No. VPN gateways only provide access to VPCs but not to the Internet.

Can I use VPN Connections without a public IP?

If you use an IPsec VPN connection, you must have public IPs on both ends.
If you don't have public IPs, you can try using an SSL VPN to connect your local LAN to the cloud environment. Explore SSL VPN to see whether it meets your requirements.

Note

- Using an IPSec VPN connection requires the customer gateway to have a fixed IP address.

- An SSL VPN gateway doesn't require the customer gateway to have a fixed public IP address. It is an egress gateway through which the VPC establishes SSL VPN Connections and is used together with the SSL VPN client (mobile client). For details, see SSL VPN.

What is a customer gateway?

A customer gateway is a logical object that records the VPN gateway on the edge of the peer IDC.

What is an SPD policy? Why do I need to configure the local and peer IP ranges?

The SPD (Security Policy Database) policies consist of a series of SPD rules used to specify which IP ranges within a VPC or CCN can communicate with which IP ranges within an IDC. In the SPD configuration, you need to configure the Local Network Segment and the Peer Network Segment. The local gateway configuration is the Tencent Cloud VPN Gateway belonging to the network segment, and it cannot overlap. The Peer Network Segment is the public network segment of the customer's local gateway used to connect with Tencent Cloud. For details, see SPD policies.

What is an SSL VPN client?

An SSL VPN client is a VPN client that is deployed on user terminals and is considered a logical instance on Tencent Cloud.

Scenarios

Last updated: 2024-09-26 10:44:13

What do I do when an employee leaves the company or a project team, or when I need to temporarily revoke an employee's permissions?

You can disable the certificate on the SSL client page. For details, please see Start, Stop, and Update SSL Client Certificate.

Can I remotely connect to my VPC over a VPN connection?

Tencent Cloud provides an SSL VPN product, allowing users to remotely access their resources and services in the cloud via PCs or mobile devices by establishing a connection with cloud resources through SSL VPN. For more details, see Establishing a Connection Between Mobile Devices and VPC.

Can I access the internet over an SSL VPN connection?

It is not supported.

Can I use Tencent Cloud VPN Connections for the proxy service?

Tencent Cloud VPN Connections provides services in compliance with national laws and regulations, and does not provide the internet access or proxy service.

Can multiple IDCs communicate through a VPN gateway?

Yes, when multiple IDCs need to communicate with each other but do not need to access cloud resources, intercommunication can be achieved through a **CCN-based VPN**. Each IDC connects to the Tencent Cloud CCN-based VPN gateway (not linked to CCN) via their respective IPsec VPN devices to directly facilitate traffic exchange.

Can multiple IDCs communicate with a VPC by using a VPN gateway?

Yes. You can create a VPN gateway for CCN and associate the gateway with a CCN instance. In this case, each IDC uses its own IPsec VPN devices to access the VPN gateway for CCN to communicate with a VPC.

Can I implement redundant communication by using a DC connection as the primary connection and a VPN connection as the secondary connection?

Yes. You can create a VPC-based Direct Connect (DC) gateway and a VPC-based VPN gateway. Then, you can create a DC connection and a VPN connection. Based on the VPC route priority, the DC connection serves as the primary connection and the VPN connection serves as the secondary connection. This allows you to implement redundant communication. For more information, see Hybrid Cloud Primary/Secondary Communication (DC and VPN).

How can Tencent Cloud VPN Connections bypass network censorship?

Tencent Cloud VPN Connections provides services in compliance with national laws and regulations. It does not provide Internet features and prohibits technical means to circumvent network censorship.

How do I implement primary/secondary disaster recovery?

To achieve disaster recovery with an active-standby configuration through Tencent Cloud VPN, you can create 2 route-based IPsec VPN channels, configure subnet routes, gateway configurations, routes and weights. For specifics, please refer to IDC and Single Tencent Cloud VPC Disaster Recovery.

How do I use Tencent Cloud VPN Connections? How do I choose between IPsec VPN and SSL VPN?

Tencent Cloud VPN Connections supports both the IPsec and SSL network security protocols.

- If you are in a Site-to-Site connection scenario, you can use IPSec VPN. For access guidance, please see IPSec VPN.
- If you need remote access from mobile devices (Client-to-Site) to the cloud, you can use SSL VPN. For access guidance, please see Establishing a Connection Between Mobile Devices and VPC.

Does Tencent Cloud VPN Connections support internet access acceleration?

Currently not supported. If you need an acceleration product, please check AIA.

Can I use Tencent Cloud VPN Connections to access a hotel system that runs on Tencent Cloud from hotels in six regions?

Yes. You can use SSL VPN in this scenario. If you have higher security requirements, you can configure access control. For details, see SSL VPN Access Control and Portal Login Guide.

Can I use Tencent Cloud VPN Connections to visit Google?

No. Tencent Cloud VPN Connections provides services in compliance with national laws and regulations, and does not provide the internet access or proxy service. You are not allowed to

technically circumvent internet censorship to visit banned websites.

Can I use Tencent Cloud VPN Connections to access Tencent Cloud without a public IP address?

Yes. You can use SSL VPN in this scenario.

Can I use Tencent Cloud VPN Connections for non-Tencent Cloud products?

Yes. Tencent Cloud VPN Connections is developed based on the standard IKE and IPsec protocols. Therefore, it is compatible with all VPN devices and services in compliance with the protocols.

Does Tencent Cloud VPN Connections support primary/secondary disaster recovery based on ECMP?

No. Tencent Cloud VPN Connections does not support Equal-Cost Multipath Routing (ECMP). However, you can use Tencent Cloud VPN Connections to implement primary/secondary disaster recovery in the following way: Create two IPsec VPN tunnels (route table) and configure the subnet routing, gateway routing, as well as routing weights. For more information, see Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery.

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 enter the VPC Console to create a VPN gateway. For more details, see Create VPN Gateway.

Can communication between two VPCs be implemented through a VPN connection?

Yes. You can separately purchase VPN gateways and configure VPN tunnels and customer gateways in the two VPCs, but the configuration is complex. We recommend that you use CCN. CCN connects two VPCs by using the private network of Tencent to ensure the quality of communication.

Billing

Last updated: 2024-09-26 10:44:30

What's the billing mode for VPN connections?

- VPN tunnels and customer gateways are free of charge, but VPN gateways are charged.
- The VPN gateway offers two billing models: "annual and monthly subscription (prepaid)" and "pay-as-you-go after usage." You can choose the billing method according to your needs. For details, see Billing Overview.

For more information about VPC pricing, see VPC Pricing Overview.

Why can't I renew or upgrade VPN gateways?

A VPN gateway cannot be renewed and upgraded at the same time. If you have an unpaid renewal or upgrade order, other renewal or upgrade operations cannot be performed. The system invalidates unpaid renewal or upgrade orders at 24:00 every day, after which you must re-submit your order.

Will I receive a reminder when my VPN gateway expires?

For information about VPN gateway expiration notifications, see Expiration Notifications.

When an annual and monthly subscription VPN gateway expires, how many days can it be retained and how should it be renewed?

After an annual and monthly subscription VPN gateway expires, it will enter a frozen state within 7 days. Users can renew to resume use. If the period exceeds 7 days, resources will be released and cannot be recovered. Please note the VPN gateway expiration date.
Users can enable the auto-renewal feature for VPN connections in the VPC console. If there is sufficient account balance, the VPN gateway service will be automatically renewed to ensure uninterrupted stable business operations.

Can the billing modes between annual and monthly subscription and pay-as-you-go be switched?

> **Note:**
> Pay-as-you-go does not support switching to annual and monthly subscription (prepaid) mode.

An annual and monthly subscription VPN gateway can be switched to a pay-as-you-go VPN gateway. Please note the following:

1. The pay-as-you-go mode will become effective after the current gateway expires.
2. In the pay-as-you-go mode, gateway fees and traffic fees are billed separately.
3. Gateway and traffic fees are settled hourly. When deleting, the gateway fee for less than 1 hour will be calculated as 1 hour.
4. After switching to the pay-as-you-go mode, you cannot switch back to the annual and monthly subscription billing mode.

How to return a VPN gateway?

For information on how to return a VPN gateway, see Return Instructions.

Is an SSL VPN connection still charged after it is terminated?

After an SSL VPN connection is terminated, no traffic fees will be incurred. However, the VPN gateway instance fee and SSL connection fee are fixed and will also be charged. Please delete any resources that you no longer need in time.

Why am I charged for creating a VPN but not using it?

The billing items vary based on the VPN product type:

- The billing items of IPsec VPN include the gateway instance and public network traffic. A fixed fee is charged for the gateway instance.
- The billing items of SSL VPN include the gateway instance, SSL connections, and public network traffic. Fixed fees are charged for the gateway instance and SSL connections, and the public network traffic is charged in pay-as-you-go mode.

For billing details, see Billing Overview.

Why is a pay-as-you-go VPN connection still charged after it is deleted?

A VPN connection is hourly postpaid in pay-as-you-go billing mode (billed hourly; time less than an hour is counted as an hour). If you use a connection during 12:02-13:20, fees will be incurred for two hours (12:00-13:00 and 13:00-14:00). In addition, the billing time in pay-as-you-go mode is not fixed and may be delayed; for example, fees for 13:00-14:00 may be billed after 14:00 or 15:00.

Do I need to pay for VPN tunnels and customer gateways?

VPN tunnels and customer gateways can be used for free.

Why cannot I delete an overdue gateway?

You can delete an overdue gateway only after you delete the resources associated with the gateway.

If I use an SSL VPN connection only from 8:00 to 12:00 in the morning, is the connection charged for other time periods?

In time periods with no traffic, only the VPN gateway instance fee and the SSL connection fee are charged.

How do I enable auto-renewal?

In the upper right corner of the Tencent Cloud console, click **Fees**, and then in the left navigation pane, click **Renewal Administration**. Set up your auto-renewal resources on the **Renewal Administration** page under the **Auto-Renewal** tab.

Why does the fee still be automatically deducted even when the VPN tunnel is not connected or has been deleted?

The outbound traffic of the VPN gateway will be charged. Delete the unused VPN gateway to avoid fee deduction.

Are upgrade and downgrade configurations & billing conversions supported?

- For billing, only annual and monthly subscription billing can be converted to pay-as-you-go billing at this time.
- In terms of quota, the VPN gateway bandwidth can only be adjusted in specific bandwidth ranges. Please properly plan the bandwidth for your business.
  - Annual and Monthly Subscription: In each bandwidth range ([5 Mbps, 100 Mbps] or [200 Mbps, 1000 Mbps]), quota upgrades are supported. Downgrades and cross-range adjustments are not supported.
  - Pay-as-you-go: The VPN gateway bandwidth can only be adjusted in the current bandwidth range ([5 Mbps, 100 Mbps] or [200 Mbps, 1000 Mbps]). Cross-range adjustment is not supported.
  - The bandwidth of 1000 Mbps SSL VPN gateways and 3000 Mbps IPsec VPN gateways cannot be downgraded. Please properly plan the bandwidth for your business.

About IPsec gateways

Last updated: 2024-09-26 10:44:43

VPN Gateway

Why can't the gateway be deleted?

Before deleting, you need to remove the associated VPN channel resources. For details, refer to Deleting SSL VPN Gateway.

The gateway specification is 50Mbps. How should its bandwidth limit be understood?

The bandwidth limit in the VPN gateway interface refers to the outbound public bandwidth limit, which is the bandwidth flowing out from the VPN gateway.

The gateway bandwidth is 50Mbps, but the upload speed to the cloud is only 2MB/s. Why?

50Mbps is the bandwidth you purchased. The upload speed depends on your public network speed.

Can an IPSec VPN Gateway be switched to an SSL VPN Gateway?

No, IPSec VPN and SSL VPN are different types of VPNs and cannot be interchanged.

Does the VPN gateway support upgrades and downgrades?

Currently, only upgrades within a certain range are supported, [20,100], [200,1000]. Cross-range upgrades and downgrades are not supported. For example, upgrading from 50M to 100M is allowed, but upgrading from 100M to 200M requires creating a new 200 specification gateway.

How can I view gateway traffic?

You can configure the gateway traffic control feature. For details, refer to Enable the Gateway Traffic Monitoring Details.

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 is VPN gateway implemented and what is its availability?

VPN Gateways are implemented through Network Functions Virtualization (NFV) and adopt a dual-machine hot standby strategy. In case of a single machine failure, an automatic switch will occur without affecting normal business operations.
VPN channels operate over the public network, and issues like congestion, jitter, and latency in the public network can affect VPN network quality. If your business has low tolerance for network transmission delays and jitter, it is recommended to use DC.

How can I view VPN gateway details?

Users can go to the VPC Console to view detailed information about the VPN Gateway. For details, please refer to Viewing VPN Gateway Details.

VPN Tunnel

VPN tunnel shows connected, why can't I ping?

If the tunnel is in a normal status yet the private network cannot be connected, the possible causes are as follows:

- The VPC subnet routing table has not added a route pointing to the IDC side intranet network segment.
- The security policy on the VPC/IDC side does not make the corresponding source and destination IPs open to Internet.
- The VPN Gateway has not added a channel (routing type) pointing to the IDC side intranet network segment.
- The firewall of the operating system of private network server on the VPC/IDC side does not allow the customer IP range to pass.
- The SPD policy on the VPC/IDC side does not contain the source and destination IPs.
- The VPN Gateway has not configured a routing policy.

For details, please refer to VPN Tunnel Connected Yet Private Network Unconnected.

VPN tunnel shows unconnected?

Possible reasons are as follows:

- No traffic to activate the tunnel.
- The VPN gateway public IP is not connected.
- The security policy is not correctly configured.
- Inconsistent negotiation parameters and modes.

For details, please refer to: VPN Tunnel Unconnected.

Channel negotiation failed error code, how to interpret?

For details on channel negotiation failed error codes, please refer to IPSec VPN Negotiation Failed Error Notes.

What could be the reason for a sudden disruption during continuous usage?

Possible Causes:

- Your Public IP is an international IP. Accessing the cloud host is isolated due to compliance issues.
- You have made local configuration changes, such as protocol changes, or local upgrades have enabled new protocol parameters by default, which are not configured on the Tencent side.
- The local firewall has blocked cloud access.
- Negotiation parameter configuration values are inconsistent, such as SA lifetime, etc.
- The VPN tunnel has been deleted.

Why do we need an SPD Policy?

The SPD Policy specifies which network segments within the VPN Gateway can communicate with which segments in the IDC.

> **Note**
> Rules within the same VPN Gateway cannot overlap among all tunnels.

How to configure a health check?

1. First, ensure that the peer connected to the VPN is a routed gateway, which needs to be connected accordingly.
2. Configure a health check on the Tencent Cloud console side. For details, please refer to Configuring Health Check.

> **Note**

- Before configuring the health check, make sure to have primary and backup tunnels in place to prevent business impact. It is not recommended to configure a health check without primary and backup tunnels.
- You need to ensure there are no IP conflicts on both ends. If the IPs on both ends are in the same network segment, there is no need to configure routes separately to specify the peer.

3. Configure VPN gateway routes and set the priority.

The channel health status is "unhealthy". What's the reason?

The IP Ping for the health check you configured has failed. Please check the health check configuration.

Does VPN support Barbaric Mode?

It is not supported.

How to configure SPD policy, and can the peer IP range be filled arbitrarily?

The SPD Policy specifies which network segments within the VPN gateway can communicate with which segments in the IDC. The peer IP range is a subset of your local network's IPs accessible to the public network and cannot overlap.

Does the SPD Policy–based VPN channel have an order requirement for the local and peer ends?

There is no order requirement for the local and peer ends in the same SPD policy.

How to modify VPN channel configuration?

Users can go to the VPC Console to modify VPN channel configuration. For details, please refer to Modifying VPN Channel Configuration.

How to create a VPN channel?

Users can go to the VPC Console to create a VPN channel. For details, please refer to Creating VPN Channel.

What is the matching relationship between the local and peer ends in the SPD policy?

For the matching relationship, please refer to SPD Policy.

About SSL

Last updated: 2024-09-26 10:44:57

How do I specify the local and peer IP ranges when I create an SSL VPN server?

- Tencent Cloud IP range: Enter the Tencent Cloud IP range to be accessed by mobile clients, which is the IP range of the subnet in which your VPN gateway resides. For example, enter 10.0.0.0/24, 10.0.0.0/26, 10.0.0.0/28, or 10.0.0.0/30 for the 10.0.0.0/18 subnet.
- Client IP range: Enter the IP range that the SSL VPN gateway assigns to the client for communication with Tencent Cloud. You can enter any IP range whose subnet mask is less than or equal to 24. Take note that the IP range must not conflict with the VPC CIDR of Tencent Cloud or your local private network.

Why does the SSL connection fail?

1. The public network connection failed. Check the connectivity of the public network.
2. Is the Public IP abnormal, especially the cross-border Public IP? Cross-border Public IPs are prohibited from directly accessing cloud resources and will be blocked upon detection.
3. The subnet route is not configured. For subnet routing configuration, refer to Step 4: Configuring Tencent Cloud Side Routing Policy.
4. The SSL client certificate is used by multiple users. Only one user can use the SSL client certificate.

Can I change the number of SSL connections?

Currently not supported. Please plan the SSL connection count in advance before creation.

Does an SSL VPN require fixed public IP addresses?

No. SSL VPN connections do not require fixed IP addresses on the user side. An SSL VPN allows Windows, MAC, and Linux clients, as well as mobile phones that use OpenVPN, to connect to instances on Tencent Cloud VPCs.

Can I switch an SSL VPN to an IPsec VPN?

No, IPSec VPN and SSL VPN are different types of VPNs and cannot be interchanged.

Can multiple clients use the same certificate?

No, each SSL client configuration certificate can be used only by one client.

What is the maximum number of SSL connections allowed?

The maximum number of SSL connections allowed varies based on the bandwidth specification. A bandwidth specification of [5 Mbps, 100 Mbps] supports up to 100 SSL connections. A bandwidth specification of [200 Mbps, 500 Mbps] supports up to 500 SSL connections. A bandwidth specification of 1000 Mbps supports up to 1000 SSL connections.

General

Last updated: 2024-09-26 10:45:08

How to enable gateway flow control details?

Users can enter the VPC Console to enable gateway flow control details. For more information, see enabling gateway flow control details.

How to set gateway flow control details?

Users can enter the VPC Console to set gateway flow control details. For more information, see setting gateway flow control details.

How to view gateway flow control details?

Users can enter the VPC Console to view gateway flow control details. For more information, see viewing gateway flow control details.

How to bind an Anti-DDoS package?

Users can enter the Anti-DDoS Management Console to bind an Anti-DDoS package. For more information, see binding an Anti-DDoS package.

How to view VPN connection monitoring data?

Users can enter the VPC Console to view VPN connection monitoring data. For more information, see viewing monitoring data.

How to set up VPN connection alarms?

Users can enter the VPC Console to set VPN connection alarms. For more information, see setting alarms.