VPN Connections

Operation Guide

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide

VPN Gateway

IPSec VPN Gateway

Creating a IPSec VPN Gateway

Last updated：2024-01-10 17:25:33

A VPN gateway is a VPN connection instance. Therefore, please create an IPsec VPN gateway before using a VPN connection to securely access the Tencent Cloud Virtual Private Cloud (VPC) from external networks. This document shows you how to create a VPN gateway in the console.

Prerequisites

To create a VPC-based VPN gateway, you need to create a VPC in the same region as the VPN gateway first. For more information, see Creating VPCs.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click **+New**.
4. Configure the following gateway parameters in the pop-up window.

Note:

Only new gateways but not existing gateways are supported on 200 Mbps, 500 Mbps, 1,000 Mbps and 3,000 Mbps bandwidths.

If the VPN gateway uses 200 Mbps, 500 Mbps, 1,000 Mbps or 3,000 Mbps bandwidths, AES128+MD5 is recommended for VPN tunnel encryption.

Parameter Name	Configuration
Gateway Name	Enter the VPN gateway name (up to 60 characters)
Region	Display the region of the VPN gateway
AZ	Select the availability zone of the current gateway

Protocol Type	IPSec and SSL protocols are supported.
Bandwidth cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Associated Network	This parameter indicates whether you create a CCN-based VPN/VPN gateway or a VPC-based VPN/VPN gateway. If you want to use a VPN connection to implement the interconnection with multiple VPCs or other Direct Connect networks, please create the CCN based VPN. **Note:** You cannot associate the CCN-based VPN gateway with a CCN instance during its creation. You can associate a created VPN gateway to a CCN instance in the gateway details page. If you create a policy-based VPN tunnel, you also need to enable the route published to the CCN in the IDC IP range of the VPN gateway. If you want to communicate with a single VPC through a VPN connection, please create a VPC based VPN.
Network	Specify the VPC to be associated with the VPN gateway only when the associated network is VPC.
Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.
Billing Mode	Bill-by-traffic mode is supported. This billing mode is applicable to scenarios with significant bandwidth fluctuations.

5. After completing the gateway parameter settings, click **Create**, and the Status of the gateway is **Creating**. In 1 to 2 minutes after the gateway is successfully created, the status turns to **Running**, and the system assigns a public IP to the VPN gateway.

Configuring The Routing Policies From The Tencent Cloud To User

Last updated：2024-01-09 14:29:29

Prerequisites

You have completed the configurations of VPN gateway, customer gateway and VPN tunnel before configuring a routing policy.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Gateway** on the left sidebar.
3. On the **VPN Gateway** page, select the target region and VPC, and click the **ID**/**Name** of the VPN gateway to go to its details page.
4. Click the **Route Table** tab.
5. Click **Add a route** and configure routing policies.

Configuration Item	Description
Destination	Enter the IP range of the network to access.
Next hop type	Select **VPN tunnel** or **CCN**. **Note：** if the VPN gateway for CCN is associates with a CCN instance, the routing policy with CCN as the next hop will be automatically obtained and displayed in the route table. Do not manually configure it.
Next hop	Select the instance ID of the next hop. If you select VPN tunnel for the Next hop type, select a VPN tunnel that has been created. If you select CCN for the Next hop type, the CCN instance associated with the VPN gateway will be automatically displayed.
Weight	Choose the weighted values of VPN tunnels: 0: high priority 100: low priority
Add a line	Configure multiple routing policies as needed.

Delete	Delete the routing policies, except for the last one.

6. Click **OK**.

7. Perform other operations as needed.

7.1 Enable or disable routing policies.

7.2 Delete the disabled routing policies.

Associating a CCN Instance

Last updated：2024-01-09 14:29:29

If you are creating a CCN-based VPN gateway, you need to associate the created VPN gateway to a CCN instance on the gateway details page.

Prerequisites

You've created a CCN-based IPsec VPN gateway, as instructed in Creating VPN Gateways

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click the ID of the target VPN gateway to go to the details page.
4. On the **Basic Information** tab of the gateway details page, click the edit icon on the right side of **Network**, and then select the CCN instance to be associated with and the routing table in the pop-up dialog box.
5. Click **Save**.

Publishing IDC IP Ranges to CCN

Last updated：2024-01-09 14:29:29

This document describes how to publish the IP range to CCN for connecting the VPN to the CCN.

Note:

If the communication mode of the VPN tunnel is "destination route", then you don't need to publish the IDC IP range to the CCN.

Prerequisites

You have created a CCN-based IPsec VPN gateway as instructed in Creating VPN Gateways and bound it to a CCN instance as instructed in Associating a CCN Instance.

You've configured a SPD policy for the VPN tunnel. For more information, see Creating VPN Tunnel

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click the ID of the target VPN gateway to go to the details page.
4. Public the IP range to the CCN in the **Publish IP Range** tab.

The IP range here is the IP range of the customer gateway in configuring the SPD policy for the VPN tunnel.

Modifying IPSec VPN Gateways

Last updated：2024-01-09 14:29:29

After a VPN gateway is created, the VPN gateway name, tag and bandwidth cap can be modified.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Modify the gateway name on the **VPN Gateway** page.

Click the “Edit” icon next to the VPN gateway name to modify the name.

You can also modify the gateway name on the details page. Click the gateway ID and then click **Modify**.

4. Modify the bandwidth cap.

Note:

The fee varies based on the bandwidth cap. Evaluate the cost before you adjust the bandwidth cap.

The adjustment of VPN gateway bandwidth is limited to [5,100] Mbps and [200,1000] Mbps.

Pay-as-you-go

Method I: In the VPN gateway instance list, find the instance that you want to upgrade. Click the Edit icon in the **Bandwidth Cap** column and select the desired bandwidth.

Method II: Go to the instance details page, click the Edit icon next to **Bandwidth Cap** and select the desired bandwidth.

5. To modify tags, click **Edit tags** on the gateway list page or click the Edit icon on the gateway details page.

Deleting IPSec VPN Gateway

Last updated：2024-01-09 14:29:29

You can delete VPN gateways that are no longer used.

Prerequisites

The associated VPN tunnels have been deleted. For detailed directions, see Deleting VPN Tunnel.

The associated customer gateways have been deleted. For detailed directions, see Deleting Customer Gateways.

Directions

1. Log in to the VPC console.
2. Select **VPN Connection** > **VPN Gateway** on the left sidebar to access the **VPN Gateway** page.
3. Locate the VPN to be deleted, click **Delete** under the **Operation** column, and click **Delete** in the pop-up.

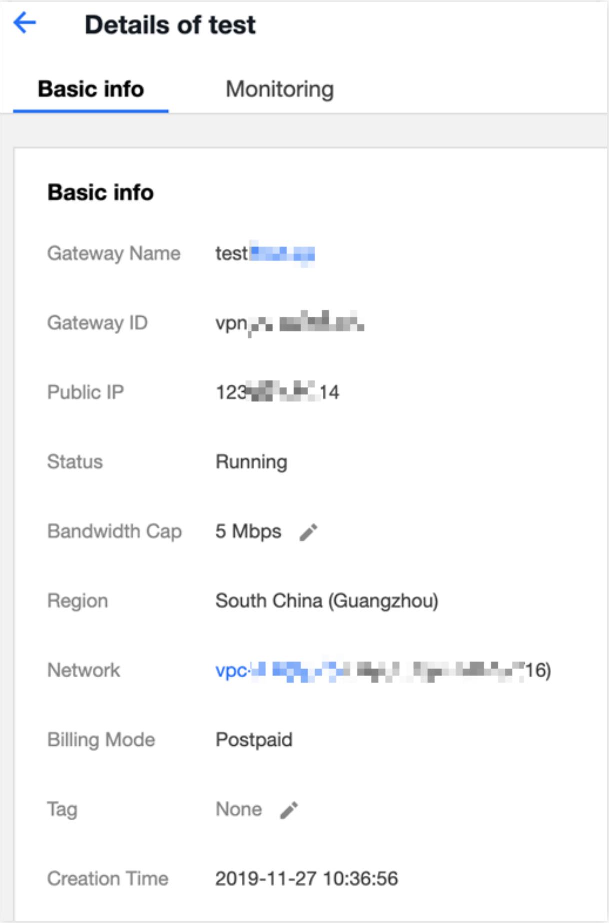
Note:

Note that all the associated connections will be immediately interrupted after the VPN gateway is deleted.

Viewing IPSec VPN Gateway

Last updated：2024-01-09 14:29:29

1. Log in to VPC Console.
2. In the left sidebar, choose **VPN Connection** > **VPN Gateway** to go to the management page.
3. Click the ID of the target VPN gateway to go to the details page.
4. View the details of the VPN gateway.



Basic info

Gateway Name	test[redacted]
Gateway ID	vpn[redacted]
Public IP	123[redacted]14
Status	Running
Bandwidth Cap	5 Mbps
Region	South China (Guangzhou)
Network	vpc[redacted]16)
Billing Mode	Postpaid
Tag	None
Creation Time	2019-11-27 10:36:56

SSL VPN Gateway

Creating an SSL VPN Gateway

Last updated：2024-01-09 14:29:29

An SSL VPN gateway works as the egress of an SSL VPN connection on the VPC side. It helps establish the secure and reliable encrypted network communication between Tencent Cloud VPC and mobile clients.

Prerequisites

You've created a VPC. See Creating VPCs.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click **+New**.
4. Configure the following gateway parameters in the pop-up window.

Parameter	Configuration
Gateway name	Enter the VPN gateway name (up to 60 characters)
Region	Display the region of the VPN gateway
AZ	Select the availability zone of the current gateway
Protocol Type	IPSec and SSL protocols are supported.
Bandwidth cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Associated Network	This parameter specifies whether you create a CCN-based VPN/VPN gateway or a VPC-based VPN/VPN gateway. If you want to use a VPN connection to enable interconnection with multiple VPCs or other Direct Connect networks, create a CCN-based VPN. **Note：** You cannot associate the CCN-based VPN gateway with a CCN instance during its creation. You can associate a created VPN gateway to a CCN instance in the gateway details page. If you create a policy-based VPN tunnel, you also need to enable the route published to the CCN in the IDC IP range of the VPN gateway.

	If you want to communicate with a single VPC by using a VPN connection, create a VPC-based VPN.
Network	If you set Associated Network to VPC, you must select the VPC that you want to associate with the VPN gateway.After you create a gateway for a CCN instance, you must associate the created gateway with the CCN instance on the details page. For more information, see Associating a CCN instance.
SSL VPN Connections	If you select SSL for Protocol type, you must configure this parameter. The number of supported VPN connections vary based on the gateway. For more information, see Use Limits.
Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.
Billing Mode	The SSL VPN gateway supports only the pay-as-you-go billing mode.

5. Click **Create**.

Associating a CCN Instance

Last updated：2024-01-09 14:29:29

If you are creating a CCN-based VPN gateway, you need to associate the created VPN gateway to a CCN instance on the details page of the gateway.

Prerequisites

You have created a CCN-based IPsec VPN gateway.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click the ID of the target VPN gateway to go to the details page.
4. On the **Basic Information** tab of the gateway details page, click the edit icon on the right side of **Network**, and then select the CCN instance to be associated with and the routing table in the pop-up dialog box.
5. Click **Save**.

Modifying SSL VPN Gateways

Last updated：2024-01-09 14:29:29

You can modify the name, tag, and bandwidth cap of a created SSL VPN gateway.

Directions

1. Log in to the VPC console.
2. Select **VPN Connections** > **VPN Gateway** in the left sidebar to enter the admin page.
3. Modify the name of the gateway on the **VPN Gateway** page.

You can modify the gateway name in the editing interface. Click the edit icon next to the name of VPN gateway using the **SSL** protocol.

You can also modify the gateway name on the details page. Click the gateway ID and then click **Modify**.

4. Modify the bandwidth cap.

Note:

Modifying the bandwidth cap will change the fee to charge. Please evaluate the fee before the adjustment.

The adjustment of the VPN gateway bandwidth is limited to [5,100] Mbps and [200,1000] Mbps.

The bandwidth 1000 Mbps can not be downgraded.

Method I: In the VPN gateway instance list, find the instance whose bandwidth cap you want to modify. Click the edit icon in the **Bandwidth cap** column and select the bandwidth that you want.

Method II: Go to the instance details page, click the edit icon next to **Bandwidth cap** and select the bandwidth that you want.

Deleting SSL VPN Gateways

Last updated：2024-01-09 14:29:29

You can delete SSL VPN gateways that are no longer used.

Prerequisites

The SSL VPN servers mounted to the gateways have been deleted. For directions, see Deleting SSL VPN Server.
The SSL VPN clients mounted to the gateways have been deleted. For directions, see Deleting SSL VPN Client.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Find the target SSL VPN gateway, then click **Delete** in the operation column, and click **Delete** in the pop-up window.

Note:

Note that all the associated connections will be immediately interrupted after the VPN gateway is deleted.

Viewing SSL VPN Gateways

Last updated：2024-01-09 14:29:29

Viewing VPN Gateways

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory.
 This page shows the SSL VPN gateway ID, name and status, public IP, associated network, bandwidth cap, and other information.
3. Click the ID of the SSL VPN gateway to enter the details page.
4. View details of the SSL VPN gateway.

Setting the Display Columns for VPN Gateway List

To customize the display columns of VPN gateway list, click the settings button next to the search box on the right, select the fields to display, and then click **OK**.

VPN Tunnel

Creating a VPN Tunnel

Last updated：2024-01-09 14:29:29

A VPN tunnel is an encrypted public network tunnel used to transmit data packets in a VPN connection. The VPN tunnel on Tencent Cloud uses the Internet Key Exchange (IKE) protocol to establish a session during IPsec implementation. IKE provides a self-protection mechanism that can securely verify identities, distribute keys, and establish IPsec sessions in insecure networks. This topic describes how to create a VPN tunnel in the console. You can also manage VPN tunnels by using APIs and SDKs. For more information, see API documentation.

The following configuration information is required to create a VPN tunnel:

Basic information

Communication mode

IKE configuration (optional)

IPsec configuration (optional)

Background

Destination route

A routing policy specifies the IP ranges in the IDC that the network to which the VPN gateway belongs can communicate with. After you create a tunnel, you need to configure a routing policy in the route table of the VPN gateway. For more information, see Configuring The Routing Policies From The User To Tencent Cloud.

SPD policies

Note:

An SPD policy consists of a series of SPD rules that are used to specify the IP ranges in a VPC or CCN and the IP ranges in an IDC that can communicate with each other. Each SPD rule contains at least one CIDR block for the local IP range and at least one CIDR block for the peer IP range. A CIDR block for the local IP range and a CIDR block for the peer IP range form a mapping. An SPD rule may involve multiple **mappings**.

VPN Gateway will negotiate with the customer gateway according to the **mappings** in sequence. Make sure that your customer gateway device supports mapping-based negotiation; for example, it is supported if the `also` keyword is used in `StrongSwan` configuration.

All SPD rules under the same VPN gateway can form up to **200** mappings. If you need more, we recommend you use **Route-Based VPN Connections**.

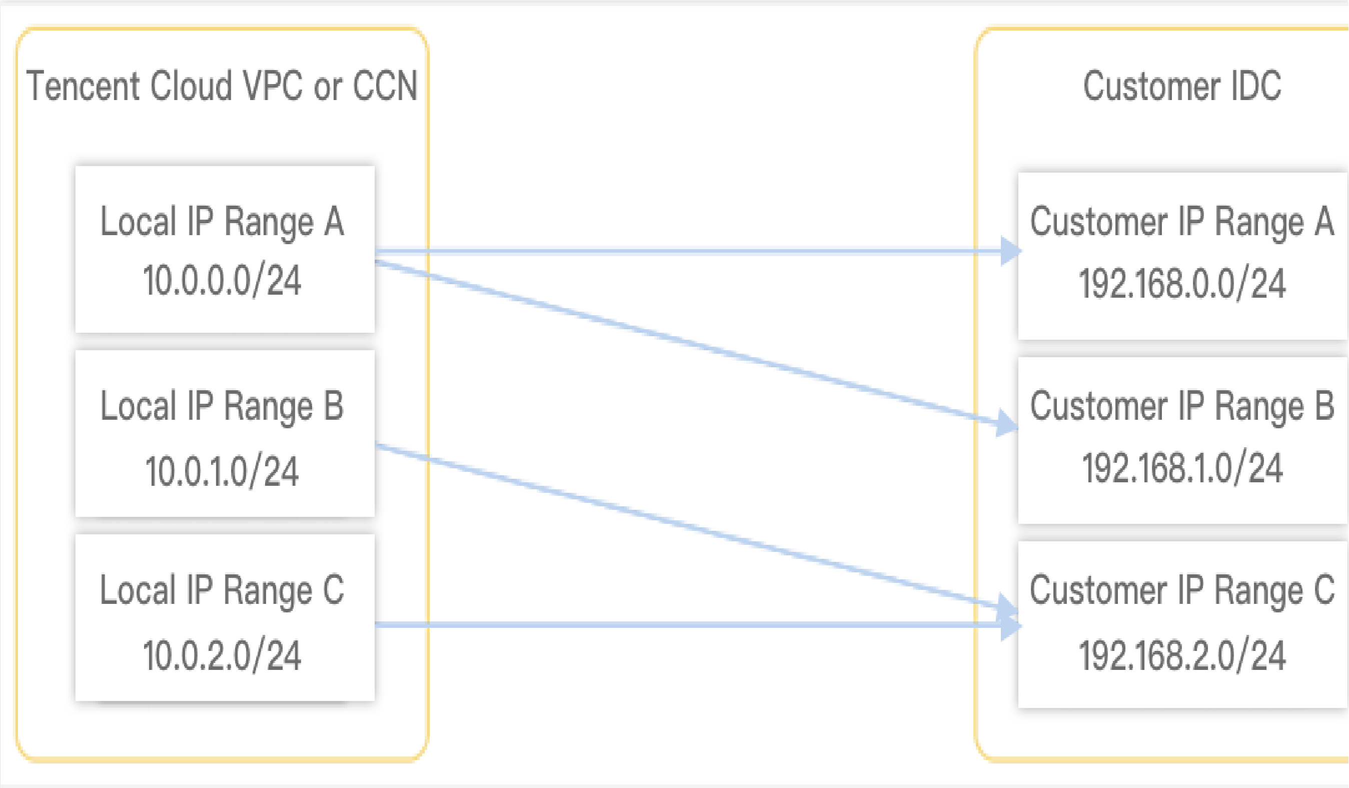
The rules for all tunnels of the same VPN gateway cannot contain overlapped mappings. In other words, the local IP range and customer IP range in a mapping cannot have a duplicate address range.

We recommend you configure a matching rule in the SPD policies in Tencent Cloud and customer gateway. For example, if the local IP range `10.11.12.0/24` and peer IP range `192.168.1.0/24` are configured in the SPD policy in Tencent Cloud, set the local and peer IP ranges also to `192.168.1.0/24` and `10.11.12.0/24` respectively in the SPD policy in your customer gateway.

After an SPD policy is configured, the VPN gateway will automatically distribute the routes, eliminating your need to add routes in the VPN gateway.

Example:

As shown in the figure below, a VPN gateway has the following SPD rules:



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` . In this rule, two mappings are available.

SPD rule 2: The local IP range is `10.0.1.0/24` , and the peer IP range is `192.168.2.0/24` . In this rule, one mapping is available.

SPD rule 3: The local IP range is `10.0.1.0/24` , and the peer IP range is `192.168.2.0/24` . In this rule, one mapping is available.

The mappings are as follows:

`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`

The four mappings cannot overlap. In other words, the local IP range and peer IP range in a mapping cannot have a

duplicate address range.
A new mapping `10.0.0.0/24` ----- `192.168.1.0/24` cannot be added to SPD rules because it overlaps with an existing mapping.
A new mapping `10.0.1.0/24` ----- `192.168.1.0/24` can be added to SPD rules because it does not overlap with existing mappings.

Prerequisites

You have created a VPN gateway on Tencent Cloud as instructed in VPN Connections and created a customer gateway as instructed in Creating Customer Gateways.
Make sure that the number of created VPN tunnels doesn't exceed the quota. You can adjust the quota as instructed in Use Limits.

Directions

1. Log in to the VPC console.
2. Choose **VPN Connection** > **VPN Tunnel** in the left sidebar.
3. On the **VPN Connections** page, click **Create**.
4. Configure the basic information of the VPN tunnel in the pop-up dialog box.

4.1 **Configure basic settings**

In this step, configure the basic information of the tunnel, including the name, network, associated VPN gateway, customer gateway, shared key, negotiation type, and communication mode.

Parameter	Description
Tunnel name	Custom tunnel name with 60 characters at most.
Region	The region of the VPN gateway that is associated with the VPN tunnel to be created.
VPN gateway type	Two types of VPN gateways are available: VPN gateway for VPC and VPN gateway for CCN. For more information about the two types of VPN gateways, see Overview.
VPC	Select the VPC of the VPN gateway only when the **VPN gateway type** is **VPC**. The VPN for CCN doesn't have such a parameter.
VPN gateway	Select a VPN gateway from the list.
Customer gateway	Select a customer gateway that has been created. Otherwise, create one.
Customer	The public IP address of the customer gateway

gateway IP	
Pre-shared key	Used to verify the identities of local and customer gateways that must use the same pre-shared key.
Negotiation type	Traffic-triggered: After the VPN tunnel is created, the negotiation will start when the traffic flows to the local end. Active: After the tunnel is created, the local end actively initiates negotiation with the peer end. Passive: The negotiation is launched by the peer end.
Communication mode	Destination route and SPD policy are supported. We recommend that you use Destination route. For more information about SPD policies, see SPD policies.

4.2 Configure advanced settings

In this step, configure the DPD, health check, IKE, and IPsec options.

Parameter	Description
Enable DPD	DPD is enabled by default and used to check whether the peer is alive or not. If the response of the DPD request message actively sent by the local end is not received within the specified timeout period, it is considered that the peer is offline and timeout action is performed.
DPD timeout period	The overall DPD timeout period. Valid range: 30-60s. The default value is 30s.
DPD timeout action	Disconnect: The current SA is cleared and the current VPN tunnel is disconnected Retry: Reconnect to the peer

4.3 Set health check options

Parameter	Description
Enable health check	Health check is used for primary/secondary tunnels. For more information, see Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery. If your business does not involve primary/secondary tunnels, you do not need to enable this feature (which is disabled by default). Otherwise, complete the health check configuration on the local and peer addresses as instructed in Configuring Health Checks. **Note：** Once you enable health check and create a VPN tunnel, the system immediately performs network quality analysis (NQA) to check the health of the tunnel. If the tunnel is not linked or your configured peer address doesn't respond to NQA detection, the system will consider the tunnel as unhealthy after multiple detection failures and interrupt the business traffic until the tunnel recovers.

VPN gateway IP for health check	This parameter is required only when health check is enabled. You can use the IP address assigned by the system or specify one. **Note：** The specified address cannot conflict with the private network address or IP range of the VPC, CCN, or IDC or the peer address in health check, and it cannot be a multicast, broadcast, or local loopback address.
Customer gateway IP for health check	This parameter is required only when health check is enabled. You can use the IP address assigned by the system or specify one. **Note：：** The specified address cannot conflict with the private network address or IP range of the VPC, CCN, or IDC or the local address in health check, and it cannot be a multicast, broadcast, or local loopback address.

4.4 Configure IKE options

Configuration Item	Description
Version	IKE V1 or IKE V2
Identity verification method	AES-128, AES-192, AES-256, 3DES, DES, and SM4 are supported. We recommend that you use AES-128.
Verification algorithm	The algorithm used to verify identities. MD5, SHA1, SHA256, ASE-383, SHA512, and SM3 are supported. We recommend that you use MD5.
Negotiation mode	Main mode and aggressive mode are supported. In aggressive mode, more information can be sent with fewer packets so that a connection can be quickly established, but the identity of a security gateway is sent in plain text. The configuration parameters, such as Diffie-Hellman and PFS, cannot be negotiated and must have compatible configurations on both sides.
Local ID	IP Address (default) and FQDN (full domain name) are supported.
Customer ID	IP Address (default) and FQDN are supported. Default value: IP Address.
DH group	The DH group used for the IKE key. Key exchange security and the exchange duration increase with the DH group size. DH1: a DH group that uses the 768-bit modular exponential (MODP) algorithm. DH2: a DH group that uses the 1024-bit MODP algorithm. DH5: a DH group that uses the 1536-bit MODP algorithm.

	DH14: a DH group that uses the 2048-bit MODP algorithm. This option is not supported for dynamic VPNs. DH24: a DH group that uses the 2048-bit MODP algorithm with a 256-bit prime order subgroup.
IKE SA lifetime	Unit: s The SA lifetime proposed for IKE security. Before a preset lifetime expires, another SA is negotiated in advance to replace the old one. The old SA is used before a new one is determined through negotiation. The new SA is used immediately after establishment, and the old one is automatically cleared after its lifetime expires.

4.5 (Optional) Configure IPsec options

Configuration Item	Description
Encryption algorithm	AES-128, AES-192, AES-256, 3DES, DES, and SM4 are supported.
Verification algorithm	The algorithm used to verify identities. MD5, SHA1, SHA256, SHA384, SHA512, and SM3 are supported.
Packet encapsulation mode	Tunnel
Security protocol	ESP
PFS	Disable, DH-GROUP1, DH-GROUP2, DH-GROUP5, DH-GROUP14, and DH-GROUP24 are supported.
IPsec SA lifetime(s)	Unit: s.
IPsec SA lifetime (KB)	Unit: KB.

5. Click **Next** to enter the **Communication mode** configuration interface.

Note：

To enter multiple peer IP ranges, separate them with line breaks.

6. Click **Next** to go to the **IKE configuration (optional)** page. Directly click **Next** if no advanced configuration is required.

Configuration Item	Description
Version	IKE V1, IKE V2
Identity verification method	Default pre-shared key

Encryption algorithm	AES-128, AES-192, AES-256, 3DES, DES, and SM4 are supported.
Verification algorithm	The algorithm used to verify identities. MD5, SHA1, SHA256, ASE-383, SHA512, and SM3 are supported.
Negotiation mode	Main mode and aggressive mode supported In aggressive mode, more information can be sent with fewer packets so that a connection can be established quickly, but the identity of a security gateway is sent in plain text. The configuration parameters such as Diffie-Hellman and PFS cannot be negotiated and they must have compatible configurations.
Local ID	IP Address (default) and FQDN (full domain name) are supported.
Customer ID	IP Address (default) and FQDN are supported.
DH group	Used when IKE is specified. The security of key exchange increases as the DH group expands, but the exchange time also becomes longer DH1: DH group that uses the 768-bit modular exponential (MODP) algorithm DH 2: DH group that uses the 1,024-bit MODP algorithm DH5: DH group that uses the 1,536-bit MODP algorithm DH14: DH group that uses the 2,048-bit MODP algorithm. Dynamic VPN is not supported for this option DH 24: DH group that uses the 2,048-bit MODP algorithm with a 256-bit prime order subgroup.
IKE SA lifetime	Unit: s The SA lifetime proposed for IKE security. Before a preset lifetime expires, another SA is negotiated in advance to replace the old one. The old SA is used before a new one is determined through negotiation. The new SA is used immediately after establishment, and the old one is automatically cleared after its lifetime expires.

7. Enter the **IPsec configuration (optional)** interface. Click **Complete** if no advanced configuration is required.

Configuration Item	Description
Encryption algorithm	Supports AES-128, AES-192, AES-256, 3DES, DES, and SM4
Verification algorithm	Used to verify identities, and supports MD5, SHA1, SHA256, SHA384, SHA512, and SM3
Packet encapsulation mode	Tunnel
Security protocol	ESP
PFS	Supports disable, DH-GROUP1, DH-GROUP2, DH-GROUP5, DH-GROUP14, and

	DH-GROUP24
IPsec SA lifetime(s)	Unit: s
IPsec SA lifetime (KB)	Unit: KB

Viewing VPN Tunnels

Last updated：2024-01-09 14:29:29

You can view details of the created VPN tunnels on the VPN tunnel admin page

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** in the left directory to enter the admin page.
3. Click the ID of the VPN tunnel instance to enter the details page.

Configuring Health Checks

Last updated：2024-01-09 14:29:29

Tencent Cloud VPN Connections provides a complete solution to guarantee the high availability of your business. Not only the VPN gateway itself supports a high availability, but also primary/secondary tunnels are supported. The VPN gateway uses health check to identify the tunnel status and triggers the traffic switch between the primary and secondary tunnels based on their status. This document describes how to configure health check.

Note:

We recommend you use a route-based tunnel for health check. If you use an SPD policy-based tunnel, you need to configure an SPD policy for `0.0.0.0/0`.

How Health Check Works

VPN tunnel health check uses the NQA mechanism and the `ping` command by default. In this way, the VPN gateway regularly uses the local address of health check to ping (encrypted in the tunnel) the peer address, so as to determine the connectivity. If the ping fails multiple times in a row, the VPN gateway will consider the tunnel as abnormal and switch the traffic from the primary tunnel to the secondary tunnel. At the same time, the customer gateway also needs to implement a similar mechanism to switch the traffic to the secondary tunnel. To this end, you need to configure two IP addresses that are mutually pingable in the tunnel or adopt such two IP addresses automatically assigned by the system for health check. The IP ranges of the two addresses cannot conflict with those of the VPC and IDC.

Prerequisites

You have created a VPN gateway as instructed in Creating a VPN Gateway and configured the customer gateway as instructed in Creating Customer Gateways. The version of the VPN gateway must be v3.0 or later.

You have created the primary and secondary tunnels.

You have planned health check addresses or use the addresses automatically assigned by the system.

Configuring the Health Checks When Creating VPN Tunnels

This section only introduces the parameters for health checks. For other steps for creating a VPN tunnel, see Creating a VPN Tunnel.

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** in the left sidebar.

3. In the **VPN Connections** page, click **Create**.

4. Configure the basic information in the pop-up dialog box. Then, enable health check and configure the IPs in **Advanced configuration**.

5. The health check configuration takes effect upon the tunnel creation.

Configuring the Health Check After Creating VPN Tunnels

You can also configure health check on the VPN tunnel details page after the tunnel is created.

Note:

Note that your business may be interrupted for a short time.

1. Log in to the VPC console.

2. Click **VPN Connection** > **VPN Tunnel** in the left sidebar.

3. In the **VPN Tunnels** page, locate and click the target VPN tunnel to , and click **Edit** on the **Basic Information** tab.

4. Enable the health check and configure the relevant parameters.

Parameter	Description
VPN gateway IP for health check	It defaults to an IP within the range of `169.254.128.0/17` . You can also specify `0.0.0.0` or an IP within `224.0.0.0` - `239.255.255.255` but outside the VPC IP range.
Customer gateway IP for health check	It defaults to an IP within the range of `169.254.128.0/17` . You can also specify an available on-premises IP.

5. We recommend you select **Destination route** for the communication mode. If **Destination Route** is unavailable, we recommend you enter `0.0.0.0/0` for the local and peer IP ranges in the SPD policy to ensure that the communication between the local and peer health check IPs is encrypted based on the VPN tunnel.

6. Click **Save**.

Generate Peer End Configuration

Last updated：2025-01-10 10:20:06

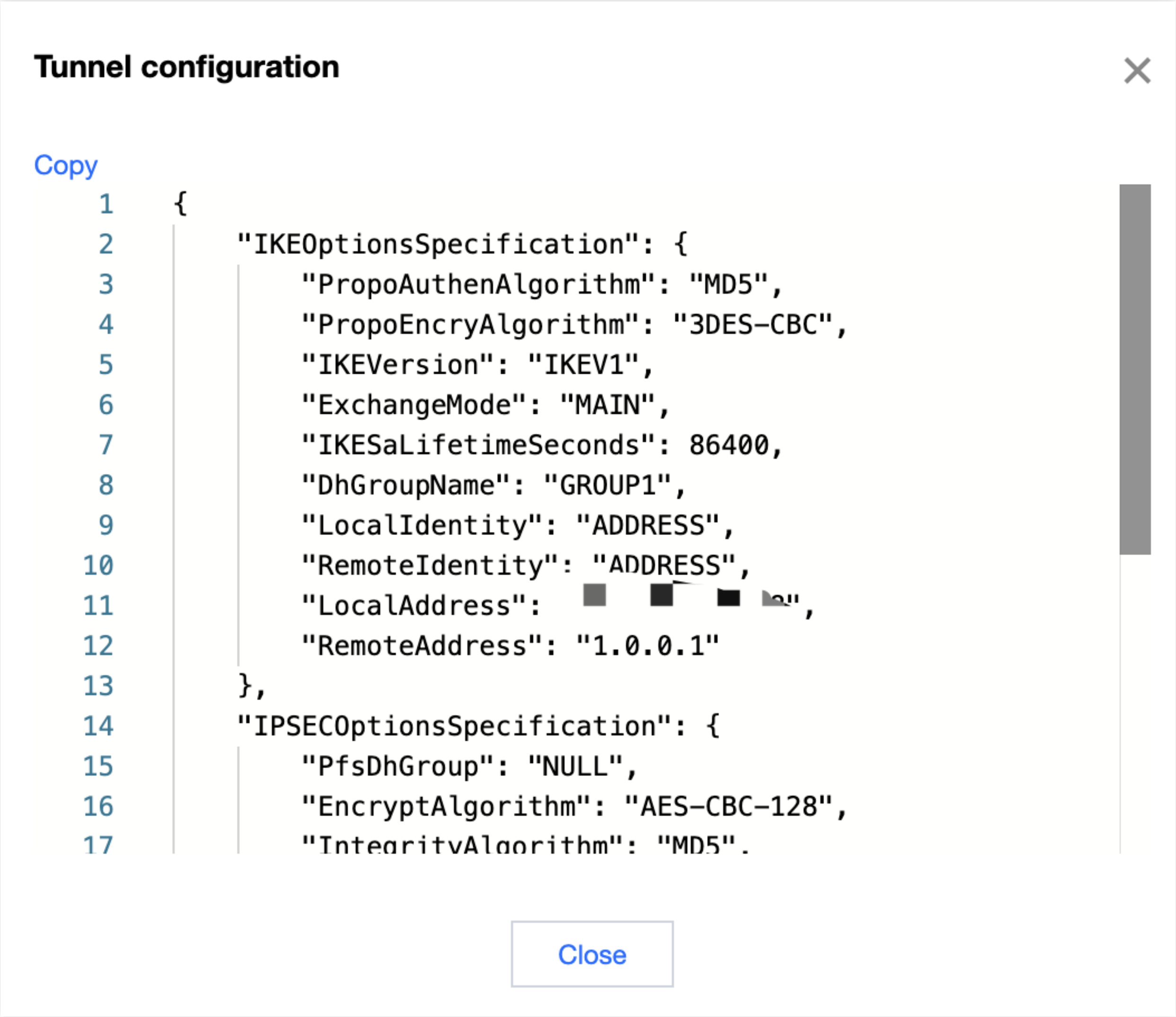
After the local VPN tunnel is configured, you can generate a configuration file for your local VPN setup. After copying the content, you can directly configure your local VPN.

Prerequisites

A VPN tunnel has been created.

Operation Steps

1. log in to the VPN tunnel console and enter the management page.
2. On the "VPN Connections" management page, click **More** on the right side of the tunnel instance and select **Generate Peer configuration.**
3. In the pop-up **Tunnel Configuration** page, copy the configuration content and configure it locally according to your actual situation.



```
{
    "IKEOptionsSpecification": {
        "PropoAuthenAlgorithm": "MD5",
        "PropoEncryAlgorithm": "3DES-CBC",
        "IKEVersion": "IKEV1",
        "ExchangeMode": "MAIN",
        "IKESaLifetimeSeconds": 86400,
        "DhGroupName": "GROUP1",
        "LocalIdentity": "ADDRESS",
        "RemoteIdentity": "ADDRESS",
        "LocalAddress": [redacted],
        "RemoteAddress": "1.0.0.1"
    },
    "IPSECOptionsSpecification": {
        "PfsDhGroup": "NULL",
        "EncryptAlgorithm": "AES-CBC-128",
        "IntegrityAlgorithm": "MD5",
```

Viewing Tunnel Logs

Last updated：2024-01-09 14:29:29

You can query logs on the VPN tunnel management page and troubleshoot failures during the VPN tunnel connection according to the log information.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. On the **VPN Tunnel** management page, click **More** > **Logs** on the right of the tunnel to go to the log retrieval page.
4. You can view the log details in different time frames on the log retrieval page.

Modifying VPN Tunnel

Last updated：2024-01-09 14:29:29

After a VPN tunnel is created, you can modify the basic information of it, such as the tunnel name, pre-shared key, tag information, and SPD policy, as well as advanced configurations such as IKE configuration and IPsec configuration. You can also reset all the configurations of the VPN tunnel.

Impact on the System

The reset operation will interrupt data transmission over the existing VPN tunnel and reestablish the connection. Please get ready for network change in advance.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. On the **VPN Tunnel** page, click the ID of the target VPN tunnel to go to the details page.
4. Click the **Edit** icon on the **Basic Info** page to modify the tunnel name, pre-shared key, tag information and SPD policy rules. Then click **Save**.
You can also modify the tunnel name and pre-shared key by clicking the edit icon on the VPN tunnel list page, as shown in the figure below.
5. Click the **Advanced Configuration** tab to modify the IKE and IPsec configurations, and click **Save**.
6. Please be aware that, by clicking **Reset**, all your custom tunnel configurations will be cleared.

Deleting VPN Tunnel

Last updated：2024-01-09 14:29:29

You can delete VPN tunnels that are no longer used.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. In the **VPN Tunnel** page, click **More** > **Delete** on the right of the target tunnel.
4. Click **Delete** in the confirmation dialog box to delete the VPN tunnel.

Customer Gateway

Creating Customer Gateways

Last updated：2024-01-09 14:29:29

1. Log in to the VPC console.
2. Click **VPN Connection** > **Customer Gateway** on the left sidebar to go to the management page.
3. Choose the region and click **+New** on the “Customer Gateway” management page.
4. Enter the name of the customer gateway and public IP. Public IP refers to the static public IP of the VPN gateway device of the customer IDC. Configure tags according to demand.
5. Click **Create**. A successfully created customer gateway is shown in the picture below.

Viewing Customer Gateways

Last updated：2024-01-09 14:29:29

Follow the directions below to view details of the created customer gateways.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **Customer Gateway** in the left directory to enter the admin page.

Search and view the required customer gateway information, including ID/name, public IP, number of tunnels, etc.

Modifying Customer Gateways

Last updated：2024-01-09 14:29:29

After creating a customer gateway, you can modify the name and descriptions of it.

Operation Directions.

1. Log in to the VPC console.
2. Click **VPN Connection** > **Customer Gateway** on the left sidebar to go to the management page.
3. On the “Customer Gateway” management page, click the “Edit” icon on the right of the gateway name to modify the name, and then click **Save**.
4. Click **Edit Tag** on the right to modify the tag information.

Deleting Customer Gateways

Last updated：2024-01-09 14:29:29

If you do not use the customer gateway anymore and haven’t created any VPN tunnels, you can delete the customer gateway.

Operation Directions.

1. Log in to the VPC console.
2. Choose **VPN Connection** > **Customer Gateway** on the left sidebar to go to the management page.
3. On the “Customer Gateway” management page, click **Delete** on the right of the customer gateway instance to be deleted.
4. Click **Delete** in the confirmation dialog box.

SSL VPN Server

Creating the SSL VPN Server

Last updated：2024-01-09 14:29:29

This document describes how to create an SSL VPN server on Tencent Cloud side to provide SSL services for clients.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Server** in the left directory to enter the admin page.

Note：

One VPN gateway supports only one SSL VPN server. For more information, see Use Limits.

3. Click **+New**.
4. Configure the following parameters in the pop-up window.

Note：

Under Windows systems, if your client OpenVPN is version 3.4.0 or above, the encryption and authentication algorithms need to be configured when configuring the SSL server. The authentication algorithm only supports SHA1.

Parameter	Configuration
Name	Enter the SSL VPN server name (up to 60 characters)
Region	Display the region of the SSL VPN server
VPN gateway	Select an existing VPN gateway
Server IP range	Tencent Cloud IP ranges accessed by mobile clients.
Client IP Range	Enter the IP range assigned to the mobile client for communication. The IP range must not conflict with the VPC CIDR block of Tencent Cloud or your local IP range.
Protocol	Transmission protocol of the server
Port	Enter the SSL VPN server port used for data forwarding
Verification algorithm	Supported authentication algorithms: SHA1 and MD5.
Encryption algorithm	Supported encryption algorithms: AES-128-CBC, AES-192-CBC, and AES-256-CBC.

Compressed	No
Verification method	**Certificate authentication** and **Certificate authentication** + **Identity authentication** are supported. In this example,Certificate authentication is used. Certificate authentication: The SSL VPN server can be accessed by SSL VPN clients. Certificate authentication + Identity authentication: Only connections that comply with the access policies specified in the control policy are allowed. You can configure access policies for a specific user group or all users and select the corresponding Enterprise Identity and Access Management (EIAM) applications for an enabled policy.

5. Click **Create**.

Viewing the SSL VPN Server

Last updated：2024-01-09 14:29:29

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Server** in the left directory.

This page displays the SSL VPN server ID, name and status, VPN gateway, server IP range, client IP range and other information.

3. Click the SSL VPN server ID to enter the details page.

View the basic information and configurations of the target SSL VPN server.

Deleting the SSL VPN Server

Last updated：2024-01-09 14:29:29

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

Prerequisites

The SSL VPN clients associated with the SSL VPN server have been deleted.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Server** in the left directory to enter the admin page.
3. Find the target SSL VPN server, then click **Delete** in the operation column, and click **Delete** in the pop-up window.

Note:

Note that all the associated connections will be immediately interrupted after the SSL VPN server is deleted.

Export SSL server list

Last updated：2024-01-09 14:29:29

This document describes how to Export SSL VPN server list information.

Prerequisites

You've created an SSL VPN server as instructed in Creating the SSL VPN Server.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Server** in the left directory.
3. On the SSL VPN Server admin page, click the Export button next to the search box.

SSO Authentication

Last updated：2024-01-09 14:29:29

If you download the SSL VPN client configuration on the self-service portal, you can enable SSO authentication on the SSL VPN server.

Note:

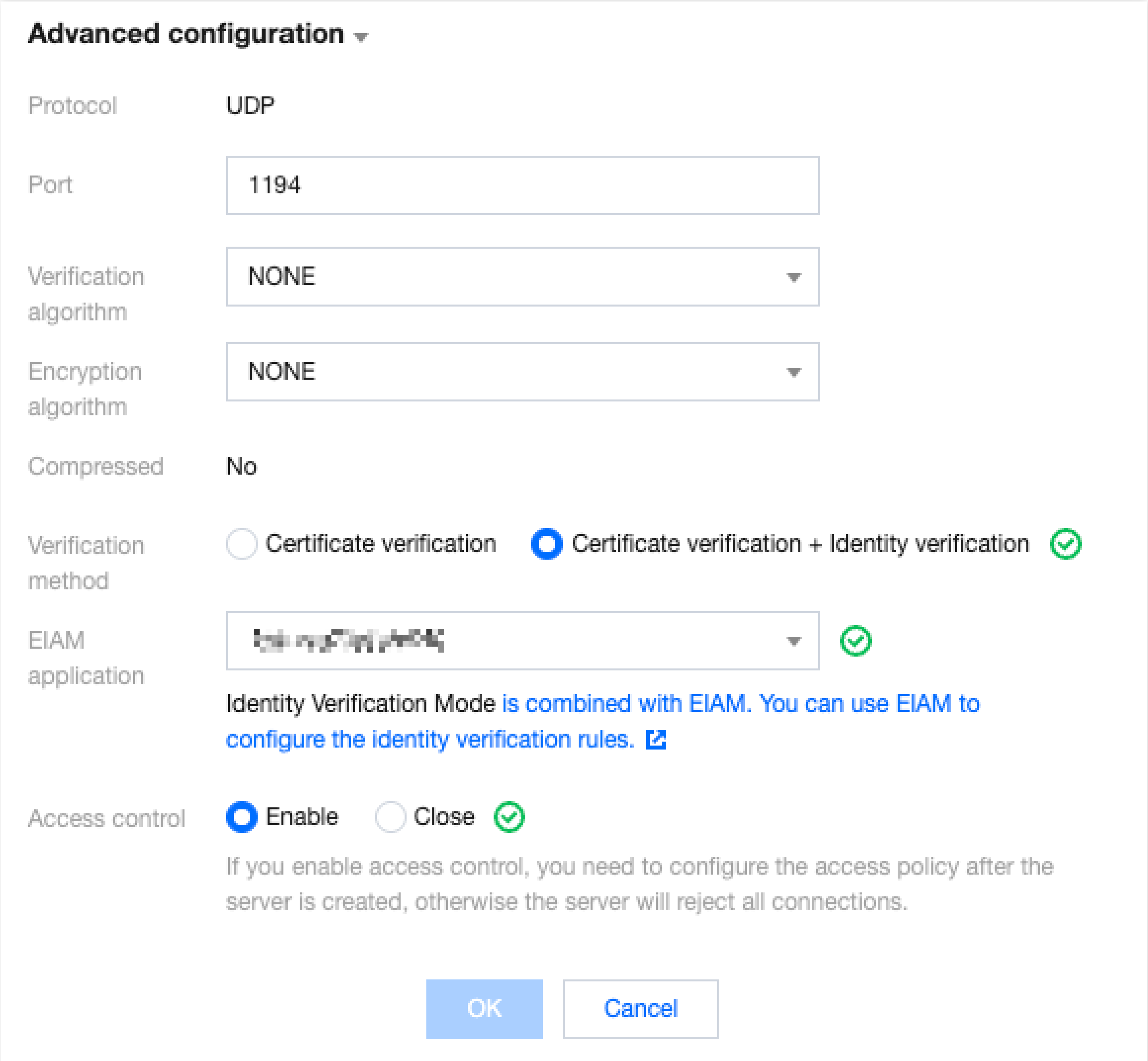
Currently, the SSO authentication feature is in beta test and is available only in Singapore region. To try it out, submit a ticket for application.

Prerequisites

You have created a user group, added a user, and granted the application access permission to the user group in the EIAM console.

Enabling the feature while creating an SSL VPN server

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.
3. Click **Create**.
4. In the **Create an SSL VPN server** pop-up window, select **Certificate verification + Identity verification** for **Verification method** and select your EIAM application.



Advanced configuration

Protocol UDP

Port 1194

Verification algorithm NONE

Encryption algorithm NONE

Compressed No

Verification method ○ Certificate verification ● Certificate verification + Identity verification ✓

EIAM application [redacted] ✓

Identity Verification Mode is combined with EIAM. You can use EIAM to configure the identity verification rules.

Access control ● Enable ○ Close ✓

If you enable access control, you need to configure the access policy after the server is created, otherwise the server will reject all connections.

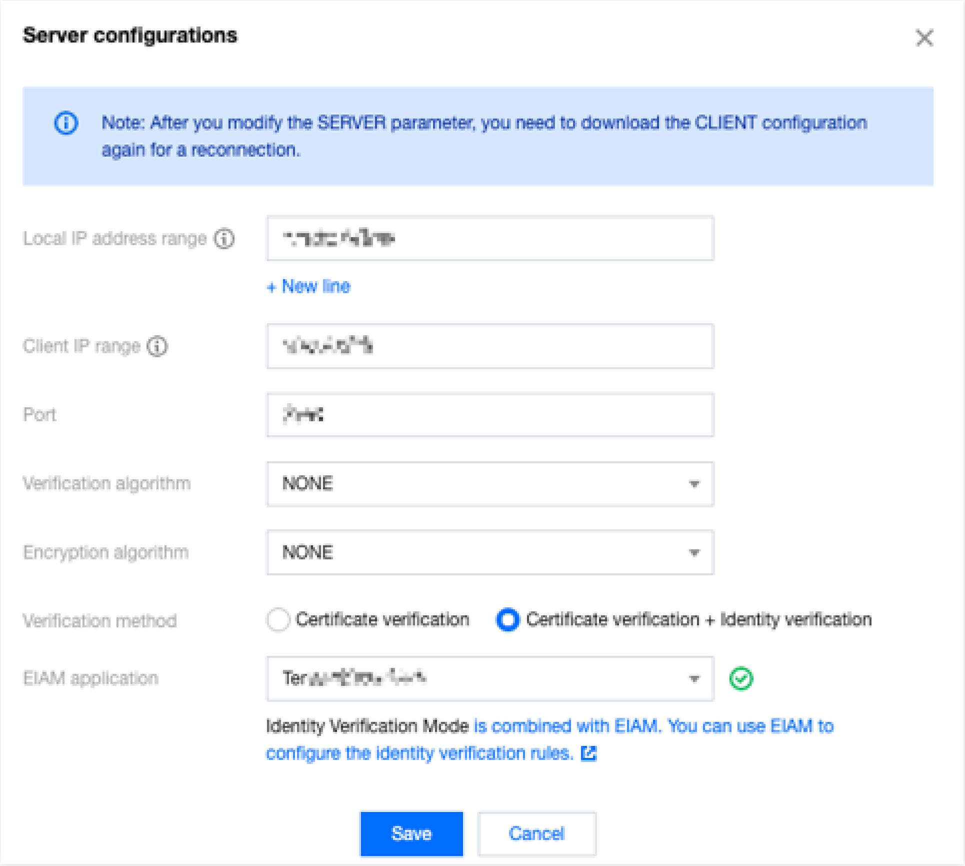
Parameter	Description
Protocol	Transmission protocol of the server
Port	Enter the SSL VPN server port used for data forwarding
Verification algorithm	Supported verification algorithms: SHA1 and MD5.
Encryption algorithm	Supported encryption algorithms: AES-128-CBC, AES-192-CBC, and AES-256-CBC
Compressed	No
Verification method	Certificate verification: In this verification method, the SSL VPN server can be accessed through all SSL VPN client connections by default. Certificate verification + Identity verification: In this verification method, only connections allowed by the access control policy can be established. You can configure the access control policy for specified user groups or all users. After this option is selected, you need to select an EIAM application.
EIAM Application	An application created in the EIAM console, which is used for access control.

Access control	SSL VPN server access control switch

5. You can **enable access control** as needed. For more information, see Enabling Access Control.

Enabling the feature after creating an SSL VPN server

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.
3. Click the name of the target instance.
4. On the instance details page, click **Edit** in the **Server configurations** section on the **Basic information** tab.
5. Select **Certificate verification + Identity verification** for **Verification Method**, select an EIAM application, and click **Save**.



Server configurations

Note: After you modify the SERVER parameter, you need to download the CLIENT configuration again for a reconnection.

Local IP address range: [redacted]

+ New line

Client IP range: [redacted]

Port: [redacted]

Verification algorithm: NONE

Encryption algorithm: NONE

Verification method: ○ Certificate verification ● Certificate verification + Identity verification

EIAM application: [redacted]

Identity Verification Mode is combined with EIAM. You can use EIAM to configure the identity verification rules.

Enabling Access Control

Last updated：2024-01-09 14:29:29

To guarantee your business security, SSL VPN provides the SSL VPN server access control feature to improve your linkage security.

Notes

If you enable access control, you need to configure the access policy after the server is created; otherwise, the server will reject all connections.

If you select **Certificate verification** as the verification method, the SSL VPN server will accept all connections by default.

Note:

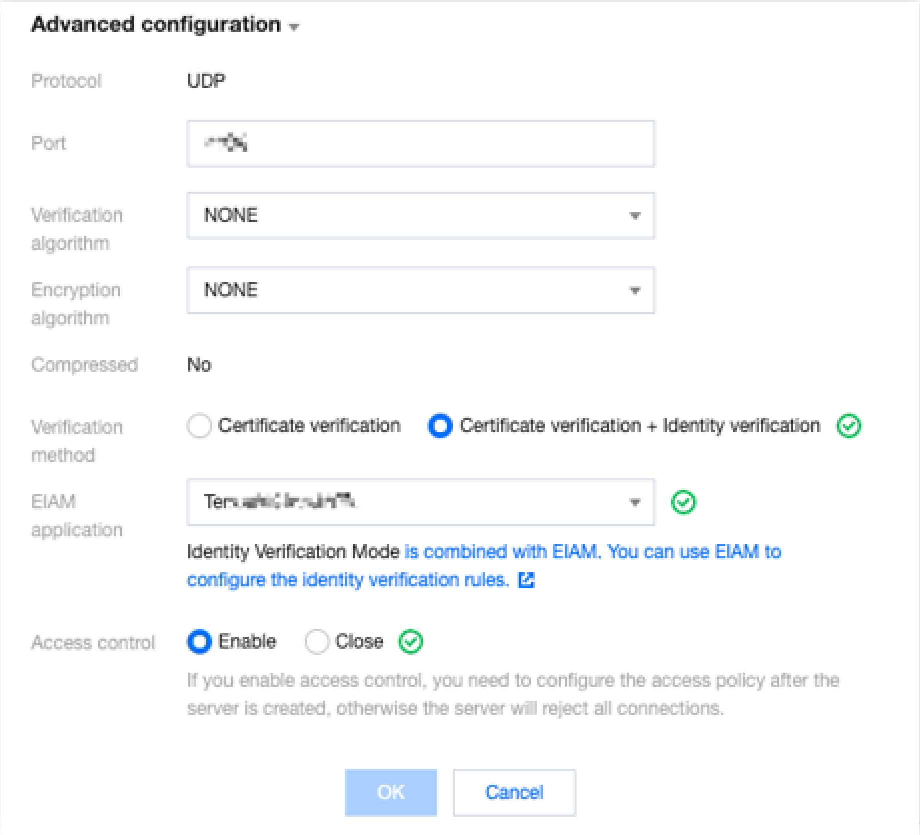
Currently, only SSO authentication-enabled SSL VPN servers support the access control feature. For more information, see SSO Authentication.

Enabling access control while creating an SSL VPN server

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.
3. Click **+New**.
4. In the **Create an SSL VPN server** pop-up window, enable access control and configure relevant parameters while enabling identity verification.

Note:

If you enable access control, you need to configure the access policy after the server is created; otherwise, the server will reject all connections.



Advanced configuration ▾

Protocol UDP

Port [redacted]

Verification algorithm NONE ▾

Encryption algorithm NONE ▾

Compressed No

Verification method ○ Certificate verification ● Certificate verification + Identity verification ✓

EIAM application [redacted] ▾ ✓

Identity Verification Mode is combined with EIAM. You can use EIAM to configure the identity verification rules.

Access control ● Enable ○ Close ✓

If you enable access control, you need to configure the access policy after the server is created, otherwise the server will reject all connections.

Parameter	Description
Verification method	Certificate verification: In this verification method, the SSL VPN server can be accessed through all SSL VPN client connections by default. Certificate verification + Identity verification: In this verification method, only connections allowed by the access control policy can be established. You can configure the access control policy for specified user groups or all users. After this option is selected, you need to select an EIAM application.
EIAM application	An application created in the EIAM console, which is used for access control.
Access control	SSL VPN server access control switch

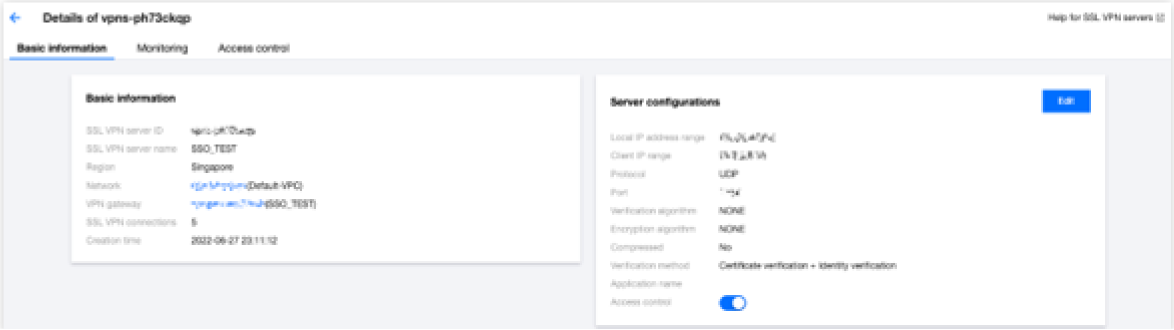
Enabling access control after creating an SSL VPN server

Note:

If you enable access control, you need to configure the access policy after the server is created; otherwise, the server will reject all connections.

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.
3. Click the name of the target instance.

4. On the instance details page, **enable access control** in the **Server configurations** section on the **Basic information** tab.



Details of vpns-ph73ckqp

Basic information

SSL VPN server ID	vpns-ph73ckqp
SSL VPN server name	SSO_TEST
Region	Singapore
Network	[illegible](Default-VPC)
VPN gateway	[illegible](SSO_TEST)
SSL VPN connections	5
Creation time	2022-06-27 23:11:12

Server configurations

Local IP address range	[illegible]
Client IP range	[illegible]
Protocol	UDP
Port	[illegible]
Verification algorithm	NONE
Encryption algorithm	NONE
Compressed	No
Verification method	Certificate verification + Identity verification
Application name	
Access control	●

Disabling Access Control

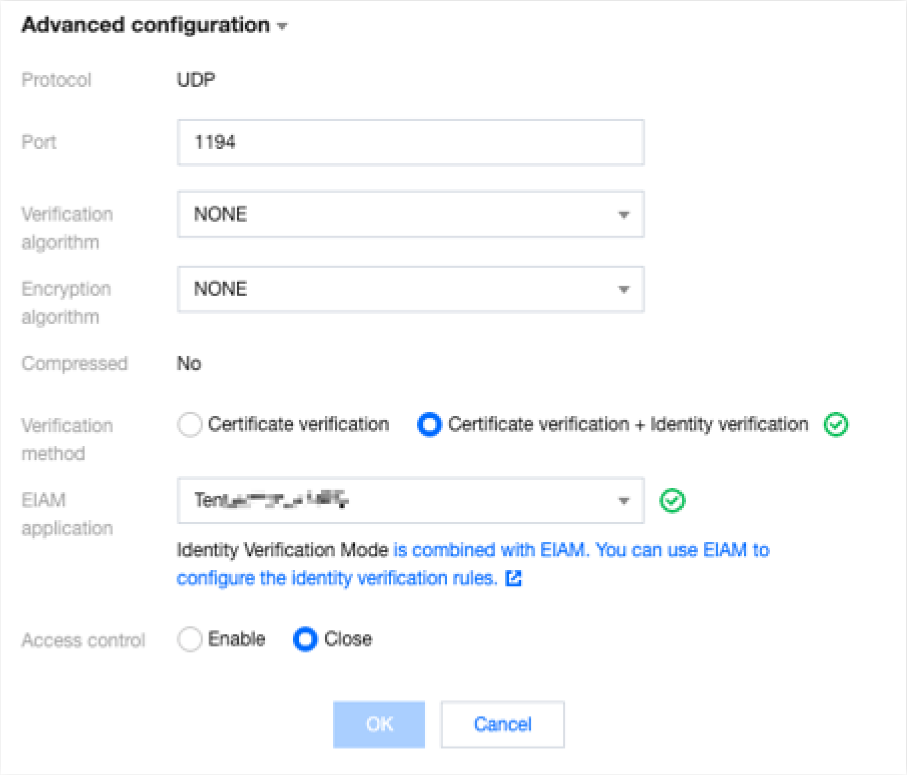
Last updated：2024-01-09 14:29:29

Note:

If you disable access control, all access policies you have configured will be cleared, and the server will accept all connections by default.

Disabling the feature while creating an SSL VPN server

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.
3. Click **+New**.
4. In the **Create an SSL VPN server** pop-up window, **disable access control** and configure other parameters.



Advanced configuration

Protocol	UDP
Port	1194
Verification algorithm	NONE
Encryption algorithm	NONE
Compressed	No
Verification method	○ Certificate verification ● Certificate verification + Identity verification ✓
EIAM application	[redacted] ✓
Access control	○ Enable ● Close

Identity Verification Mode is combined with EIAM. You can use EIAM to configure the identity verification rules.

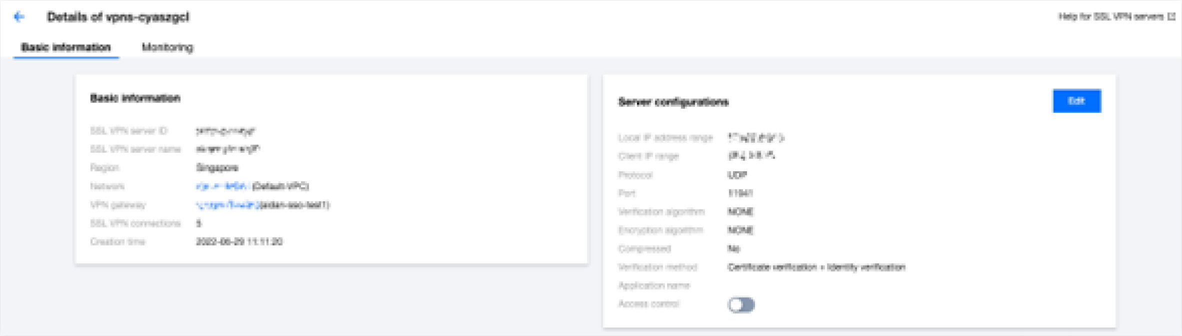
5. Click **OK**.

Disabling the feature after creating an SSL VPN server

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.

3. Click the name of the target instance.

4. On the instance details page, **disable access control** in the **Server configurations** section on the **Basic information** tab.



Details of vpns-cyaszgcl

Basic information

SSL VPN server ID	[illegible]
SSL VPN server name	[illegible]
Region	Singapore
Network	[illegible] (Default-VPC)
VPN gateway	[illegible](aidan-sso-test1)
SSL VPN connections	5
Creation time	2022-06-29 11:11:20

Server configurations

Local IP address range	[illegible]
Client IP range	[illegible]
Protocol	UDP
Port	11941
Verification algorithm	NONE
Encryption algorithm	NONE
Compressed	No
Verification method	Certificate verification + Identity verification
Application name	
Access control	○

5.

Configuring Access Control Policy

Last updated：2024-01-09 14:29:29

To guarantee your business security, SSL VPN provides the SSL VPN server access control feature for you to manage your SSL VPN servers in a fine-grained manner.

Note:

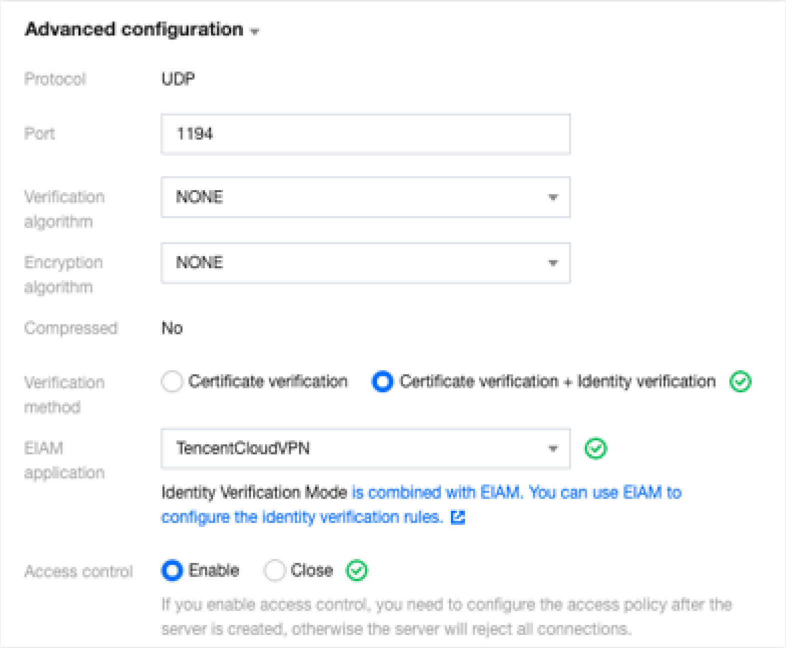
Currently, only SSO authentication-enabled SSL VPN servers support the access control feature. For more information, see SSO Authentication.

Prerequisites

You have created a user group, added a user, and granted the application access permission to the user group in the EIAM console.

You have enabled certificate verification + identity verification and access control for the SSL VPN server in the VPC console.

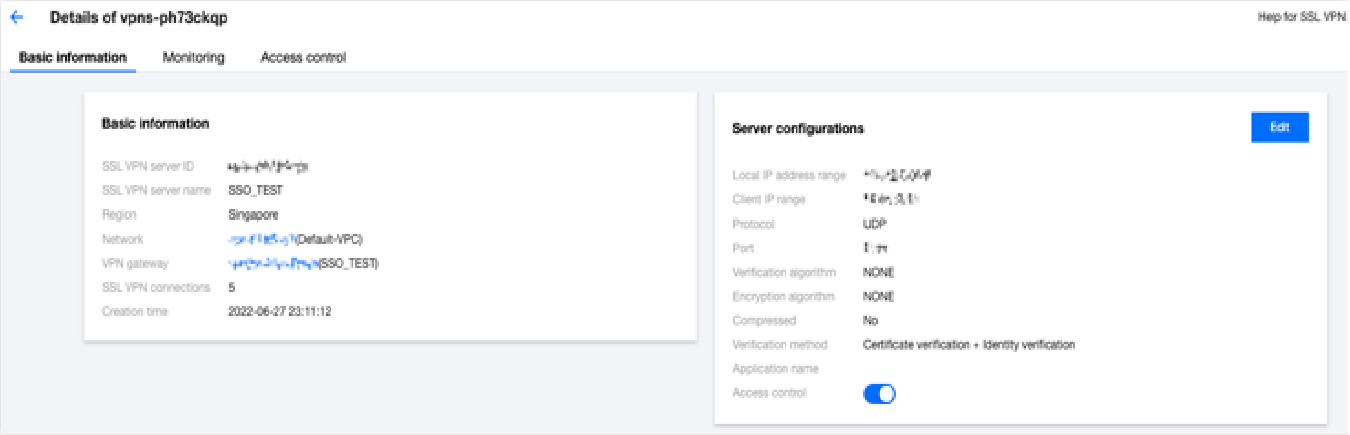
Option 1. Enable the feature while creating an SSL VPN server.



Advanced configuration

Protocol	UDP
Port	1194
Verification algorithm	NONE
Encryption algorithm	NONE
Compressed	No
Verification method	○ Certificate verification ● Certificate verification + Identity verification ✓
EIAM application	TencentCloudVPN ✓ Identity Verification Mode is combined with EIAM. You can use EIAM to configure the identity verification rules.
Access control	● Enable ○ Close ✓ If you enable access control, you need to configure the access policy after the server is created, otherwise the server will reject all connections.

Option 2. Enable the feature after creating an SSL VPN server.



Basic information

SSL VPN server ID	[redacted]
SSL VPN server name	SSO_TEST
Region	Singapore
Network	[redacted](Default-VPC)
VPN gateway	[redacted](SSO_TEST)
SSL VPN connections	5
Creation time	2022-06-27 23:11:12

Server configurations

Local IP address range	[redacted]
Client IP range	[redacted]
Protocol	UDP
Port	[redacted]
Verification algorithm	NONE
Encryption algorithm	NONE
Compressed	No
Verification method	Certificate verification + Identity verification
Application name	
Access control	●

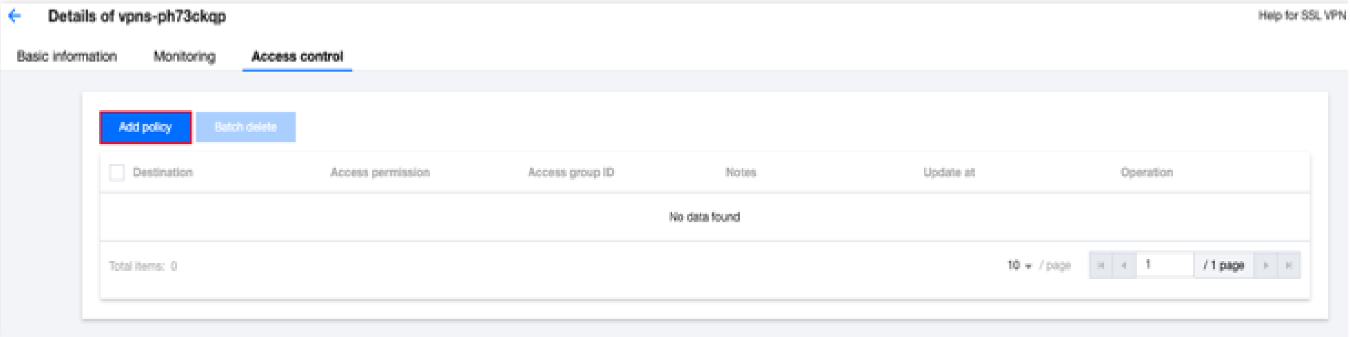
Note:

If you select **Certificate verification** as the verification method, the SSL VPN server can be accessed through all client connections by default, that is, any client can connect to it.

If you enable access control, you need to configure the access policy after the SSL VPN server is created; otherwise, the server will reject all connections.

Configuring an access control policy

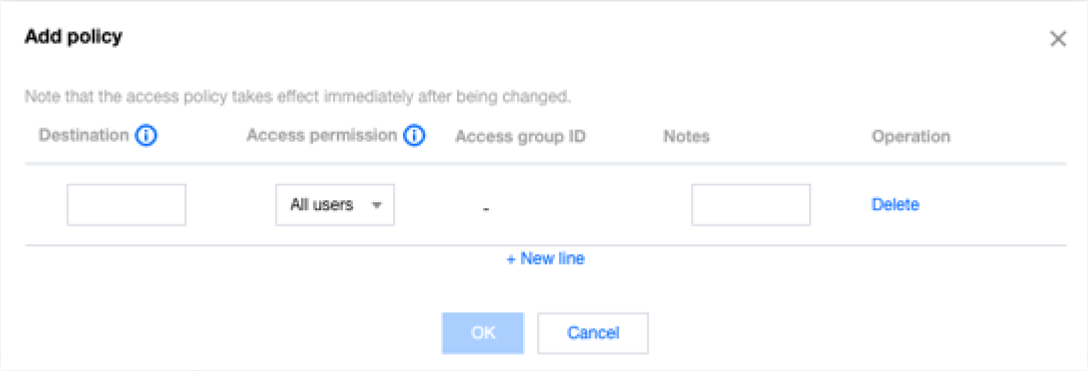
1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.
3. Click the name of the target instance.
4. On the instance details page, click **Access control** > **Add policy**.



□ Destination	Access permission	Access group ID	Notes	Update at	Operation
No data found					

Total items: 0 10 ▾ / page 1 / 1 page

5. In the pop-up window, configure an access control policy.



Add policy

Note that the access policy takes effect immediately after being changed.

Destination ⓘ	Access permission ⓘ	Access group ID	Notes	Operation
	All users ▾	-		Delete

Parameter	Description
Destination	Enter the local IP range, i.e., IP range for accessing the cloud. **Note：** The destination IP range needs to be in the same IP range as the local IP range. If you change the local IP range, you need to modify the destination address of the access control.
Access permission	Specific user group: The access control policy will take effect for the specified user group, and you need to configure the access group ID after selecting this option. All users: The access control policy will take effect for all users. **Note：** You can choose to configure access policies for specific user groups or all users. Specific user groups can be user groups configured on the [identity verification platform](https://console.tencentcloud.com/eiam).
Access group ID	An access group ID is the ID of a user group in the EIAM application. You can select multiple IDs, and then the access control policy will take effect only for the selected user groups.
Notes	Enter the policy remarks, which are required and make it easier for you to find the policy.

6. Click **OK**.

After completing the configuration, the SSL VPN server will accept all connections from users in the user group.

Deleting an access control policy

Note:

After an access control policy is deleted, clients of users in user groups associated with the policy cannot access the SSL VPN server.

If all access control policies are deleted, the SSL VPN server will reject the access requests from all clients by default. If you want the server to be accessible again, you can configure an access control policy or change the verification method to **Certificate verification**.

1. Log in to the VPC console.

2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.

3. Click the name of the target instance and delete the target policy on the **Access control** tab.

Delete multiple policies: Select policies to be deleted in the policy list and click **Batch delete**.

Delete one policy: Click **Delete** in the **Operation** column of the policy to be deleted.

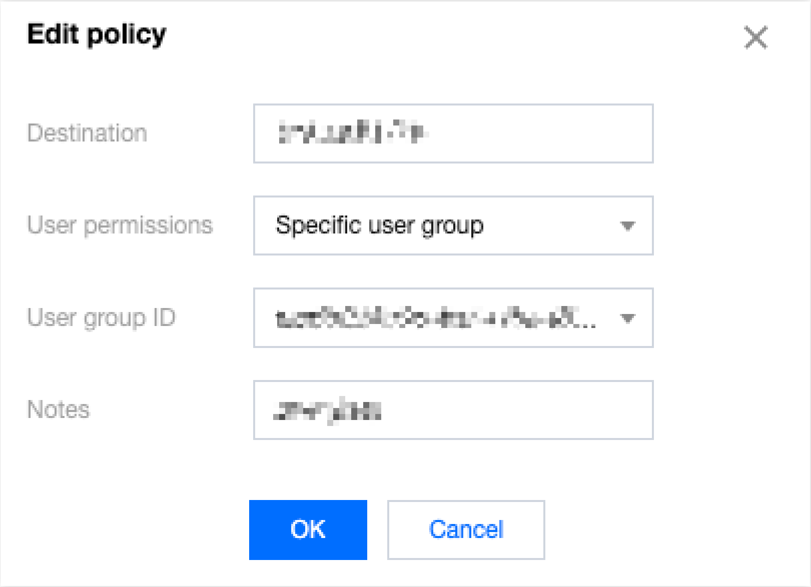
4. In the pop-up window, click **OK**.

Editing an access control policy

1. Log in to the VPC console.

2. Click **VPN Connections** > **SSL VPN server** on the left sidebar to enter the management page.

3. Click the name of the target instance. On the **Access control** tab, click **Edit** in the **Operation** column of the target policy and modify its parameters as needed.



Edit policy

Destination [redacted]

User permissions Specific user group

User group ID [redacted]

Notes [redacted]

4. Click **OK**.

SSL VPN Client

Creating SSL VPN Client

Last updated：2024-01-09 14:29:29

After creating the SSL VPN gateway and server, you need to create an SSL VPN client certificate on Tencent Cloud. This certificate records the information about the SSL certificate assigned by Tencent Cloud to the client, and is used for mutual authentication between the server and the mobile client. You can download the certificate to the mobile terminal and use it to communicate with Tencent Cloud through OpenVPN.

Directions

1. Log in to the VPC console.
2. Click **VPN Connection** > **SSL VPN Client** in the left directory to enter the admin page.
3. Click **New**.
4. Configure the following parameters in the pop-up window.

Parameter	Configuration
Name	Enter the SSL VPN server name (up to 60 characters)
Region	Display the region of the SSL VPN server
SSL VPN Server	Select an existing SSL VPN server.

5. Click **Create** after configuring the SSL VPN client parameters. When the **Certificate Status** becomes **Available**, the creation is completed.

Viewing SSL VPN Client

Last updated：2024-01-09 14:29:29

You can view details of the created SSL VPN client on the SSL VPN client page.

Prerequisites

You’ve created an SSL VPN client. See Creating SSL VPN client.

Viewing SSL VPN Client

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Client** in the left directory.
 This page shows the SSL VPN client ID and name, and the SSL VPN server connected to the client, as well as certificate validity, expiration time and status, etc.
3. Click the SSL VPN server ID to open the details page.

Deleting SSL VPN Client

Last updated：2024-01-09 14:29:29

You can delete the SSL VPN client certificate on the SSL VPN client page.

Prerequisites

You’ve created an SSL VPN server. See Creating SSL VPN server.

You’ve created an SSL VPN client. See Creating SSL VPN client.

Deleting the SSL VPN Client Certificate

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Client** in the left directory to enter the admin page.

Click the SSL VPN server ID to redirect to the corresponding SSL VPN server and view the relevant information.

3. Click **Delete** in the line of the target SSL VPN client certificate.

Note:

Note that all the associated connections will be immediately interrupted after the SSL VPN client certificate is deleted.

Downloading SSL VPN Client Configuration

Last updated：2024-01-09 14:29:29

After successfully creating an SSL VPN client, you can download the client configuration for connecting to the SSL VPN server on the SSL VPN client management page. Two-way authentication will be performed when you use OpenVPN or a compatible VPN client to connect to the SSL VPN server through the downloaded client configuration. To guarantee your communication security, only after two-way authentication is passed can you access Tencent Cloud resources (such as CVM instances in a VPC) associated with the SSL VPN server gateway from the mobile client.

Downloading the SSL VPN Client Configuration as a Tenant Admin

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN client** on the left sidebar.
3. Download the SSL VPN client configuration.

Click **Download the configuration** on the row of the target SSL VPN client certificate instance.
You need to distribute the downloaded configuration file to the user (such as an employee in your company) who needs to connect to Tencent Cloud through SSL VPN. This user must use the file to configure OpenVPN or a compatible VPN client in order to interconnect with the VPC. For detailed directions, see Step 5: Configure the Mobile Client.

Note:

Do not share the configuration file to unauthorized persons. If the configuration file is disclosed, disable the SSL VPN client promptly. For more information, see Managing SSL VPN Client Certificate.

Downloading the SSL VPN Client Configuration on the Self-Service Portal

If identity verification is enabled when you create an SSL VPN server, the mobile client user (such as an employee in your company) can download the configuration file required by OpenVPN or a compatible VPN client on their own. In addition, Tencent Cloud uses an authentication mechanism to guarantee the security throughout the entire download process.

Prerequisites

The tenant admin has created a user group, added a user and granted the application access permission to the user group in the EIAM console.

The tenant admin has created an SSL VPN server supporting identity verification in the VPC console.

The tenant admin has distributed the ID of the SSL VPN server with identity verification enabled to you (as a user). If you don't have the ID, contact your admin to get it.

Directions

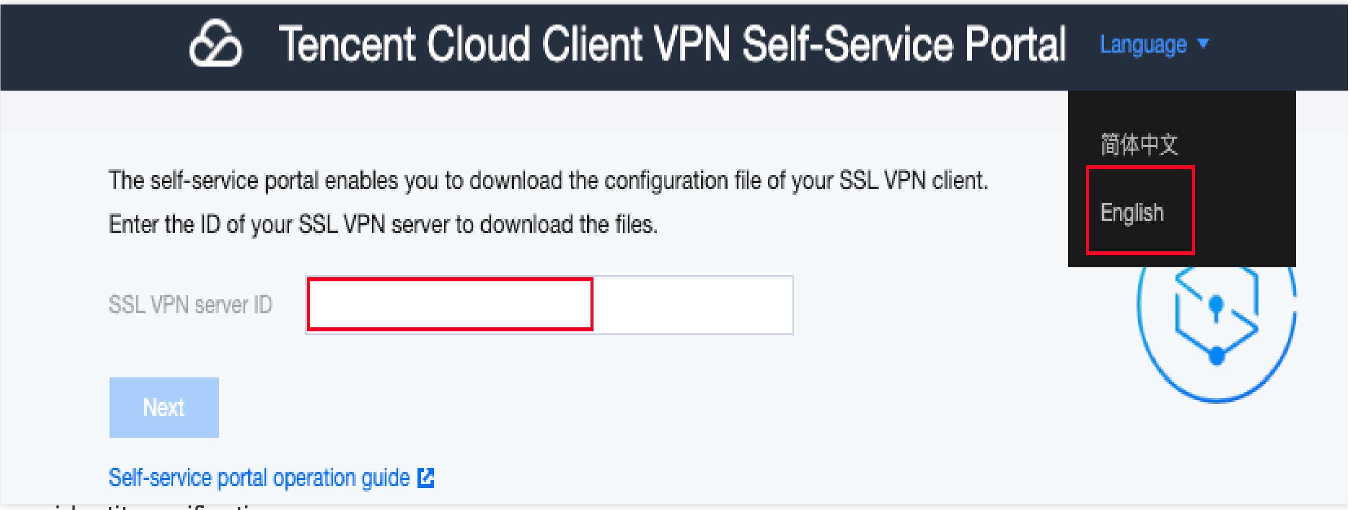
The following steps are performed by a mobile client user (such as an employee of your enterprise) on their own:

1. Log in to the Tencent Cloud Client VPN Self-Service Portal.

Note:

We recommend you use the latest version of Chrome.

2. In the **SSL VPN server ID** input box, enter the ID distributed by the admin and click **Next** to access the login page.



Tencent Cloud Client VPN Self-Service Portal

The self-service portal enables you to download the configuration file of your SSL VPN client. Enter the ID of your SSL VPN server to download the files.

SSL VPN server ID

3. Perform identity verification.

Click

to perform SAML authentication and click **Go to SAML** for login. You need to use the authentication method specified by your tenant admin. For example, if the admin specifies authentication by connecting to your enterprise account system in EIAM, you will see the domain account login page of your enterprise in the browser, and you need to enter your domain account for authentication. If the admin specifies another method such as WeCom, you need to enter the corresponding account for authentication.

Note:

1. Currently, login can be authenticated only through SAML. Make sure that you are in the EIAM user group associated with the SSL VPN access control policy. If "You are not authorized to access this application. Contact the admin." is displayed, you can contact the admin to add you to the EIAM user group.

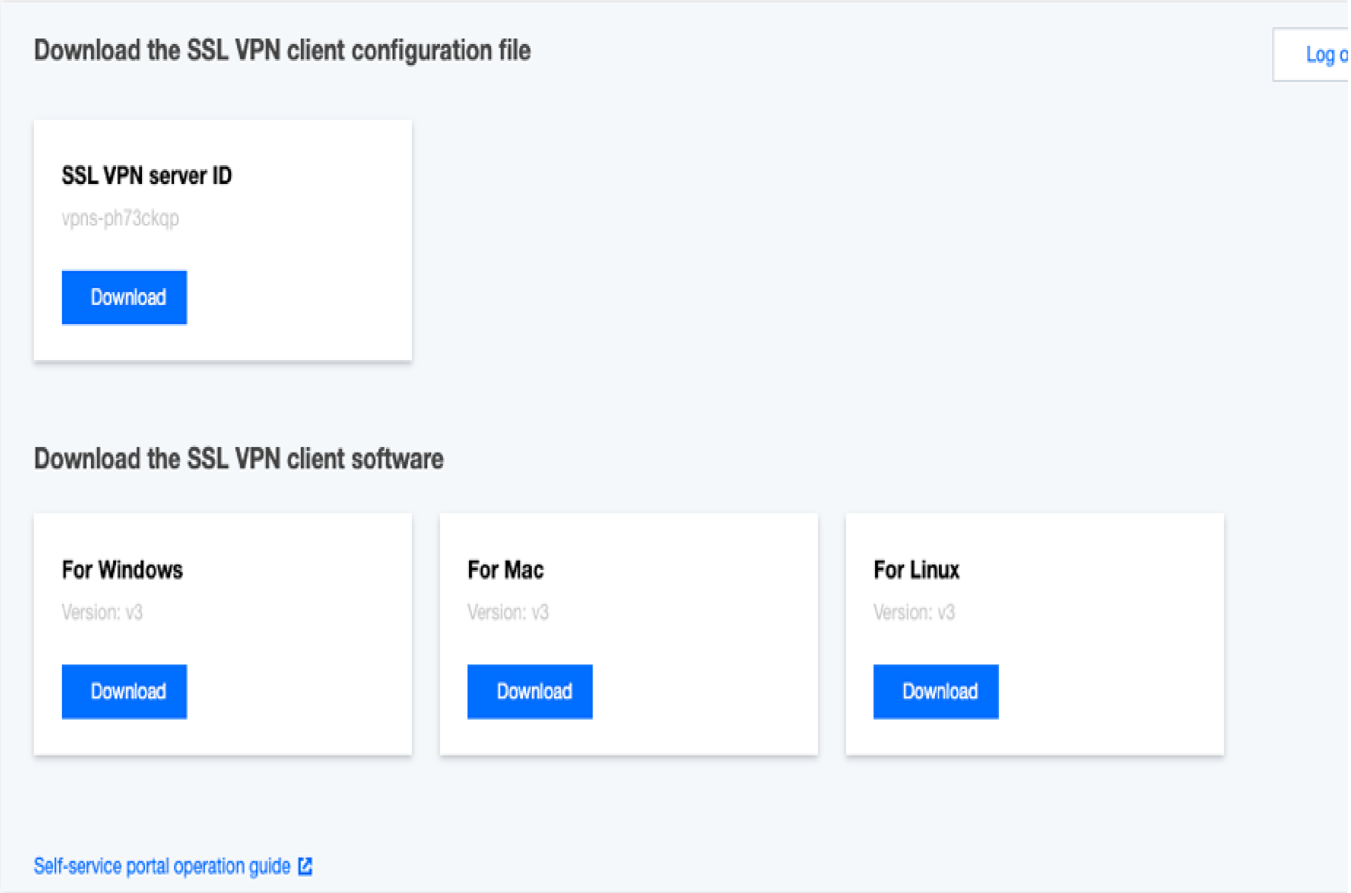
2. If you need to change the EIAM application, make sure that users in the original EIAM application have been moved to the new application for uninterrupted access.

3. After the EIAM application switch, established SSL VPN connections won't be closed.

4. Download the SSL VPN client configuration file and client.

5. In the **Download SSL VPN client configuration file** section, find the target configuration file and click **Download**.

6. In the **Download SSL VPN client** section, download an appropriate SSL VPN client and install it.



Download the SSL VPN client configuration file

SSL VPN server ID

vpns-ph73ckqp

Download the SSL VPN client software

For Windows

Version: v3

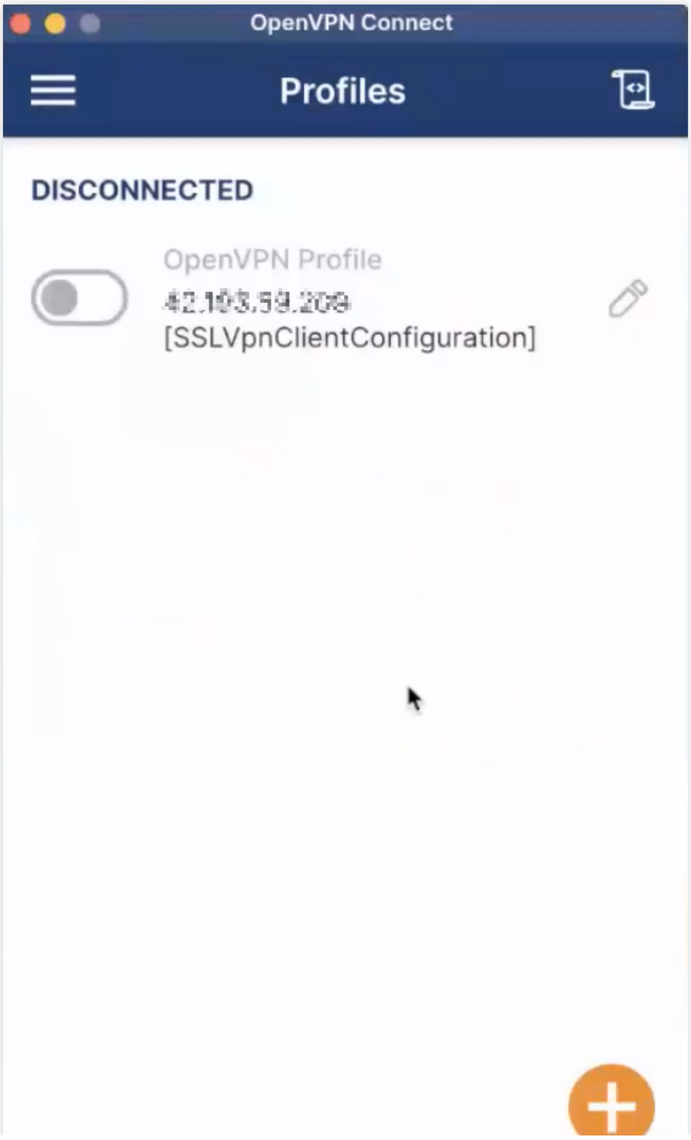
For Mac

Version: v3

For Linux

Version: v3

7. After installing the SSL VPN client, upload the downloaded configuration file. Then, the client will automatically connect to the SSL VPN server.



DISCONNECTED

OpenVPN Profile
[redacted]
[SSLVpnClientConfiguration]

Managing SSL VPN Client Certificate

Last updated：2024-01-09 14:29:29

The SSL VPN client certificate created in the SSL client is enabled by default. You can disable it if needed.

Enabling the SSL VPN Client Certificate

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Client** in the left directory.
3. Enable the target certificate.

Disabling the SSL VPN Client Certificate

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Client** in the left directory.
3. Disable the target certificate.

Binding an Anti-DDoS Instance

Last updated：2022-04-24 15:42:58

1. Log in to Anti-DDoS Pro Console, choose **Resource List**, and select a region.
For single IP instances, select the **Single IP Instance** tab.
For multi-IP instances, select the **Multi-IP Instance** tab.
2. Find the Anti-DDoS Pro instance to be bound in the list, and click **Change Resource** in the **Operation** column for the instance.
3. Select the associated device type and associated device from the pop-up box. Select **VPN Gateway** as the device type and select the VPN gateway you want to associate from the list.
4. Click **OK**.

Alarming and Monitoring

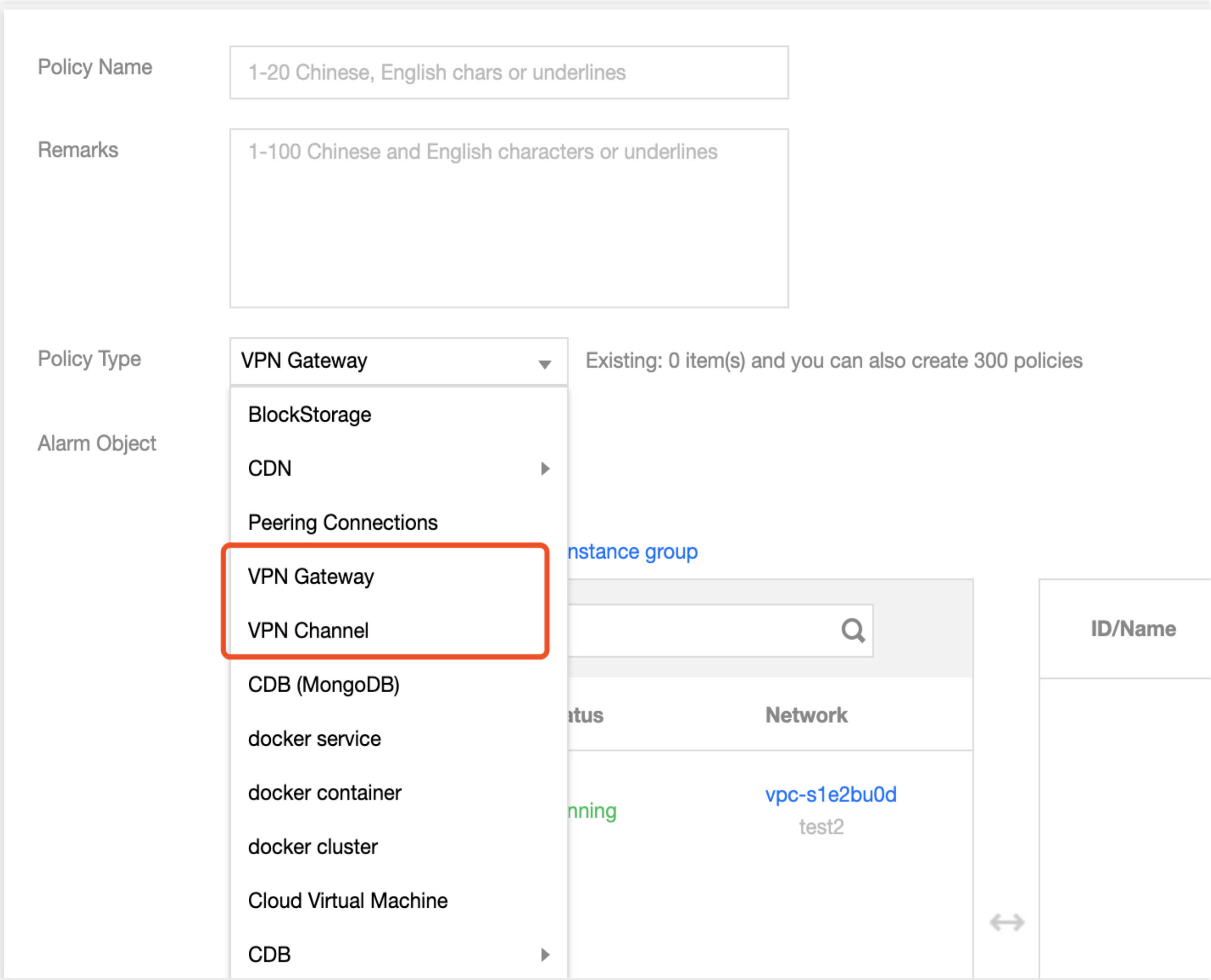
Setting Alarms

Last updated：2024-01-09 14:29:29

You can customize traffic alarms for VPN connections. When a metric value exceeds its threshold, alarm notifications are sent to you automatically via email and SMS. Alarm services are free of charge, helping you quickly locate problems.

Operation Directions

1. Log in to Cloud Monitor Console.
2. On the left sidebar, choose **Alarm Configuration** > **Alarm Policy** to go to the alarm policy configuration page, and then click **Add**.
3. Enter the alarm policy name, choose **VPC** > **VPN Tunnel** for **Policy Type**, select an alarm object, set an alarm policy, select a recipient group and an alarm channel, and click **Complete**. You can view the alarm policy in the alarm policy list.



Policy Name: 1-20 Chinese, English chars or underlines

Remarks: 1-100 Chinese and English characters or underlines

Policy Type: VPN Gateway

Existing: 0 item(s) and you can also create 300 policies

4. View alarm information

When the alarm condition is triggered, you will receive an alarm notification via SMS, email, or WeChat. You can also click **Alarm History** on the left sidebar to find the alarm. For more information about alarms, see Alarm Configuration.

Viewing Monitoring Data

Last updated：2024-01-09 14:29:29

With VPN tunnels and VPN gateways, you can view monitoring data, and quickly locate failures if they occur. The monitoring service is free of additional charges.

VPN Gateway

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Gateway** on the left navigation bar.
3. Select a region and a VPC, and click the monitoring icon of a VPN gateway in the list to view its monitoring data. You can also view the monitoring data on the **Monitoring** tab by clicking the gateway ID.
4. Click **VPN Connection** > **VPN Tunnel** on the left navigation bar.

VPN Tunnel

1. Log in to the VPC console.
2. Click **VPN Connection** > **VPN Tunnel** on the left navigation bar.
3. Select a region and a VPC, and click the monitoring icon of a VPN tunnel in the list to view its monitoring data.

Documentation

VPN Gateway Monitoring Metrics

VPN Tunnel Monitoring Metrics

SSL VPN Configuration Guide

SSL VPN Configuration Guide

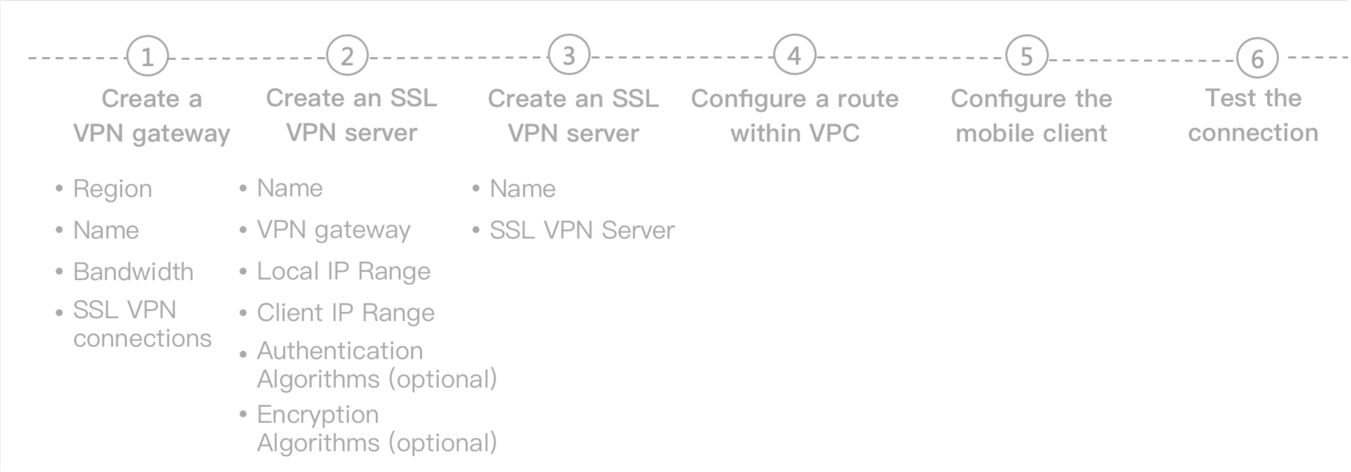
Last updated：2024-01-09 14:29:29

Prerequisites

The local private IP range and the Tencent Cloud VPC cannot overlap.

The client has connected to the public network.

Configuration



1. Create an SSL VPN gateway.

Create a VPN gateway using the SSL protocol

2. Create an SSL VPN server.

Specify the Tencent Cloud IP range and the client IP range to connect in the SSL VPN server.

3. Create an SSL VPN client.

The client uses certificate and key to connect with the VPN gateway. The client and the server verify each other's certificate. After verification, the server assigns an IP from the client IP address pool to the client for connecting with CVMs in VPC.

4. Configure a route within VPC.

Configure the routing and forwarding policies for the mobile client to connect with Tencent Cloud VPC. Set an address of the client IP range as the destination, and VPN tunnel as the next hop type. Next hop to SSL VPN gateway.

5. Configure the client on the mobile device.

Configure the SSL certificate on the mobile device.

6. Test the connectivity

Use `ping` to verify the connectivity of SSL VPN connection after the above configurations.

IPSec VPN Configuration Guide

IPSec VPN Configuration Guidelines

Last updated：2024-01-09 14:29:29

Prerequisite

The local private IP range and the Tencent Cloud VPC cannot overlap.

Configuration

1. Create an IPSec VPN gateway

Create a VPN gateway using the IPSec protocol.

2. Create a customer gateway

Specify the Tencent Cloud IP range and the client IP range to connect in the SSL VPN server.

3. Create a VPN tunnel

The client uses certificate and key to connect with the VPN gateway. The client and the server verify their certificates bidirectionally. After verification, the server assigns an IP from the client IP address pool to the client for connecting with CVM in VPC.

4. Configure a local gateway.

Complete the gateway configuration at the client side.

Note:

Tencent IPSec VPN supports the mainstream client gateway (firewall) in the industry. See Local Gateway Configurations.

5. Configure a route within VPC.

Configure the routing and forwarding policies for the IDC to connect with Tencent Cloud VPC. Set the the IP range of the opposite network as the destination address, and VPN tunnel or CCN as the next hop type.

VPN tunnel: select an existing VPN tunnel

CCN: the CCN instance associated with the VPN gateway is displayed here

6. Test the connectivity

Use `ping` to verify the connectivity of IPSec VPN connection after the above configurations.

Operations Overview

Last updated：2024-01-09 14:29:29

Through an encrypted public network channel, a VPN connection can facilitate the safe communication between the user IDC and internal office network and Tencent Cloud Virtual Private Cloud (VPC). A VPN gateway provides IPsec VPN connections. You can configure and manage VPN connections, such as viewing monitoring data, modifying VPN tunnels and binding anti-DDoS products, on the VPN console. This document provides the console operation guides of VPN connections.