ALIBABA CLOUD

Alibaba Cloud

VPN Gateway

Best Practices

Document Version: 20220624

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

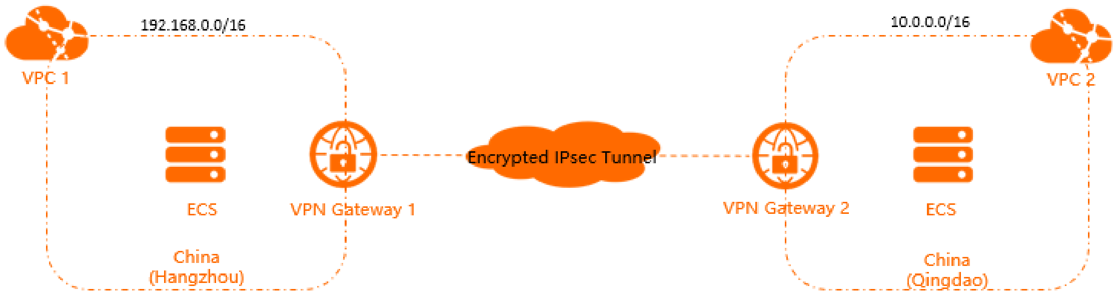
1.Establish IPsec-VPN connections between two VPCs

This topic describes how to use IPsec-VPN to establish a secure connection between two virtual private clouds (VPCs). This way, the cloud resources in one VPC can access the cloud resources in the other VPC.

Scenarios

An enterprise created a VPC named VPC 1 in the China (Hangzhou) region and created a VPC named VPC 2 in the China (Qingdao) region. Elastic Compute Service (ECS) instances are deployed in the VPCs, and services are deployed on the ECS instances. Due to business development, the services in VPC 1 and VPC 2 need to communicate with each other.

To ensure network security, the enterprise decides to use VPN gateways to establish an IPsec-VPN connection between VPC 1 and VPC 2. This way, data transmission between the VPCs is encrypted and the cloud resources can communicate with each other in a secure manner.



Prerequisites

- A VPC named VPC 1 is created in the China (Hangzhou) region, and a VPC named VPC 2 is created in the China (Qingdao) region. ECS instances are deployed in the VPCs, and services are deployed on the ECS instances.

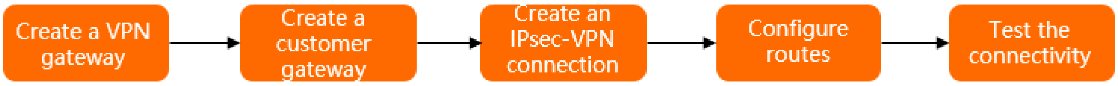
  The following table describes the configurations of VPC 1 and VPC 2 in this example.

  > **Note** You can specify the CIDR blocks based on your business requirements. Make sure that the CIDR blocks that need to communicate do not overlap.

VPC name	Region	VPC CIDR block	VPC ID	Name of ECS instance	IP address of ECS instance
VPC1	China (Hangzhou)	192.168.0.0/16	vpc-bp1e0yx3nsosmitth****	ECS1	192.168.20.161
VPC2	China (Qingdao)	10.0.0.0/16	vpc-m5e83sapxp88cgp5f****	ECS2	10.0.1.110

- You are aware of the security group rules that are applied to the ECS instances in the VPCs. Make sure that the security group rules allow the ECS instances to communicate with each other.

Procedure



Step 1: Create a VPN gateway

1.
2. In the top navigation bar, select the region where you want to create the VPN gateway.

   In this example, the **China (Hangzhou)** region is selected.

   > **Note** The VPN gateway must belong to the same region as the VPC that you want to associate with the VPN gateway.

3.
4. On the buy page, set the following parameters, click **Buy Now**, and then complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway. In this example, *VPN Gateway 1* is entered.
Region	Select the region where you want to deploy the VPN gateway. In this example, the **China (Hangzhou)** region is selected.
VPC	Select the VPC with which you want to associate the VPN gateway. In this example, VPC 1 is selected.
Specify VSwitch	Specify whether to deploy the VPN gateway in a specified vSwitch of the VPC. In this example, **No** is selected.
Maximum Bandwidth	Specify a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
Traffic	Select a metering method for the VPN gateway. Default value: **Pay-by-data-transfer**. For more information, see Pay-as-you-go.
IPsec-VPN	Specify whether to enable IPsec-VPN. In this example, **Enable** is selected.
SSL-VPN	Specify whether to enable SSL-VPN. In this example, **Disable** is selected.
Duration	Specify the billing cycle. Default value: **By Hour**.

Parameter	Description
Service-linked Role	Click **Create Service-linked Role** and the system automatically creates the service-linked role AliyunServiceRoleForVpn. For more information about how a VPN gateway assumes the role to access other cloud resources, see AliyunServiceRoleForVpn. If **Created** is displayed, the service-linked role is created and you do not need to create it again.

For more information, see 创建和管理VPN网关实例.

5. Return to the **VPN Gateways** page to view the VPN gateway.

   After you create a VPN gateway, it is in the **Preparing** state. After 1 to 5 minutes, the VPN gateway changes to the **Normal** state. After the VPN gateway changes to the **Normal** state, the VPN gateway is ready for use.

6. Repeat Substep 2 to Substep of Step 1 to create a VPN gateway named *VPN Gateway 2* in the **China (Qingdao)** region. Specify VPC 2 for the VPC parameter. Specify the same values as VPN Gateway 1 for the other parameters.

   The following table describes the information about the VPN gateways that are created in this example.

Region	VPN gateway name	VPC name	VPN gateway ID	VPN gateway IP address
China (Hangzhou)	VPN Gateway 1	VPC1	vpn-bp1l5zihic47jprwa****	120.XX.XX.40
China (Qingdao)	VPN Gateway 2	VPC2	vpn-m5eqjnr4ii6jajpms****	118.XX.XX.20

Step 2: Create a customer gateway

1.
2. In the top navigation bar, select the region where you want to create the customer gateway.

   > ⓘ **Note** Make sure that the customer gateway and the VPN gateway to be connected are deployed in the same region.

3. On the **User Gateway** page, click **Create Customer Gateway**.
4. In the **Create Customer Gateway** panel, set the following parameters and click **OK**.

   You must create a customer gateway in the China (Hangzhou) region and the China (Qingdao) region. The following table describes the parameters of the customer gateways.

Parameter	Description	China (Hangzhou)	China (Qingdao)
Name	Enter a name for the customer gateway.	*Customer1*	*Customer2*

Parameter	Description	China (Hangzhou)	China (Qingdao)
IP Address	Enter the public IP address of the customer gateway.	In this example, the IP address of VPN Gateway 2, *118.XX.XX.XX. 20*, is entered **Note** In this example, VPN Gateway 1 is the customer gateway of VPC 2, and VPN Gateway 2 is the customer gateway of VPC 1.	In this example, the IP address of VPN Gateway 1, *120.XX.XX.40*, is entered

For more information, see Create a customer gateway.

The following table describes the information about the VPN gateway, customer gateway, and VPC in each region.

Region	VPC name	VPN gateway name	Customer gateway name	Customer gateway ID	Customer gateway IP address
China (Hangzhou)	VPC1	VPN Gateway 1	Customer1	cgw-bp1er5cw26c2b35vm****	118.XX.XX.20
China (Qingdao)	VPC2	VPN Gateway 2	Customer2	cgw-m5e6qdvuxquse3fvm****	120.XX.XX.40

Step 3: Create an IPsec-VPN connection

After you create the VPN gateways and customer gateways, you can create IPsec-VPN connections to connect the VPN gateways to the customer gateways.

1.
2.
3. On the **IPsec Connections** page, click **Create IPsec Connection**.
4. On the **Create IPsec Connection** page, set the following parameters for the IPsec-VPN connection, and click **OK**.

   You must create an IPsec-VPN connection in the China (Hangzhou) region and the China (Qingdao) region. The following table describes the parameters of the IPsec-VPN connections.

Parameter	Description	China (Hangzhou)	China (Qingdao)
Name	Enter a name for the IPsec-VPN connection.	*IPsec-VPN Connection 1*	*IPsec-VPN Connection 2*
VPN Gateway	Select the VPN gateway that you created.	VPN Gateway 1	VPN Gateway 2
Customer Gateway	Select the customer gateway that you created.	Customer1	Customer2
Routing Mode	Select a routing mode.	Select **Destination Routing Mode**.	Select **Destination Routing Mode**.
Effective Immediately	Specify whether to immediately start negotiations for the connection. ○ **Yes**: starts negotiations after the configuration is complete. ○ **No**: starts negotiations when inbound traffic is detected.	**No** is selected in this example.	**No** is selected in this example.
Pre-Shared Key	Enter a pre-shared key. If you do not enter a value, the system generates a random 16-bit string as the pre-shared key.	*fddsFF123***** **Notice** You must configure the same pre-shared key for the IPsec-VPN connections.	

Use the default settings for the other parameters. For more information, see Create an IPsec-VPN connection.

5. In the **Established** dialog box, click **OK**.

Step 4: Configure routes

1.
2.
3. On the **VPN Gateway** page, find the VPN gateway that you want to manage and click its ID.
4. On the **Destination-based Routing** tab, click **Add Route Entry**.
5. In the **Add Route Entry** panel, set the following parameters and click **OK**.

   You must add a route to VPN Gateway 1 and VPN Gateway 2. The following table describes the parameters of routes.

Parameter	Description	VPN Gateway 1	VPN Gateway 2
Destination CIDR Block	Enter the destination CIDR block to be connected.	Enter *10.0.0.0/16*, which is the private CIDR block of VPC 2.	Enter *192.168.0.0/16*, which is the private CIDR block of VPC 1.
Next Hop Type	Select the next hop type.	In this example, **IPsec Connection** is selected.	In this example, **IPsec Connection** is selected.
Next Hop	Select the next hop.	Select IPsec-VPN Connection 1.	Select IPsec-VPN Connection 2.
Publish to VPC	Specify whether to advertise the route to the VPC that is associated with the VPN gateway.	**Yes** is selected in this example.	**Yes** is selected in this example.
Weight	Specify a weight for the route. ○ **100**: specifies a high priority for the route. ○ **0**: specifies a low priority for the route.	The default value **100** is used in this example.	The default value **100** is used in this example.

For more information, see Create a destination-based route.

Step 5: Test network connectivity

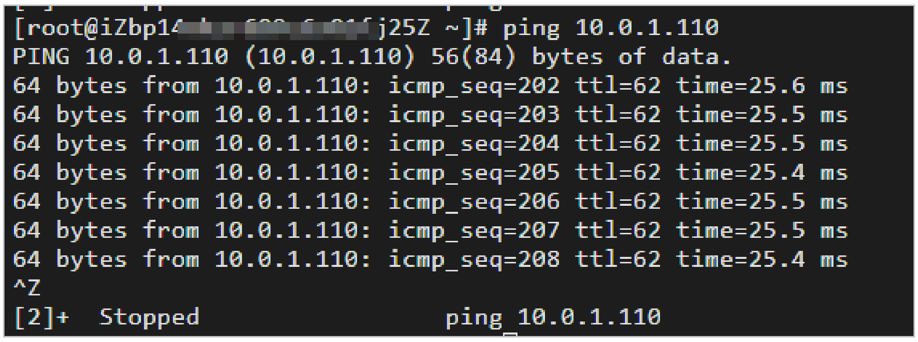
1. Log on to ECS 1 in VPC 1.

   For more information about how to log on to an ECS instance, see Methods used to connect to ECS instances.

2. Run the **ping** command to ping the IP address of ECS 2 to test network connectivity.

```
ping <IP address of ECS 2>
```

If you can receive echo reply packets as shown in the following figure, the connection is established.



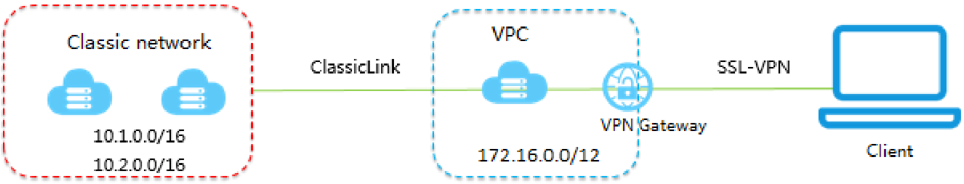
```
[root@iZbp14[redacted]j25Z ~]# ping 10.0.1.110
PING 10.0.1.110 (10.0.1.110) 56(84) bytes of data.
64 bytes from 10.0.1.110: icmp_seq=202 ttl=62 time=25.6 ms
64 bytes from 10.0.1.110: icmp_seq=203 ttl=62 time=25.5 ms
64 bytes from 10.0.1.110: icmp_seq=204 ttl=62 time=25.5 ms
64 bytes from 10.0.1.110: icmp_seq=205 ttl=62 time=25.4 ms
64 bytes from 10.0.1.110: icmp_seq=206 ttl=62 time=25.5 ms
64 bytes from 10.0.1.110: icmp_seq=207 ttl=62 time=25.5 ms
64 bytes from 10.0.1.110: icmp_seq=208 ttl=62 time=25.4 ms
^Z
[2]+  Stopped                 ping 10.0.1.110
```

2.Use SSL-VPN in the classic network

2.1. Access cloud resources in a classic network from a Linux client

This topic describes how to configure SSL-VPN on VPN gateways to access cloud resources deployed in a classic network from a Linux client.

If you have already configured an SSL-VPN connection on the Linux client, skip to Step 5 to connect Elastic Compute Service (ECS) instances that are deployed in a classic network to a virtual private cloud (VPC).



Prerequisites

Before you start, make sure that the following requirements are met:

- The Linux client can access the Internet.
- We recommend that you create a new VPC and set the CIDR block of the VPC to 172.16.0.0/12. If you specify an existing VPC, make sure that the VPC meets the requirements in the following table.

CIDR block of the VPC	Limit
172.16.0.0/12	The VPC does not contain a custom route whose destination CIDR block is 10.0.0.0/8. To view the routes that are configured for the VPC, you can log on to the VPC console and navigate to the route table details page.
192.168.0.0/16	○ The VPC does not contain a custom route whose destination CIDR block is 10.0.0.0/8. ○ A route is added for each ECS instance in the classic network. The route points 192.168.0.0/16 to the Elastic Network Interface (ENI) of the ECS instance. You can add the route by using the provided script. Download script. Note Before you run the script, read the readme file in the downloaded package.

Step 1: Create a VPN gateway

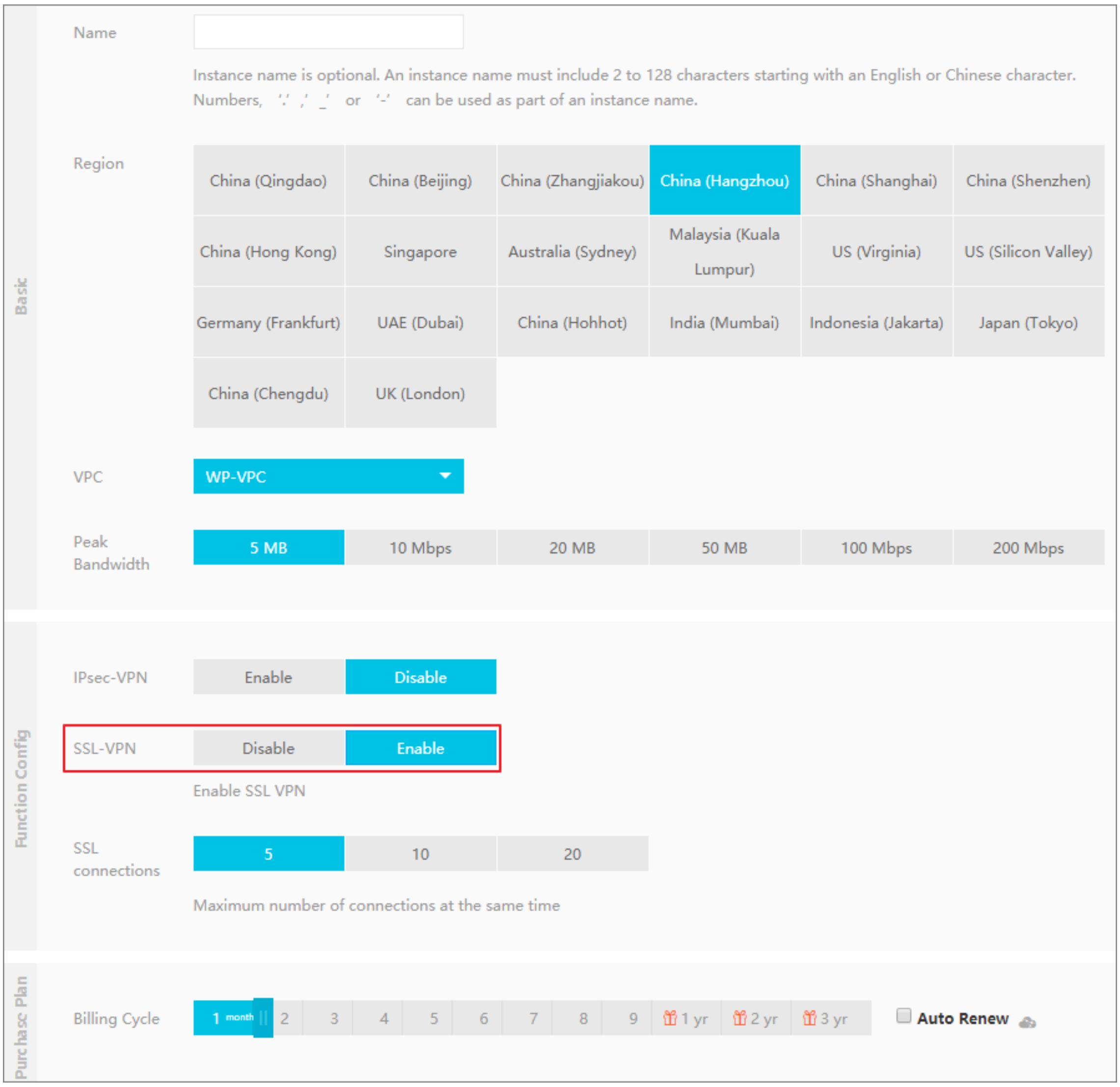
If the VPN gateway is deployed in a VPC and you want to use the VPN gateway in a classic network, you can create a ClassicLink to connect the VPC and classic network.

Perform the following operations to create a VPN gateway:

1. Log on to the VPC console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. On the VPN Gateways page, click **Create VPN Gateway**.
4. Set the parameters on the buy page and complete the payment. The VPN gateway in this example is configured based on the following information:
    - **Region**: Select the region where you want to deploy the VPN gateway. In this example, China (Hangzhou) is selected.

        > ? **Note** Make sure that the VPN gateway and the VPC for which the VPN gateway is created are deployed in the same region.

    - **VPC**: Select the VPC for which the VPN gateway is created.
    - **Bandwidth**: Specify the maximum bandwidth of the VPN gateway. The bandwidth is provided for data transfer over the Internet.
    - **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway. IPsec-VPN connections are site-to-site connections.
    - **SSL-VPN**: Specify whether to enable SSL-VPN for the VPN gateway. In this example, SSL-VPN is enabled.
    - **SSL Connections**: Specify the maximum number of concurrent SSL connections that the VPN gateway supports.



Basic

Name

Instance name is optional. An instance name must include 2 to 128 characters starting with an English or Chinese character. Numbers, '.' ,' _' or '-' can be used as part of an instance name.

Region

China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
China (Hong Kong)	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
Germany (Frankfurt)	UAE (Dubai)	China (Hohhot)	India (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
China (Chengdu)	UK (London)				

VPC: WP-VPC

Peak Bandwidth: 5 MB | 10 Mbps | 20 MB | 50 MB | 100 Mbps | 200 Mbps

Function Config

IPsec-VPN: Enable | Disable

SSL-VPN: Disable | Enable

Enable SSL VPN

SSL connections: 5 | 10 | 20

Maximum number of connections at the same time

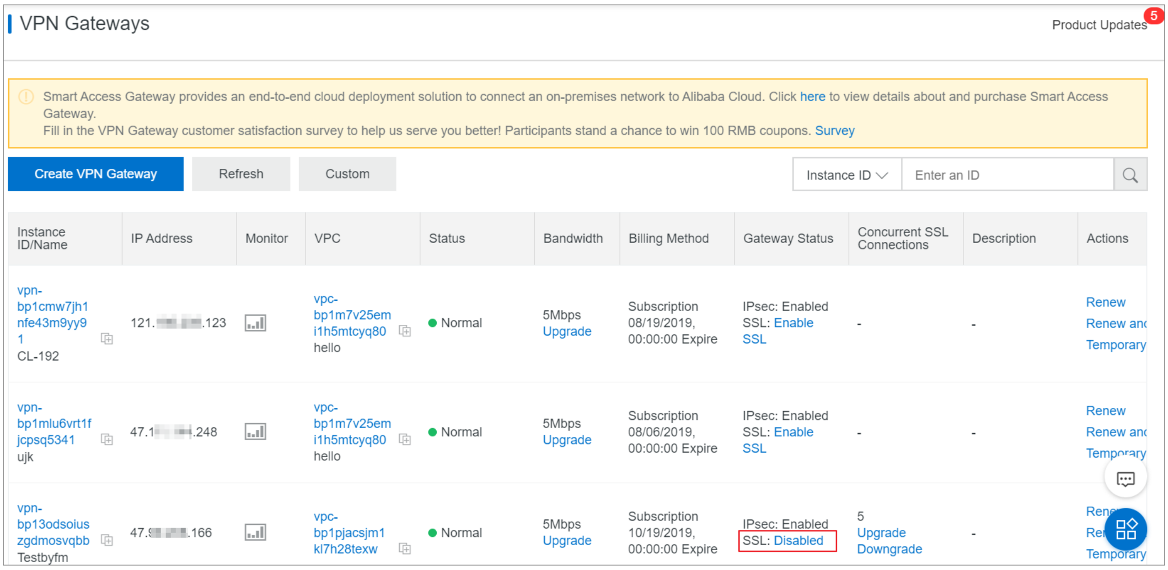
Purchase Plan

Billing Cycle: 1 month | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 yr | 2 yr | 3 yr □ Auto Renew

5. Navigate to the VPN Gateways page to view the VPN gateway.

   After the VPN gateway is created, it is in the Preparing state. The VPN gateway changes to the Normal state after about two minutes. If the state of the VPN gateway is Normal, it indicates that the VPN gateway is initialized and ready for use.

   > **Note** It takes about one to five minutes to create a VPN gateway.



VPN Gateways

Product Updates 5

Smart Access Gateway provides an end-to-end cloud deployment solution to connect an on-premises network to Alibaba Cloud. Click here to view details about and purchase Smart Access Gateway.
Fill in the VPN Gateway customer satisfaction survey to help us serve you better! Participants stand a chance to win 100 RMB coupons. Survey

Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Gateway Status	Concurrent SSL Connections	Description	Actions
vpn-bp1cmw7jh1nfe43m9yy91 CL-192	121.[redacted].123		vpc-bp1m7v25emi1h5mtcyq80 hello	● Normal	5Mbps Upgrade	Subscription 08/19/2019, 00:00:00 Expire	IPsec: Enabled SSL: Enable SSL	-	-	Renew Renew and Temporary
vpn-bp1mlu6vrt1fjcpsq5341 ujk	47.1[redacted].248		vpc-bp1m7v25emi1h5mtcyq80 hello	● Normal	5Mbps Upgrade	Subscription 08/06/2019, 00:00:00 Expire	IPsec: Enabled SSL: Enable SSL	-	-	Renew Renew and Temporary
vpn-bp13odsoiuszgdmosvqbb Testbyfm	47.[redacted].166		vpc-bp1pjacsjm1kl7h28texw	● Normal	5Mbps Upgrade	Subscription 10/19/2019, 00:00:00 Expire	IPsec: Enabled SSL: Disabled	5 Upgrade Downgrade	-	Rene Re Temporary

Step 2: Create an SSL server

Perform the following operations to create an SSL server:

1. In the left-side navigation pane, choose **VPN > SSL Servers**.
2. Click **Create SSL Server**. The SSL server in this example is configured based on the following information:
   - **Name**: Enter a name for the SSL server.
   - **VPN Gateway**: Select the VPN gateway that you created in Step 1 from the drop-down list.
   - **Local Network**: Enter the private CIDR block of the ECS instance that is deployed in the classic network that you want to access. Click **Add Local Network** to add more CIDR blocks.

     In this example, 10.1.0.0/16 and 10.2.0.0/16 are added.

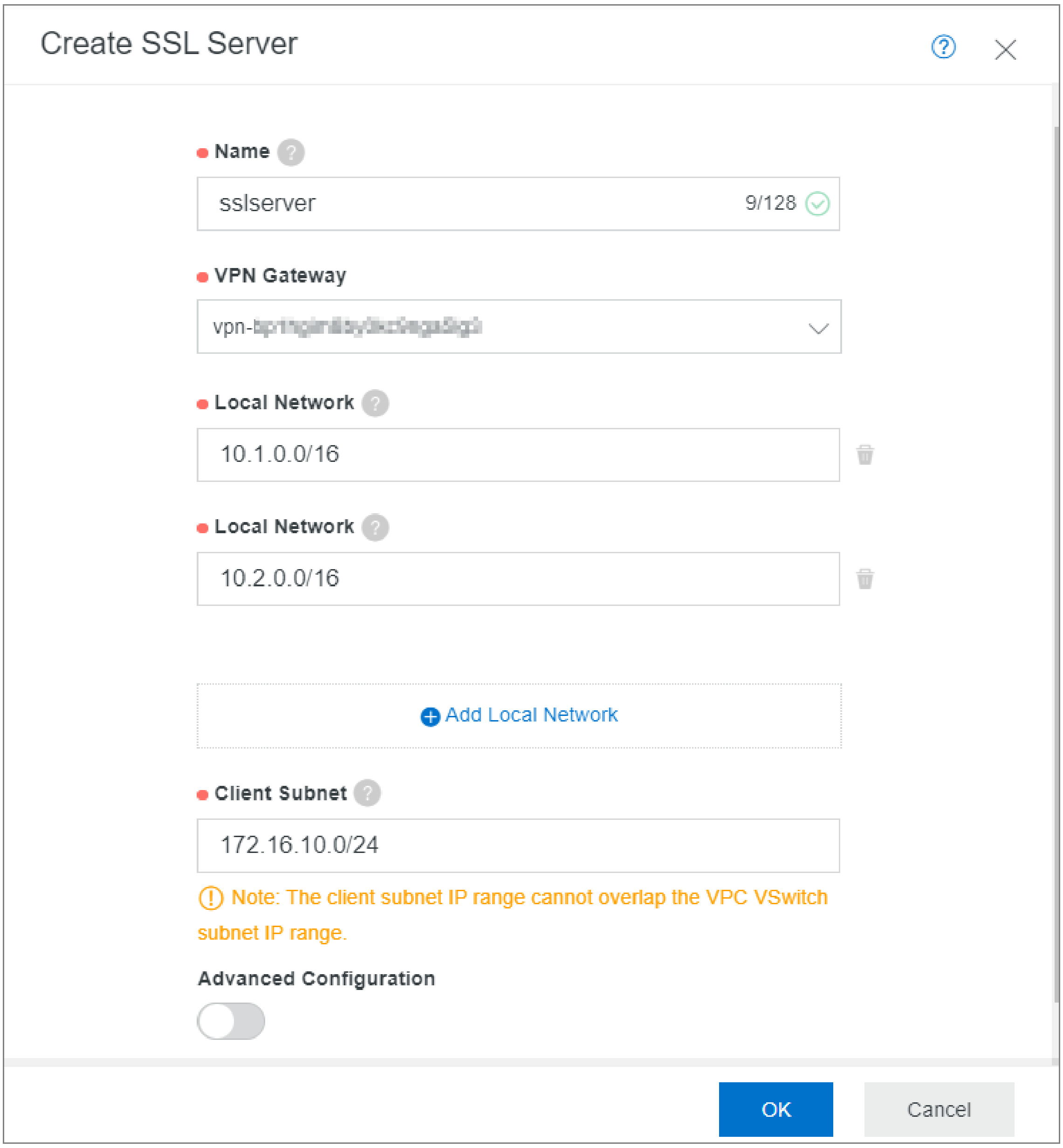
     > **Note** If the IP address of the ECS instance does not fall within the added private CIDR blocks, you must add the private CIDR block to which the IP address of the ECS instance belongs.

   - **Client CIDR Block**: Enter the CIDR block that is used by the client to connect to the SSL server. The client CIDR block must fall within the CIDR block of the VPC to which the VPN gateway belongs.

     In this example, the client CIDR block is 172.16.10.0/24.

     > **Note** The client CIDR block does not refer to the CIDR block of the client. The client CIDR block is used to allocate IP addresses to the client. After the client is assigned an IP address, it can remotely access resources through an SSL-VPN connection.

   - **Advanced Configuration**: In this example, the default setting is used.



Name: sslserver 9/128

VPN Gateway: vpn-[redacted]

Local Network: 10.1.0.0/16

Local Network: 10.2.0.0/16

Client Subnet: 172.16.10.0/24

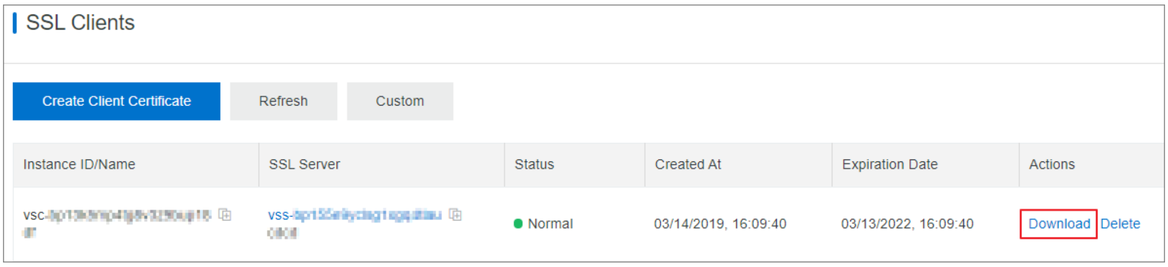
Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Advanced Configuration: ○

Step 3: Create an SSL client certificate

Perform the following operations to create an SSL client certificate:

1. In the left-side navigation pane, choose **VPN > SSL Clients**.
2. Click **Create Client Certificate**.
3. In the **Create Client Certificate** dialog box, enter a name for the SSL client certificate, select the SSL server to which the SSL client certificate is to be imported, and then click **OK**.
4. On the **SSL Clients** page, find the SSL client certificate that you created, and click **Download** to download the SSL client certificate.



SSL Clients

Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
vsc-[redacted]	vss-[redacted]	● Normal	03/14/2019, 16:09:40	03/13/2022, 16:09:40	Download Delete

Step 4: Configure the client

Perform the following operations to configure the client:

1. Run the following command to install OpenVPN:

   ```
   yum install -y openvpn
   ```

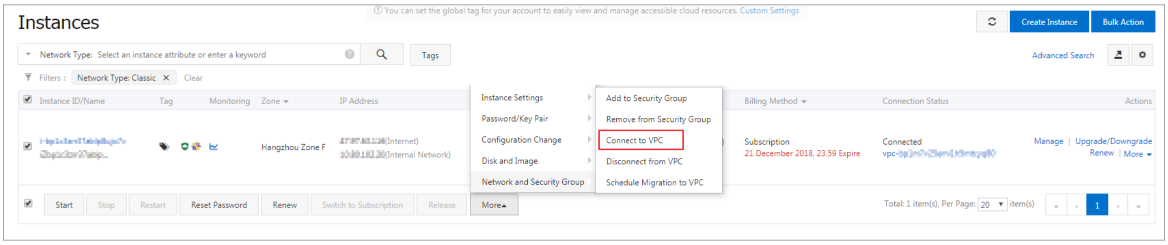
2. Decompress the client certificate package that you downloaded in Step 3 and copy the SSL client certificate file to the */etc/openvpn/conf/* folder where OpenVPN is installed.
3. Run the following command to launch OpenVPN:

   ```
   openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   ```

Step 5: Establish a ClassicLink

Perform the following operations to establish a ClassicLink:

1. Log on to the VPC console.
2. Select the region where the VPC is deployed and click the ID of the VPC.
3. On the **VPC Details** page, click **Enable ClassicLink**.
4. In the message that appears, click **OK**.
5. Log on to the ECS console.
6. In the left-side navigation pane, click **Instances**.
7. Select one or more ECS instances deployed in the classic network that you want to access, and choose **More > Connect to VPC**.



Instances

ⓘ You can set the global tag for your account to easily view and manage accessible cloud resources. Custom Settings

Network Type: Select an instance attribute or enter a keyword

Filters : Network Type: Classic ✕ Clear

☑	Instance ID/Name	Tag	Monitoring	Zone	IP Address	Billing Method	Connection Status	Actions
☑	[redacted]			Hangzhou Zone F	[redacted](Internet) [redacted](Internal Network)	Subscription 21 December 2018, 23.59 Expire	Connected vpc-[redacted]	Manage | Upgrade/Downgrade Renew | More

Total: 1 item(s), Per Page: 20 item(s)

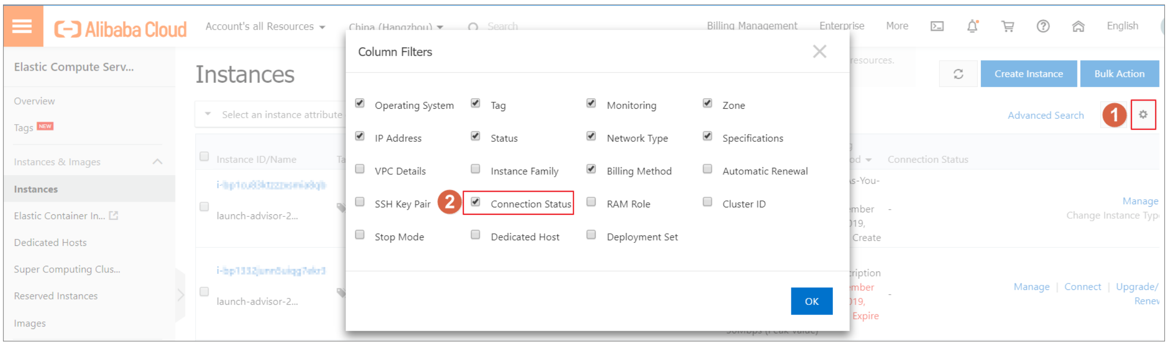
8. In the dialog box that appears, specify the VPC to which you want to connect, and click **OK**.
9. In the left-side navigation pane, choose **Networks and Security > Security Groups**.
10. On the **Security Groups** page, click the **Inbound** tab, and then click **Add Security Group Rule**. Set the following parameters to configure the security group:
    - **Rule Direction**: Inbound.
    - **Action**: Allow.
    - **Protocol Type**: All.

- **Authorization Type**: IPv4 CIDR Block.
- **Authorization Object**: Enter the private IP address (for example, 172.16.3.44/32) of the client that needs to access the ECS instance through the VPN gateway.

  Run the **ifconfig** command on the Linux client, and then find the message that is similar to `inet 172.16.10.6 --> 172.16.10.5 netmask 0xffffffff`. In the message, `172.16.10.6` is the IP address of the client (the authorization object specified in the security group).

  > **Note** If you fail to access the ECS instance through the VPN gateway, it indicates that the client IP address has changed and you must add a new security group rule.

11. Go back to the Instances page of the ECS console, and click the Column Filters icon in the upper-right corner. In the dialog box that appears, select **Connection Status** and click **OK**.

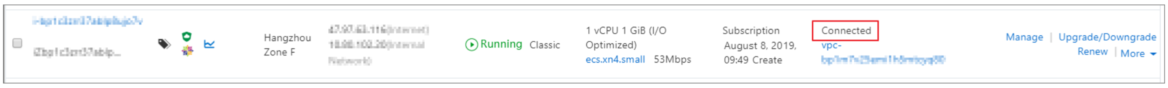


Column Filters

☑ Operating System ☑ Tag ☑ Monitoring ☑ Zone
☑ IP Address ☑ Status ☑ Network Type ☑ Specifications
□ VPC Details □ Instance Family ☑ Billing Method □ Automatic Renewal
□ SSH Key Pair ☑ Connection Status □ RAM Role □ Cluster ID
□ Stop Mode □ Dedicated Host □ Deployment Set

OK

12. You can view the state of the connection established to the ECS instance.

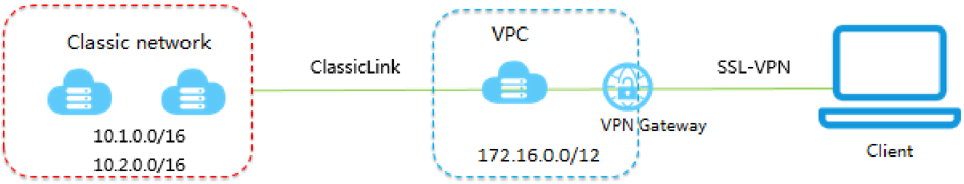

Hangzhou Zone F
Running Classic
1 vCPU 1 GiB (I/O Optimized) ecs.xn4.small 53Mbps
Subscription August 8, 2019, 09:49 Create
Connected vpc-

If the connection is in the Connected state, it indicates that you can access the applications on the ECS instance from the Linux client.

2.2. Access cloud resources in a classic network from a Mac client

This topic describes how to configure SSL-VPN on VPN gateways to access cloud resources deployed in a classic network from a Mac client.

If you have already configured an SSL-VPN connection on the client, skip to Step 5 to connect Elastic Compute Service (ECS) instances that are deployed in a classic network to a virtual private cloud (VPC).



Prerequisites

Before you start, make sure that the following requirements are met:

- The client can access the Internet.

- We recommend that you create a new VPC and set the CIDR block of the VPC to 172.16.0.0/12. If you specify an existing VPC, make sure that the VPC meets the requirements in the following table.

CIDR block of the VPC	Requirement
172.16.0.0/12	The VPC does not contain a custom route whose destination CIDR block is 10.0.0.0/8. You can log on to the VPC console and navigate to the route table details page to view the routes that are configured for the VPC.
192.168.0.0/16	○ The VPC does not contain a custom route whose destination CIDR block is 10.0.0.0/8. ○ A route is added for each ECS instance in the classic network. The route points 192.168.0.0/16 to the Elastic Network Interface (ENI) of the ECS instance. You can use the provided script to add the route. Download the script. ⓘ Note Before you run the script, read the readme file in the downloaded package.

Step 1: Create a VPN gateway

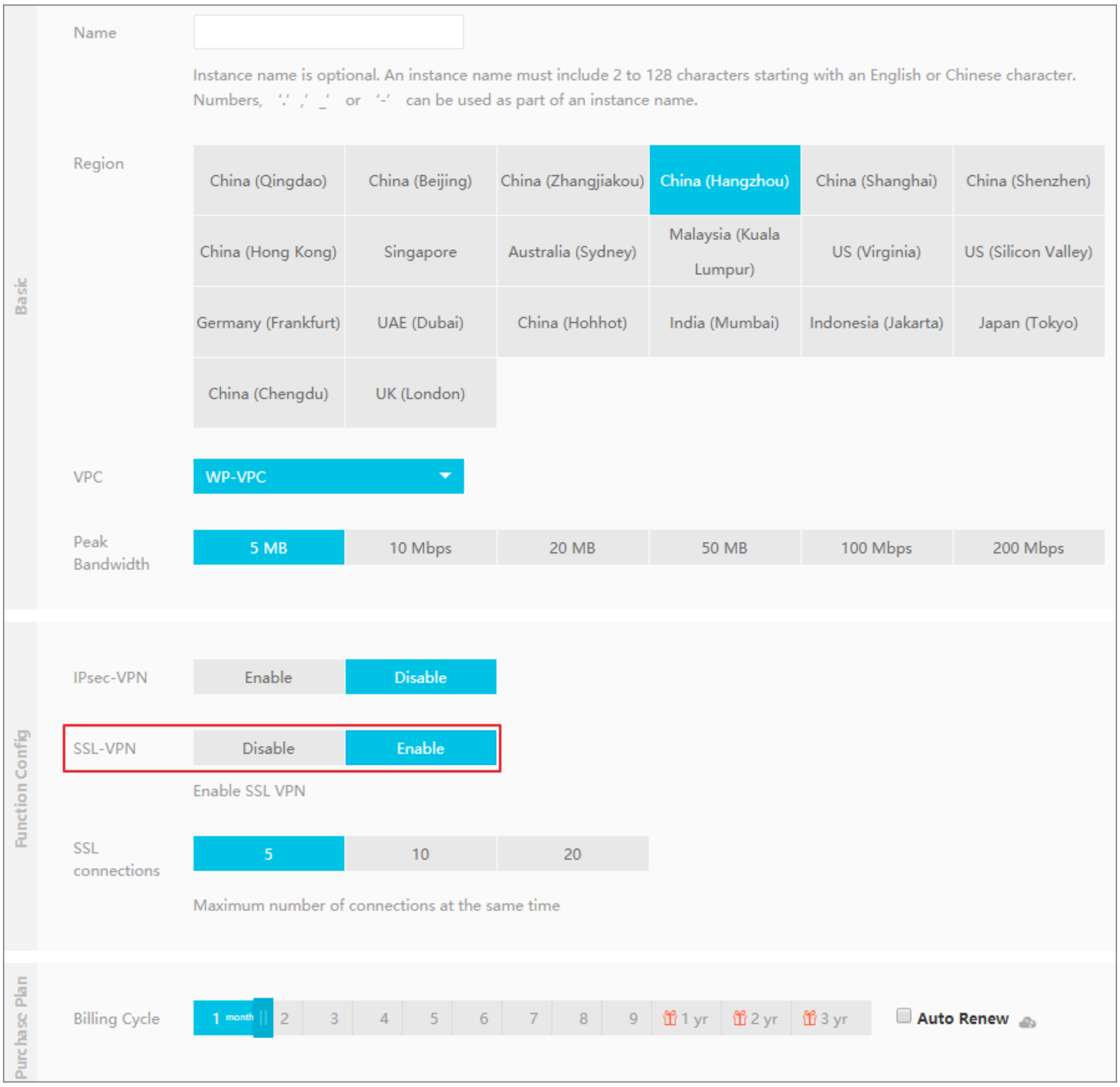
If the VPN gateway is deployed in a VPC and you need to use the VPN gateway in a classic network, you can create a ClassicLink to connect the VPC and classic network.

Perform the following operations to create a VPN gateway:

1. Log on to the new VPC console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. On the VPN Gateways page, click **Create VPN Gateway**.
4. Set the parameters on the buy page and complete the payment. Set the following parameters to create a VPN gateway:
   - **Region**: Select the region where you want to deploy the VPN gateway. In this example, **China (Hangzhou)** is selected.

     > ⓘ Note Make sure that the VPN gateway and the VPC for which the VPN gateway is created are deployed in the same region.

   - **VPC**: Select the VPC for which the VPN gateway is created.
   - **Bandwidth**: Specify the maximum bandwidth for the VPN gateway. The bandwidth is provided for data transfer over the Internet.
   - **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway. If you enable IPsec-VPN, you can use the VPN gateway to create IPsec-VPN connections.
   - **SSL-VPN**: Specify whether to enable SSL-VPN. In this example, **Enable** is selected.
   - **SSL Connections**: Specify the maximum number of concurrent SSL connections that the VPN gateway supports.



Name

Instance name is optional. An instance name must include 2 to 128 characters starting with an English or Chinese character. Numbers, '.' , '_' or '-' can be used as part of an instance name.

Region

China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
China (Hong Kong)	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
Germany (Frankfurt)	UAE (Dubai)	China (Hohhot)	India (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
China (Chengdu)	UK (London)				

VPC: WP-VPC

Peak Bandwidth: 5 MB | 10 Mbps | 20 MB | 50 MB | 100 Mbps | 200 Mbps

IPsec-VPN: Enable | Disable

SSL-VPN: Disable | Enable

Enable SSL VPN

SSL connections: 5 | 10 | 20

Maximum number of connections at the same time

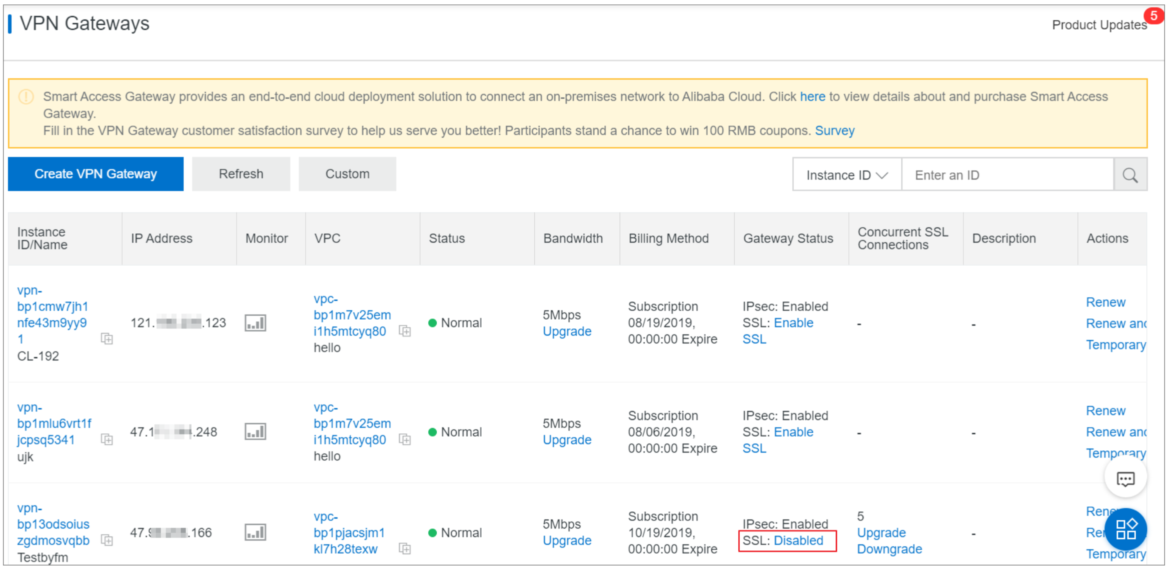
Billing Cycle: 1 month | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 yr | 2 yr | 3 yr

□ Auto Renew

5. Navigate to the VPN Gateways page to view the newly created VPN gateway.

   The newly created VPN gateway is in the Preparing state. The VPN gateway changes to the Normal state after about two minutes. If the state of the VPN gateway is Normal, it indicates that the VPN gateway is initialized and ready for use.

   > **Note** It takes about one to five minutes to create a VPN gateway.



VPN Gateways

Product Updates 5

Smart Access Gateway provides an end-to-end cloud deployment solution to connect an on-premises network to Alibaba Cloud. Click here to view details about and purchase Smart Access Gateway.
Fill in the VPN Gateway customer satisfaction survey to help us serve you better! Participants stand a chance to win 100 RMB coupons. Survey

Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Gateway Status	Concurrent SSL Connections	Description	Actions
vpn-bp1cmw7jh1nfe43m9yy91 CL-192	121.[redacted].123		vpc-bp1m7v25emi1h5mtcyq80 hello	● Normal	5Mbps Upgrade	Subscription 08/19/2019, 00:00:00 Expire	IPsec: Enabled SSL: Enable SSL	-	-	Renew Renew anc Temporary
vpn-bp1mlu6vrt1fjcpsq5341 ujk	47.1[redacted].248		vpc-bp1m7v25emi1h5mtcyq80 hello	● Normal	5Mbps Upgrade	Subscription 08/06/2019, 00:00:00 Expire	IPsec: Enabled SSL: Enable SSL	-	-	Renew Renew anc Temporary
vpn-bp13odsoiuszgdmosvqbb Testbyfm	47.[redacted].166		vpc-bp1pjacsjm1kl7h28texw	● Normal	5Mbps Upgrade	Subscription 10/19/2019, 00:00:00 Expire	IPsec: Enabled SSL: Disabled	5 Upgrade Downgrade	-	Rene Re Temporary

Step 2: Create an SSL server

Perform the following operations to create an SSL server:

1. In the left-side navigation pane, choose **VPN > SSL Servers**.
2. Click **Create SSL Server**. Set the following parameters to create an SSL server:
   - **Name**: Enter a name for the SSL server.
   - **VPN Gateway**: Select the VPN gateway that you created in Step 1 from the drop-down list.
   - **Local Network: Enter the private CIDR block of the ECS instance that is deployed in the classic network that you want to access.** Click **Add Local Network** to add more CIDR blocks.

     In this example, 10.1.0.0/16 and 10.2.0.0/16 are added.

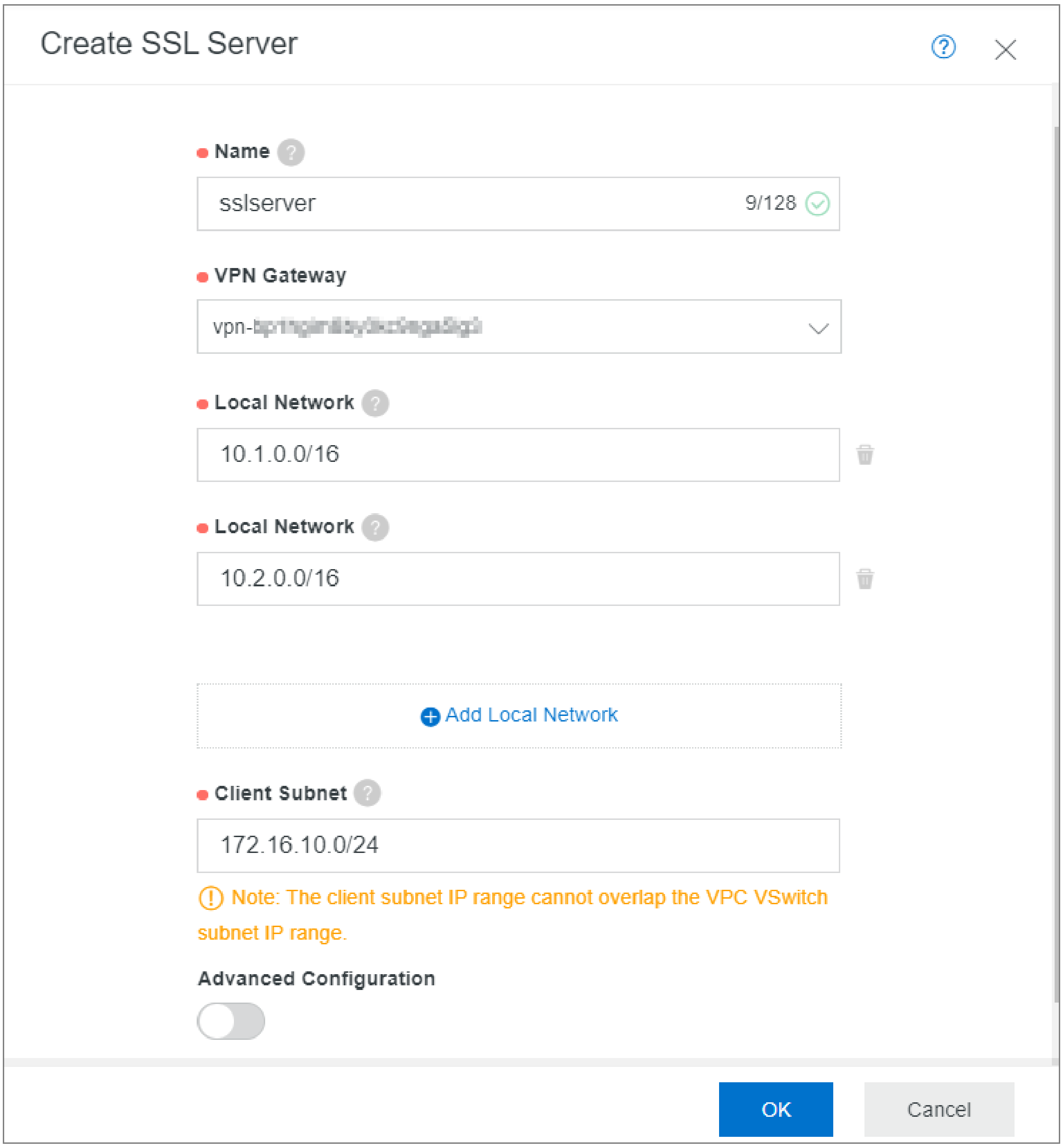
     > **Note** If the IP address of the ECS instance does not fall within the added private CIDR blocks, you must add the private CIDR block to which the IP address of the ECS instance belongs.

   - **Client CIDR Block: Enter the CIDR block that is used by the client to connect to the SSL server. The client CIDR block must fall within the CIDR block of the VPC to which the VPN gateway belongs.**

     In this example, the client CIDR block is 172.16.10.0/24.

     > **Note** The client CIDR block does not refer to the CIDR block of the client. The client CIDR block is used to allocate IP addresses to the client. After the client is assigned an IP address, it can remotely access resources through an SSL-VPN connection.

   - **Advanced Configuration**: In this example, the default setting is used.



Create SSL Server

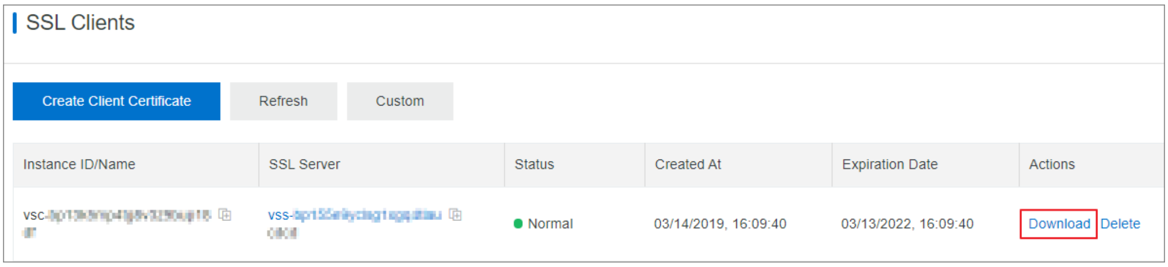
- Name: sslserver 9/128
- VPN Gateway: vpn-[redacted]
- Local Network: 10.1.0.0/16
- Local Network: 10.2.0.0/16
- Client Subnet: 172.16.10.0/24

Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Step 3: Create an SSL client certificate

Perform the following operations to create an SSL client certificate:

1. In the left-side navigation pane, choose **VPN > SSL Clients**.
2. Click **Create Client Certificate**.
3. In the **Create Client Certificate** dialog box, enter a name for the SSL client certificate, select the SSL server to which the SSL client certificate is to be imported, and then click **OK**.
4. On the **SSL Clients** page, find the SSL client certificate that you created, and click **Download** to download the SSL client certificate.



Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
vsc-[redacted]	vss-[redacted]	● Normal	03/14/2019, 16:09:40	03/13/2022, 16:09:40	Download Delete

Step 4: Configure the client

Perform the following operations to configure the client:

1. Run the following command to install OpenVPN:

   ```
   brew install openvpn
   ```

   Note Make sure that homebrew is installed before you install OpenVPN.

2. Decompress the SSL client certificate package that you downloaded in Step 3 and copy the SSL client certificate file to the folder where OpenVPN is installed. Then, initiate an SSL-VPN connection.

   i. Backup the default configuration file, and then run the following command to delete the default configuration file:

   ```
   rm /usr/local/etc/openvpn/*
   ```

   ii. Run the following command to copy the file to the configuration directory:

   ```
   cp cert_location /usr/local/etc/openvpn/
   ```

   In the preceding command, `cert_location` represents the path that stores the SSL client certificate downloaded in Step 3. For example, */Users/example/Downloads/certs6.zip* is the path to the SSL client certificate.

   iii. Run the following command to decompress the SSL client certificate package:

   ```
   unzip /usr/local/etc/openvpn/certs6.zip
   ```

   iv. Run the following command to initiate a connection:

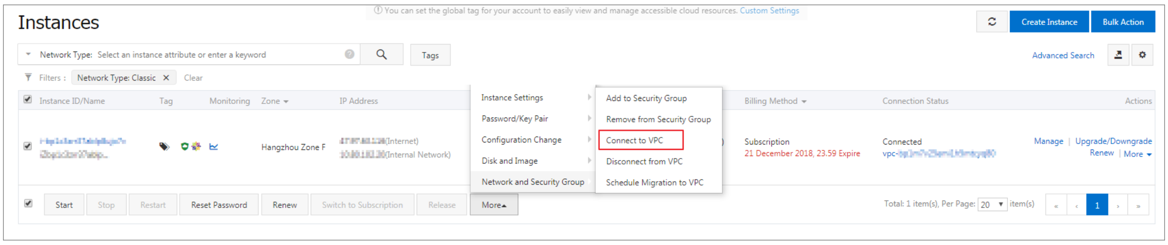
   ```
   sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovp
   n
   ```

Step 5: Establish a ClassicLink

Perform the following operations to establish a ClassicLink:

1. Log on to the VPC console.
2. Select the region where the VPC is deployed and click the ID of the VPC.
3. On the **VPC Details** page, click **Enable ClassicLink**.
4. In the message that appears, click **OK**.
5. Log on to the ECS console.

6. In the left-side navigation pane, click **Instances**.
7. Select one or more ECS instances deployed in the classic network that you want to access, and choose **More > Connect to VPC**.

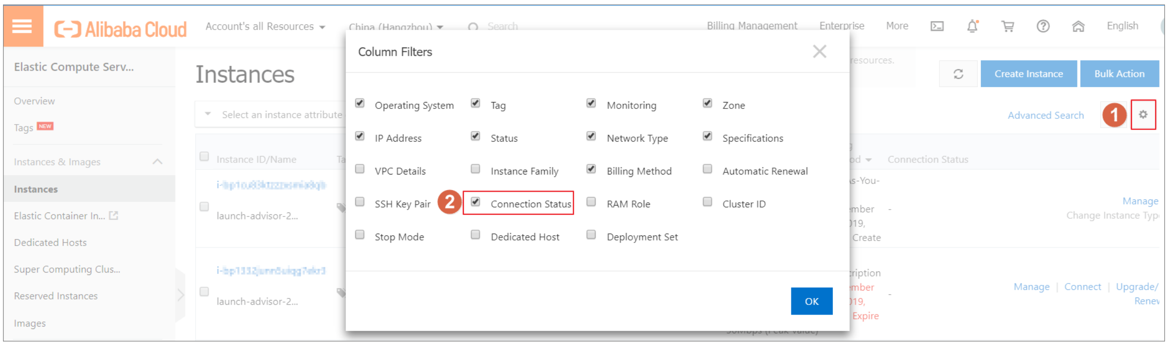


8. In the dialog box that appears, specify the VPC that you want to connect, and click **OK**.
9. In the left-side navigation pane, choose **Networks and Security > Security Groups**.
10. On the **Security Groups** page, click the **Inbound** tab, and then click **Add Security Group Rule**. Set the following parameters to configure the security group:
    - **Rule Direction**: Inbound
    - **Action**: Allow
    - **Protocol Type**: All
    - **Authorization Type**: IPv4 CIDR Block
    - **Authorization Object**: Enter the private IP address (for example, 172.16.3.44/32) that needs to access the ECS instance through the VPN gateway.

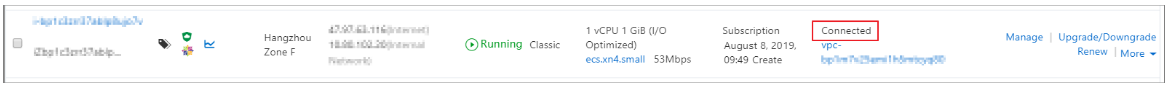
      Run the **ifconfig** command on the Mac client, and then find the information that is similar to `inet 172.16.10.6 --> 172.16.10.5 netmask 0xffffffff`. `172.16.10.6` is the IP address of the client. This is also the authorization object configured for the security group.

    > **Note** If you fail to access the ECS instance through the VPN gateway, it indicates that the client IP address has changed and you must add a new security group rule.

11. Navigate to the Instances page of the ECS console, click the Column Filters icon in the upper-right corner. In the dialog box that appears, select **Connection Status**, and click **OK**.



12. You can view the state of the connection established to the ECS instance.



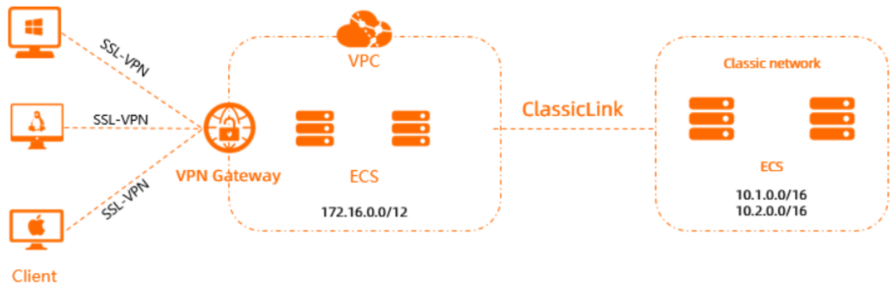
If the connection is in the Connected state, it indicates that you can access the applications on the ECS instance from the Mac client.

2.3. Establish SSL-VPN connections to access resources in classic networks

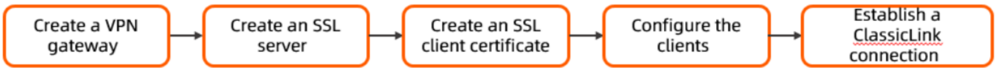
This topic describes how to establish SSL-VPN connections between Alibaba Cloud classic networks and clients that run Linux, macOS, or Windows. These clients can access resources in Alibaba Cloud classic networks over SSL-VPN connections.

Scenarios

The following scenario is used as an example. You must first establish SSL-VPN connections between the clients and a virtual private cloud (VPC). Then, use the ClassicLink feature of the VPC to connect a classic network to the VPC. This way, the clients are connected to the classic network over the VPC.



Procedure


Create a VPN gateway
Create an SSL server
Create an SSL client certificate
Configure the clients
Establish a ClassicLink connection

> **Note** If SSL-VPN is already configured, you can connect the clients to the classic network by establishing ClassicLink connections between the VPC and Elastic Compute Service (ECS) instances in the classic network. For more information, see Step 5: Establish a ClassicLink connection.

Prerequisites

- A VPC is created. For more information, see Create an IPv4 VPC.

  The CIDR block of the VPC must meet the requirements described in the following table.

- The private CIDR block of the data center that needs to communicate with the classic network must fall within the CIDR block of the VPC and cannot conflict with the CIDR blocks of vSwitches in the VPC. Otherwise, the data center and the VPC cannot communicate with each other.

Step 1: Create a VPN gateway

Before you can use SSL-VPN, you must first create a VPN gateway. After you create a VPN gateway, a public IP address is assigned to the VPN gateway.

1.

2.

3. On the **VPN Gateway** page, set the following parameters, click **Buy Now**, and then complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway.
Region	The region where you want to create the VPN gateway. **Note** The VPN gateway and the VPC must belong to the same region.
Gateway Type	Select a type for the VPN gateway. In this example, **Standard** is selected.
Network Type	Select a network type for the VPN gateway. In this example, **Public** is selected.
VPC	Select the VPC where you want to create the VPN gateway.
Specify VSwitch	Specify whether to select a vSwitch for the VPN gateway. In this example, **No** is selected.
Maximum Bandwidth	Specify a maximum bandwidth value for the VPN gateway. The bandwidth is used to limit the data transfer rate over the Internet.
Traffic	By default, the VPN gateway uses the pay-by-data-transfer metering method. For more information, see Pay-as-you-go.
IPsec-VPN	Specify whether to enable the IPsec-VPN feature. In this example, **Disable** is selected.
SSL-VPN	Specify whether to enable the SSL-VPN feature. In this example, **Enable** is selected.
SSL Connections	Select the maximum number of concurrent SSL connections that the VPN gateway supports.
Duration	By default, the VPN gateway is billed on an hourly basis.
	Click **Create Service-linked Role** and the system automatically creates the service-linked role AliyunServiceRoleForVpn. For more information about how a VPN gateway assumes the role to access other cloud resources, see AliyunServiceRoleForVpn. If **Created** is displayed, the service-linked role is created and you do not need to create it again.

4. Return to the **VPN Gateways** page to view the VPN gateway that you created.

   It takes about 1 to 5 minutes to create a VPN gateway. A newly created VPN gateway is in the Preparing state. After about 2 minutes, it enters the Normal state. The Normal state indicates that the VPN gateway is initialized and ready for use.

Step 2: Create an SSL server

After you create a VPN gateway, you must create an SSL server. The SSL server is used to establish an SSL-VPN connection.

1.
2.
3.
4. In the **Create SSL Server** panel, set the following parameters and click **OK**.

Parameter	Description
Name	Enter a name for the SSL server.
VPN Gateway	In this example, the VPN gateway that is created in Step 1 is selected.
Local Network	Enter the private CIDR block of the ECS instance that is deployed in the classic network that you want to access. Click **Add Local Network** to add more CIDR blocks. In this example, 10.1.0.0/16 and 10.2.0.0/16 are entered. ⓘ **Note** If the IP address of an ECS instance does not fall within the specified private CIDR blocks, you must add the private CIDR block to which the IP address of the ECS instance belongs.
Client Subnet	Enter the CIDR block that is used by the client to connect to the SSL server. The system assigns an IP address from the CIDR block to the client. The client uses the IP address to access resources in the VPC. The client CIDR block must fall within the CIDR block of the VPC to which the VPN gateway belongs. In this example, 172.16.10.0/24 is entered.
Advanced Configuration	In this example, the default settings are used.

Step 3: Create an SSL client certificate

After you create an SSL server, you must create an SSL client certificate based on the configuration of the SSL server.

1.
2.
3. In the **Create Client Certificate** panel, enter a name for the SSL client certificate, select an SSL server, and then click **OK**.
4. On the **SSL Client** page, find the client certificate that you created and click **Download** in the **Actions** column to download the client certificate.

Step 4: Configure the clients

After you download the SSL client certificate, you must install the client certificate on the client. After you install the certificate, the client can connect to the VPN gateway over an SSL-VPN connection. The following section describes how to configure Linux, macOS, and Windows clients.

Configure a Linux client

1. Run the following command to install OpenVPN:

   ```
   yum install -y openvpn
   ```

2. Extract and copy the SSL client certificate to the */etc/openvpn/conf/* directory.
3. Run the following command to start OpenVPN:

   ```
   openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   ```

Configure a macOS client

1. Open the command-line interface (CLI).
2. If Homebrew is not installed on your client, run the following command to install Homebrew:

   ```
   /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
   ```

3. Run the following command to install OpenVPN:

   ```
   brew install openvpn
   ```

4. Copy the SSL client certificate package that you downloaded to the configuration directory of OpenVPN and decompress the package.

   i. Back up all configuration files in the */usr/local/etc/openvpn* folder.

   ii. Run the following command to delete the configuration files of OpenVPN:

   ```
   rm /usr/local/etc/openvpn/*
   ```

   iii. Run the following command to copy the SSL client certificate package to the */usr/local/etc/openvpn/* directory.

   ```
   cp cert_location /usr/local/etc/openvpn/
   ```

   In the preceding command, replace `cert_location` with the directory of the SSL client certificate, for example, */Users/example/Downloads/certs6.zip*.

5. Run the following command to decompress the package:

   ```
   cd  /usr/local/etc/openvpn/
   unzip /usr/local/etc/openvpn/certs6.zip
   ```

6. Run the following command to establish an SSL-VPN connection:

   ```
   sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
   ```

Configure a Windows client

1. Download and install OpenVPN.

Download the installation package for OpenVPN.

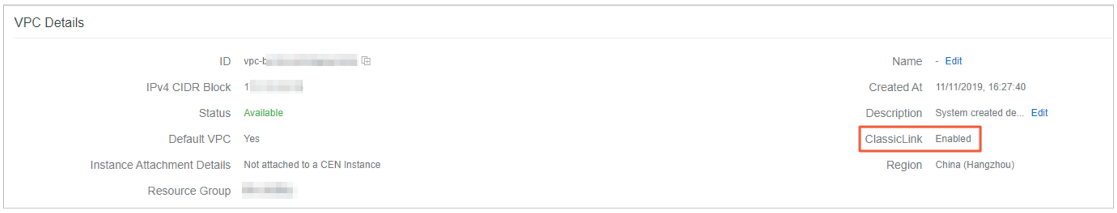
2. Extract and copy the SSL client certificate to the *OpenVPN\config* directory of OpenVPN.
3. Start OpenVPN and click **Connect** to initiate a connection.

Step 5: Establish a ClassicLink connection

VPC provides the ClassicLink feature. This feature allows ECS instances in a classic network to communicate with cloud resources in a VPC.

1. Enable ClassicLink.
    i. Log on to the VPC console.
    ii. In the top navigation bar, select the region where the VPC is deployed.
    iii. On the **VPCs** page, find the VPC that you want to manage and click its ID.
    iv. In the upper-right corner of the VPC details page, click **Enable ClassicLink**.
    v. In the **Enable ClassicLink** message, click **OK**.

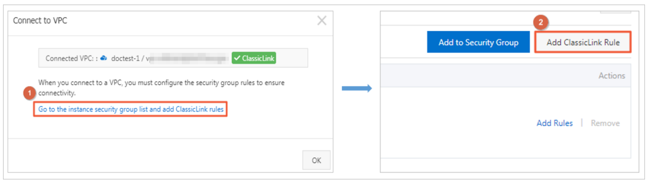
    After ClassicLink is enabled, the status of ClassicLink in the VPC Details section changes to **Enabled**.



VPC Details

ID: vpc-b[redacted]
IPv4 CIDR Block: 1[redacted]
Status: Available
Default VPC: Yes
Instance Attachment Details: Not attached to a CEN Instance
Resource Group: [redacted]
Name: - Edit
Created At: 11/11/2019, 16:27:40
Description: System created de... Edit
ClassicLink: Enabled
Region: China (Hangzhou)

2. Log on to the ECS console.
3. In the left-side navigation pane, choose **Instances & Images** > **Instances**.
4. Select the region where the ECS instance that you want to manage is deployed.
5. Connect the ECS instance to the VPC.
    i. On the **Instances** page, find the ECS instance that you want to manage and choose **More** > **Network and Security Group** > **Set classic link** in the **Actions** column.
    ii. In the **Connect to VPC** dialog box, select a VPC and click **OK**.
6. Configure a security group rule for ClassicLink.
    i. Click **Go to the instance security group list and add ClassicLink rules**, and click **Add ClassicLink Rule**.



Connect to VPC

Connected VPC: : doctest-1 / v[redacted] ✓ ClassicLink

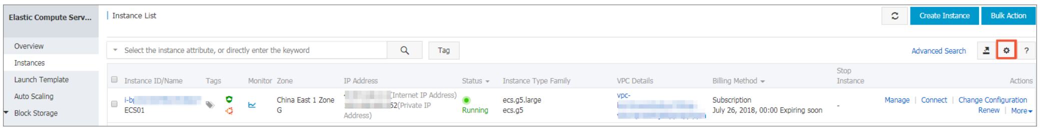
When you connect to a VPC, you must configure the security group rules to ensure connectivity.

ii. In the **Add ClassicLink Rule** dialog box, set the following parameters and click **OK**.

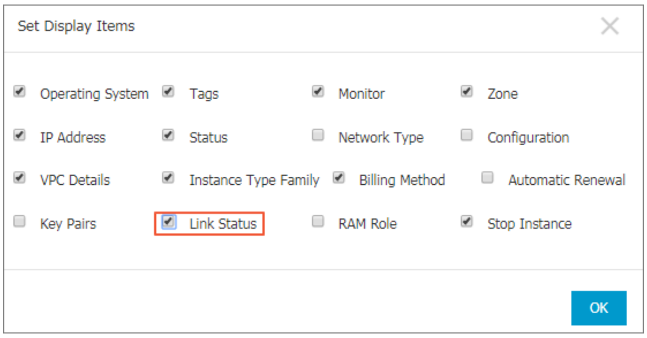
Parameter	Description
Classic Security Group	Displays the name of the security group of the classic network.
Select VPC Security Group	Select a security group of the VPC.
Authorization Method	Select one of the following authorization methods: ■ Classic <=> VPC: allows the ECS instance in the classic network and cloud resources in the VPC to access each other. This method is recommended. ■ Classic => VPC: allows the ECS instance in the classic network to access cloud resources in the VPC. ■ VPC => Classic: allows the cloud resources in the VPC to access the ECS instance in the classic network.
Protocol Type	Select the protocol for communication.
Port Range	Specify the ports that are used for communication. Specify the ports in the xx/xx format. For example, to specify port 80, enter 80/80.
Priority	Specify a priority for the rule. A smaller value specifies a higher priority.
Description	Enter a description for the security group.

7. Go back to the ECS console, and click the Column Filters icon in the upper-right corner. In the dialog box that appears, select **Link Status**, and click **OK** to view the connection status of the ECS instance.

Column Filters



Connection Status


Set Display Items

☑ Operating System ☑ Tags ☑ Monitor ☑ Zone

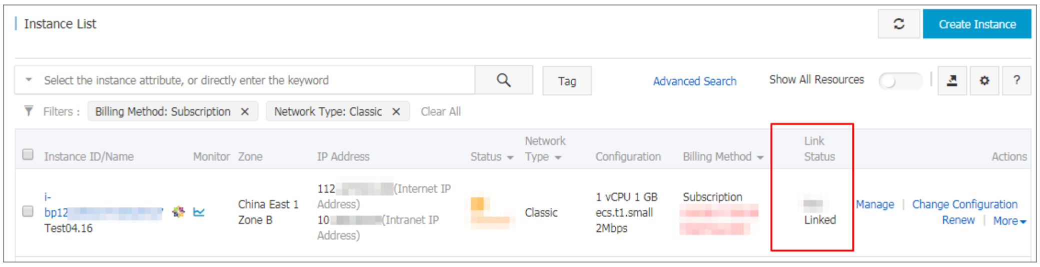
☑ IP Address ☑ Status ☐ Network Type ☐ Configuration

☑ VPC Details ☑ Instance Type Family ☑ Billing Method ☐ Automatic Renewal

☐ Key Pairs ☑ Link Status ☐ RAM Role ☑ Stop Instance

OK

Connection Status



□	Instance ID/Name	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Link Status	Actions
□	i-bp12[redacted] Test04.16		China East 1 Zone B	112[redacted](Internet IP Address) 10[redacted](Intranet IP Address)	[redacted]	Classic	1 vCPU 1 GB ecs.t1.small 2Mbps	Subscription [redacted]	[redacted] Linked	Manage | Change Configuration Renew | More

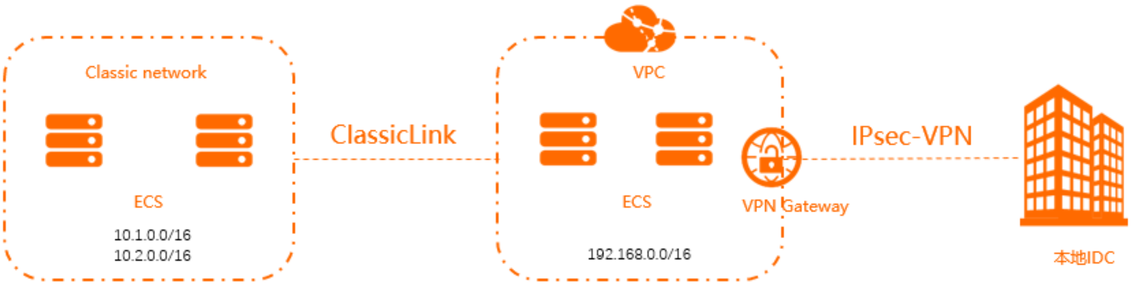
After you complete the preceding configurations, your client can access the applications deployed on the ECS instance in the classic network.

3.Connect a data center to a classic network by using IPsec-VPN

This topic describes how to connect a data center to a classic network by using IPsec-VPN. This way, the data center and the classic network can communicate with each other.

Context

To connect a data center to a classic network by using IPsec-VPN, you must create a virtual private network (VPC) to forward traffic. You must first establish an IPsec-VPN connection between the data center and the VPC, and then connect the VPC to the classic network by using ClassicLink. This way, the VPC serves as a transit point and allows the the data center and the classic network to communicate with each other.



Prerequisites

- A VPC is created. For more information, see Create an IPv4 VPC.

  The CIDR block of the VPC must meet the requirements described in the following table.

- The private CIDR block of the data center that needs to communicate with the classic network must fall within the CIDR block of the VPC and cannot conflict with the CIDR blocks of vSwitches in the VPC. Otherwise, the data center and the VPC cannot communicate with each other.

Procedure

1. Establish an IPsec-VPN connection between the data center and the VPC.

   For more information, see Connect a data center to a VPC.

2. Enable ClassicLink.

   For more information, see Enable ClassicLink.

3. Establish a ClassicLink connection.

   For more information, see Establish a ClassicLink connection.

4. Test the connectivity.

   To test the connectivity between the data center and the classic network, run the `ping` command in the data center to access an Elastic Compute Service (ECS) instance in the classic network.

4.Two-factor authentication

4.1. Set up two-factor authentication for Windows clients

This topic describes how to set up two-factor authentication for Windows clients to access virtual private clouds (VPCs).

Prerequisites

Before you start, make sure that the following requirements are met:

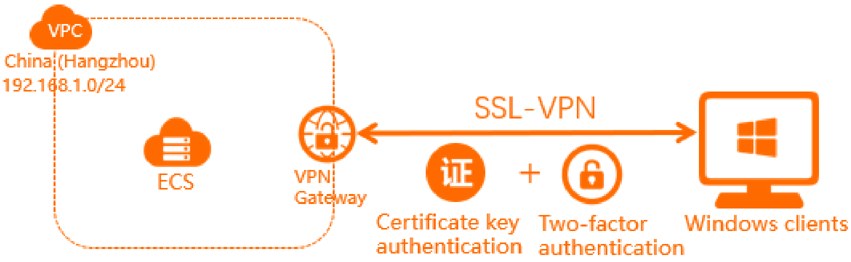
- An Identity as a Service (IDaaS) instance is purchased and the user information of the IDaaS instance is updated on Alibaba Cloud. For more information, see Organizations and Accounts.

  > **Note** IDaaS is a unified identity authentication service. IDaaS allows one account to access all services. After you enable and select an IDaaS instance, you must pass certificate key authentication and two-factor authentication when you use OpenVPN to initiate SSL-VPN connections. Then, you can access cloud resources in the cloud. This prevents unauthorized access and reinforces security.

- A VPC is created. For more information, see Create and manage a VPC.

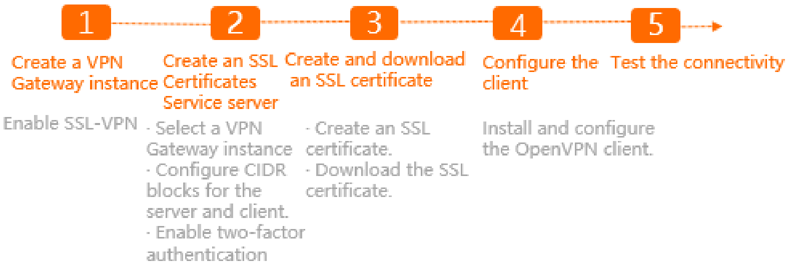
Context

In this example, a company has created a VPC in the China (Hangzhou) region and the CIDR block of the VPC is 192.168.1.0/24. Due to business requirements, staff on business trips need to access resources deployed in the VPC from Windows clients.



You can create a VPN gateway on Alibaba Cloud as shown in the preceding figure, configure an SSL-VPN server, and then enable two-factor authentication. To access a VPC from a Windows client over SSL-VPN connections, you must pass both SSL authentication and two-factor authentication. This improves the security and manageability of VPN connections.

Procedure


1
2
3
4
5
Create a VPN Gateway instance
Create an SSL Certificates Service server
Create and download an SSL certificate
Configure the client
Test the connectivity
Enable SSL-VPN
· Select a VPN Gateway instance
· Configure CIDR blocks for the server and client.
· Enable two-factor authentication
· Create an SSL certificate.
· Download the SSL certificate.
Install and configure the OpenVPN client.

Step 1: Create a VPN gateway

VPN Gateway is an Internet-based service that connects enterprise data centers, office networks, or Internet-facing terminals to Alibaba Cloud VPCs over encrypted connections.

> **Notice** Make sure that the VPN gateway was created after 00:00, March 5, 2020. Otherwise, two-factor authentication is not supported.

1.
2. In the top navigation bar, select the region where the VPC is deployed.

   In this example, the **China (Hangzhou)** region is selected.

   > **Note** Make sure that the VPN gateway and the VPC are deployed in the same region.

3. In the left-side navigation pane, choose **Interconnections > VPN > VPN Gateways**.
4. On the **VPN Gateways** page, click **Create VPN Gateway**.
5. On the buy page, set the following parameters and click **Buy Now** to complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway.
Region	Select the region where you want to create the VPN gateway. In this example, the **China (Hangzhou)** region is selected.
VPC	Select the VPC where you want to create the VPN gateway.
Specify VSwitch	Specify whether to deploy the VPN gateway in a vSwitch of the VPC. In this example, **No** is selected.
Maximum Bandwidth	Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
Traffic	Default value: **Pay-by-data-transfer**.
IPsec-VPN	You can enable or disable the IPsec-VPN feature. After you enable this feature, you can establish connections between a data center and a VPC or between two VPCs. In this example, **Disable** is selected.

Parameter	Description
SSL-VPN	You can enable or disable the SSL-VPN feature. After you enable this feature, you can connect to VPCs from clients over SSL-VPN connections. In this example, **Disable** is selected.
SSL Connections	Select the maximum number of concurrent SSL connections that the VPN gateway supports. **5** is selected in this example. ⓘ **Note** This parameter is available only if you choose to enable SSL-VPN.
Duration	Select a subscription duration. You can select only By Hour.

Step 2: Create an SSL server

SSL-VPN is based on the OpenVPN framework. You must use an SSL server to specify the CIDR blocks that you want to connect to and the CIDR blocks that clients use, and enable two-factor authentication.

1.
2. In the left-side navigation pane, choose **Interconnections > VPN > SSL Servers**.
3. In the top navigation bar, select the region where you want to create the SSL server.

   In this example, the **China (Hangzhou)** region is selected.
4. On the **SSL Servers** page, click **Create SSL Server**.
5. In the **Create SSL Server** panel, set the following parameters and click **OK**.
   - **Name**: Enter a name for the SSL server.
   - **VPN Gateway**: Select the VPN gateway that you created in Step 1.
   - **Local Network**: Enter the CIDR block to be accessed by the client over the SSL-VPN connection. **192.168.0.0/24** is used in this example.
   - **Client Subnet**: Enter a CIDR block that the client uses when the client is connected to the SSL server. **10.0.0.0/24** is used in this example.
   - **Advanced Configuration**: Enable advanced configurations and set the following parameters.
     - **Protocol**: Select the protocol for the SSL-VPN connection. Valid values: UDP and TCP. In this example, the default setting is used.
     - **Port**: Enter the port number used in the SSL-VPN connection. In this example, the default setting is used.
     - **Encryption Algorithm**: The encryption algorithm used in the SSL-VPN connection. Supported encryption algorithms include AES-128-CBC, AES-192-CBC, and AES-256-CBC. In this example, the default setting is used.
     - **Enable Compression**: Specify whether to compress the transmitted data. In this example, the default setting is used.

- **Two-factor Authentication**: Enable two-factor authentication and select an IDaaS instance.

> **Note** If this is your first time using two-factor authentication, you must authorize the VPN gateway to access the IDaaS instance before you create the SSL server.

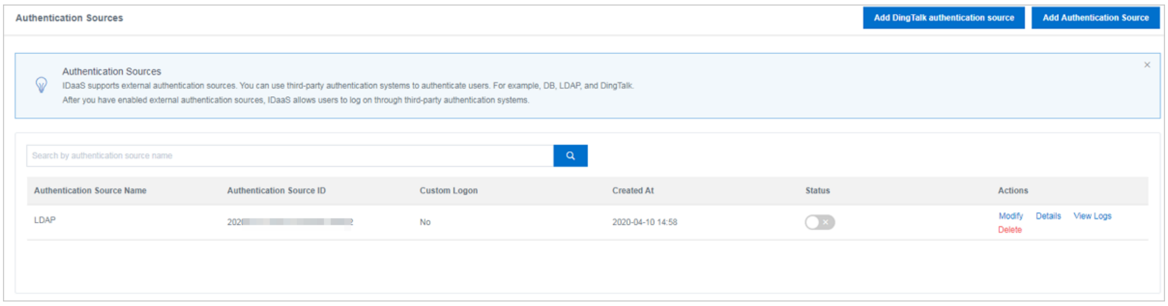
Step 3 (optional): Configure Active Directory (AD) authentication for cloud services

By default, you can use the username and password of IDaaS for two-factor authentication. You can also use Active Directory (AD) authentication. After you complete the configuration, SSL-VPN supports AD authentication. If you only use the username and password of the IDaaS instance for authentication, skip this step.

1. Log on to the IDaaS console.
2. On the **Instances** page, find the IDaaS instance you want to manage and click **Management** in the **Actions** column.
3. In the left-side navigation pane, choose **Authentication > Authentication Source** and click **Add Authentication Source**.
4. On the **Add Authentication Source** page, find **LDAP** and click **Add Authentication Source** in the **Actions** column.
5. In the **Add Authentication Source (LDAP)** dialog box, create an LDAP authentication source.

   For more information, see LDAP as Authentication Source.

   After you create an authentication source, you can view it.



Authentication Sources
Add DingTalk authentication source
Add Authentication Source

Authentication Sources

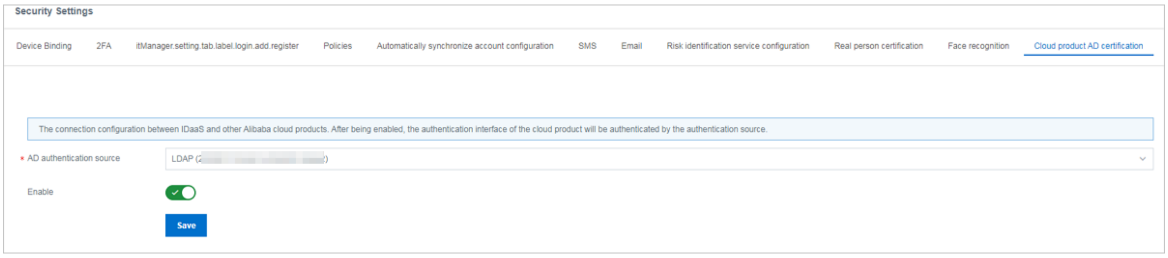
IDaaS supports external authentication sources. You can use third-party authentication systems to authenticate users. For example, DB, LDAP, and DingTalk.

After you have enabled external authentication sources, IDaaS allows users to log on through third-party authentication systems.

Search by authentication source name

Authentication Source Name	Authentication Source ID	Custom Logon	Created At	Status	Actions
LDAP	202[redacted]	No	2020-04-10 14:58	○	Modify Details View Logs Delete

6. On the **Authentication Source** page, find the authentication source that you want to manage, click ○ in the **Status** column, and then click **OK** in the dialog box that appears.
7. In the left-side navigation pane, choose **Settings > Security Settings**.
8. On the **Security Settings** page, click the **Cloud Product AD Authentication** tab.
9. Select the AD authentication source that you have created, enable this feature, and then click **Save**.



Security Settings
Device Binding
2FA
itManager.setting.tab.label.login.add.register
Policies
Automatically synchronize account configuration
SMS
Email
Risk identification service configuration
Real person certification
Face recognition
Cloud product AD certification

The connection configuration between IDaaS and other Alibaba cloud products. After being enabled, the authentication interface of the cloud product will be authenticated by the authentication source.

* AD authentication source: LDAP ([redacted])

Enable: ✓

Step 4: Create and download an SSL client certificate

Create and download an SSL client certificate based on the configurations of the SSL server.

1.
2. In the left-side navigation pane, choose **Interconnections > VPN > SSL Clients**.
3. In the top navigation bar, select the region where the SSL client is deployed.

   In this example, the **China (Hangzhou)** region is selected.
4. On the **SSL Clients** page, click **Create Client Certificate**.
5. In the **Create Client Certificate** panel, set the following parameters and click **OK**.
   - **Name**: Enter a name for the SSL client certificate.
   - **SSL Server**: Select the SSL server created in Step 2.
6. On the **SSL Clients** page, find the SSL client certificate and click **Download** in the **Actions** column.

   The SSL client certificate is downloaded to your on-premises machine.

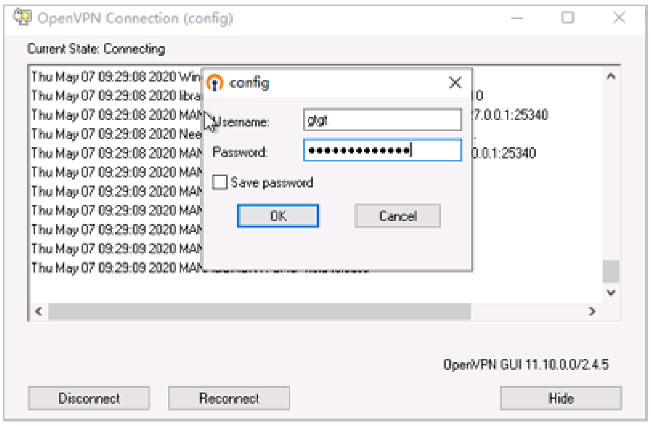
Step 5: Configure the Windows client

Perform the following steps to configure the Windows client.

1. Download and install OpenVPN.

   Download OpenVPN.
2. Extract the certificate from the package downloaded in Step 4 and copy the certificate to *OpenVPN\config*.

   In this example, the certificate is copied to *C:\Program Files\OpenVPN\config*. You must copy the certificate to the directory where the OpenVPN client is installed.
3. Start the OpenVPN client and enter the username and password for authentication.



OpenVPN Connection (config)

Current State: Connecting

```
Thu May 07 09:29:08 2020 Win                              0
Thu May 07 09:29:08 2020 libra
Thu May 07 09:29:08 2020 MAN                              7.0.0.1:25340
Thu May 07 09:29:08 2020 Nee
Thu May 07 09:29:08 2020 MAN                              0.0.1:25340
Thu May 07 09:29:09 2020 MAN
Thu May 07 09:29:09 2020 MAN
Thu May 07 09:29:09 2020 MAN
Thu May 07 09:29:09 2020 MAN
Thu May 07 09:29:09 2020 MAN
Thu May 07 09:29:09 2020 MAN
```

config

Username: gtgt

Password: •••••••••••••

□ Save password

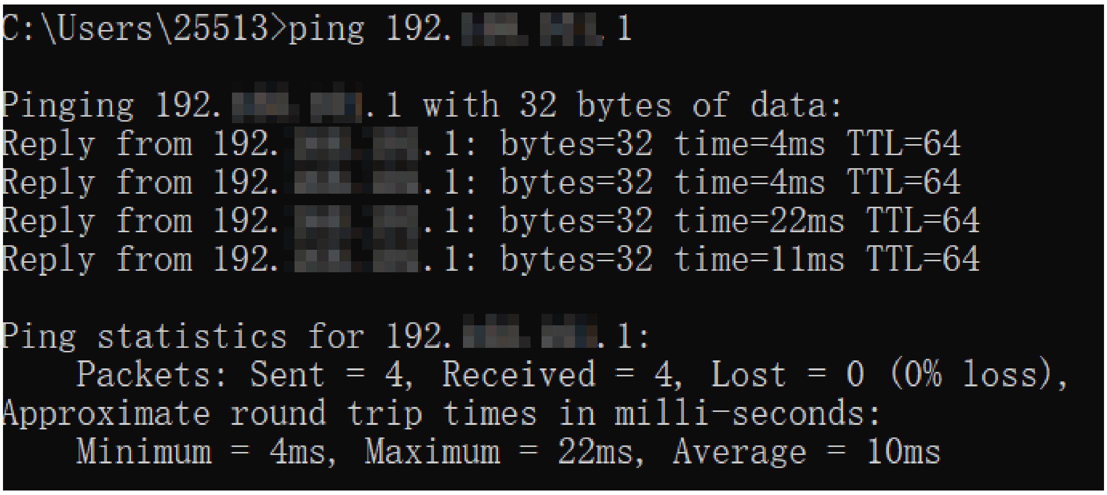
Step 6: Test the connectivity

Perform the following steps to test the connectivity between the Windows client and VPC:

1. Open the CLI on the Windows client.
2. Run the `ping` command to `ping` the IP address of an Elastic Compute Service (ECS) instance deployed in the VPC. This command is used to test the connectivity between the Windows client and the VPC.

> Note Make sure that the security group rules of the ECS instance allow remote access from the Windows client. For more information, see Security groups for different use casesConfiguration guide for ECS security groups.

The test result shows that the Windows client can access the ECS instance.



```
C:\Users\25513>ping 192.[redacted] [redacted].1

Pinging 192.[redacted] [redacted].1 with 32 bytes of data:
Reply from 192.[redacted] [redacted].1: bytes=32 time=4ms TTL=64
Reply from 192.[redacted] [redacted].1: bytes=32 time=4ms TTL=64
Reply from 192.[redacted] [redacted].1: bytes=32 time=22ms TTL=64
Reply from 192.[redacted] [redacted].1: bytes=32 time=11ms TTL=64

Ping statistics for 192.[redacted] [redacted].1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 22ms, Average = 10ms
```

4.2. Enable two-factor authentication for Linux clients

This topic describes how to enable two-factor (username and password) authentication to authenticate SSL-VPN requests from Linux clients to virtual private clouds (VPCs).

Prerequisites

Before you start, make sure that the following requirements are met:

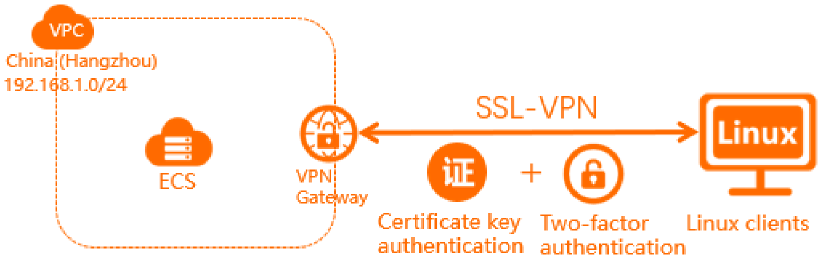
- An Identity as a Service (IDaaS) instance is purchased and the user information of the IDaaS instance is updated on Alibaba Cloud. For more information, see Organizations and Accounts.

  > Note IDaaS is a unified identity authentication service. IDaaS allows one account to access all services. After you enable and select an IDaaS instance, you must pass certificate key authentication and two-factor authentication when you use OpenVPN to initiate SSL-VPN connections. Then, you can access cloud resources in the cloud. This prevents unauthorized access and reinforces security.

- A VPC is created. For more information, see Create and manage a VPC.

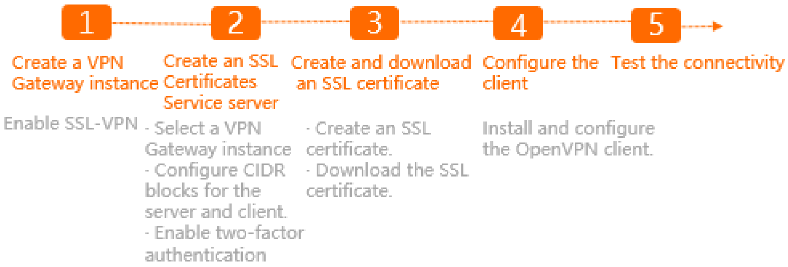
Scenario

In this example, a company has created a VPC in the China (Hangzhou) region and the CIDR block of the VPC is 192.168.1.0/24. Due to business requirements, employees on business trips need to access resources deployed in the VPC from Linux clients.



You can create a VPN gateway on Alibaba Cloud as shown in the preceding figure, configure an SSL-VPN server, and then enable two-factor authentication. To access resources in the VPC from Linux clients over SSL-VPN connections, you must first pass certificate key authentication and two-factor authentication. This reinforces security and facilitates management of VPN connections.

Procedure


1
Create a VPN Gateway instance
Enable SSL-VPN
2
Create an SSL Certificates Service server
· Select a VPN Gateway instance
· Configure CIDR blocks for the server and client.
· Enable two-factor authentication
3
Create and download an SSL certificate
· Create an SSL certificate.
· Download the SSL certificate.
4
Configure the client
Install and configure the OpenVPN client.
5
Test the connectivity

Step 1: Create a VPN gateway

VPN Gateway is an Internet-based service that connects enterprise data centers, office networks, or Internet-facing terminals to Alibaba Cloud VPCs over encrypted connections.

> **Notice** Make sure that the VPN gateway was created after 00:00, March 5, 2020. Otherwise, two-factor authentication is not supported.

1.
2. In the top navigation bar, select the region where the VPC is deployed.

   In this example, the **China (Hangzhou)** region is selected.

   > **Note** Make sure that the VPN gateway and the VPC are deployed in the same region.

3. In the left-side navigation pane, choose **Interconnections > VPN > VPN Gateways**.
4. On the **VPN Gateways** page, click **Create VPN Gateway**.
5. On the buy page, set the following parameters and click **Buy Now** to complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway.
Region	Select the region where you want to create the VPN gateway. In this example, the **China (Hangzhou)** region is selected.
VPC	Select the VPC where you want to create the VPN gateway.

Parameter	Description
Specify VSwitch	Specify whether to deploy the VPN gateway in a vSwitch of the VPC. In this example, **No** is selected.
Maximum Bandwidth	Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
Traffic	Default value: **Pay-by-data-transfer**.
IPsec-VPN	You can enable or disable the IPsec-VPN feature. After you enable this feature, you can establish connections between a data center and a VPC or between two VPCs. In this example, **Disable** is selected.
SSL-VPN	You can enable or disable the SSL-VPN feature. After you enable this feature, you can connect to VPCs from clients over SSL-VPN connections. In this example, **Disable** is selected.
SSL Connections	Select the maximum number of concurrent SSL connections that the VPN gateway supports. **5** is selected in this example. ⓘ **Note** This parameter is available only if you choose to enable SSL-VPN.
Duration	Select a subscription duration. You can select only By Hour.

Step 2: Create an SSL server

SSL-VPN is based on the OpenVPN framework. You must use an SSL server to specify the CIDR blocks that you want to connect to and the CIDR blocks that clients use, and enable two-factor authentication.

1.
2. In the left-side navigation pane, choose **Interconnections > VPN > SSL Servers**.
3. In the top navigation bar, select the region where you want to create the SSL server.

   In this example, the **China (Hangzhou)** region is selected.
4. On the **SSL Servers** page, click **Create SSL Server**.
5. In the **Create SSL Server** panel, set the following parameters and click **OK**.
   - **Name**: Enter a name for the SSL server.
   - **VPN Gateway**: Select the VPN gateway that you created in Step 1.
   - **Local Network**: Enter the CIDR block to be accessed by the client over the SSL-VPN connection. **192.168.0.0/24** is used in this example.
   - **Client Subnet**: Enter a CIDR block that the client uses when the client is connected to the SSL server. **10.0.0.0/24** is used in this example.

- **Advanced Configuration**: Enable advanced configurations and set the following parameters.
    - **Protocol**: Select the protocol for the SSL-VPN connection. Valid values: UDP and TCP. In this example, the default setting is used.
    - **Port**: Enter the port number used in the SSL-VPN connection. In this example, the default setting is used.
    - **Encryption Algorithm**: The encryption algorithm used in the SSL-VPN connection. Supported encryption algorithms include AES-128-CBC, AES-192-CBC, and AES-256-CBC. In this example, the default setting is used.
    - **Enable Compression**: Specify whether to compress the transmitted data. In this example, the default setting is used.
    - **Two-factor Authentication**: Enable two-factor authentication and select an IDaaS instance.

    > **Note** If this is your first time using two-factor authentication, you must authorize the VPN gateway to access the IDaaS instance before you create the SSL server.

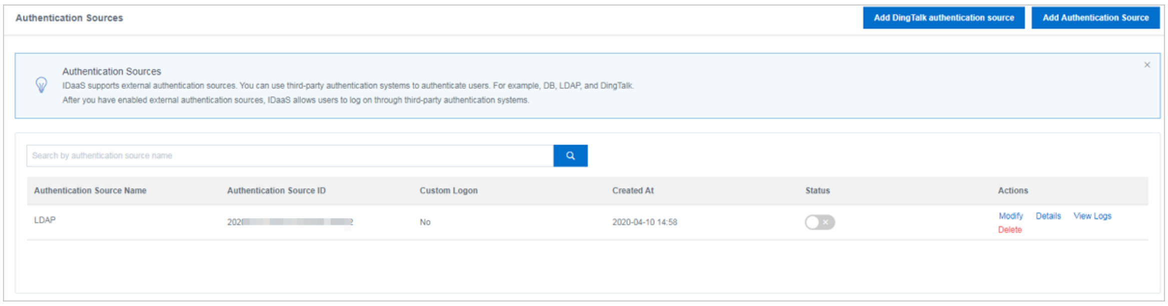
Step 3 (optional): Configure Active Directory (AD) authentication for cloud services

By default, you can use the username and password of IDaaS for two-factor authentication. You can also use Active Directory (AD) authentication. After you complete the configuration, SSL-VPN supports AD authentication. If you only use the username and password of the IDaaS instance for authentication, skip this step.

1. Log on to the IDaaS console.
2. On the **Instances** page, find the IDaaS instance you want to manage and click **Management** in the **Actions** column.
3. In the left-side navigation pane, choose **Authentication > Authentication Source** and click **Add Authentication Source**.
4. On the **Add Authentication Source** page, find **LDAP** and click **Add Authentication Source** in the **Actions** column.
5. In the **Add Authentication Source (LDAP)** dialog box, create an LDAP authentication source.

    For more information, see LDAP as Authentication Source.

    After you create an authentication source, you can view it.

    Authentication Sources
Add DingTalk authentication source
Add Authentication Source

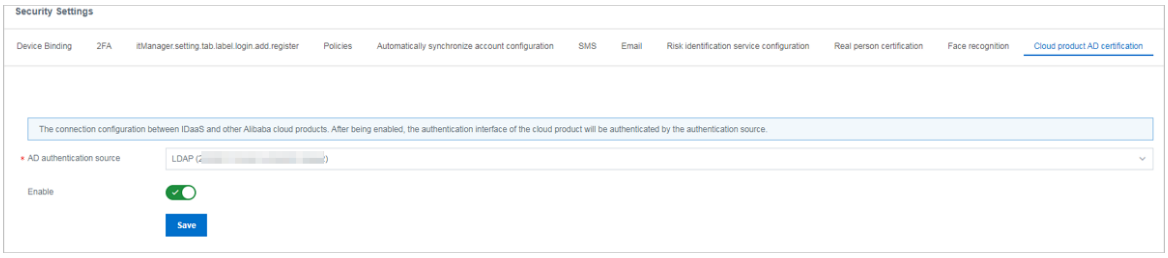
    Authentication Sources
    IDaaS supports external authentication sources. You can use third-party authentication systems to authenticate users. For example, DB, LDAP, and DingTalk.
    After you have enabled external authentication sources, IDaaS allows users to log on through third-party authentication systems.

    Search by authentication source name

Authentication Source Name	Authentication Source ID	Custom Logon	Created At	Status	Actions
LDAP	202[redacted]	No	2020-04-10 14:58	○ ✕	Modify Details View Logs Delete

6. On the **Authentication Source** page, find the authentication source that you want to manage, click ○ ✕ in the **Status** column, and then click **OK** in the dialog box that appears.

7. In the left-side navigation pane, choose **Settings** > **Security Settings**.
8. On the **Security Settings** page, click the **Cloud Product AD Authentication** tab.
9. Select the AD authentication source that you have created, enable this feature, and then click **Save**.


Security Settings
Device Binding
2FA
itManager.setting.tab.label.login.add.register
Policies
Automatically synchronize account configuration
SMS
Email
Risk identification service configuration
Real person certification
Face recognition
Cloud product AD certification
Save

The connection configuration between IDaaS and other Alibaba cloud products. After being enabled, the authentication interface of the cloud product will be authenticated by the authentication source.

* AD authentication source: LDAP ([redacted])

Enable: ✓

Step 4: Create and download an SSL client certificate

Create and download an SSL client certificate based on the configurations of the SSL server.

1.
2. In the left-side navigation pane, choose **Interconnections** > **VPN** > **SSL Clients**.
3. In the top navigation bar, select the region where the SSL client is deployed.

   In this example, the **China (Hangzhou)** region is selected.
4. On the **SSL Clients** page, click **Create Client Certificate**.
5. In the **Create Client Certificate** panel, set the following parameters and click **OK**.
   - **Name**: Enter a name for the SSL client certificate.
   - **SSL Server**: Select the SSL server created in Step 2.
6. On the **SSL Clients** page, find the SSL client certificate and click **Download** in the **Actions** column.

   The SSL client certificate is downloaded to your on-premises machine.

Step 5: Configure the client

Perform the following steps to configure the Linux client:

1. Run the following command on the Linux client to install OpenVPN:

   ```
   yum install -y openvpn
   ```
2. Extract and copy the certificate downloaded in Step 4 to the */etc/openvpn/conf/* directory.

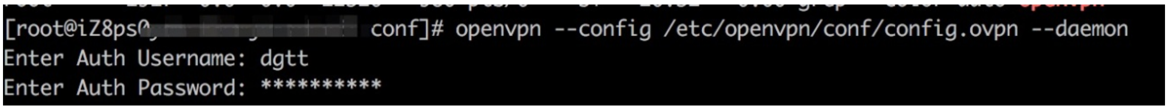
   i. Run the following command to copy the file to the configuration directory:

   ```
   cp cert_location /usr/local/etc/openvpn/conf/
   ```

   ii. Run the following command to extract the certificate:

   ```
   unzip /usr/local/etc/openvpn/conf/certs6.zip
   ```
3. Run the following command to start OpenVPN, and enter the username and password for authentication:

   ```
   openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   ```



```
[root@iZ8ps0[redacted] conf]# openvpn --config /etc/openvpn/conf/config.ovpn --daemon
Enter Auth Username: dgtt
Enter Auth Password: **********
```

Step 6: Test the connectivity

Perform the following steps to test the connectivity between the Linux client and the VPC:

1. Log on to the Linux client.
2. Run the `ping` command to ping the IP address of an Elastic Compute Service (ECS) instance in the VPC to test the connectivity.

   > **Note** Make sure that the security group rules of the ECS instance allow remote access from Linux clients. For more information, see Configure security groups in different scenarios.

   The test result shows that the Linux client can access the ECS instance.

4.3. Enable two-factor authentication for macOS clients

This topic describes how to enable two-factor authentication to authenticate access from macOS clients to virtual private clouds (VPCs).

Prerequisites

Before you start, make sure that the following requirements are met:

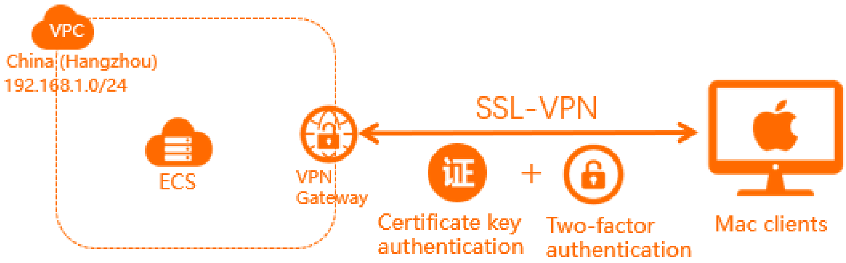
- An Identity as a Service (IDaaS) instance is purchased and the user information of the IDaaS instance is updated on Alibaba Cloud. For more information, see Organizations and Accounts.

  > **Note** IDaaS is a unified identity authentication service. IDaaS allows one account to access all services. After you enable and select an IDaaS instance, you must pass certificate key authentication and two-factor authentication when you use OpenVPN to initiate SSL-VPN connections. Then, you can access cloud resources in the cloud. This prevents unauthorized access and reinforces security.

- A VPC is created. For more information, see Create and manage a VPC.
- Homebrew is installed. If Homebrew is not installed, install Homebrew first.

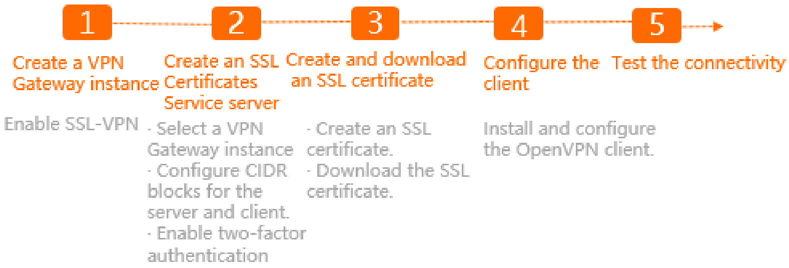
Scenario

In this example, a company has created a VPC in the China (Hangzhou) region and the CIDR block of the VPC is 192.168.1.0/24. Due to business requirements, employees on business trips need to access resources deployed in the VPC from macOS clients.



You can create a VPN gateway on Alibaba Cloud as shown in the preceding figure, configure an SSL-VPN server, and then enable two-factor authentication. To access resources in the VPC from macOS clients over SSL-VPN connections, you must first pass certificate key authentication and two-factor authentication. This reinforces security and facilitates management of VPN connections.

Procedure


1
Create a VPN Gateway instance
Enable SSL-VPN
2
Create an SSL Certificates Service server
· Select a VPN Gateway instance
· Configure CIDR blocks for the server and client.
· Enable two-factor authentication
3
Create and download an SSL certificate
· Create an SSL certificate.
· Download the SSL certificate.
4
Configure the client
Install and configure the OpenVPN client.
5
Test the connectivity

Step 1: Create a VPN gateway

VPN Gateway is an Internet-based service that connects enterprise data centers, office networks, or Internet-facing terminals to Alibaba Cloud VPCs over encrypted connections.

> **Notice** Make sure that the VPN gateway was created after 00:00, March 5, 2020. Otherwise, two-factor authentication is not supported.

1.
2. In the top navigation bar, select the region where the VPC is deployed.

   In this example, the **China (Hangzhou)** region is selected.

   > **Note** Make sure that the VPN gateway and the VPC are deployed in the same region.

3. In the left-side navigation pane, choose **Interconnections** > **VPN** > **VPN Gateways**.
4. On the **VPN Gateways** page, click **Create VPN Gateway**.
5. On the buy page, set the following parameters and click **Buy Now** to complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway.

Parameter	Description
Region	Select the region where you want to create the VPN gateway. In this example, the **China (Hangzhou)** region is selected.
VPC	Select the VPC where you want to create the VPN gateway.
Specify VSwitch	Specify whether to deploy the VPN gateway in a vSwitch of the VPC. In this example, **No** is selected.
Maximum Bandwidth	Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
Traffic	Default value: **Pay-by-data-transfer**.
IPsec-VPN	You can enable or disable the IPsec-VPN feature. After you enable this feature, you can establish connections between a data center and a VPC or between two VPCs. In this example, **Disable** is selected.
SSL-VPN	You can enable or disable the SSL-VPN feature. After you enable this feature, you can connect to VPCs from clients over SSL-VPN connections. In this example, **Disable** is selected.
SSL Connections	Select the maximum number of concurrent SSL connections that the VPN gateway supports. **5** is selected in this example. ? **Note** This parameter is available only if you choose to enable SSL-VPN.
Duration	Select a subscription duration. You can select only By Hour.

Step 2: Create an SSL server

SSL-VPN is based on the OpenVPN framework. You must use an SSL server to specify the CIDR blocks that you want to connect to and the CIDR blocks that clients use, and enable two-factor authentication.

1.
2. In the left-side navigation pane, choose **Interconnections > VPN > SSL Servers**.
3. In the top navigation bar, select the region where you want to create the SSL server.

   In this example, the **China (Hangzhou)** region is selected.
4. On the **SSL Servers** page, click **Create SSL Server**.
5. In the **Create SSL Server** panel, set the following parameters and click **OK**.
   - **Name**: Enter a name for the SSL server.
   - **VPN Gateway**: Select the VPN gateway that you created in Step 1.
   - **Local Network**: Enter the CIDR block to be accessed by the client over the SSL-VPN connection.

192.168.0.0/24 is used in this example.

- **Client Subnet**: Enter a CIDR block that the client uses when the client is connected to the SSL server. **10.0.0.0/24** is used in this example.
- **Advanced Configuration**: Enable advanced configurations and set the following parameters.
  - **Protocol**: Select the protocol for the SSL-VPN connection. Valid values: UDP and TCP. In this example, the default setting is used.
  - **Port**: Enter the port number used in the SSL-VPN connection. In this example, the default setting is used.
  - **Encryption Algorithm**: The encryption algorithm used in the SSL-VPN connection. Supported encryption algorithms include AES-128-CBC, AES-192-CBC, and AES-256-CBC. In this example, the default setting is used.
  - **Enable Compression**: Specify whether to compress the transmitted data. In this example, the default setting is used.
  - **Two-factor Authentication**: Enable two-factor authentication and select an IDaaS instance.

    > ⓘ **Note** If this is your first time using two-factor authentication, you must authorize the VPN gateway to access the IDaaS instance before you create the SSL server.

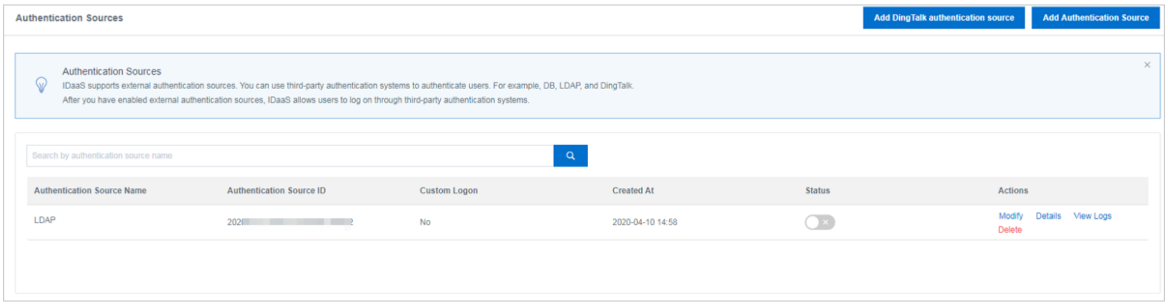
Step 3 (optional): Configure Active Directory (AD) authentication for cloud services

By default, you can use the username and password of IDaaS for two-factor authentication. You can also use Active Directory (AD) authentication. After you complete the configuration, SSL-VPN supports AD authentication. If you only use the username and password of the IDaaS instance for authentication, skip this step.

1. Log on to the IDaaS console.
2. On the **Instances** page, find the IDaaS instance you want to manage and click **Management** in the **Actions** column.
3. In the left-side navigation pane, choose **Authentication > Authentication Source** and click **Add Authentication Source**.
4. On the **Add Authentication Source** page, find **LDAP** and click **Add Authentication Source** in the **Actions** column.
5. In the **Add Authentication Source (LDAP)** dialog box, create an LDAP authentication source.

   For more information, see LDAP as Authentication Source.

   After you create an authentication source, you can view it.



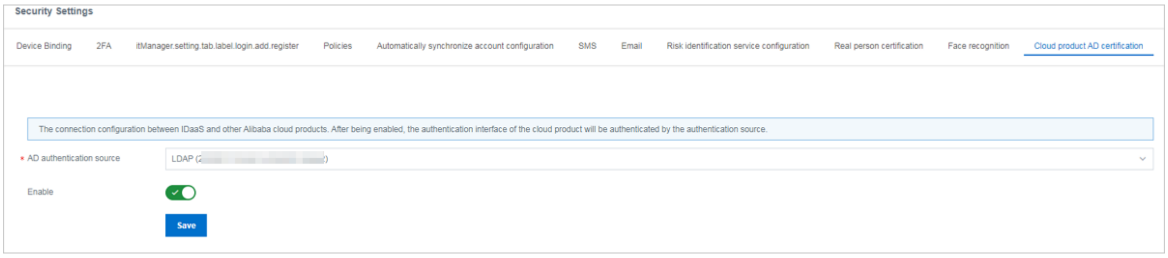
Authentication Sources
Add DingTalk authentication source
Add Authentication Source
Search by authentication source name

Authentication Sources

IDaaS supports external authentication sources. You can use third-party authentication systems to authenticate users. For example, DB, LDAP, and DingTalk.
After you have enabled external authentication sources, IDaaS allows users to log on through third-party authentication systems.

Authentication Source Name	Authentication Source ID	Custom Logon	Created At	Status	Actions
LDAP	202[redacted]	No	2020-04-10 14:58	✕	Modify Details View Logs Delete

6. On the **Authentication Source** page, find the authentication source that you want to manage, click ○✕ in the **Status** column, and then click **OK** in the dialog box that appears.
7. In the left-side navigation pane, choose **Settings** > **Security Settings**.
8. On the **Security Settings** page, click the **Cloud Product AD Authentication** tab.
9. Select the AD authentication source that you have created, enable this feature, and then click **Save**.


Security Settings
Device Binding
2FA
itManager.setting.tab.label.login.add.register
Policies
Automatically synchronize account configuration
SMS
Email
Risk identification service configuration
Real person certification
Face recognition
Cloud product AD certification
Save

The connection configuration between IDaaS and other Alibaba cloud products. After being enabled, the authentication interface of the cloud product will be authenticated by the authentication source.

* AD authentication source: LDAP ([redacted])

Enable: ✓

Step 4: Create and download an SSL client certificate

Create and download an SSL client certificate based on the configurations of the SSL server.

1.
2. In the left-side navigation pane, choose **Interconnections** > **VPN** > **SSL Clients**.
3. In the top navigation bar, select the region where the SSL client is deployed.

   In this example, the **China (Hangzhou)** region is selected.
4. On the **SSL Clients** page, click **Create Client Certificate**.
5. In the **Create Client Certificate** panel, set the following parameters and click **OK**.
   - **Name**: Enter a name for the SSL client certificate.
   - **SSL Server**: Select the SSL server created in Step 2.
6. On the **SSL Clients** page, find the SSL client certificate and click **Download** in the **Actions** column.

   The SSL client certificate is downloaded to your on-premises machine.

Step 5: Configure the client

Perform the following steps to configure the macOS client:

1. Run the following command on the macOS client to install OpenVPN:

```
brew install openvpn
```

> **Note** We recommend that you install Homebrew.

2. Run the following command to delete the default configuration file:

```
rm /usr/local/etc/openvpn/*
```

3. Run the following command to copy the file to the configuration directory:

```
cp cert_location /usr/local/etc/openvpn/
```

In the preceding command, replace `cert_location` with the directory of the certificate downloaded in Step 4. For example: */Users/example/Downloads/certs.zip*.

4. Run the following commands to extract the certificate downloaded in Step 4:

```
cd  /usr/local/etc/openvpn
unzip /usr/local/etc/openvpn/certs.zip
```

5. Run the following command to establish a connection and enter the username and password for authentication.

```
sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
```

Step 6: Test the connectivity

Perform the following steps to test the connectivity between the macOS client and the VPC:

1. Open the CLI of the macOS client.
2. Run the `ping` command to ping the IP address of an Elastic Compute Service (ECS) instance in the VPC to test the connectivity.

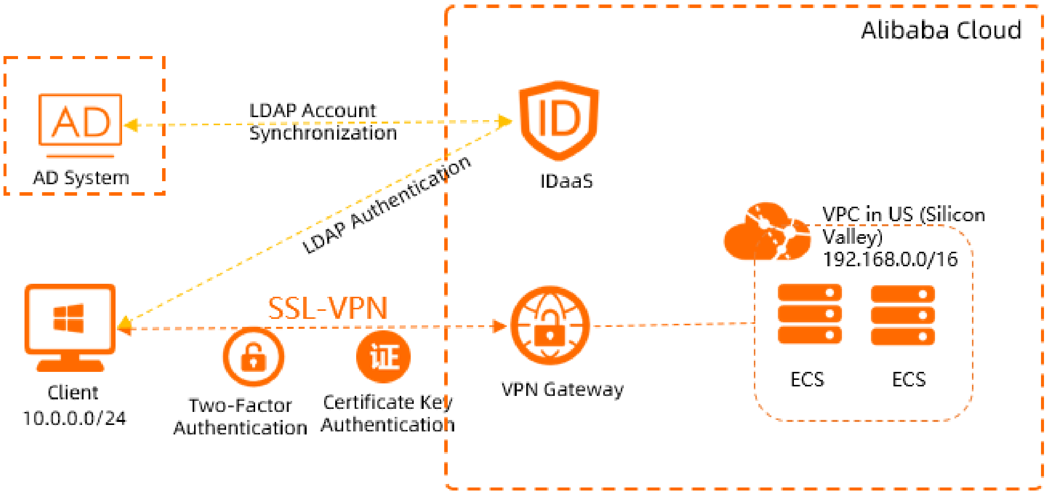
> **Note** Make sure that the security group rules of the ECS instance allow remote access from macOS clients. For more information, see Configure security groups in different scenarios.

4.4. Establish an SSL-VPN connection by using LDAP authentication

This topic describes how to establish an SSL-VPN connection by using the Lightweight Directory Access Protocol (LDAP) authentication feature of Identity as a Service (IDaaS).

Context

A company has created a virtual private cloud (VPC) in the US (Silicon Valley) region. The CIDR block of the VPC is 192.168.0.0/16. Due to business requirements, staff on business trips need to access resources deployed in the VPC from remote clients.


Alibaba Cloud
AD
AD System
LDAP Account Synchronization
ID
IDaaS
LDAP Authentication
VPC in US (Silicon Valley) 192.168.0.0/16
SSL-VPN
Client 10.0.0.0/24
Two-Factor Authentication
证
Certificate Key Authentication
VPN Gateway
ECS
ECS

The company has built an Active Directory (AD) system. For security purposes, the company requires that staff must pass identity authentication provided by the AD system before the staff can access resources deployed in the VPC.

You can create a VPN gateway in the cloud, configure the SSL server, enable two-factor authentication, and specify an IDaaS instance to perform LDAP authentication. Before an employee can log on to the OpenVPN client and establish an SSL-VPN connection, the employee must pass the LDAP authentication provided by the IDaaS system. The LDAP authentication sends the username and password provided by the employee to the AD system, and returns a result. Only after the employee passes the authentication, the VPN gateway establishes an SSL-VPN connection. Then, the employee can use the SSL-VPN connection to access resources deployed on the VPC.

Prerequisites

Before you start, make sure that the following requirements are met:

- A Standard Edition IDaaS instance is purchased.

  In this example, a Standard Edition IDaaS instance is purchased in the Singapore (Singapore) region.

- A VPC is created. For more information, see Create and manage a VPC.

  In this example, a VPC is created in the US (Silicon Valley) region and the CIDR block of the VPC is 192.168.0.0/16. The CIDR block of the Elastic Compute Service (ECS) instance is 192.168.0.0/24.

- The public IP address and service port of the server (LDAP server) where the AD system is deployed are obtained.

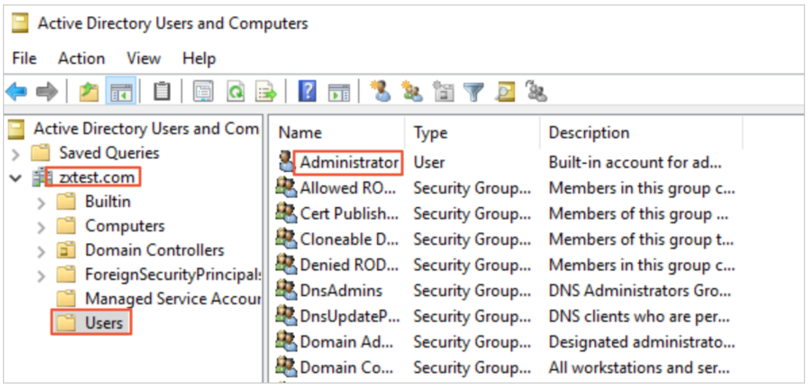
  In this example, the AD system is deployed on a server that runs Windows Server 2019. The public IP address of the server is *47.XX.XX.8* and the service port is *389*.

- The Base DN of the LDAP server is obtained.

  In this example, the Base DN of the LDAP server is *dc=zxtest,dc=com*.

- The DN, username, and password of the administrator of the LDAP server are obtained.

  In this example, the administrator username is Administrator and the password is 1****2. The administrator DN is *cn=Administrator,cn=Users,dc=zxtest,dc=com*, as shown in the following figure.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...

Procedure

1
Enable LDAP Authentication
2
Deploy SSL-VPN
3
Configure the Client
4
Test the Connectivity

Step 1: Enable LDAP authentication

Before you can establish an SSL-VPN connection, you must enable LDAP authentication in the IDaaS instance and synchronize Alibaba Cloud account data for further authentication.

1. Add the LDAP authentication source.

   i. Log on to the IDaaS console.

   ii. On the **Instances** page, find the IDaaS instance and click its ID.

   iii. In the left-side navigation pane, click **Authentication Sources**.

   iv. In the upper-right corner of the **Authentication Sources** page, click **Add Authentication Source**.

   v. On the **Add Authentication Source** page, find LDAP and click **Add Authentication Source** in the **Actions** column.

   vi. In the **Add Authentication Source (LDAP)** panel, set the following parameters and click **Submit**.

   - **ID**: This value is automatically generated by the system.
   - **Name**: Enter a custom name.
   - **LDAP URL**: Enter the URL of the LDAP server. The LDAP server refers to the server where the AD system is deployed. Enter the address in the following format: *ldap://127.0.0.1:389/*. In this example, *ldap://47.XX.XX.8:389/* is used.

     If the server uses an IPv6 address, set the value in the following format: *ldap://[0000:0000:0000:0000:0000:0000:0001]:389/*.

     > **Note** IDaaS can be accessed only over the Internet. The LDAP server must provide a public IP address and open port 389. You can configure the security group of the LDAP server to allow only the public IP address of IDaaS to access the LDAP server. For more information about the public IP address of IDaaS, submit a ticket to consult the Alibaba Cloud IDaaS team.

   - **LDAP Base**: Enter the Base DN of the LDAP server. *dc=zxtest,dc=com* is used in this example.
   - **LDAP Account**: Enter the administrator account DN of the LDAP server. *cn=Administrator,cn=Users,dc=zxtest,dc=com* is used in this example.
   - **LDAP account password**: Enter the password of the administrator of the LDAP server.
   - **Filter Condition**: Enter the filter condition used to query account names. *(sAMAccountName=$username$)* is used in this example.

     For more information about filter conditions, see LDAP Filters. $username$ specifies the IDaaS username and is a fixed value.

   For more information, see LDAP as Authentication Source.

   vii. On the **Authentication Source** page, find the authentication source, click in the **Status** column, and then click **OK** in the dialog box that appears to enable the authentication source.

2. Synchronize the LDAP account configurations by importing the account data of the LDAP server to the IDaaS system.

   i. In the left-side navigation pane, click **Organizations and Groups**.

   ii. In the upper-right corner of the **Organizations and Groups** page, click **Configure LDAP**. In the **Configure LDAP** panel, click **Create**.

   iii. On the **Server Connection** tab of the **Configure LDAP** panel, set the following parameters and click **Save**.

      - **AD/LDAP Name**: Enter a custom name.
      - **Server Address**: Enter the public IP address of the LDAP server. In this example, *47.XX.XX.8* is used.
      - **Port Number**: Enter the number of the port used by the LDAP server to provide services. *389* is used in this example.
      - **Base DN**: Enter the Base DN of the account with which you want to synchronize. *dc=zxtest,dc=com* is used in this example.

        > **Note** After you specify the Base DN, you cannot change it. If the **Base DN** is changed when IDaaS synchronizes data with LDAP or AD, the synchronization will fail because the organization directories of IDaaS and LDAP or AD do not match. If you want to synchronize data of different directories, we recommend that you add multiple LDAP configurations.

      - **Administrator DN**: Enter the administrator DN. *cn=Administrator,cn=Users,dc=zxtest,dc=com* is used in this example.
      - **Password**: Enter the password of the administrator.
      - **Select Type**: Select the type of your LDAP server. **Windows AD** is selected in this example.
      - **Owned OU node**: Select the IDaaS organization node to which account data is imported. If you ignore this parameter, data is imported to the root organization unit (OU). The default value is used in this example.
      - **From LDAP to IDaaS**: If you select Enable, you can manually synchronize data from the LDAP server to the IDaaS system. **Enable** is selected in this example.
      - **Provision from IDaaS to LDAP**: If you select Enable, data from the IDaaS system can be automatically synchronized to the LDAP server. **Enable** is selected in this example.

      After you set the preceding parameters, you can click **Connection** to test the connectivity. If the test fails, check the network connectivity and whether the parameters are correctly set.

iv. On the **Field Matching Rules** tab of the **Configure LDAP** panel, set the following parameters and click **Save**.

Field matching rules are used to match the fields of the IDaaS system with the attributes of the LDAP server. For example, the cn field of the LDAP server corresponds to the username of the IDaaS system.

- **Username**: cn is used in this example.

> **Note** If the value of the cn field is set in Chinese in the AD system, the field cannot be matched with the IDaaS system. We recommend that you use the sAMAccountName field.

- **External ID**: If the type of the LDAP server is Windows AD, enter objectGUID. If the type of the LDAP server is OpenLdap, enter uid. objectGUID is used in this example.
- **Password Attribute**: If the type of the LDAP server is Windows AD, enter unicodePwd. If the type of the LDAP server is OpenLdap, enter userPassword. unicodePwd is used in this example.
- **User Unique Identifier**: If the type of the LDAP server is Windows AD, enter DistinguishedName. If the type of the LDAP server is OpenLdap, enter EntryDN. DistinguishedName is used in this example.
- **Email**: mail is used in this example.

For more information, see LDAP Provision Configuration.

v. On the **OUs and Groups** page, choose **Import > LDAP > OU**.

vi. In the **LDAP list** panel, find the LDAP and click **Import**. In the dialog box that appears, click **OK**. In the **OU Temporary Data** panel, confirm the organization information and click **Confirm Import**.

vii. In the **OUs** section of the current page, select the OU. In the OU details section, choose **Import > LDAP > Account**.

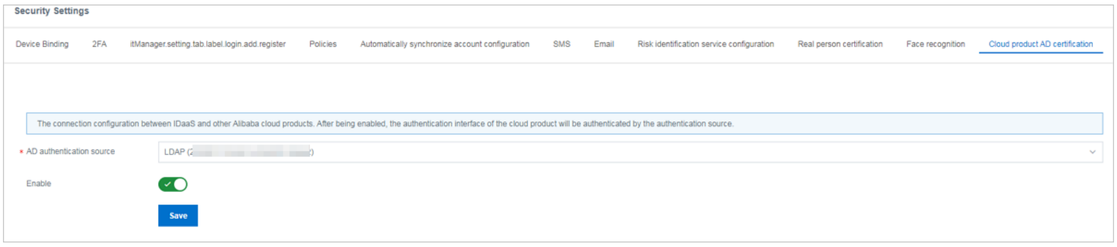
viii. In the **LDAP List** panel, find the LDAP and click **Import**. In the dialog box that appears, click **OK**. In the **Account Temporary Data LDAP List** panel, confirm the account information and click **Confirm Import** to synchronize the account information from the LDAP server to the IDaaS system.

3. Enable LDAP authentication for cloud services.

i. In the left-side navigation pane, choose **Settings > Security Settings**.

ii. On the **Security Settings** page, click the **Cloud Product AD Authentication** tab.

iii. Select the LDAP authentication source that you created, enable this feature, and then click **Save**.


Security Settings
Device Binding
2FA
itManager.setting.tab.label.login.add.register
Policies
Automatically synchronize account configuration
SMS
Email
Risk identification service configuration
Real person certification
Face recognition
Cloud product AD certification
Save

The connection configuration between IDaaS and other Alibaba cloud products. After being enabled, the authentication interface of the cloud product will be authenticated by the authentication source.

* AD authentication source: LDAP (2[redacted])

Enable: on

Step 2: Deploy SSL-VPN

After you enable LDAP authentication, you can deploy SSL-VPN, enable two-factor authentication for SSL-VPN, and associate the IDaaS instance. Then, you can establish an SSL-VPN connection after you pass the LDAP authentication.

1. Create a VPN gateway.
   i. Log on to the VPN Gateways console.
   ii. In the left-side navigation pane, choose **VPN > VPN Gateways**.
   iii. On the **VPN Gateways** page, click **Create VPN Gateway**.
   iv. On the buy page, set the following parameters and click **Buy Now** to complete the payment:
      - **Name**: Enter a name for the VPN Gateway instance.
      - **Region**: Select the region where you want to deploy the VPN gateway. **US (Silicon Valley)** is selected in this example.

        > Note Make sure that the VPN gateway and VPC are deployed in the same region.

      - **VPC**: Select the VPC to be associated with the VPN gateway.
      - **Specify vSwitch**: Specify whether to create the VPN gateway in a vSwitch of the VPC. **No** is selected in this example.

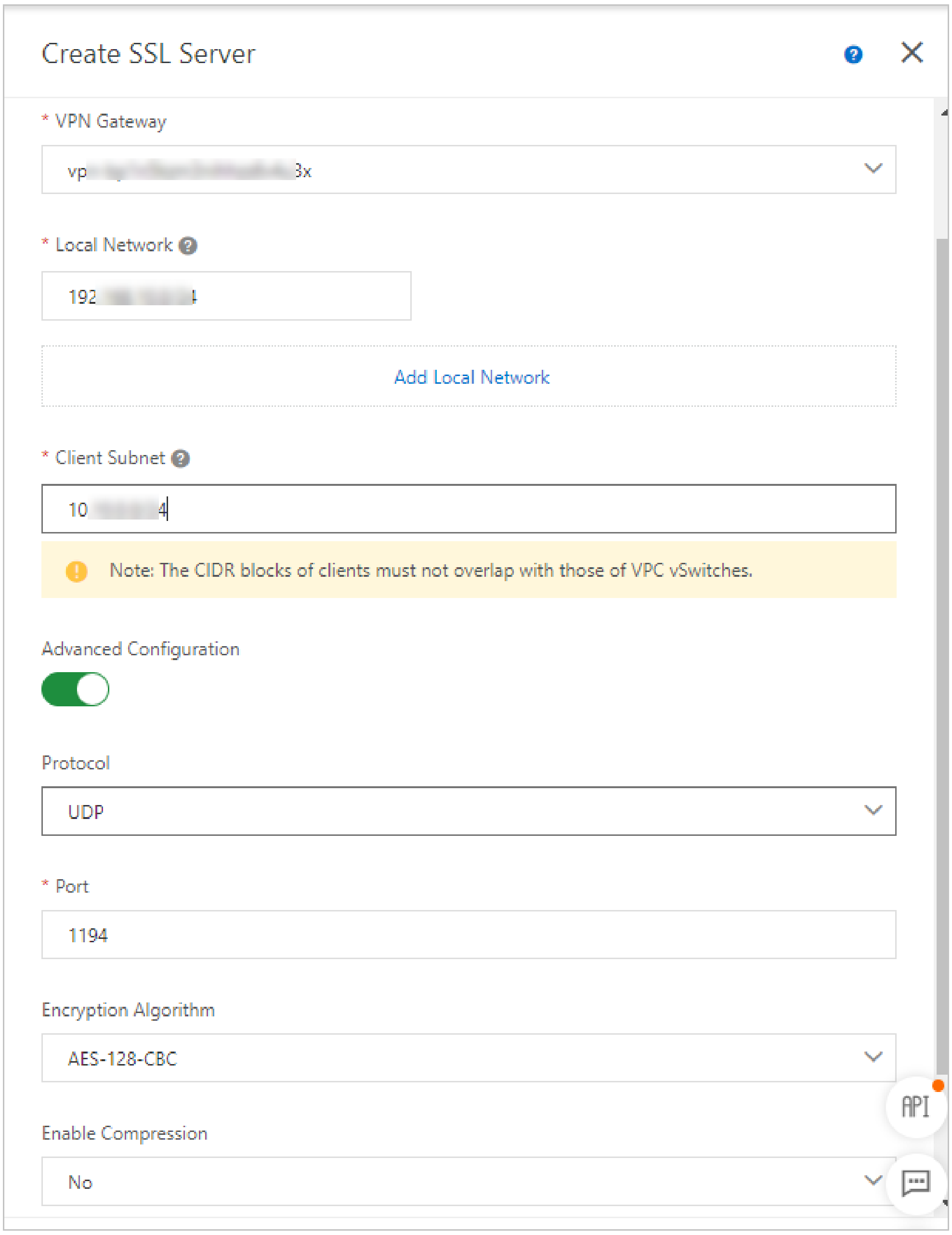
        If you select **Yes**, you must also specify a **vSwitch**.

      - **Peak Bandwidth**: Specify the maximum bandwidth for the VPN gateway. The bandwidth is used for data transfer over the Internet. **10 Mbit/s** is selected in this example.
      - **Traffic**: Pay-by-data-transfer is selected by default. For more information, see Pay-as-you-go.
      - **IPsec-VPN**: You can enable or disable the IPsec-VPN feature. After you enable this feature, you can establish connections between a data center and a VPC or between two VPCs. **Disable** is selected in this example.
      - **SSL-VPN**: You can enable or disable the SSL-VPN feature. After you enable this feature, you can connect to the VPC from a client regardless of the location. **Enable** is selected in this example.
      - **SSL connections**: Select the maximum number of concurrent SSL-VPN connections. **5** is selected in this example.

        > Note You can set this parameter only when the SSL-VPN feature is enabled.

      - **Duration**: By default, VPN gateways are billed on an hourly basis.
2. Create an SSL server.
   i. In the left-side navigation pane, choose **VPN > SSL Servers**.
   ii. In the top navigation bar, select the region where you want to create the SSL server.

      US (Silicon Valley) is selected in this example.
   iii. On the **SSL Servers** page, click **Create SSL Server**.
   iv. In the **Create SSL Server** panel, set the following parameters and click **OK**.



Create SSL Server

* VPN Gateway

vp[redacted]3x

* Local Network

192[redacted]4

* Client Subnet

10[redacted]4

Note: The CIDR blocks of clients must not overlap with those of VPC vSwitches.

Advanced Configuration

Protocol

UDP

* Port

1194

Encryption Algorithm

AES-128-CBC

Enable Compression

No

- **Name**: Enter a name for the SSL server.

  The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter.

- **VPN Gateway**: Select the VPN gateway you created.
- **Local Network**: Enter the CIDR block to be accessed by the client over the SSL-VPN connection. **192.168.0.0/24** is used in this example.
- **Client Subnet**: Enter a CIDR block that the client uses when the client is connected to the SSL server. **10.0.0.0/24** is used in this example.

- **Advanced Configuration**: Enable advanced configurations and set the following parameters.
  - **Protocol**: Select the protocol for the SSL-VPN connection. Valid values: UDP and TCP. The default value **UDP** is used in this example.
  - **Port** : Enter the port number used in the SSL-VPN connection. The default value **1194** is used in this example.
  - **Encryption Algorithm**: The encryption algorithm used in the SSL-VPN connection. Supported encryption algorithms include AES-128-CBC, AES-192-CBC, and AES-256-CBC. The default algorithm **AES-128-CBC** is used in this example.
  - **Enable Compression**: Specify whether to compress the transmitted data. The default settings **No** is selected in this example.
  - **Two-factor Authentication**: Enable two-factor authentication and select an IDaaS instance.
    - **IDaaS Instance Region**: Select the region where the IDaaS instance is deployed. **Singapore (Singapore)** is selected in this example.
    - **IDaaS Instance**: Select the IDaaS instance.

> **Note** If this is your first time using two-factor authentication, you must authorize the VPN gateway to access the IDaaS instance before you create the SSL server.

3. Create and download an SSL client certificate.

   i. In the left-side navigation pane, choose **VPN > SSL Clients**.

   ii. In the top navigation bar, select the region where the SSL client is deployed.

   US (Silicon Valley) is selected in this example.

   iii. On the **SSL Clients** page, click **Create Client Certificate**.

   iv. In the **Create Client Certificate** panel, set the following parameters and click **OK**.

   - **Name**: Enter a name for the SSL client certificate.

     The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter.

   - **SSL Server**: Select the SSL server that you created.

   v. On the **SSL Clients** page, find the SSL client certificate and click **Download** in the **Actions** column.

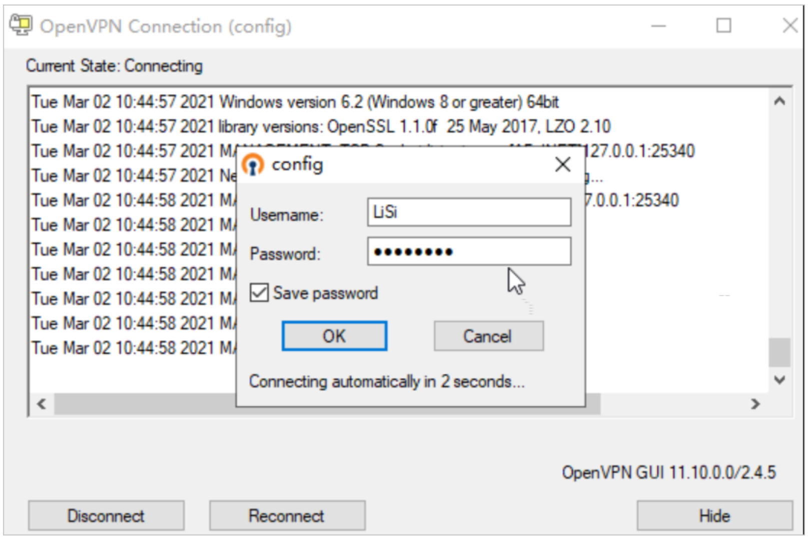
   The SSL client certificate is downloaded to your on-premises device.

Step 3: Configure the client

- If you use a Windows client, perform the following steps:

  i. Decompress the downloaded SSL client certificate package and copy the SSL client certificate to the *OpenVPN\confi* directory. In this example, the certificate is copied to the *C:\Program Files\OpenVPN\config* directory. You must copy the certificate to the directory where OpenVPN is installed.

  ii. Start the OpenVPN client and enter the username and password for authentication.



OpenVPN Connection (config)

Current State: Connecting

```
Tue Mar 02 10:44:57 2021 Windows version 6.2 (Windows 8 or greater) 64bit
Tue Mar 02 10:44:57 2021 library versions: OpenSSL 1.1.0f  25 May 2017, LZO 2.10
Tue Mar 02 10:44:57 2021 M                                    127.0.0.1:25340
Tue Mar 02 10:44:57 2021 Ne                                    ...
Tue Mar 02 10:44:58 2021 M                                    7.0.0.1:25340
Tue Mar 02 10:44:58 2021 M
Tue Mar 02 10:44:58 2021 M
Tue Mar 02 10:44:58 2021 M
Tue Mar 02 10:44:58 2021 M
Tue Mar 02 10:44:58 2021 M
Tue Mar 02 10:44:58 2021 M
```

config

Username: LiSi

Password: ••••••••

☑ Save password

Connecting automatically in 2 seconds...

- If you use a Linux client, perform the following steps:

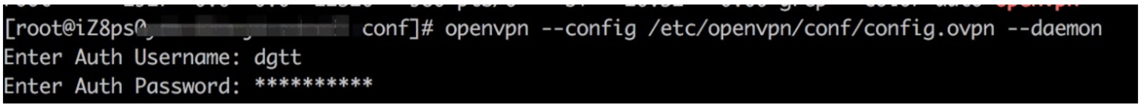
  i. Run the following command to install OpenVPN:

  ```
  yum install -y openvpn
  ```

  ii. Extract and copy the downloaded SSL client certificate to the */etc/openvpn/conf/* directory.

  iii. Run the following command to start the OpenVPN client and enter the username and password for authentication.

  ```
  openvpn --config /etc/openvpn/conf/config.ovpn --daemon
  ```



```
[root@iZ8ps0[redacted] conf]# openvpn --config /etc/openvpn/conf/config.ovpn --daemon
Enter Auth Username: dgtt
Enter Auth Password: **********
```

- If you use a Mac client, perform the following steps:

  i. Run the following command to install OpenVPN:

  ```
  brew install openvpn
  ```

  > Note If Homebrew is not installed, install Homebrew first.

  ii. Run the following command to delete the default configuration file:

  ```
  rm /usr/local/etc/openvpn/*
  ```

  iii. Run the following command to copy the file to the configuration directory:

  ```
  cp cert_location /usr/local/etc/openvpn/
  ```

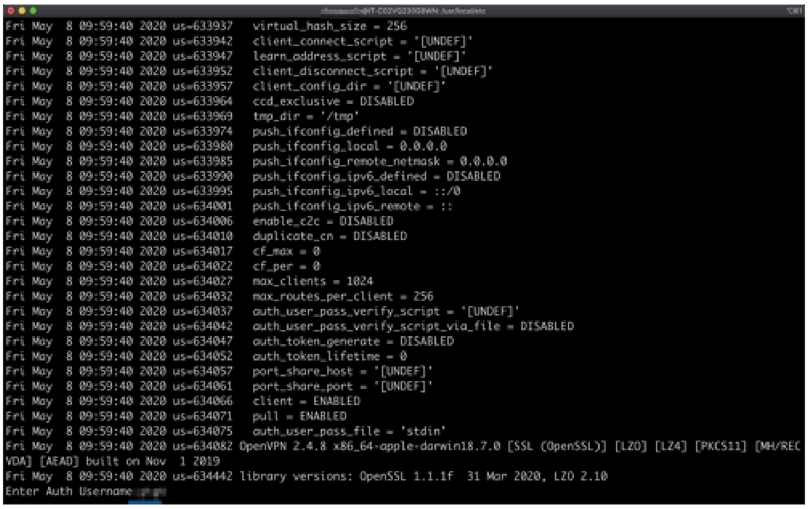
  In the preceding command, replace `cert_location` with the directory where the SSL client certificate is downloaded. For example, */Users/example/Downloads/certs.zip*.

  iv. Run the following command to extract the downloaded certificate and copy it to the directory where the OpenVPN client is installed:

  ```
  cd  /usr/local/etc/openvpn
  unzip /usr/local/etc/openvpn/certs.zip
  ```

v. Run the following command to establish a connection and enter the username and password for authentication.

```
sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
```



```
Fri May  8 09:59:40 2020 us=633937   virtual_hash_size = 256
Fri May  8 09:59:40 2020 us=633942   client_connect_script = '[UNDEF]'
Fri May  8 09:59:40 2020 us=633947   learn_address_script = '[UNDEF]'
Fri May  8 09:59:40 2020 us=633952   client_disconnect_script = '[UNDEF]'
Fri May  8 09:59:40 2020 us=633957   client_config_dir = '[UNDEF]'
Fri May  8 09:59:40 2020 us=633964   ccd_exclusive = DISABLED
Fri May  8 09:59:40 2020 us=633969   tmp_dir = '/tmp'
Fri May  8 09:59:40 2020 us=633974   push_ifconfig_defined = DISABLED
Fri May  8 09:59:40 2020 us=633980   push_ifconfig_local = 0.0.0.0
Fri May  8 09:59:40 2020 us=633985   push_ifconfig_remote_netmask = 0.0.0.0
Fri May  8 09:59:40 2020 us=633990   push_ifconfig_ipv6_defined = DISABLED
Fri May  8 09:59:40 2020 us=633995   push_ifconfig_ipv6_local = ::/0
Fri May  8 09:59:40 2020 us=634001   push_ifconfig_ipv6_remote = ::
Fri May  8 09:59:40 2020 us=634006   enable_c2c = DISABLED
Fri May  8 09:59:40 2020 us=634010   duplicate_cn = DISABLED
Fri May  8 09:59:40 2020 us=634017   cf_max = 0
Fri May  8 09:59:40 2020 us=634022   cf_per = 0
Fri May  8 09:59:40 2020 us=634027   max_clients = 1024
Fri May  8 09:59:40 2020 us=634032   max_routes_per_client = 256
Fri May  8 09:59:40 2020 us=634037   auth_user_pass_verify_script = '[UNDEF]'
Fri May  8 09:59:40 2020 us=634042   auth_user_pass_verify_script_via_file = DISABLED
Fri May  8 09:59:40 2020 us=634047   auth_token_generate = DISABLED
Fri May  8 09:59:40 2020 us=634052   auth_token_lifetime = 0
Fri May  8 09:59:40 2020 us=634057   port_share_host = '[UNDEF]'
Fri May  8 09:59:40 2020 us=634061   port_share_port = '[UNDEF]'
Fri May  8 09:59:40 2020 us=634066   client = ENABLED
Fri May  8 09:59:40 2020 us=634071   pull = ENABLED
Fri May  8 09:59:40 2020 us=634075   auth_user_pass_file = 'stdin'
Fri May  8 09:59:40 2020 us=634082 OpenVPN 2.4.8 x86_64-apple-darwin18.7.0 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [MH/REC
VDA] [AEAD] built on Nov  1 2019
Fri May  8 09:59:40 2020 us=634442 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Enter Auth Username:[redacted]
```

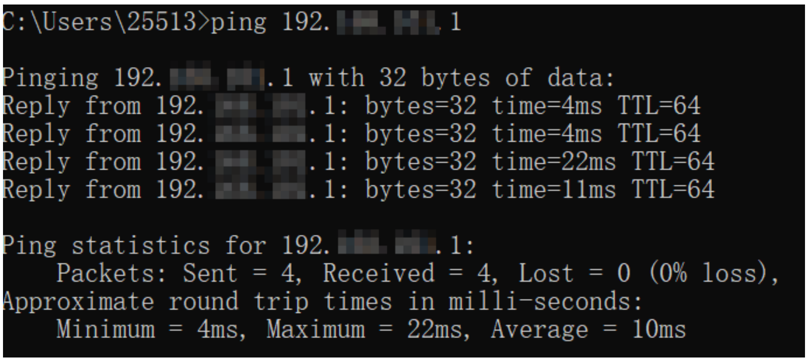
Step 4: Test the connectivity

After you complete the preceding steps, you can run the `ping` command to test the connectivity between the client and VPC. A Windows client is used in the following example to describe how to test the connectivity between the client and the VPC.

1. Open the command prompt in the Windows client.
2. Run the `ping` command to `ping` the IP address of the ECS instance deployed in the VPC. This command tests the connectivity between the Windows client and VPC.

   > **Note** Make sure that the security group rules of the ECS instance allow remote access from the Windows client. For more information, see Security groups for different use casesConfiguration guide for ECS security groups.

   The test result shows that the Windows client can access the ECS instance.



```
C:\Users\25513>ping 192.[redacted].1

Pinging 192.[redacted].1 with 32 bytes of data:
Reply from 192.[redacted].1: bytes=32 time=4ms TTL=64
Reply from 192.[redacted].1: bytes=32 time=4ms TTL=64
Reply from 192.[redacted].1: bytes=32 time=22ms TTL=64
Reply from 192.[redacted].1: bytes=32 time=11ms TTL=64

Ping statistics for 192.[redacted].1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 22ms, Average = 10ms
```

5.High availability architecture using IPsec-VPN connections

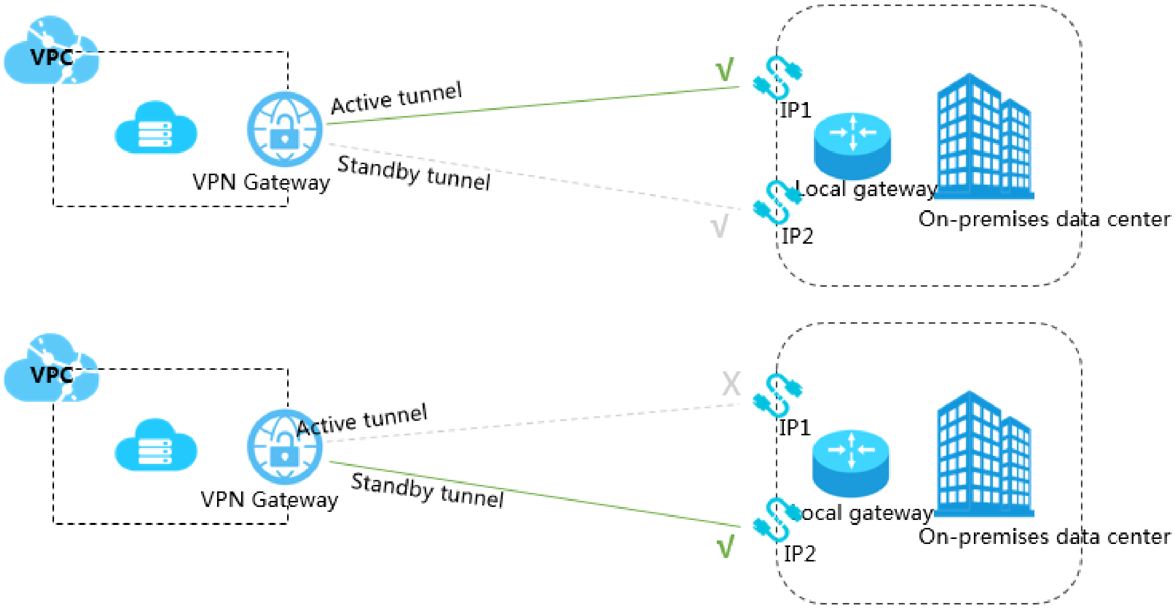
5.1. Create two IPsec-VPN connections for high availability

This topic describes how to create active/standby IPsec-VPN connections for high availability. If your gateway device is assigned two public IP addresses, you can use them to create two IPsec-VPN connections to a VPN gateway.

Overview

A gateway device is provided with two connections to the Internet. Each connection is established from a separate public IP address. The public IP addresses are used to establish IPsec-VPN connections to the VPN gateway. Health checks are enabled for these connections. Two routes are created and assigned different weights so that they serve as active/standby routes. The IPsec-VPN connection with which the active route is associated serves as the active IPsec-VPN connection. The IPsec-VPN connection with which the standby route is associated serves as the standby IPsec-VPN connection.

- If the IPsec-VPN connection that uses IP address 1 to connect the VPN gateway to the gateway device is active, traffic between the virtual private cloud (VPC) and the on-premises network is transmitted only through the active IPsec-VPN connection.
- If the IPsec-VPN connection that uses IP address 1 to connect the VPN gateway to the gateway device is down, traffic between the VPC and the on-premises network is transmitted through the standby IPsec-VPN connection.



Prerequisites

Before you start, make sure that the following requirements are met:

- The gateway device in the on-premises network is checked. VPN Gateway supports the standard IKEv1 and IKEv2 protocols. Any gateway device that supports these two protocols can connect to Alibaba Cloud VPN gateways, such as gateway devices that are manufactured by H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
- Make sure that a static public IP address for the gateway device is assigned in the on-premises network.
- The CIDR block of the on-premises network must not overlap with that of the VPC.

Step 1: Create a VPN gateway

Take the following steps to create a VPN gateway:

1. Log on to the VPN gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. On the **VPN Gateways** page, click **Create VPN Gateway**.
4. On the buy page, set the following parameters, click **Buy Now**, and complete the payment.
   - **Name**: Enter a name for the VPN gateway.
   - **Region**: Select the region where you want to deploy the VPN gateway.

     > ? **Note** Make sure that the VPC network and the VPN gateway associated with the VPC network are deployed in the same region.

   - **VPC**: Select the VPC network to be associated with the VPN gateway.
   - **Bandwidth**: Specify the maximum bandwidth of the VPN gateway. The bandwidth is provided for data transfer over the Internet.
   - **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway.
   - **SSL-VPN**: Specify whether to enable SSL-VPN. SSL-VPN allows you to connect a client to a VPC network from any places.
   - **SSL Connections**: Specify the maximum number of concurrent SSL connections that the VPN gateway supports.

     > ? **Note** This parameter is available only after SSL-VPN is enabled.

   - **Billing Cycle**: Specify the subscription duration.
5. Go to the VPN Gateways page to view the newly created VPN gateway.

   The newly created VPN gateway is in the Preparing state. Its status changes to Normal after about two minutes. The Normal state indicates that the VPN gateway is initialized and ready for use.

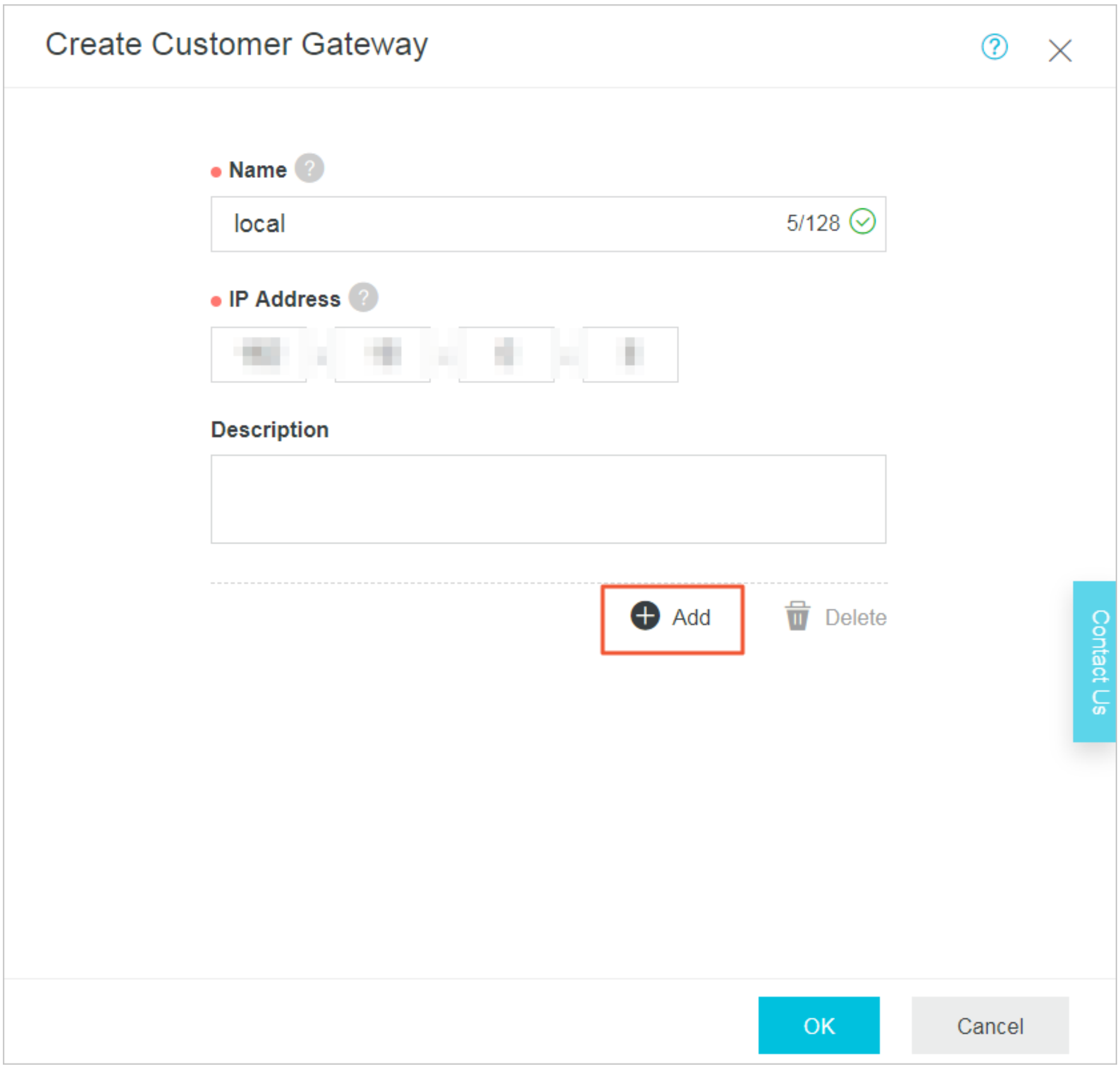
   > ? **Note** It takes about one to five minutes to create a VPN gateway.

Step 2: Create two customer gateways

Perform the following operations to create two customer gateways and register the public IP addresses of the gateway device to the customer gateways:

1. In the left-side navigation pane, choose **VPN > Customer Gateways**.
2. Select the region where you want to deploy the customer gateways.

3. On the **Customer Gateways** page, click **Create Customer Gateway**.
4. Set the following parameters to create two customer gateways:
   - **Name**: Enter a name for the first customer gateway.
   - **IP Address**: Enter one of the public IP addresses of the gateway device that you want to connect to the VPC.
   - **Description**: Enter a description for the first customer gateway.
5. On the **Create Customer Gateway** page, click **+Add** to create the other customer gateway.



Create Customer Gateway

Name: local 5/128

IP Address: [redacted]

Description:

Step 3: Create two IPsec-VPN connections

Perform the following operations to create two IPsec-VPN connections between the customer gateways and the VPN gateway, and enable health checks:

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. Select the region where you want to create the IPsec-VPN connections.
3. On the **IPsec Connections** page, click **Create IPsec Connection**.
4. Set the following parameters and click **OK**:

- **Name**: Enter a name for the IPsec-VPN connection.
- **VPN Gateway**: Select a VPN gateway from the drop-down list.
- **Customer Gateway**: Select the customer gateway to be connected through the IPsec-VPN connection.
- **Local Network**: Enter the CIDR block of the VPC where the VPN gateway is deployed.
- **Remote Network**: Enter the CIDR block of the on-premises network.
- **Effective Immediately**: Specify whether to immediately start negotiations.
  - Yes: immediately negotiates after the configuration is completed.
  - No: negotiates when traffic is detected.
- **Pre-Shared Key**: Enter the pre-shared key. The pre-shared key must be the same as the one specified on the gateway device.
- **Health Check**: Enable health checks, and specify the destination IP address, source IP address, retry interval, and number of retries.

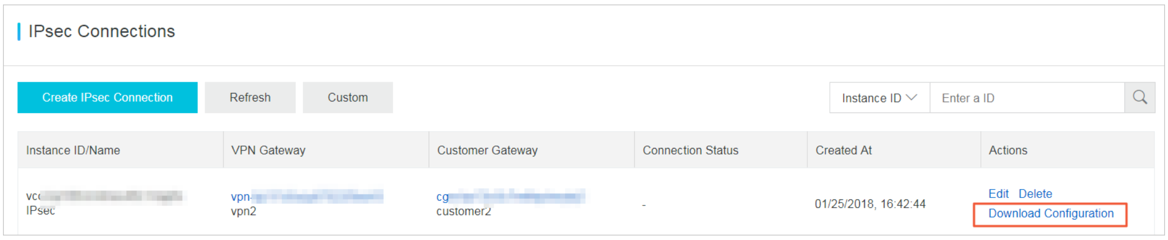
  Use the default settings for other parameters.

5. Repeat the preceding operations to create the other IPsec-VPN connection.

Step 4: Load the configurations of the IPsec-VPN connections to the gateway device

Perform the following operations to load the configurations of the IPsec-VPN connections to the gateway device:

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. Select the region where you want to establish the IPsec-VPN connection.
3. Find the IPsec-VPN connections that you created, and click **Download Configuration** in the Actions column.

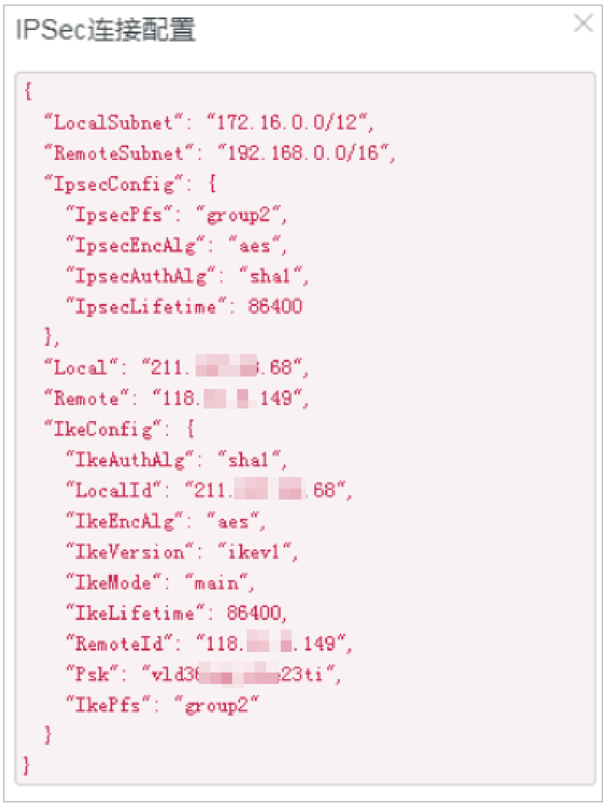


IPsec Connections

Instance ID/Name	VPN Gateway	Customer Gateway	Connection Status	Created At	Actions
vc[redacted] IPsec	vpn-[redacted] vpn2	cg[redacted] customer2	-	01/25/2018, 16:42:44	Edit Delete Download Configuration

4. Load the configurations of the IPsec-VPN connections to the gateway device. For more information about how to load the configuration of an IPsec-VPN connection to a gateway device, see Configure local gateways.

   The values of RemoteSubnet and LocalSubnet in the downloaded configurations and the values specified when you create the IPsec-VPN connections are swapped between each other. For a VPN gateway, RemoteSubnet refers to the CIDR block of the on-premises network, whereas LocalSubnet refers to the CIDR block of the VPC. For a gateway device, LocalSubnet refers to the CIDR block of the on-premises network, whereas RemoteSubnet refers to the CIDR block of the VPC.



IPSec连接配置

```
{
  "LocalSubnet": "172.16.0.0/12",
  "RemoteSubnet": "192.168.0.0/16",
  "IpsecConfig": {
    "IpsecPfs": "group2",
    "IpsecEncAlg": "aes",
    "IpsecAuthAlg": "sha1",
    "IpsecLifetime": 86400
  },
  "Local": "211.[redacted].68",
  "Remote": "118.[redacted].149",
  "IkeConfig": {
    "IkeAuthAlg": "sha1",
    "LocalId": "211.[redacted].68",
    "IkeEncAlg": "aes",
    "IkeVersion": "ikev1",
    "IkeMode": "main",
    "IkeLifetime": 86400,
    "RemoteId": "118.[redacted].149",
    "Psk": "v1d3[redacted]23ti",
    "IkePfs": "group2"
  }
}
```

Step 5: Configure two routes on the VPN gateway

Perform the following operations to configure two routes on the VPN gateway:

1. In the left-side navigation pane, choose **VPN > VPN Gateways**.
2. On the **VPN Gateways** page, select the region where the VPN gateway is created.
3. Find the VPN gateway that you want to manage and click its ID in the **Instance ID/Name** column.
4. On the **Destination-based routing** tab, click **Add Route Entry**.
5. Set the following parameters and click **OK** to configure the routes:
    - **Destination CIDR Block**: Enter the private CIDR block of the on-premises network.
    - **Next Hop**: Select one of the IPsec-VPN connections.
    - **Publish to VPC**: Specify whether to automatically advertise this route to the route table of the VPC.
    - **Weight**: Select a weight.

    > **Notice** You must specify different weights to the routes so that they can serve as active/standby routes. You cannot set the weights of both routes to 100 or 0.

    The following table describes the routes in this example.

Destination CIDR block	Next hop	Advertise to VPC	Weight
Private CIDR block of the gateway device	IPsec-VPN connection 1	Yes	100

Destination CIDR block	Next hop	Advertise to VPC	Weight
Private CIDR block of the gateway device	IPsec-VPN connection 2	Yes	0

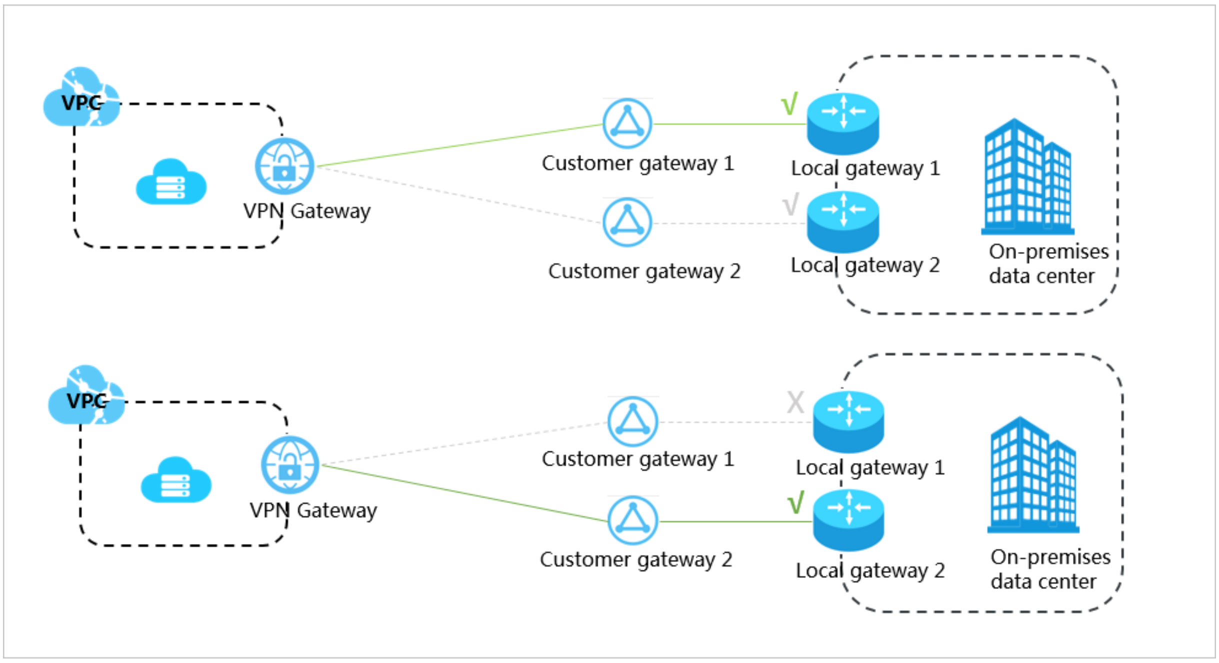
5.2. Use two customer gateways for high availability

This topic describes how to configure active/standby IPsec-VPN connections for high availability. You can connect a VPN gateway to two customer gateways that are created for two customer-premises equipment (CPE) in the on-premises network.

Overview

You can create a VPN gateway for a virtual private cloud (VPC) and create two customer gateways for the gateway devices in the on-premises network.

Then, create two IPsec-VPN connections to connect the two customer gateways to the same VPN gateway. You can enable health checks for the IPsec-VPN connections to ensure that the negotiations are successful. If the health check result shows that one of the two customer gateways is malfunctioning, traffic is automatically routed to the other customer gateway.



Prerequisites

Before you start, make sure that the following requirements are met:

- The gateway devices in the on-premises network are checked. VPN Gateway supports the standard IKEv1 and IKEv2 protocols. Any gateway device that supports these two protocols can connect to Alibaba Cloud VPN gateways, such as gateway devices that are manufactured by H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
- Make sure that a static public IP address is assigned to each gateway device in the on-premises network.

- The CIDR block of the on-premises network must not overlap with that of the VPC.

Step 1: Create a VPN gateway

Take the following steps to create a VPN gateway:

1. Log on to the VPN gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. On the **VPN Gateways** page, click **Create VPN Gateway**.
4. On the buy page, set the following parameters, click **Buy Now**, and complete the payment.
   - **Name**: Enter a name for the VPN gateway.
   - **Region**: Select the region where you want to deploy the VPN gateway.

     > **Note** Make sure that the VPC network and the VPN gateway associated with the VPC network are deployed in the same region.

   - **VPC**: Select the VPC network to be associated with the VPN gateway.
   - **Bandwidth**: Specify the maximum bandwidth of the VPN gateway. The bandwidth is provided for data transfer over the Internet.
   - **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway.
   - **SSL-VPN**: Specify whether to enable SSL-VPN. SSL-VPN allows you to connect a client to a VPC network from any places.
   - **SSL Connections**: Specify the maximum number of concurrent SSL connections that the VPN gateway supports.

     > **Note** This parameter is available only after SSL-VPN is enabled.

   - **Billing Cycle**: Specify the subscription duration.
5. Go to the VPN Gateways page to view the newly created VPN gateway.

   The newly created VPN gateway is in the Preparing state. Its status changes to Normal after about two minutes. The Normal state indicates that the VPN gateway is initialized and ready for use.

   > **Note** It takes about one to five minutes to create a VPN gateway.

Step 2: Create two customer gateways

Perform the following operations to create two customer gateways and register the public IP addresses of the gateway devices in the on-premises network to the customer gateways.

1. In the left-side navigation pane, click **VPN > Customer Gateways**.
2. Select the region where the customer gateways are deployed.
3. On the **Customer Gateways** page, click **Create Customer Gateway**.
4. On the **Create Customer Gateway** page, set the following parameters and click **OK**:
   - **Name**: Enter a name for the first customer gateway.
   - **IP Address**: Enter one of the public IP addresses of the gateway devices that you want to connect to the VPC.

- **Description**: Enter a description for the first customer gateway.
- **+Add**: Add another customer gateway.

Step 3: Create two IPsec-VPN connections

Perform the following operations to create two IPsec-VPN connections between the customer gateways and the VPN gateway, and enable the health check feature:

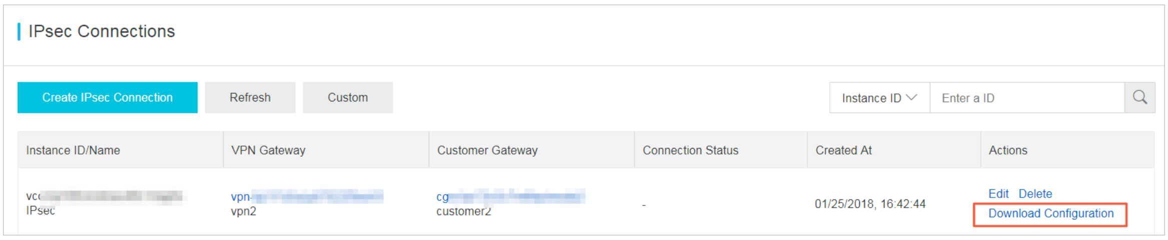
1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. Select the region where you want to create the IPsec-VPN connection.
3. On the **IPsec Connections** page, click **Create IPsec Connection**.
4. Set the following parameters and then click **OK**:
   - **Name**: Enter a name for the IPsec-VPN connection.
   - **VPN Gateway**: Select a VPN gateway from the drop-down list.
   - **Customer Gateway**: Select the customer gateway to be connected through the IPsec-VPN connection.
   - **Local Network**: Enter the CIDR block of the VPC where the VPN gateway is deployed.
   - **Remote Network**: Enter the CIDR block of the on-premises network.
   - **Effective Immediately**: Specify whether to immediately start negotiations.
     - Yes: immediately negotiates after the configuration is completed.
     - No: negotiates when traffic is detected.
   - **Pre-Shared Key**: Enter the pre-shared key. The pre-shared key must be the same as the one specified on the gateway device.
   - **Health Check**: Enable health checks, and specify the destination IP address, source IP address, retry interval, and number of retries.

     Use the default settings for other parameters.
5. Repeat the preceding operations to create the other IPsec-VPN connection.

Step 4: Load the configurations of the IPsec-VPN connections to the gateway devices

Perform the following operations to load the configurations of the two IPsec-VPN connections to the gateway devices:

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. Select the region where the IPsec-VPN connections are created.
3. Find the IPsec-VPN connections that you have created and click **Download Configuration** in the Actions column.



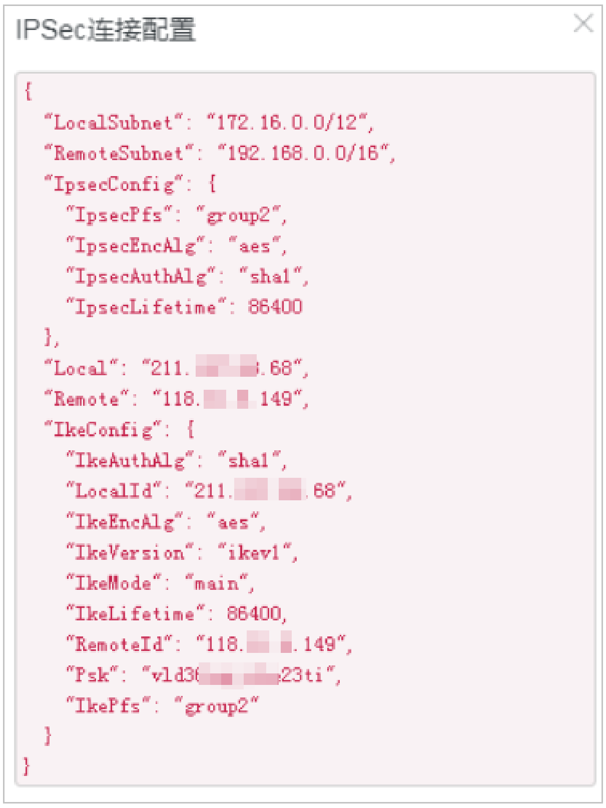
IPsec Connections

Instance ID/Name	VPN Gateway	Customer Gateway	Connection Status	Created At	Actions
vc[redacted] IPsec	vpn-[redacted] vpn2	cg[redacted] customer2	-	01/25/2018, 16:42:44	Edit Delete Download Configuration

4. Load the configurations of the IPsec-VPN connections to the gateway device. For more

information about how to load the configuration of an IPsec-VPN connection to a gateway device, see Configure local gateways.

The RemotSubnet and LocalSubnet values in the configurations that you have downloaded are opposite to the RemotSubnet and LocalSubnet values that you have specified when you create the IPsec-VPN connections. For a VPN gateway, RemotSubnet refers to the CIDR block of the on-premises network and LocalSubnet refers to the CIDR block of the VPC. For a gateway device, LocalSubnet refers to the CIDR block of the on-premises network and RemotSubnet refers to the CIDR block of the VPC.



```
{
  “LocalSubnet”: “172.16.0.0/12”,
  “RemoteSubnet”: “192.168.0.0/16”,
  “IpsecConfig”: {
    “IpsecPfs”: “group2”,
    “IpsecEncAlg”: “aes”,
    “IpsecAuthAlg”: “sha1”,
    “IpsecLifetime”: 86400
  },
  “Local”: “211.[redacted].68”,
  “Remote”: “118.[redacted].149”,
  “IkeConfig”: {
    “IkeAuthAlg”: “sha1”,
    “LocalId”: “211.[redacted].68”,
    “IkeEncAlg”: “aes”,
    “IkeVersion”: “ikev1”,
    “IkeMode”: “main”,
    “IkeLifetime”: 86400,
    “RemoteId”: “118.[redacted].149”,
    “Psk”: “vld3[redacted]23ti”,
    “IkePfs”: “group2”
  }
}
```

Step 5: Configure two routes on the VPN gateway

Perform the following operations to configure two routes on the VPN gateway:

1. In the left-side navigation pane, choose **VPN > VPN Gateways**.
2. On the **VPN Gateway** page, select the region where the VPN gateway is deployed.
3. Find the VPN gateway that you want to manage and click its ID in the **Instance ID/Name** column.
4. On the **Destination-based routing** tab, click **Add Route Entry**.
5. Set the following parameters and click **OK** to configure two routes:
    - **Destination CIDR Block**: Enter the private CIDR block of the on-premises network.
    - **Next Hop**: Select one of the IPsec-VPN connections.
    - **Publish to VPC**: Specify whether to automatically advertise this route to the route table of the VPC.
    - **Weight**: Select a weight.

Notice You must specify different weights to the routes so that they can serve as active/standby routes. You cannot set the weights of both routes to 100 or 0.

The following table describes the routes in this example.

Destination CIDR block	Next hop	Advertise to VPC	Weight
Private CIDR block of the gateway device	IPsec-VPN connection 1	Yes	100
Private CIDR block of the gateway device	IPsec-VPN connection 2	Yes	0

6.Use IPsec-VPN and CEN to build a high-quality global network

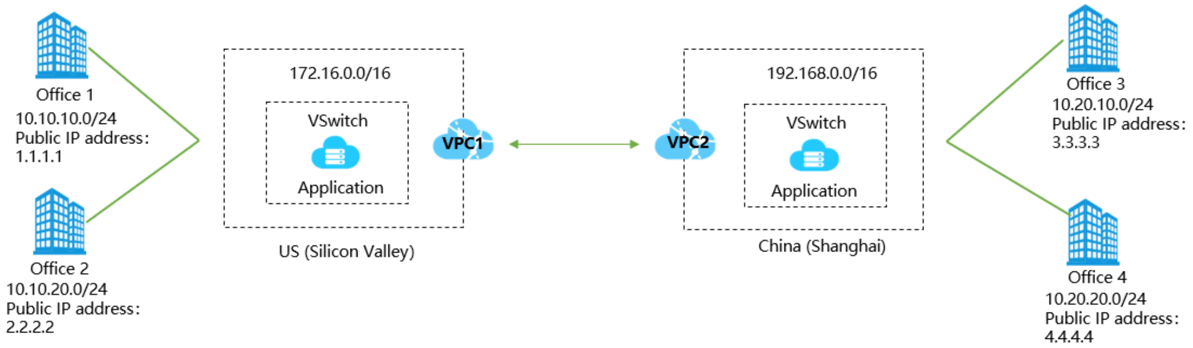
This topic describes how to use VPN Gateway and Cloud Enterprise Network (CEN) to connect data centers to Alibaba Cloud and build a cross-border enterprise network that is high quality and cost-effective.

Prerequisites

Before you start, make sure that the following requirements are met:

- Virtual private clouds (VPCs) are created, and applications are deployed in the VPCs. For more information, see Create and manage a VPC.
- A gateway device is deployed in each office and a static public IP address is allocated to each gateway device.
- A CEN instance is created. For more information, see Create a CEN instance.
- A CEN bandwidth plan is purchased and the bandwidth for inter-region communication is allocated. For more information, see Use a bandwidth plan and Manage bandwidth for cross-region connections.
- The CIDR blocks to be connected must not overlap with each other.

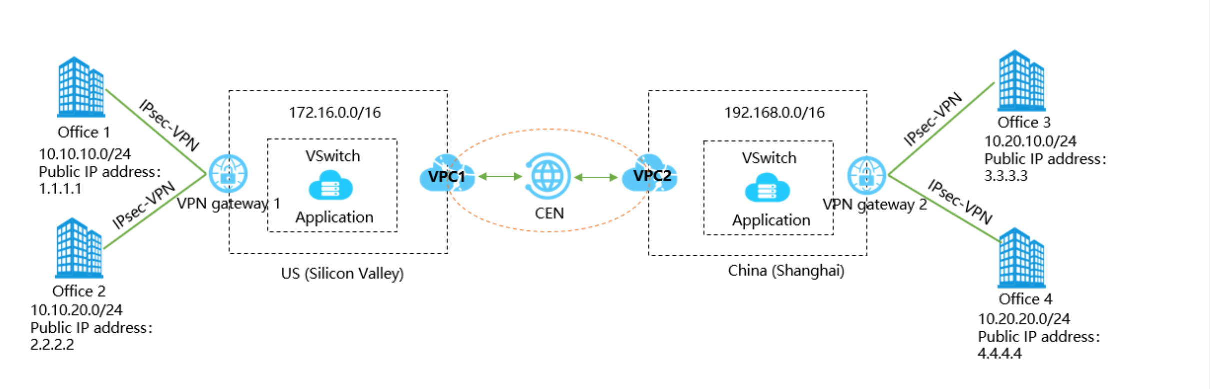
Context



An international company has two offices in Silicon Valley and two offices in Shanghai. The company has created VPC1 in the US (Silicon Valley) region and VPC2 in the China (Shanghai) region. An application is deployed in each VPC. Due to business development, the company wants to connect the following networks: the networks of the offices in Shanghai and Silicon Valley, VPC1, and VPC2. The following table describes the CIDR blocks of the networks.

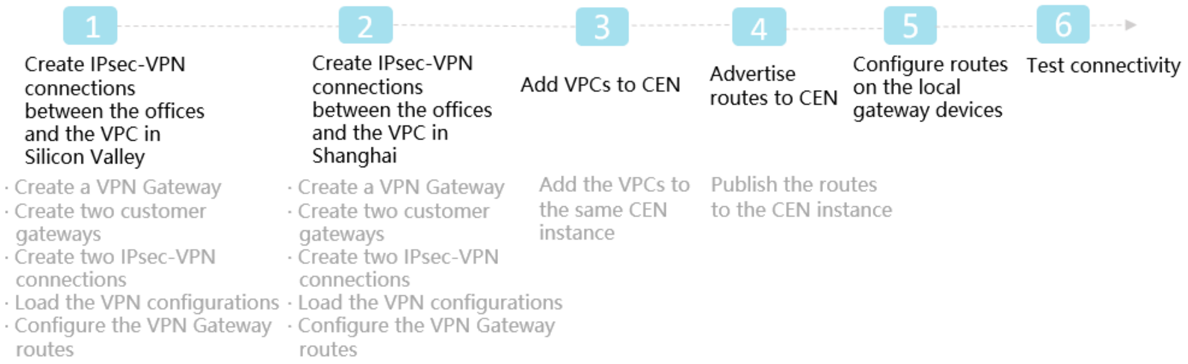
Network	CIDR block
Office1 in Silicon Valley	10.10.10.0/24
Office2 in Silicon Valley	10.10.20.0/24
VPC1 in US (Silicon Valley)	172.16.0.0/16

Network	CIDR block
Office3 in Shanghai	10.20.10.0/24
Office4 in Shanghai	10.20.20.0/24
VPC2 in China (Shanghai)	192.168.0.0/16



You can use a VPN gateway (VPNgateway1) to connect Office1 and Office2 to VPC1, and use another VPN gateway (VPNgateway2) to connect Office3 and Office4 to VPC2, as shown in the preceding figure. Then, you can attach VPC1 and VPC2 to the same CEN instance to enable cross-border communication.

Procedure



1 Create IPsec-VPN connections between the offices and the VPC in Silicon Valley
- Create a VPN Gateway
- Create two customer gateways
- Create two IPsec-VPN connections
- Load the VPN configurations
- Configure the VPN Gateway routes

2 Create IPsec-VPN connections between the offices and the VPC in Shanghai
- Create a VPN Gateway
- Create two customer gateways
- Create two IPsec-VPN connections
- Load the VPN configurations
- Configure the VPN Gateway routes

3 Add VPCs to CEN
Add the VPCs to the same CEN instance

4 Advertise routes to CEN
Publish the routes to the CEN instance

5 Configure routes on the local gateway devices

6 Test connectivity

Step 1: Create IPsec-VPN connections to connect Office1 and Office2 to VPC1

To create IPsec-VPN connections in the US (Silicon Valley) region to connect Office1 and Office2 to VPC1, perform the following operations:

1. Create a VPN gateway in VPC1.

   Set the following parameters:

   - **Name**: Enter a name for the VPN gateway. In this example, *VPNgateway1* is used.
   - **Region**: Select **US (Silicon Valley)**.
   - **VPC**: Select the VPC in the **US (Silicon Valley)** region.
   - **Specify VSwitch**: Select **No**.

- **Maximum Bandwidth**: Select **10 Mbit/s**.
- **Traffic**: Select **Pay-by-data-transfer**.
- **IPsec-VPN**: Select **Enable**.
- **SSL-VPN**: Select **Disable**.
- **Duration**: Select **By Hour**.
- **Service-linked Role**: Click **Create Service-linked Role** and the system automatically creates the service-linked role AliyunServiceRoleForVpn.

  > **Note** For more information about how a VPN gateway assumes the role to access other cloud resources, see AliyunServiceRoleForVpn.

  If **Created** is displayed, the service-linked role is created and you do not need to create it again.

For more information, see 创建和管理VPN网关实例.

2. Create two customer gateways and register the public IP addresses of the gateway devices in Office1 and Office2 to the customer gateways. The public IP addresses are used to create IPsec-VPN connections.

   Set the following parameters to create a customer gateway for Office1:

   - **Name**: Enter a name for the customer gateway. In this example, *customer_gt1* is used.
   - **IP Address**: Enter the static public IP address of the gateway device in Office1. In this example, *1.1.XX.XX* is used.

   Set the following parameters to create a customer gateway for Office2:

   - **Name**: Enter a name for the customer gateway. In this example, *customer_gt2* is used.
   - **IP Address**: Enter the static public IP address of the gateway device in Office2. In this example, *2.2.XX.XX* is used.

   For more information, see Create a customer gateway.

3. Create two IPsec-VPN connections to connect the gateway devices in Office1 and Office2 to VPNgateway1.

   Set the following parameters to create an IPsec-VPN connection between Office1 and the VPNgateway1:

   - **Name**: Enter a name for the IPsec-VPN connection. In this example, *IPsec1* is used.
   - **VPN Gateway**: Select the VPN gateway created in the US (Silicon Valley) region. In this example, VPNgateway1 is selected.
   - **Customer Gateway**: Select the customer gateway to be connected. In this example, customer_gt1 is selected.
   - **Routing Mode**: Select **Protected Data Flows**.
   - **Local Network**: Enter the CIDR block of the VPC to be connected to the office. In this example, *172.16.0.0/16* is entered.
   - **Remote Network**: Enter the CIDR block of Office1 to be connected to the VPC. In this example, *10.10.10.0/24* is entered.
   - **Effective Immediately**: Specify whether to negotiate immediately. In this example, **Yes** is selected.
     - **Yes**: starts connection negotiations after the configuration is completed.

    - **No**: starts negotiations when inbound traffic is detected.

  - **Pre-Shared Key**: Enter a pre-shared key for identity verification between VPNgateway1 and customer_gt1. In this example, *123456* is entered.

  Use the default settings for the other parameters.

  Set the following parameters to create an IPsec-VPN connection between Office2 and VPNgateway1:

  - **Name**: Enter a name for the IPsec-VPN connection. In this example, *IPsec2* is used.
  - **VPN Gateway**: Select the VPN gateway created in the US (Silicon Valley) region. In this example, VPNgateway1 is selected.
  - **Customer Gateway**: Select the customer gateway to be connected. In this example, customer_gt2 is selected.
  - **Routing Mode**: Select **Protected Data Flows**.
  - **Local Network**: Enter the CIDR block of the VPC to be connected to the office. In this example, *172.16.0.0/16* is entered.
  - **Remote Network**: Enter the CIDR block of Office1 to be connected to the VPC. In this example, *10.10.20.0/24* is entered.
  - **Effective Immediately**: Specify whether to negotiate immediately. In this example, **Yes** is selected.
    - **Yes**: starts connection negotiations after the configuration is completed.
    - **No**: starts negotiations when inbound traffic is detected.
  - **Pre-Shared Key**: Enter a pre-shared key for identity verification between VPNgateway1 and customer_gt2. In this example, *123456* is entered.

  Use the default settings for the other parameters.

  For more information, see Create an IPsec-VPN connection.

4. Load the configurations of the IPsec-VPN connections to the gateway devices in Office1 and Office2.

   For more information, see Configure local gateways.

5. Configure routes on VPNgateway1.

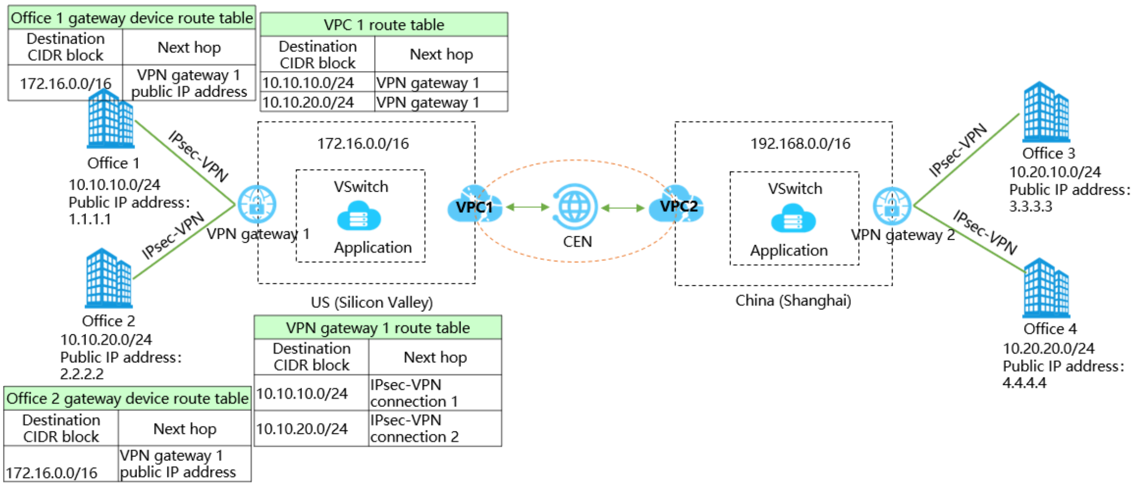
   Configure the following route on VPNgateway1 to route network traffic that is destined for Office1:

   - **Destination CIDR Block**: Enter the private CIDR block of the destination. In this example, *10.10.10.0/24* is entered.
   - **Next Hop Type**: Select IPsec Connection.
   - **Next Hop**: Select an IPsec-VPN connection. In this example, IPsec1 is selected.
   - **Publish to VPC**: Specify whether to automatically advertise this route to the route table of VPC1. In this example, **Yes** is selected.
     - **Yes**: automatically advertises the route to the route table of the VPC. We recommend that you select this value.
     - **No**: does not advertise the route to the route table of the VPC.
   - **Weight**: Specify a weight. In this example, **0** is specified.

Configure the following route on VPNgateway1 to route network traffic that is destined for Office2:

- **Destination CIDR Block**: Enter the private CIDR block of the destination. In this example, *10.10.10.0/24* is entered.
- **Next Hop Type**: Select IPsec Connection.
- **Next Hop**: Select an IPsec-VPN connection. In this example, IPsec2 is selected.
- **Publish to VPC**: Specify whether to automatically advertise this route to the route table of VPC1. In this example, **Yes** is selected.
  - **Yes**: automatically advertises the route to the route table of the VPC. We recommend that you select this value.
  - **No**: does not advertise the route to the route table of the VPC.
- **Weight**: Specify a weight. In this example, **0** is specified.

The following figure shows the route tables of Office1, Office2, VPNgateway1, and VPC1.



Office 1 gateway device route table

Destination CIDR block	Next hop
172.16.0.0/16	VPN gateway 1 public IP address

VPC 1 route table

Destination CIDR block	Next hop
10.10.10.0/24	VPN gateway 1
10.10.20.0/24	VPN gateway 1

VPN gateway 1 route table

Destination CIDR block	Next hop
10.10.10.0/24	IPsec-VPN connection 1
10.10.20.0/24	IPsec-VPN connection 2

Office 2 gateway device route table

Destination CIDR block	Next hop
172.16.0.0/16	VPN gateway 1 public IP address

Step 2: Create IPsec-VPN connections to connect Office3 and Office4 to VPC2

To create IPsec-VPN connections in the China (Shanghai) region to connect Office3 and Office4 to VPC2, perform the following operations:

1. Create a VPN gateway in VPC2.

   Set the following parameters:

   - **Name**: Enter a name for the VPN gateway. In this example, *VPNgateway2* is used.
   - **Region**: Select **US (Silicon Valley)**.
   - **VPC**: Select the VPC in the **US (Silicon Valley)** region.
   - **Specify VSwitch**: Select **No**.
   - **Maximum Bandwidth**: Select **10 Mbit/s**.
   - **Traffic**: Select **Pay-by-data-transfer**.
   - **IPsec-VPN**: Select **Enable**.
   - **SSL-VPN**: Select **Disable**.

- **Duration**: Select **By Hour**.
- **Service-linked Role**: Click **Create Service-linked Role** and the system automatically creates the service-linked role AliyunServiceRoleForVpn.

  > ⓘ **Note** For more information about how a VPN gateway assumes the role to access other cloud resources, see AliyunServiceRoleForVpn.

  If **Created** is displayed, the service-linked role is created and you do not need to create it again.

For more information, see 创建和管理VPN网关实例.

2. Create two customer gateways and register the public IP addresses of the gateway devices in Office3 and Office4 to the customer gateways. The public IP addresses are used to create IPsec-VPN connections.

   Set the following parameters to create a customer gateway for Office3:

   - **Name**: Enter a name for the customer gateway. In this example, *customer_gt3* is used.
   - **IP Address**: Enter the static public IP address of the gateway device in Office3. In this example, 3.3.XX.XX is used.

   Set the following parameters to create a customer gateway for Office4:

   - **Name**: Enter a name for the customer gateway. In this example, *customer_gt4* is used.
   - **IP Address**: Enter the static public IP address of the gateway device in Office4. In this example, 4.4.XX.XX is entered.

   For more information, see Create a customer gateway.

3. Create two IPsec-VPN connections to connect the gateway devices in Office3 and Office4 to VPNgateway2.

   Set the following parameters to create an IPsec-VPN connection between Office3 and VPNgateway2:

   - **Name**: Enter a name for the IPsec-VPN connection. In this example, *IPsec3* is used.
   - **VPN Gateway**: Select the VPN gateway created in the China (Shanghai) region. In this example, VPNgateway2 is selected.
   - **Customer Gateway**: Select the customer gateway to be connected. In this example, customer_gt3 is selected.
   - **Routing Mode**: Select **Protected Data Flows**.
   - **Local Network**: Enter the CIDR block of the VPC to be connected to the office. In this example, *192.168.0.0/16* is entered.
   - **Remote Network**: Enter the CIDR block of Office3 to be connected to the VPC. In this example, *10.20.10.0/24* is entered.
   - **Effective Immediately**: Specify whether to negotiate immediately. In this example, **Yes** is selected.
     - **Yes**: starts connection negotiations after the configuration is completed.
     - **No**: starts negotiations when inbound traffic is detected.
   - **Pre-Shared Key**: Enter a pre-shared key for identity verification between VPNgateway2 and customer_gt3. In this example, *123456* is entered.

   Use the default settings for the other parameters.

Set the following parameters to create an IPsec-VPN connection between Office4 and VPNgateway2:

- **Name**: Enter a name for the IPsec-VPN connection. In this example, *IPsec4* is used.
- **VPN Gateway**: Select the VPN gateway created in the China (Shanghai) region. In this example, VPNgateway2 is selected.
- **Customer Gateway**: Select the customer gateway to be connected. In this example, customer_gt4 is selected.
- **Routing Mode**: Select Protected Data Flows.
- **Local Network**: Enter the CIDR block of the VPC to be connected to the office. In this example, *192.168.0.0/16* is entered.
- **Remote Network**: Enter the CIDR block of Office4 to be connected to the VPC. In this example, *10.20.20.0/24* is entered.
- **Effective Immediately**: Specify whether to negotiate immediately. In this example, **Yes** is selected.
  - **Yes**: starts connection negotiations after the configuration is completed.
  - **No**: starts negotiations when inbound traffic is detected.
- **Pre-Shared Key**: Enter a pre-shared key for identity verification between VPNgateway2 and customer_gt4. In this example, *654321* is entered.

Use the default settings for the other parameters.

For more information, see Create an IPsec-VPN connection.

4. Load the configurations of the IPsec-VPN connections to the gateway devices in Office3 and Office4.

   For more information, see Configure local gateways.

5. Configure routes on VPNgateway2.

   Configure the following route on VPNgateway2 to route network traffic that is destined for Office3:

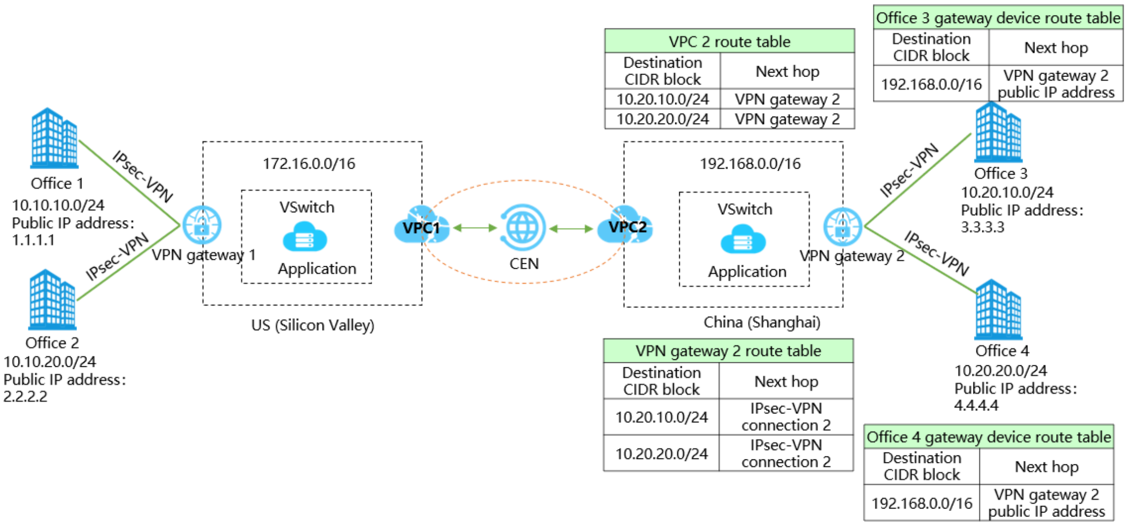
   - **Destination CIDR Block**: Enter the private CIDR block of the destination. In this example, *10.20.10.0/24* is entered.
   - **Next Hop Type**: Select IPsec Connection.
   - **Next Hop**: Select an IPsec-VPN connection. In this example, IPsec3 is selected.
   - **Publish to VPC**: Specify whether to automatically advertise this route to the route table of VPC2. In this example, **Yes** is selected.
     - **Yes**: automatically advertises the route to the route table of the VPC. We recommend that you select this value.
     - **No**: does not advertise the route to the route table of the VPC.
   - **Weight**: Specify a weight. In this example, **0** is specified.

   Configure the following route on VPNgateway2 to route network traffic that is destined for Office4:

   - **Destination CIDR Block**: Enter the private CIDR block of the destination. In this example, *10.20.20.0/24* is entered.
   - **Next Hop Type**: Select IPsec Connection.

- **Next Hop**: Select an IPsec-VPN connection. In this example, IPsec4 is selected.
- **Publish to VPC**: Specify whether to automatically advertise this route to the route table of VPC2. In this example, **Yes** is selected.
  - **Yes**: automatically advertises the route to the route table of the VPC. We recommend that you select this value.
  - **No**: does not advertise the route to the route table of the VPC.
- **Weight**: Specify a weight. In this example, **0** is specified.

The following figure shows the route tables of Office3, Office4, VPNgateway2, and VPC2.



VPC 2 route table

Destination CIDR block	Next hop
10.20.10.0/24	VPN gateway 2
10.20.20.0/24	VPN gateway 2

Office 3 gateway device route table

Destination CIDR block	Next hop
192.168.0.0/16	VPN gateway 2 public IP address

VPN gateway 2 route table

Destination CIDR block	Next hop
10.20.10.0/24	IPsec-VPN connection 2
10.20.20.0/24	IPsec-VPN connection 2

Office 4 gateway device route table

Destination CIDR block	Next hop
192.168.0.0/16	VPN gateway 2 public IP address

Step 3: Attach VPC1 and VPC2 to the same CEN instance

After you connect the offices to the VPCs, you must attach VPC1 and VPC2 to the same CEN instance.

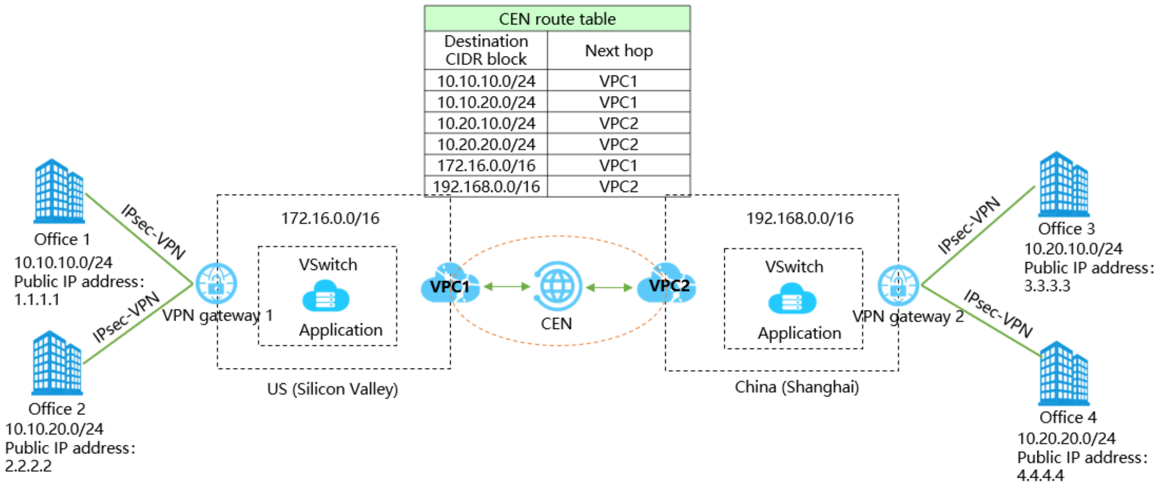
> ? **Note** In this example, the previous version of the CEN console is used. For more information, see Usage notes on the previous console version.

1. Log on to the CEN console.
2. On the **Instances** page, find the CEN instance that you want to manage and click its ID.
3. Click the **Networks** tab, and then click **Attach Network**.
4. Click the **Your Account** tab.
5. Set the following parameters and click **OK**:
   - **Network Type**: Select **VPC**.
   - **Region**: Select **US (Silicon Valley)**.
   - **Networks**: Select VPC1.
6. Repeat the preceding operations to attach VPC2 to the same CEN instance.

Step 4: Advertise routes to the CEN instance

To enable other VPCs that are attached to the CEN instance to learn the routes that point to the offices, you must advertise the routes of the VPCs in the US (Silicon Valley) and China (Shanghai) regions to the CEN instance. For more information, see Advertise routes to CEN.

The following figure shows the CEN route table after the routes are advertised.



CEN route table	
Destination CIDR block	Next hop
10.10.10.0/24	VPC1
10.10.20.0/24	VPC1
10.20.10.0/24	VPC2
10.20.20.0/24	VPC2
172.16.0.0/16	VPC1
192.168.0.0/16	VPC2

Step 5: Configure routes on the gateway devices

After the routes are advertised to the CEN instance, you must configure routes that point to Office3 and Office4 on the gateway devices of Office1 and Office2. You must also configure routes that point to Office1 and Office2 on the gateway devices of Office3 and Office4.

The configurations in the following table are for reference only. The configurations may vary based on the manufacturer of the gateway devices.

Office	Routes

Office1	`ip route 192.168.0.0/16 5.5.XX.XX`
	`ip route 10.20.10.0/24 5.5.XX.XX`
	`ip route 10.20.20.0/24 5.5.XX.XX`
	`ip route 10.10.20.0/24 5.5.XX.XX   #5.5.XX.XX is the public IP address of VPNgateway1.`

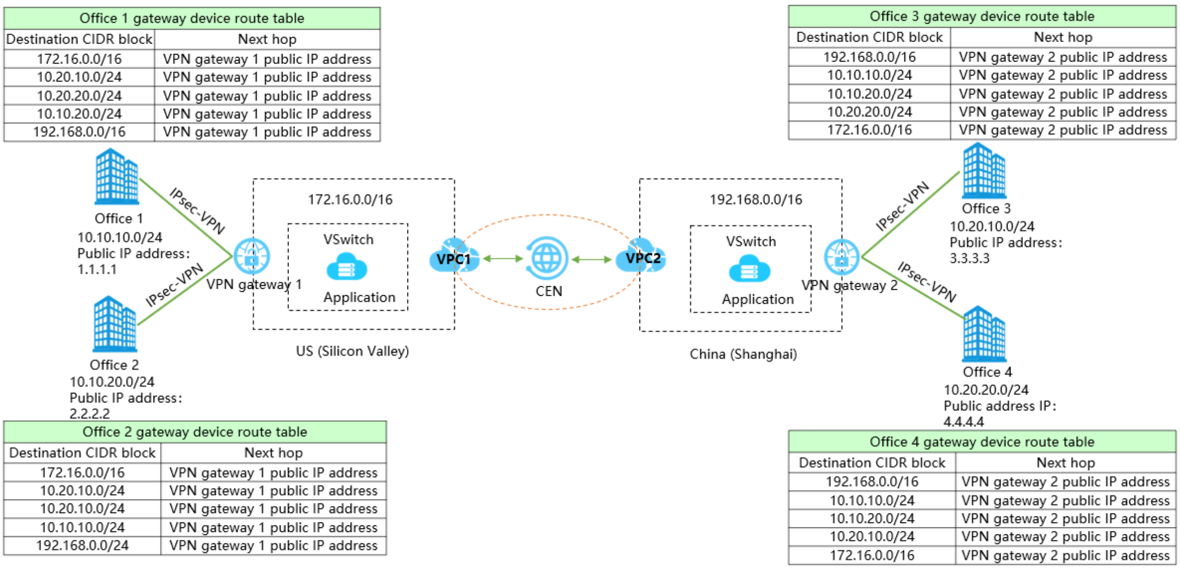
Office2	`ip route 192.168.0.0/16 5.5.XX.XX`
	`ip route 10.20.10.0/24 5.5.XX.XX`
	`ip route 10.20.20.0/24 5.5.XX.XX`
	`ip route 10.10.10.0/24 5.5.XX.XX   #5.5.XX.XX is the public IP address of VPNgateway1.`

Office3	`ip route 172.16.0.0/16 6.6.XX.XX`
	`ip route 10.10.10.0/24 6.6.XX.XX`
	`ip route 10.10.20.0/24 6.6.XX.XX`
	`ip route 10.20.20.0/24 6.6.XX.XX   #6.6.XX.XX is the public IP address of VPNgateway2.`

Office	Routes

Office4	`ip route 172.16.0.0/16 6.6.XX.XX`
	`ip route 10.10.10.0/24 6.6.XX.XX`
	`ip route 10.10.20.0/24 6.6.XX.XX`
	`ip route 10.20.10.0/24 6.6.XX.XX   #6.6.XX.XX is the public IP address of VPNgateway2.`

The following figure shows the route tables of the offices.



Office 1 gateway device route table

Destination CIDR block	Next hop
172.16.0.0/16	VPN gateway 1 public IP address
10.20.10.0/24	VPN gateway 1 public IP address
10.20.20.0/24	VPN gateway 1 public IP address
10.10.20.0/24	VPN gateway 1 public IP address
192.168.0.0/16	VPN gateway 1 public IP address

Office 2 gateway device route table

Destination CIDR block	Next hop
172.16.0.0/16	VPN gateway 1 public IP address
10.20.10.0/24	VPN gateway 1 public IP address
10.20.10.0/24	VPN gateway 1 public IP address
10.10.10.0/24	VPN gateway 1 public IP address
192.168.0.0/24	VPN gateway 1 public IP address

Office 3 gateway device route table

Destination CIDR block	Next hop
192.168.0.0/16	VPN gateway 2 public IP address
10.10.10.0/24	VPN gateway 2 public IP address
10.10.20.0/24	VPN gateway 2 public IP address
10.20.20.0/24	VPN gateway 2 public IP address
172.16.0.0/16	VPN gateway 2 public IP address

Office 4 gateway device route table

Destination CIDR block	Next hop
192.168.0.0/16	VPN gateway 2 public IP address
10.10.10.0/24	VPN gateway 2 public IP address
10.10.20.0/24	VPN gateway 2 public IP address
10.20.10.0/24	VPN gateway 2 public IP address
172.16.0.0/16	VPN gateway 2 public IP address

Step 6: Test the connectivity

In this example, a client in Office1 is used to access the clients in Office2, Office3, and Office4 to test the connectivity.

1. Open the CLI on a client in Office1.
2. Run the `ping` command to ping the clients in Office2, Office3, and Office4. If echo reply packets are returned, it indicates that the connections are established.

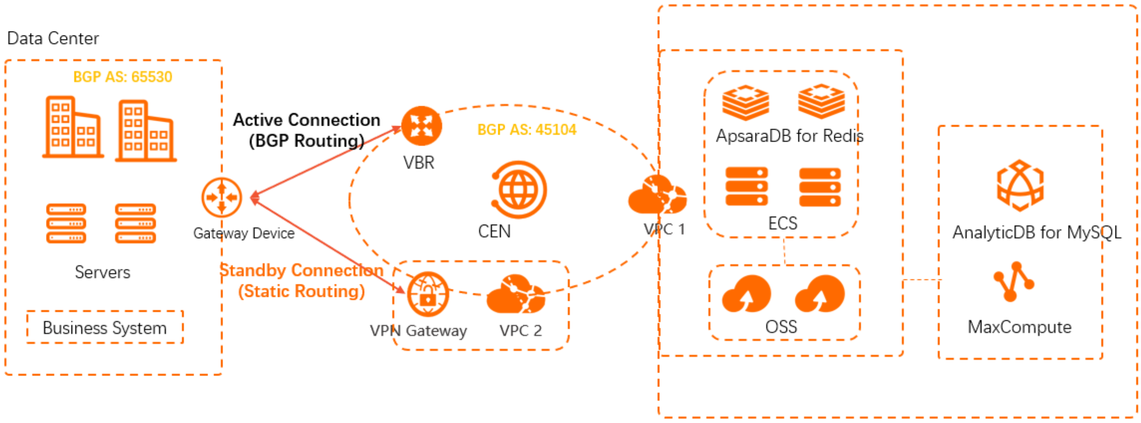
7.Configure active/standby connections by using IPsec-VPN and an Express Connect circuit

This topic describes how to configure active/standby connections between a data center and a virtual private cloud (VPC) by using IPsec-VPN and an Express Connect circuit.

Scenario

This topic uses the following scenario to show how to use both IPsec-VPN and an Express Connect circuit to connect a data center to a VPC. A company has a data center in Hangzhou, and has deployed VPC 1 in the China (Hangzhou) region. In VPC 1, cloud services such as Elastic Compute Service (ECS) are deployed for interaction and data analytics. The company wants to establish active/standby connections between the data center and VPC 1. The following section describes the connections:

- A VPN gateway is associated with an independent VPC (VPC 2). In this example, no service is deployed in VPC 2. VPC 2 serves as a transit VPC to establish IPsec-VPN connections between the data center and VPC 1.
- When the Express Connect circuit and IPsec-VPN connection are working as expected, all traffic between the data center and VPC 1 is forwarded through the Express Connect circuit. When the Express Connect circuit is not working as expected, the IPsec-VPN connection takes over.



Prerequisites

- You must plan routing protocols for the data center and network instances. In this topic, the following routing protocols are used:
  - Static routing is used between the gateway device of the data center and the VPN gateway.

- Border Gateway Protocol (BGP) dynamic routing is used between the gateway device of the data center and the virtual border router (VBR).

> ⓘ **Note** In scenarios where the VPN gateway serves as the standby connection and the Express Connect circuit serves as the active connection:
>
> - If the VPN gateway is associated with an independent VPC (for example, VPC 2 in this topic), the VBR must use BGP dynamic routing. The VPN gateway can use static routing or BGP dynamic routing.
> - If the VPN gateway is associated with a VPC where services are deployed (for example, VPC 1 in this topic), both the VBR and VPN gateway must use BGP dynamic routing.

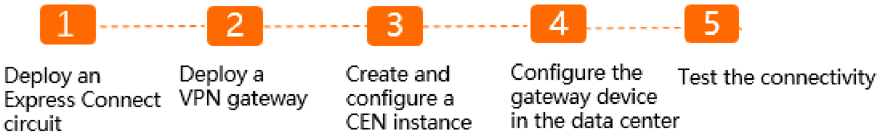
- You must plan networks for the data center and network instances. Make sure that the CIDR block of the data center does not overlap with those of the network instances. In this topic, the following CIDR blocks are used.

Item	CIDR block	Public IP address
VPC1	192.168.0.0/16	IP address of the ECS instance: 192.168.20.161
VPC2	10.0.0.0/16	N/A
VBR	10.1.0.0/30	○ VLAN ID: 0 ○ Peer IPv4 address on the Alibaba Cloud side: 10.1.0.1/30 ○ Peer IPv4 address on the customer side: 10.1.0.2/30 In this topic, the device on the customer side refers to the gateway device in the data center.
Data center	172.16.0.0/16	IP address of the client: 172.16.1.188
Gateway device in the data center	10.1.0.0/30	○ Public IP address: 211.XX.XX.68 ○ IP address of the interface connected to the Express Connect circuit: 10.1.0.2/30 ○ The BGP autonomous system number (ASN): 65530

- VPC 1 and VPC 2 are created in the China (Hangzhou) region. The cloud services that are used for business interaction and data analytics are deployed in VPC 1. No service is deployed in VPC 2. VPC 2 is associated with a VPN gateway and serves as a transit VPC between the data center and VPC 1. For more information, see Create and manage a VPC.
- Check the gateway device in the data center. Make sure that it supports standard IKEv1 and IKEv2 protocols. For information about whether the gateway device supports the IKEv1 and IKEv2 protocols, consult the gateway device manufacturer.
- A static IP address is assigned to the gateway device in the data center.

- You understand the security group rules of the ECS instances in VPC 1. Make sure that the rules allow the data center to access the ECS instances in VPC 1. For more information, see Query security group rules and Add a security group rule.

Procedure


1
Deploy an Express Connect circuit
2
Deploy a VPN gateway
3
Create and configure a CEN instance
4
Configure the gateway device in the data center
5
Test the connectivity

Step 1: Deploy an Express Connect circuit

1. Deploy an Express Connect circuit.

   You must apply for an Express Connect circuit in the China (Hangzhou) region. For more information, see Create a dedicated connection over an Express Connect circuit or Overview.

2. Create a VBR.

   i. Log on to the Express Connect console.

   ii. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.

   iii. In the top navigation bar, select the region where you want to create a VBR.

   In this example, the **China (Hangzhou)** region is selected.

   iv. On the **Virtual Border Routers (VBRs)** page, click **Create VBR**.

   v. In the **Create VBR** panel, set the following parameters and click **OK**.

   - **Account**: Select **Current account**.
   - **Name**: VBR is used in this example.
   - **Physical Connection Interface**: Select the Express Connect circuit you have applied for.
   - **VLAN ID**: Set this parameter to 0.
   - **IPv4 Address of Gateway at Alibaba Cloud**: Set this parameter to 10.1.0.1.
   - **IPv4 Address of Gateway at Customer Side**: Set this parameter to 10.1.0.2.
   - **Subnet Mask**: Set this parameter to 255.255.255.252.

3. Create a BGP group.

   i. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR.

   ii. On the details page of the VBR, click the **BGP Groups** tab and click **Create BGP Group**.

   iii. In the **Create BGP Group** panel, set the following parameters and click **OK**.

   - **Name**: Enter a name for the BGP group. In this example, test is used.
   - **Peer ASN**: Enter the ASN of the gateway device in the data center. In this example, 65530 is used.
   - **BGP Key**: Enter the key of the BGP group. This parameter is not set in this example.
   - **Description**: Enter the description of the BGP group. In this example, test is used.

4. Create a BGP peer.

   i. On the details page of the VBR, click the **BGP Peers** tab and click **Create BGP Peer**.

ii. In the **Create BGP Peer** panel, set the following parameters and click **OK**.

- **BGP Group**: Select a BGP group. The BGP group test is used in this example.
- **BGP peer IP address**: Enter the IP address of the BGP peer. In this example, 10.1.0.2 is used, which is the port IP address of the gateway device in the data center.

Step 2: Deploy a VPN gateway

1. Create a VPN gateway.

i.

ii. In the top navigation bar, select the **China (Hangzhou)** region.

iii.

iv. On the buy page, set the following parameters, click **Buy Now**, and then complete the payment.

- **Name**: Enter a name for the VPN gateway.
- **Region**:Select the region where you want to deploy the VPN gateway.

  In this example, the VPN gateway is to be associated with VPC 2. Make sure that VPC 2 and the VPN gateway are deployed in the same region. In this example, the **China (Hangzhou)** region is selected.
- **VPC**:Select the VPC to be associated with the VPN gateway. VPC 2 is selected in this example.
- **Specify VSwitch**: Specify whether to create the VPN gateway in a vSwitch of the VPC. **No** is selected in this example.

  If you select **Yes**, you must also specify a **vSwitch**.
- **Peak Bandwidth**: Specify the maximum bandwidth for the VPN gateway. The bandwidth is used for data transfer over the Internet.
- **Traffic**: By default, the VPN gateway uses the pay-by-data-transfer metering method. For more information, see Pay-as-you-go.
- **IPsec-VPN**: You can enable or disable the IPsec-VPN feature. After you enable this feature, you can establish connections between a data center and a VPC or between two VPCs. **Enable** is selected in this example.
- **SSL-VPN**: You can enable or disable the SSL-VPN feature. After you enable this feature, you can connect to the VPC from a client regardless of the location. **Disable** is selected in this example.
- **Duration**: By default, the VPN gateway is billed on an hourly basis.

v. Return to the **VPN Gateways** page, check and record the public IP address of the VPN gateway that you created. This address is used in configuring the router in the data center.

A newly created VPN gateway is in the **Preparing** state. After about 1 to 5 minutes, its status changes to **Normal**. The **Normal** state indicates that the VPN gateway is initialized and ready for use.

2. Creates a customer gateway.

i.

ii.

iii. On the **Create Customer Gateway** page, set the following parameters and click **OK**.

- **Name**: Enter a name for the customer gateway.
- **IP Address**: Enter the public IP address of the gateway device in the data center that you want to connect to VPC2. In this example,211.XX.XX.68 is entered.
- **ASN**: Enter the ASN of the gateway device in the data center. This parameter is not set in this example.
- **Description**: Enter a description for the customer gateway.

3. Create an IPsec-VPN connection.

i.

ii.

iii. On the **Create IPsec Connection** page, set the following parameters and click **OK**.

- **Name**: Enter a name for the IPsec-VPN connection.
- **VPN Gateway**: Select the VPN gateway that you created.
- **Customer Gateway**: Select the customer gateway you created.
- **Routing Mode**: Select a routing mode. In this example, **Destination Routing Mode** is selected.
- **Effective Immediately**: Select whether to immediately start connection negotiations. **No** is selected in this example.
  - **Yes**: immediately starts negotiations after you complete the configurations.
  - **No**: starts negotiations when data transfer is detected.
- **Pre-Shared Key**: Enter the pre-shared key. The pre-shared key of the gateway device in the data center must be the same as this value. In this example, a random value is used by default.

  Use the default settings for other parameters.

For more information, see Create an IPsec-VPN connection.

4. Configure routes on the VPN gateway.

You must use the VPN gateway to advertise the routes of the data center to VPC2.

i. After an IPsec-VPN connection is created, click **OK** in the **Established** dialog box to advertise the routes in the VPN gateway.

ii.

iii. On the **VPN Gateways** page, find the VPN gateway you created and click the ID.

iv. On the **Destination-based Routing** tab, click **Add Route Entry**.

v. In the **Add Route Entry** panel, set the following parameters, and click **OK**.

- **Destination CIDR Block**: Enter the CIDR block of the data center. In this example, 172.16.0.0/16 is entered.
- **Next Hop Type**: Select **IPsec Connection**.
- **Next Hop**: Select the IPsec-VPN connection you created.
- **Publish to VPC**: Specify whether to automatically advertise new routes to the route table of VPC 2. In this example, **Yes** is selected.
- **Weight**: Select a weight for the route. In this example, **100** is used, which indicates the highest priority.

> Note If the VPN gateway contains routes that have the same destination CIDR block, you cannot specify the weights of these routes to 100 at the same time.

5. Load the VPN configuration to the gateway device in the data center.

   i.

   ii. On the **IPsec Connections** page, find the IPsec-VPN connection you created. In the **Actions** column, select ⋮ > **Download Configuration**.

   iii. Load the configuration of the IPsec-VPN connection to the gateway device in the data center. For more information, see Configure a gateway device in a data center.

Step 3: Create and configure a CEN instance

After you configure the Express Connect circuit and VPN gateway, you must attach VPC 1, VPC 2 and the VBR to a Cloud Enterprise Network (CEN) instance. The CEN instance can connect the data center to VPC 1.

1. Create a CEN instance.

   i. Log on to the CEN console.

   ii. On the **Instances** page, click **Create CEN Instance**.

   iii. In the **Create CEN Instance** panel, set the following parameters and click **OK**.

   - **Name**: Enter a name for the CEN instance.
   - **Description**: Enter a description for the CEN instance.
   - **Network Type**: Select the type of network instance to attach. In this example, **VPC** is selected.
   - **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
   - **Networks**: Select the network instance that you want to attach. VPC 2 is selected in this example.

2. Attach VPC 1 and the VBR to the CEN instance.

   i. On the **Instances** page, find the CEN instance that you want to manage and click its ID.

   ii. Click the **Networks** tab and then click **Attach Network**.

   iii. In the **Attach Network** panel, click the **Your Account** tab.

iv. Set the following parameters and click **OK**:

- **Network Type**: Select the type of network instance to attach. In this example, **VPC** is selected.
- **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
- **Networks**: Select the network instance that you want to attach. In this example, VPC 1 is selected.

v. Repeat the preceding steps to attach the VBR to the CEN instance.

3. Advertise the routes of the data center from VPC 2 to CEN.

   After you use the VPN gateway to advertise the routes of the data center to VPC 2, the routes in VPC 2 are in the **NonPublished** state by default. You must manually advertise the routes of the data center from VPC 2 to CEN. This way, VPC 1 can learn the routes of the data center from VPC 2.

   i. Log on to the CEN console.

   ii. On the **Instances** page, find the CEN instance that you want to manage and click its ID.

   iii. On the details page of the CEN instance, click the **Routes** tab.

   iv. On the **Routes** tab, view the routes of VPC 2, find the routes of the data center, and then click **Publish** in the **Publishing Progress** column.

   v. In the **PublishRoute** message, click **OK**.

4. Configure health checks for the Express Connect circuit.

   You must configure health checks for the Express Connect circuit. A health check sends probe packets based on the time interval and number of probe packets that you specify. If probe packets are consecutively lost, the CEN instance routes traffic to the IPsec-VPN connection.

   i. Log on to the CEN console.

   ii. In the left-side navigation pane, click **Health Check**.

   iii. Select the region to which the VBR belongs and click **Set Health Check**.

   iv. In the **Set Health Check** panel, set the following parameters and click **OK**.

   - **Instances**: Select the CEN instance to which the VBR is attached.
   - **Virtual Border Router (VBR)**: Select the VBR that you want to monitor.
   - **Source IP**: In this example, **Automatic IP Address** is selected.

     If you select **Automatic IP Address**, the system automatically allocates IP addresses in the 100.96.0.0/16 CIDR block to probe the connectivity of the Express Connect circuit.
   - **Destination IP**: Enter the IP address on the customer side of the VBR.
   - **Probe Interval (Seconds)**: Specify the time interval at which probe packets are sent for health checks. Unit: seconds. The default value is used in this example.
   - **Probe Packets**: Specify the number of probe packets that are sent at each interval. Unit: packets. The default value is used in this example.

Step 4: Configure the gateway device in the data center

The following sample code is for reference only. The commands may vary from vendor to vendor. Consult the vendor for specific commands.

```
#Configure BGP dynamic routing, establish a BGP peering connection to the VBR, and advertis
e the routes of the data center to Alibaba Cloud.
interface GigabitEthernet 0/12          #The port is used to connect the gateway device of
the data center to the Express Connect circuit.
no switchport
ip address 10.1.0.2 255.255.255.252     #The IP address of the port. The IP address must be
the same as the IPv4 address of the VBR on the customer side.
router bgp 65530
bgp router-id 10.1.0.2
network 172.16.0.0 mask 255.255.0.0     #Advertise the routes of the data center to Alibaba
Cloud.
neighbor 10.1.0.1 remote-as 45104       #Establish a peering connection to the VBR.
exit
#Set the priority of the route that points to VPC 1 through the VPN gateway. The priority m
ust be lower than that of the BGP route.
ip route 192.168.0.0 255.255.0.0 <The public IP address of the VPN gateway> preference 255
#Configure the return route of the probe packets.
ip route <The source IP address for the health check> 255.255.255.255 10.1.0.1
```

Step 5: Test the connectivity

1. Open the command-line interface (CLI) on a computer in the data center.
2. On the CLI, run the `ping` command to ping the IP address of an ECS instance in VPC1. The IP address of the ECS instance falls within the 192.168.0.0/16 CIDR block. If the client receives a response packet, it indicates that the data center is connected to VPC 1.
3. On the gateway device in the data center, disable the Express Connect circuit port to close the connection. Run the `ping` command on the CLI again to test the connectivity between the data center and VPC 1. If you receive a response packet, it indicates that the standby IPsec-VPN connection is working as expected.

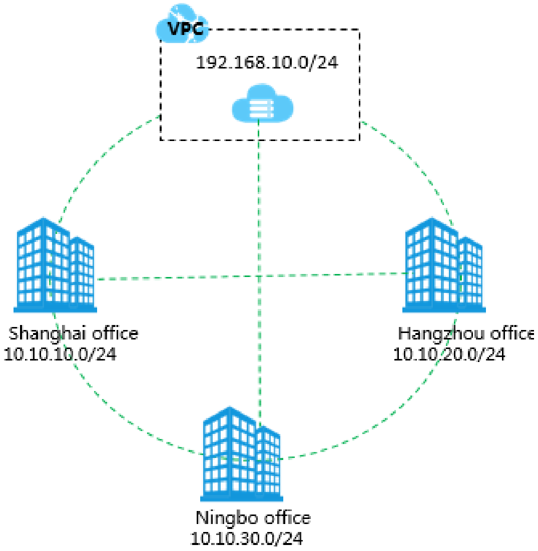
8.Configure multi-site connections

You can create IPsec-VPN connections between multiple sites and locations. With the VPN-Hub function, the connected sites can communicate with the connected VPC, and also communicate with each of the other sites. VPN-Hub meets the needs of large enterprises to establish intranet communications between different sites.

VPN-Hub overview

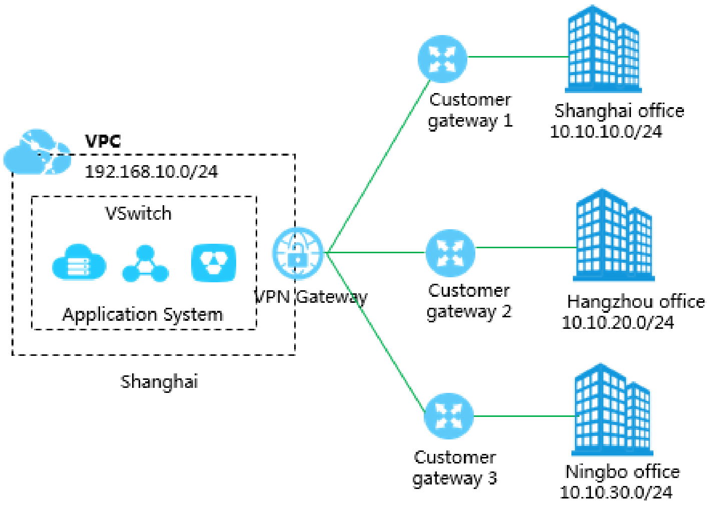
The VPN-Hub function is enabled by default. To achieve multi-site connections, you must create corresponding IPsec-VPN connections. A VPN Gateway can have up to ten IPsec-VPN connections. Therefore, you can connect up to ten office sites with one VPN Gateway.

The following scenario is used to illustrate connecting office sites in the cities of Shanghai, Hangzhou, and Ningbo. Before you begin, make sure that you have obtained the public IP address of the gateway device for each office site.



As shown in the following figure, to connect the three office sites (Shanghai, Hangzhou, and Ningbo), you only need to create a VPN Gateway and three customer gateways, and establish three IPsec-VPN connections.

> **Note** Make sure the IP address ranges of all the connected sites do not conflict with each other.



Step 1: Create a VPN Gateway

Create a VPN Gateway in the region to which the VPC belongs. Three IPsec-VPN connections will be established for the VPN Gateway and are connected to the office sites in Shanghai, Hangzhou, and Ningbo. For more information, see 创建和管理VPN网关实例.

> ⓘ **Note** Make sure that the IPsec-VPN function is enabled.

Step 2: Create an IPsec-VPN connection to the Shanghai office

1. Create a customer gateway and register the public IP address of the local gateway device to Alibaba Cloud to establish an IPsec-VPN connection.

   The IP address of the customer gateway is the public IP address of the gateway device of the Shanghai office. For more information, see Create a customer gateway.

2. Create an IPsec-VPN connection.

   Create an IPsec connection to connect the VPN Gateway and the customer gateway. For more information, see Create an IPsec-VPN connection.

3. Load VPN configurations to the gateway device of the local office site.

   Load VPN configurations according to the requirements on the gateway device of the local office site. For more information, see Configure local gateways.

Step 3: Create additional IPsec-VPN connections for the other two sites

Follow the same procedures in the Step 2 to create two IPsec connections for the Hangzhou office and the Ningbo office.

Step 4: Configure the VPN Gateway route

To configure the VPN Gateway route, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. On the **VPN Gateways** page, select the region of the VPN Gateway.

4. Find the target VPN Gateway, and click the instance ID in the **Instance ID/Name** column.
5. On the **Destination-based Routing** page, click **Add Route Entry**.
6. Configure three route entries according to the following information and then click **OK**.
   - **Destination CIDR Block**: Enter the private CIDR block to be accessed.
   - **Next Hop**: Select the target IPsec-VPN connection instance.
   - **Publish to VPC**: Select whether to publish the new route to the VPC route table.
   - **Weight**: Select a weight.

   The following are the destination-based routes configured in this example:

Destination CIDR Block	Next Hop	Publish to VPC	Weight
10.10.10.0/24	IPsec-VPN connection instance 1	Yes	100
10.10.20.0/24	IPsec-VPN connection instance 2	Yes	100
10.10.30.0/24	IPsec-VPN connection instance 3	Yes	100

The IPsec-VPN connections to the three office sites have now been established. Each office site can now communicate with the VPC and can communicate with the other office sites over their intranet.

9.Encrypt a private connection by using a private VPN gateway

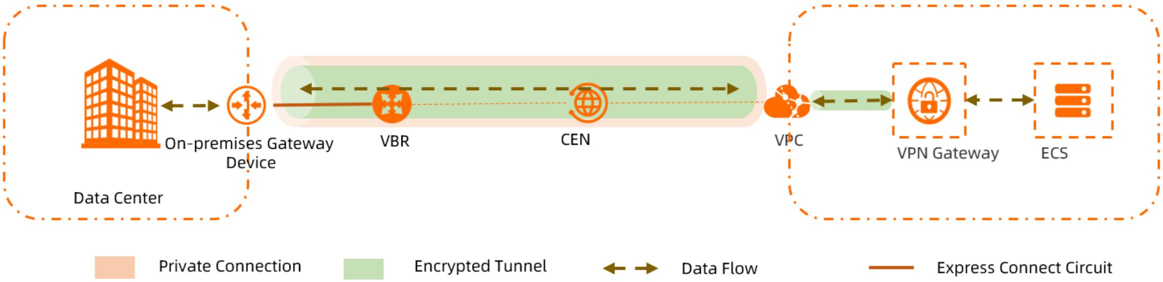
9.1. Overview of configuration methods

After you establish a private connection between a data center and a virtual private cloud (VPC) through an Express Connect circuit and Cloud Enterprise Network (CEN), the private connection is not encrypted. This causes security risks. To improve network security, you can use a private VPN gateway to encrypt the private connection over the Express Connect circuit (hereafter referred to as the private connection). This topic describes how to encrypt private connections and the configuration methods.

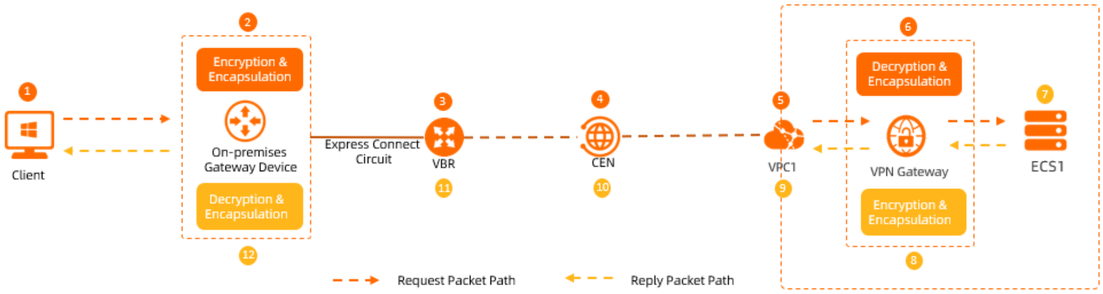
> **Note** Private VPN gateways are in invitational preview. To use a private VPN gateway, contact your sales manager or .

How it works

After you establish a private connection between a data center and a VPC through an Express Connect circuit and CEN, you can establish an encrypted tunnel between a private VPN gateway and an on-premises gateway device. You can configure routes to route network traffic between the data center and the VPC to the encrypted tunnel. This way, network traffic transmitted through the tunnel is encrypted.



The following example describes how a private connection is encrypted. In this example, a client in a data center accesses an Elastic Compute Service (ECS) instance in a VPC.


1
Client
2
Encryption & Encapsulation
On-premises Gateway Device
Decryption & Encapsulation
12
Express Connect Circuit
3
VBR
11
4
CEN
10
5
VPC1
9
6
Decryption & Encapsulation
VPN Gateway
Encryption & Encapsulation
8
7
ECS1
Request Packet Path
Reply Packet Path

Number	Node	Description
①	Client	1. The client initiates a request. 2. The client queries the route table and forwards the request packet to the on-premises gateway device.
②	On-premises gateway device	1. After the on-premises gateway device receives the request packet, the on-premises gateway device encrypts and encapsulates the request packet based on the destination IP address and IPsec configurations. After the request packet is encrypted and encapsulated, the destination IP address changes to the private IP address of the VPN gateway. 2. The on-premises gateway device queries the route table and forwards the request packet to the virtual border router (VBR) based on the new destination IP address.
③	VBR	After the VBR receives the request packet, the VBR queries the route table and forwards the request packet to the CEN instance.
④	CEN instance	After the CEN instance receives the request packet, the CEN instance queries the route table and forwards the request packet to the VPC.
⑤	VPC	After the VPC receives the request packet, the VPC queries the route table and forwards the request packet to the VPN gateway.
⑥	VPN gateway	1. After the VPN gateway receives the request packet, the VPN gateway decrypts and re-encapsulates the request packet. 2. The VPN gateway queries the route table and forwards the request packet to the ECS instance based on the destination IP address of the request packet.
⑦	ECS instance	1. After the ECS instance receives the request packet, the ECS instance sends a response packet to the client. 2. The ECS instance queries the route table and forwards the response packet to the VPN gateway based on the destination IP address of the response packet.
⑧	VPN gateway	1. After the VPN gateway receives the response packet, the VPN gateway encrypts and encapsulates the response packet. After the response packet is encrypted and encapsulated, its destination IP address changes to the VPN IP address of the on-premises gateway device. 2. The VPN gateway queries the route table and forwards the response packet to the VPC based on the new destination IP address.

Number	Node	Description
⑨	VPC	After the VPC receives the response packet, the VPC queries the route table and forwards the response packet to the CEN instance.
⑩	CEN instance	After the CEN instance receives the response packet, the CEN instance queries the route table and forwards the response packet to the VBR.
⑪	VBR	After the VBR receives the response packet, the VBR queries the route table and forwards the response packet to the on-premises gateway device.
⑫	On-premises gateway device	1. After the on-premises gateway device receives the response packet, the on-premises gateway device decrypts and re-encapsulates the response packet. 2. The on-premises gateway device queries the route table and forwards the response packet to the client based on the destination IP address of the response packet.

Configuration methods

To encrypt a private connection by using a private VPN gateway, you can configure the VPN gateway and the VBR connected to the VPN gateway in different manners. The following table describes the differences between the configuration methods and provides links to the tutorials.

Configuration method	Description	Tutorial	Impact on communication after the VPN connection is interrupted
Method 1	Configure static routing for the VBR and VPN gateway.	Encrypt private connections by using static routes	• The private connection is no longer encrypted. • The private connection between the data center and the VPC is interrupted. You can manually withdraw the routes that are advertised on the VPN gateway. After you withdraw the routes, the VPC is connected to the data center through an Express Connect circuit and CEN.

Configuration method	Description	Tutorial	Impact on communication after the VPN connection is interrupted
Method 2	- Configure static routing for the VBR. - Configure Border Gateway Protocol (BGP) dynamic routing for the VPN gateway. ⓘ **Note** You cannot configure BGP dynamic routing for the VBR if static routing is configured for the VPN gateway.	Encrypt private connections by using static routing and BGP routing	- The private connection is no longer encrypted. - The system automatically withdraws the BGP dynamic routes that are advertised on the VPN gateway. - The VPC is connected to the data center through an Express Connect circuit and CEN.
Method 3	Configure BGP dynamic routing for the VBR and VPN gateway.	Encrypt private connections by using BGP routing	- The private connection is no longer encrypted. - The system automatically withdraws the BGP dynamic routes that are advertised on the VPN gateway. - The VPC is connected to the data center through an Express Connect circuit and CEN.

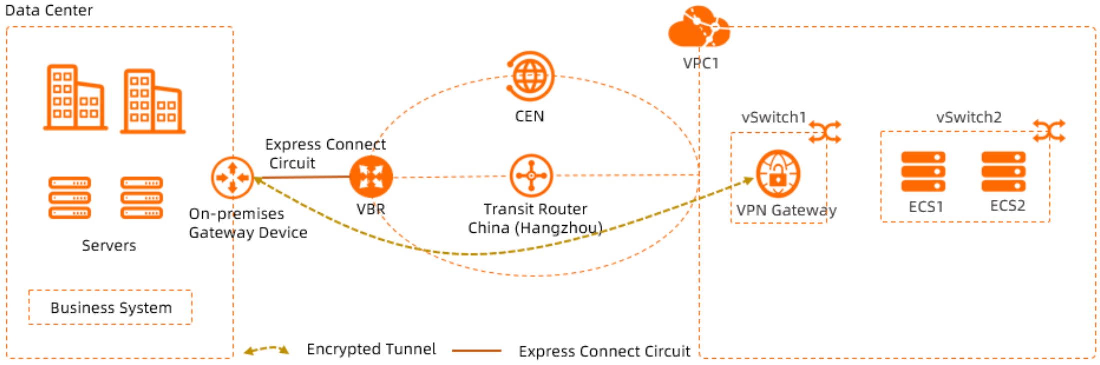
9.2. Encrypt private connections by using static routes

This topic describes how to encrypt the private connection between a data center and a virtual private cloud (VPC) by using a private VPN gateway (hereafter referred to as "VPN gateway"). To encrypt the private connection between a data center and a VPC, you can configure static routes for the VPN gateway and the virtual border router (VBR) that connects the data center to the VPC.

Background information

Before you start, we recommend that you understand how private connections are encrypted and the configuration methods. For more information, see Overview of configuration methods.

Scenarios



The preceding scenario is used as an example in this topic. An enterprise owns a data center in Hangzhou and has a VPC (VPC1) deployed in the China (Hangzhou) region. Applications are deployed on Elastic Compute Service (ECS) instances in VPC1. Due to business growth, the enterprise wants to connect VPC1 to the data center through Express Connect circuits and Cloud Enterprise Network (CEN). In addition, the enterprise wants to encrypt the connection between VPC1 and the data center due to security concerns.

After VPC1 is connected to the data center through CEN and Express Connect circuits, the enterprise can create a VPN gateway in VPC1 and establish an IPsec-VPN connection between the VPN gateway and an on-premises gateway device. Then, the enterprise can configure static routes for both the VBR and VPN gateway to encrypt the private connection.

Preparations

- Private VPN gateways are in invitational preview. Make sure that you have applied for the required permissions from your sales manager or to apply for the required permissions.
- You must plan networks for the data center and network instances. Make sure that the CIDR block of the data center does not overlap with those of the network instances. The following table describes the CIDR blocks in this example.

Item	CIDR block	IP address
VPC1	○ Primary CIDR block: 10.0.0.0/16 ○ CIDR block to which vSwitch1 belongs: 10.0.0.0/24 ○ CIDR block to which vSwitch2 belongs: 10.0.1.0/24	○ ECS1: 10.0.1.1 ○ ECS2: 10.0.1.2

Item	CIDR block	IP address
VBR	10.0.0.0/30	○ VLAN ID: 0 ○ IPv4 address on the Alibaba Cloud side: 10.0.0.2/30 ○ IPv4 address on the user side: 10.0.0.1/30 In this example, the IPv4 address on the user side is the IPv4 address of the gateway device in the data center.
Data center	○ Primary CIDR block: 192.168.0.0/16 ○ Subnet1: 192.168.0.0/24 ○ Subnet2:192.168.1.0/24	Client: 192.168.1.1
On-premises gateway device	○ 10.0.0.0/30 ○ 192.168.0.0/24	○ VPN IP address: 192.168.0.251 The VPN IP address refers to the IP address of the interface of the on-premises gateway device to be connected to the VPN gateway. ○ IP address of the interface connected to the Express Connect circuit: 10.0.0.1

- VPC1 is deployed in the China (Hangzhou) region and applications are deployed on the ECS instances in VPC1. For more information, see Create and manage a VPC.

  Make sure that VPC1 in the China (Hangzhou) region contains at least one vSwitch in a zone that supports Enterprise Edition transit routers. In addition, each vSwitch must have at least one idle IP address so that VPC1 can be attached to the CEN instance. For more information, see Create a VPC connection.

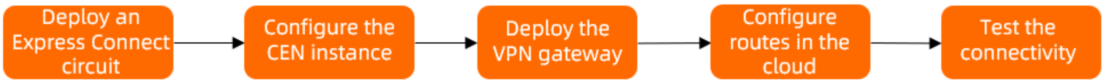
  In this example, VPC1 contains two vSwitches (vSwitch1 and vSwitch2). vSwitch1 is deployed in Zone H and vSwitch2 is deployed in Zone I. ECS instances are deployed on vSwitch2. vSwitch1 is used only to associate with the VPN gateway.

  > **Note** When you create a VPC, we recommend that you create a dedicated vSwitch in the VPC for the VPN gateway. This way, the vSwitch can allocate a private IP address to the VPN gateway.

- Check the gateway device in the data center. Make sure that it supports standard IKEv1 and IKEv2 protocols. To check whether the gateway device supports the IKEv1 and IKEv2 protocols, contact the gateway vendor.
- Take note of the security group rules that apply to ECS instances in VPC1 and access control list (ACL) rules that apply to the client in the data center. Make sure that these rules allow ECS instances in VPC1 to communicate with the client in the data center. For more information, see Query security

group rules and Add a security group rule.

Procedure


Deploy an Express Connect circuit
Configure the CEN instance
Deploy the VPN gateway
Configure routes in the cloud
Test the connectivity

Step 1: Deploy an Express Connect circuit

You must deploy an Express Connect circuit to connect the data center to Alibaba Cloud.

1. Create a connection over an Express Connect circuit.

   You must apply for an Express Connect circuit in the China (Hangzhou) region. For more information, see Create a dedicated connection over an Express Connect circuit or Overview.

   In this example, a dedicated connection over an Express Connect circuit is created.

2. Create a VBR.

   i. Log on to the Express Connect console.

   ii. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.

   iii. In the top navigation bar, select the region where you want to create the VBR.

   In this example, the **China (Hangzhou)** region is selected.

   iv. On the **Virtual Border Routers (VBRs)** page, click **Create VBR**.

   v. In the **Create VBR** panel, set the following parameters and click **OK**.

   The following table describes only the key parameters. For more information about the other parameters, see Create a VBR.

Parameter	Description
Account	In this example, **Current account** is selected.
Name	In this example, *VBR* is used.
Physical Connection Interface	In this example, **Dedicated Physical Connection** is selected, and the Express Connect circuit created in Step is selected.
VLAN ID	In this example, *0* is used.
Set VBR Bandwidth Value	Specify a maximum bandwidth value for the VBR.
Peer IPv4 Address of Gateway at Alibaba Cloud Side	In this example, *10.0.0.2* is used.
Peer IPv4 Address of Gateway at Customer Side	In this example, *10.0.0.1* is used.
Subnet Mask (IPv4 Address)	In this example, *255.255.255.252* is used.

3. Add a custom route for the VBR.

   Add a custom route to advertise the on-premises CIDR block to Alibaba Cloud.

   i. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to manage.

   ii. Click the **Routes** tab and click **Add Route**.

   iii. In the **Add Route** panel, set the following parameters and click **OK**.

Parameter	Description
Next Hop Type	Select **Physical Connection Interface**.
Destination CIDR Block	Enter the CIDR block of the data center. *192.168.0.0/16* is used in this example.
Next Hop	Select the Express Connect circuit created in Step .

4. Configure the on-premises gateway device.

   You must add the following route to the on-premises gateway to route traffic destined for VPC1 from the data center to the Express Connect circuit.

   The following configurations are used for reference only. The commands may vary based on the network device vendor. Contact the vendor to obtain the information about specific commands.

```
ip route 10.0.0.0 255.255.0.0 10.0.0.2
```

Step 2: Configure a CEN instance

You must attach VPC1 and the VBR to a CEN instance. Then, the data center and VPC1 can communicate with each other through CEN.

1. Create a CEN instance.

   i. Log on to the CEN console.

   ii. On the **Instances** page, click **Create CEN Instance**.

   iii. In the **Create CEN Instance** panel, set the following parameters and click **OK**.

   - **Name**: Enter a name for the CEN instance.

     In this example, *CEN* is used.

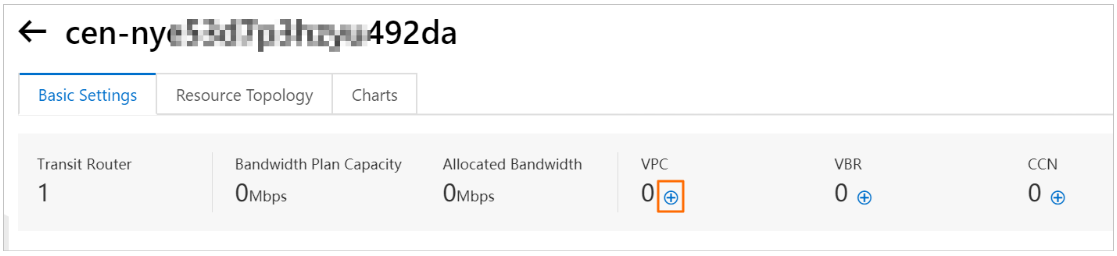
   - **Description**: Enter a description for the CEN instance.

     In this example, *CEN-for-test-private-VPN-Gateway* is used.

2. Attach VPC1 to the CEN instance

   i. On the **Instances** page, click the ID of the CEN instance created in Step .

ii. On the **Basic Settings** tab, click ⊕ in the **VPC** section.



← cen-ny[redacted]492da

Basic Settings | Resource Topology | Charts

Transit Router	Bandwidth Plan Capacity	Allocated Bandwidth	VPC	VBR	CCN
1	0Mbps	0Mbps	0 ⊕	0 ⊕	0 ⊕

iii. On the **Connection with Peer Network Instance** page, set the following parameters and click **OK**.

Parameter	Description
Network Type	Select the type of network instance that you want to attach. In this example, **VPC** is selected.
Region	Select the region where the network instance is deployed. In this example, the **China (Hangzhou)** region is selected.
Transit Router	The system automatically creates a transit router in the selected region.
Select the primary and secondary zones for the transit router	Select the primary and secondary zones for the transit router. The following configurations are used in this example: ■ **Primary Zone**: **Hangzhou Zone H** ■ **Secondary Zone**: **Hangzhou Zone I**
Resource Owner ID	Select the Alibaba Cloud account to which the network instance belongs. In this example, **Your Account** is selected.
Billing Method	In this example, the default value **Pay-As-You-Go** is selected. For more information about billing rules, see Billing.
Attachment Name	Enter a name for the network connection. In this example, *VPC1-test* is used.
Networks	Select the ID of the network instance that you want to attach. In this example, VPC1 is selected.

Parameter	Description
VSwitch	Select a vSwitch from the primary zone and a vSwitch from the secondary zone. In this example, the following vSwitches are selected: ■ **Hangzhou Zone H (Primary)**: vSwitch1 ■ **Hangzhou Zone I (Secondary)**: vSwitch2
Advanced Settings	By default, the system automatically enables the following advanced features. The default settings are used in this example.

iv. Click **Create More Connections** to return to the **Connection with Peer Network Instance** page.

3. Attach the VBR to the CEN instance.

i. On the **Connection with Peer Network Instance** page, set the following parameters and click **OK**.

Parameter	Description
Network Type	Select the type of network instance that you want to attach. In this example, **Virtual Border Router (VBR)** is selected.
Region	Select the region where the network instance is deployed. In this example, the **China (Hangzhou)** region is selected.
Transit Router	The system automatically displays the transit router in the current region.
Resource Owner ID	Select the Alibaba Cloud account to which the network instance belongs. In this example, **Your Account** is selected.
Attachment Name	Enter a name for the network connection. In this example, *VBR-test* is used.
Networks	Select the ID of the network instance that you want to attach. In this example, the VBR created in Step 1 is selected.

Parameter	Description
Advanced Settings	By default, the system automatically enables the following advanced features. ■ **Associate with Default Route Table of Transit Router** After this feature is enabled, the VBR connection is automatically associated with the default route table of the transit router. The transit router forwards the traffic of the VBR based on the default route table. ■ **Propagate System Routes to Default Route Table of Transit Router** After this feature is enabled, the system routes of the VBR are automatically advertised to the default route table of the transit router. ■ **Propagate Routes to VBR** After this feature is enabled, the system automatically advertises the routes in the route table that is associated with the VBR connection to the VBR. The default settings are used in this example.

Step 3: Deploy a VPN gateway

After you complete the preceding steps, the data center is connected to VPC1 over a private connection. However, the private connection is not encrypted. To encrypt the private connection, you must deploy a VPN gateway in VPC1.

1. Create a VPN gateway.

   i.

   ii. In the top navigation bar, select the region where you want to create the VPN gateway.

   The VPN gateway and the VPC to be associated must belong to the same region. In this example, the **China (Hangzhou)** region is selected.

   iii.

   iv. On the buy page, set the following parameters, click **Buy Now**, and then complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway. In this example, *VPNGateway1* is entered.
Region	Select the region where you want to deploy the VPN gateway. In this example, the **China (Hangzhou)** region is selected.

Parameter	Description
Network Type	Select the network type of the VPN gateway. **Private** is selected in this example.
VPC	Select the VPC with which you want to associate the VPN gateway. In this example, VPC1 is selected.
Specify VSwitch	Select whether to deploy the VPN gateway in a specified vSwitch of the VPC. **Yes** is selected in this example.
VSwitch	Select the vSwitch where you want to deploy the VPN gateway. vSwitch1 is selected in this example.
Maximum Bandwidth	Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
Traffic	The billing method of the VPN gateway. Default value: **Pay-by-data-transfer**. For more information, see Pay-as-you-go.
IPsec-VPN	Private VPN gateways support only the IPsec-VPN feature. In this example, the default value **Enable** is selected for the IPsec-VPN feature.
Duration	Specify the billing cycle. Default value: **By Hour**.
Service-linked Role	Click **Create Service-linked Role** and the system automatically creates the service-linked role AliyunServiceRoleForVpn. For more information about how a VPN gateway assumes the role to access other cloud resources, see AliyunServiceRoleForVpn. If **Created** is displayed, the service-linked role is created and you do not need to create it again.

v. Return to the **VPN Gateways** page, check and record the private IP address of the VPN gateway that you created. This IP address is used when you configure IPsec-VPN connections.

A newly created VPN gateway is in the **Preparing** state. After about 1 to 5 minutes, it enters the **Normal** state. The **Normal** state indicates that the VPN gateway is initialized and ready for use.

2. Create a customer gateway.

i.

ii.

iii. In the **Create Customer Gateway** panel, set the following parameters and click **OK**.

   The following content describes only the key parameters. For more information about the other parameters, see Create a customer gateway.

   - **Name**: Enter a name for the customer gateway.

     In this example, *Customer-Gateway* is used.

   - **IP Address**: Enter the VPN IP address of the on-premises gateway device to be connected to the VPN gateway.

     In this example, *192.168.0.251* is used.

3. Create an IPsec-VPN connection.

   i.

   ii.

iii. On the **Create IPsec Connection** page, configure the IPsec-VPN connection based on the following information and click **OK**.

The following content describes only the key parameters. For more information about the other parameters, see Create an IPsec-VPN connection.

Parameter	Description
Name	Enter a name for the IPsec-VPN connection. In this example, *IPsecConnection1* is used.
VPN Gateway	Select the VPN gateway that you created. In this example, VPNGateway1 is selected.
Customer Gateway	Select the customer gateway that you created. In this example, Customer-Gateway is selected.
Routing Mode	Select a routing mode. In this example, **Destination Routing Mode** is selected.
Effective Immediately	Specify whether to immediately start negotiations. Valid values: ■ **Yes**: starts connection negotiations after the configuration is completed. ■ **No**: starts negotiations when inbound traffic is detected. **Yes** is selected in this example.
Pre-Shared Key	Enter a pre-shared key. If you do not enter a value, the system generates a random 16-bit string as the pre-shared key. **Notice** Make sure that the on-premises gateway device and the IPsec-VPN connection use the same pre-shared key. In this example, *fddsFF123*** is used.

For Advanced Configuration, use the default settings.

iv. After you create an IPsec-VPN connection, click **OK** in the **Established** dialog box.

4. Add the VPN configurations to the on-premises gateway device.

i.

ii. On the **IPsec Connections** page, find the IPsec-VPN connection that you created. In the **Actions** column, choose ⋮ > **Download Configuration**.

iii. Add the downloaded configurations to the on-premises gateway device. For more information, see Configure on-premises gateways.

Step 4: Configure routes for the VPC, VBR, and VPN gateway

After you complete the preceding steps, an encrypted tunnel can be established between the on-premises gateway device and the VPN gateway. You must configure routes for the VPC, VBR, and VPN gateway to route traffic to the encrypted tunnel when the data center communicates with Alibaba Cloud.

1. Add custom routes for VPC1.
    i. Log on to the VPC console.
    ii. In the left-side navigation pane, click **Route Tables**.
    iii. In the top navigation bar, select the region to which the route table belongs.

        In this example, the **China (Hangzhou)** region is selected.
    iv. On the **Route Tables** page, find and click the ID of the route table that you want to manage.

        In this example, the ID of the system route table of VPC1 is clicked.
    v. On the **Route Entry List** tab, click **Custom Route** and then click **Add Route Entry**.
    vi. In the **Add Route Entry** panel, set the following parameters and click **OK**.

Parameter	Description
Name	Enter a name for the custom route.
Destination CIDR Block	Enter the destination CIDR block of the custom route. In this example, **IPv4 CIDR Block** is selected and the VPN IP address of the on-premises gateway device is used, which is *192.168.0.251/32*.
Next Hop Type	Select the type of the next hop. In this example, **Transit Router** is selected.
Transit Router	Select the next hop of the custom route. In this example, VPC1-test is selected.

2. Add a custom route for the VBR.
    i. Log on to the Express Connect console.
    ii. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.
    iii. In the top navigation bar, select the region where the VBR is deployed.

        In this example, the **China (Hangzhou)** region is selected.
    iv. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to manage.
    v. Click the **Routes** tab and click **Add Route**.

vi. In the **Add Route** panel, set the following parameters and click **OK**.

Parameter	Description
Next Hop Type	Select **Physical Connection Interface**.
Destination CIDR Block	Enter the VPN IP address of the on-premises gateway device. In this example, *192.168.0.251/32* is used.
Next Hop	Select the Express Connect circuit created in Step .

3. Add a route for the VPN gateway.

> **Notice** To route traffic destined for the data center from VPC1 to the encrypted tunnel, you must add a route whose destination CIDR block is more specific than the CIDR block of the data center. This means that the destination CIDR block must be a subset of the CIDR block of the data center. Then, you must advertise the route to VPC1.
>
> In this example, the CIDR block of the data center is 192.168.0.0/16. The destination CIDR block of the route configured for the VPN gateway is *192.168.1.0/24*, which is more specific than 192.168.0.0/16.

i.

ii.

iii. In the top navigation bar, select the region where the VPN gateway is deployed.

In this example, the **China (Hangzhou)** region is selected.

iv. On the **VPN Gateways** page, find the VPN gateway you created and click the ID.

v. On the **Destination-based Routing** tab, click **Add Route Entry**.

vi. In the **Add Route Entry** panel, set the following parameters and click **OK**.

Parameter	Description
Destination CIDR Block	Enter the CIDR block of the data center. In this example, *192.168.1.0/24* is used.
Next Hop Type	In this example, **IPsec Connection** is selected.
Next Hop	Select the IPsec-VPN connection created in Step .
Publish to VPC	Specify whether to advertise the route to the route table of the VPC. In this example, **Yes** is selected. In this case, the route is advertised to the route table of VPC1.
Weight	Specify a weight for the route. In this example, the default value **100** is used, which specifies a high priority.

Step 5: Check the network connectivity

After you complete the preceding steps, the data center can communicate with VPC1 over private and encrypted connections. The following content describes how to test the connectivity between the data center and VPC1, and check whether the private connection is encrypted by the VPN gateway.

1. Test the network connectivity.

   i. Log on to ECS1. For more information, see Connect to an ECS instance.

   ii. Run the **ping** command to ping a client in the data center to test the network connectivity between the data center and VPC1.

   ```
   ping <the IP address of a client in the data center>
   ```

   If an echo reply packet is returned, it indicates that the data center is connected to VPC1.

2. Check whether the private connection is encrypted.

   If you can view the monitoring data of data transfer on the details page of the IPsec-VPN connection, it indicates that the private connection is encrypted.

   i.

   ii. In the top navigation bar, select the region where the VPN gateway is deployed.

   In this example, the **China (Hangzhou)** region is selected.

   iii.

   iv. On the **IPsec Connections** page, find the IPsec-VPN connection created in Step and click its ID.
   Go to the details page of the IPsec-VPN connection to view the monitoring data of data transfer.

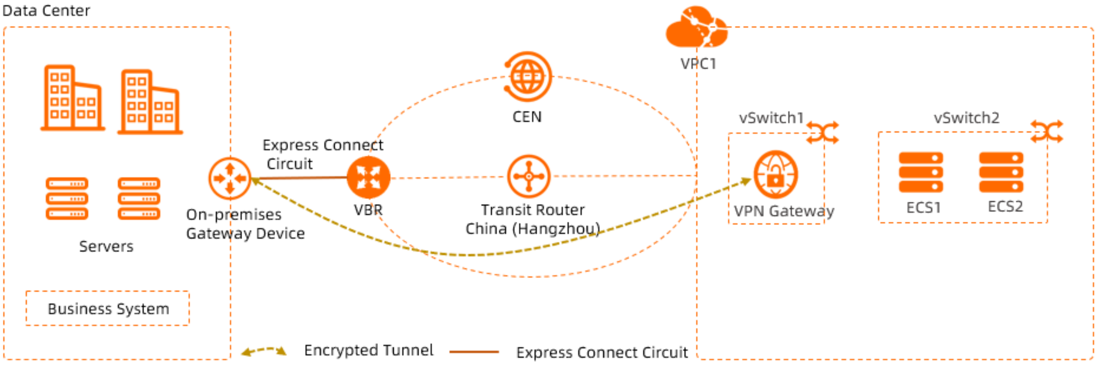
9.3. Encrypt private connections by using static routing and BGP routing

This topic describes how to encrypt the private connection between a data center and a virtual private cloud (VPC) by using a private VPN gateway (hereafter referred to as "VPN gateway"). To encrypt the private connection between a data center and a VPC, you can configure BGP routing for the VPN gateway and configure static routing for the virtual border router (VBR) that connects the data center to the VPC.

Background information

Before you start, we recommend that you understand how private connections are encrypted and the configuration methods. For more information, see Overview of configuration methods.

Scenarios



The preceding scenario is used as an example in this topic. An enterprise owns a data center in Hangzhou and has a VPC (VPC1) deployed in the China (Hangzhou) region. Applications are deployed on Elastic Compute Service (ECS) instances in VPC1. Due to business growth, the enterprise wants to connect VPC1 to the data center through an Express Connect circuit and CEN. In addition, the enterprise wants to encrypt the connection between VPC1 and the data center due to security concerns.

After VPC1 is connected to the data center through CEN and an Express Connect circuit, the enterprise can create a VPN gateway in VPC1 and establish an IPsec-VPN connection between the VPN gateway and an on-premises gateway device. Then, the enterprise can configure BGP routing for the VPN gateway and static routing for the VBR to encrypt the private connection.

Preparations

- Private VPN gateways are in invitational preview. Make sure that you have applied for the required permissions from your sales manager or to apply for the required permissions.
- You must plan networks for the data center and network instances. Make sure that the CIDR block of the data center does not overlap with those of the network instances. The following table describes the CIDR blocks in this example.

Item	CIDR block	IP address

Item	CIDR block	IP address
VPC1	○ Primary CIDR block: 10.0.0.0/16 ○ CIDR block of vSwitch1: 10.0.0.0/24 ○ CIDR block of vSwitch2: 10.0.1.0/24	○ ECS1: 10.0.1.1 ○ ECS2: 10.0.1.2
VBR	10.0.0.0/30	○ VLAN ID: 201 ○ IPv4 address on the Alibaba Cloud side: 10.0.0.2/30 ○ IPv4 address on the user side: 10.0.0.1/30 In this example, the IPv4 address on the user side is the IPv4 address of the gateway device in the data center.
Data center	○ Primary CIDR block: 192.168.0.0/16 ○ Subnet1: 192.168.0.0/24 ○ Subnet2: 192.168.1.0/24	Client: 192.168.1.1
On-premises gateway device	○ 10.0.0.0/30 ○ 192.168.0.0/24	○ VPN IP address: 192.168.0.251 The VPN IP address refers to the IP address of the interface of the on-premises gateway device to be connected to the VPN gateway. ○ IP address of the interface connected to the Express Connect circuit: 10.0.0.1/30 ○ Autonomous system number (ASN): 65530

- VPC1 is deployed in the China (Hangzhou) region and applications are deployed on the ECS instances in VPC1. For more information, see Create and manage a VPC.

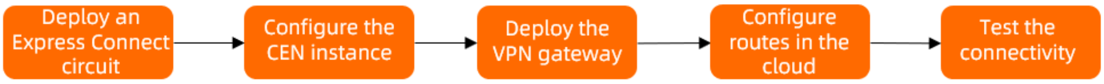
  Make sure that VPC1 in the China (Hangzhou) region contains at least one vSwitch in a zone that supports Enterprise Edition transit routers. In addition, each vSwitch must have at least one idle IP address so that VPC1 can be attached to the CEN instance. For more information, see Create a VPC connection.

  In this example, VPC1 contains two vSwitches (vSwitch1 and vSwitch2). vSwitch1 is deployed in Zone H and vSwitch2 is deployed in Zone I. ECS instances are deployed on vSwitch2. vSwitch1 is used only to associate with the VPN gateway.

  > **Note** When you create a VPC, we recommend that you create a dedicated vSwitch in the VPC for the VPN gateway. This way, the vSwitch can allocate a private IP address to the VPN gateway.

- Check the gateway device in the data center. Make sure that it supports standard IKEv1 and IKEv2 protocols. To check whether the gateway device supports the IKEv1 and IKEv2 protocols, contact the gateway vendor.
- Take note of the security group rules that apply to ECS instances in VPC1 and access control list (ACL) rules that apply to the client in the data center. Make sure that these rules allow ECS instances in VPC1 to communicate with the client in the data center. For more information, see Query security group rules and Add a security group rule.

Procedure


Deploy an Express Connect circuit
Configure the CEN instance
Deploy the VPN gateway
Configure routes in the cloud
Test the connectivity

Step 1: Deploy an Express Connect circuit

You must deploy an Express Connect circuit to connect the data center to Alibaba Cloud.

1. Create a connection over an Express Connect circuit.

   You must apply for an Express Connect circuit in the China (Hangzhou) region. For more information, see Create a dedicated connection over an Express Connect circuit or Overview.

   In this example, a dedicated connection over an Express Connect circuit is created.

2. Create a VBR.

   i. Log on to the Express Connect console.

   ii. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.

   iii. In the top navigation bar, select the region where you want to create the VBR.

   In this example, the **China (Hangzhou)** region is selected.

   iv. On the **Virtual Border Routers (VBRs)** page, click **Create VBR**.

v. In the **Create VBR** panel, set the following parameters and click **OK**.

The following table describes only the key parameters. For more information about the other parameters, see Create a VBR.

Parameter	Description
Account	In this example, **Current account** is selected.
Name	In this example, *VBR* is used.
Physical Connection Interface	In this example, **Dedicated Physical Connection** is selected, and the Express Connect circuit created in Step is selected.
VLAN ID	In this example, *201* is used. **Note** Make sure that the VLAN ID of the VBR is the same as the VLAN ID of the interface that the on-premises gateway device uses to connect to the Express Connect circuit.
Set VBR Bandwidth Value	Specify a maximum bandwidth value for the VBR.
Peer IPv4 Address of Gateway at Alibaba Cloud Side	In this example, *10.0.0.2* is used.
Peer IPv4 Address of Gateway at Customer Side	In this example, *10.0.0.1* is used.
Subnet Mask (IPv4 Address)	In this example, *255.255.255.252* is used.

3. Add a custom route for the VBR.

Add a custom route to advertise the on-premises CIDR block to Alibaba Cloud.

i. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to manage.

ii. Click the **Routes** tab and click **Add Route**.

iii. In the **Add Route** panel, set the following parameters and click **OK**.

Parameter	Description
Next Hop Type	Select **Physical Connection Interface**.
Destination CIDR Block	Enter the CIDR block of the data center. *192.168.0.0/16* is used in this example.
Next Hop	Select the Express Connect circuit created in Step .

4. Configure the on-premises gateway device.

   You must add the following route to the on-premises gateway to route traffic destined for VPC1 from the data center to the Express Connect circuit.

   The following configurations are used for reference only. The commands may vary based on the network device vendor. Contact the vendor to obtain the information about specific commands.

```
ip route 10.0.0.0 255.255.0.0 10.0.0.2
```

Step 2: Configure a CEN instance

You must attach VPC1 and the VBR to a CEN instance. Then, the data center and VPC1 can communicate with each other through CEN.

1. Create a CEN instance.

   i. Log on to the CEN console.

   ii. On the **Instances** page, click **Create CEN Instance**.

   iii. In the **Create CEN Instance** panel, set the following parameters and click **OK**.

   - **Name**: Enter a name for the CEN instance.

     In this example, *CEN* is used.

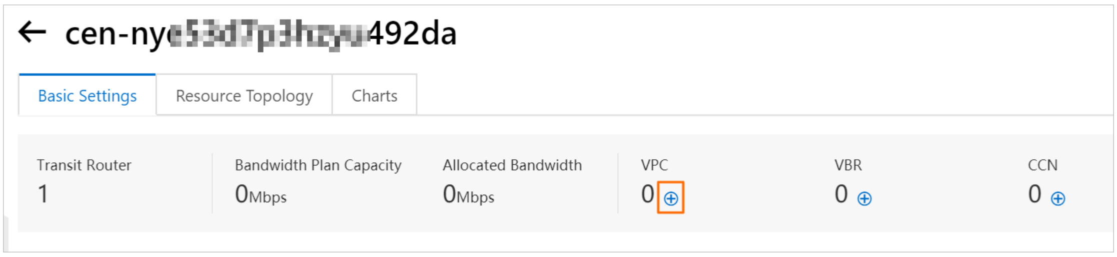
   - **Description**: Enter a description for the CEN instance.

     In this example, *CEN-for-test-private-VPN-Gateway* is used.

2. Attach VPC1 to the CEN instance

   i. On the **Instances** page, click the ID of the CEN instance created in Step .

   ii. On the **Basic Settings** tab, click ⊕ in the **VPC** section.



cen-ny[redacted]492da

Transit Router	Bandwidth Plan Capacity	Allocated Bandwidth	VPC	VBR	CCN
1	0Mbps	0Mbps	0 ⊕	0 ⊕	0 ⊕

iii. On the **Connection with Peer Network Instance** page, set the following parameters and click **OK**.

Parameter	Description
Network Type	Select the type of network instance that you want to attach. In this example, **VPC** is selected.
Region	Select the region where the network instance is deployed. In this example, the **China (Hangzhou)** region is selected.
Transit Router	The system automatically creates a transit router in the selected region.
Select the primary and secondary zones for the transit router	Select the primary and secondary zones for the transit router. The following configurations are used in this example: ■ **Primary Zone**: **Hangzhou Zone H** ■ **Secondary Zone**: **Hangzhou Zone I**
Resource Owner ID	Select the Alibaba Cloud account to which the network instance belongs. In this example, **Your Account** is selected.
Billing Method	In this example, the default value **Pay-As-You-Go** is selected. For more information about billing rules, see Billing.
Attachment Name	Enter a name for the network connection. In this example, *VPC1-test* is used.
Networks	Select the ID of the network instance that you want to attach. In this example, VPC1 is selected.
VSwitch	Select a vSwitch from the primary zone and a vSwitch from the secondary zone. In this example, the following vSwitches are selected: ■ **Hangzhou Zone H (Primary)**: vSwitch1 ■ **Hangzhou Zone I (Secondary)**: vSwitch2
Advanced Settings	By default, the system automatically enables the following advanced features. The default settings are used in this example.

3. Attach the VBR to the CEN instance.

i. On the **Connection with Peer Network Instance** page, set the following parameters and click **OK**.

Parameter	Description
Network Type	Select the type of network instance that you want to attach. In this example, **Virtual Border Router (VBR)** is selected.
Region	Select the region where the network instance is deployed. In this example, the **China (Hangzhou)** region is selected.
Transit Router	The system automatically displays the transit router in the current region.
Resource Owner ID	Select the Alibaba Cloud account to which the network instance belongs. In this example, **Your Account** is selected.
Attachment Name	Enter a name for the network connection. In this example, *VBR-test* is used.
Networks	Select the ID of the network instance that you want to attach. In this example, the VBR created in Step 1 is selected.
Advanced Settings	By default, the system automatically enables the following advanced features. ▪ **Associate with Default Route Table of Transit Router** After this feature is enabled, the VBR connection is automatically associated with the default route table of the transit router. The transit router forwards the traffic of the VBR based on the default route table. ▪ **Propagate System Routes to Default Route Table of Transit Router** After this feature is enabled, the system routes of the VBR are automatically advertised to the default route table of the transit router. ▪ **Propagate Routes to VBR** After this feature is enabled, the system automatically advertises the routes in the route table that is associated with the VBR connection to the VBR. The default settings are used in this example.

Step 3: Deploy a VPN gateway

After you complete the preceding steps, the data center is connected to VPC1 over a private connection. However, the private connection is not encrypted. To encrypt the private connection, you must deploy a VPN gateway in VPC1.

1. Create a VPN gateway.

    i.

    ii. In the top navigation bar, select the region where you want to create the VPN gateway.

    The VPN gateway and the VPC to be associated must belong to the same region. In this example, the **China (Hangzhou)** region is selected.

    iii.

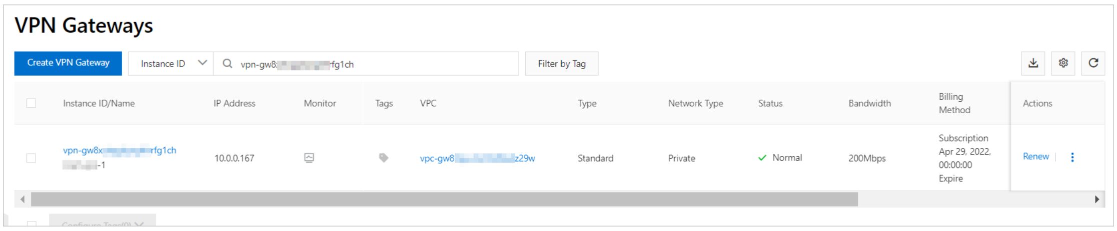
    iv. On the buy page, set the following parameters, click **Buy Now**, and then complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway. In this example, *VPNGateway1* is entered.
Region	Select the region where you want to deploy the VPN gateway. In this example, the **China (Hangzhou)** region is selected.
Network Type	Select the network type of the VPN gateway. **Private** is selected in this example.
VPC	Select the VPC with which you want to associate the VPN gateway. In this example, VPC1 is selected.
Specify VSwitch	Select whether to deploy the VPN gateway in a specified vSwitch of the VPC. **Yes** is selected in this example.
VSwitch	Select the vSwitch where you want to deploy the VPN gateway. vSwitch1 is selected in this example.
Maximum Bandwidth	Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
Traffic	The billing method of the VPN gateway. Default value: **Pay-by-data-transfer**. For more information, see Pay-as-you-go.
IPsec-VPN	Private VPN gateways support only the IPsec-VPN feature. In this example, the default value **Enable** is selected for the IPsec-VPN feature.

Parameter	Description
Duration	Specify the billing cycle. Default value: **By Hour**.
Service-linked Role	Click **Create Service-linked Role** and the system automatically creates the service-linked role AliyunServiceRoleForVpn. For more information about how a VPN gateway assumes the role to access other cloud resources, see AliyunServiceRoleForVpn. If **Created** is displayed, the service-linked role is created and you do not need to create it again.

v. Return to the **VPN Gateways** page, check and record the private IP address of the VPN gateway that you created. This IP address is used when you configure IPsec-VPN connections.

A newly created VPN gateway is in the **Preparing** state. After about 1 to 5 minutes, it enters the **Normal** state. The **Normal** state indicates that the VPN gateway is initialized and ready for use.



VPN Gateways

Create VPN Gateway | Instance ID | vpn-gw8[redacted]rfg1ch | Filter by Tag

□	Instance ID/Name	IP Address	Monitor	Tags	VPC	Type	Network Type	Status	Bandwidth	Billing Method	Actions
□	vpn-gw8x[redacted]rfg1ch [redacted]-1	10.0.0.167			vpc-gw8[redacted]z29w	Standard	Private	✓ Normal	200Mbps	Subscription Apr 29, 2022, 00:00:00 Expire	Renew ⋮

2. Create a customer gateway.

i.

ii.

iii. In the **Create Customer Gateway** panel, set the following parameters and click **OK**.

The following content describes only the key parameters. For more information about the other parameters, see Create a customer gateway.

- **Name**: Enter a name for the customer gateway.

  In this example, *Customer-Gateway* is used.

- **IP Address**: Enter the VPN IP address of the on-premises device to be connected to the VPN gateway.

  In this example, *192.168.0.251* is used.

- **ASN**: Enter the ASN of the on-premises gateway device.

  In this example, *65530* is used.

3. Create an IPsec-VPN connection.

i.

ii.

iii. On the **Create IPsec Connection** page, configure the IPsec-VPN connection based on the following information and click **OK**.

The following content describes only the key parameters. For more information about the other parameters, see Create an IPsec-VPN connection.

Parameter	Description
Name	Enter a name for the IPsec-VPN connection. In this example, *IPsecConnection1* is used.
VPN Gateway	Select the VPN gateway that you created. In this example, VPNGateway1 is selected.
Customer Gateway	Select the customer gateway that you created. In this example, Customer-Gateway is selected.
Routing Mode	Select a routing mode. In this example, **Destination Routing Mode** is selected.
Effective Immediately	Specify whether to immediately start negotiations. ■ **Yes**: starts connection negotiations after the configuration is completed. ■ **No**: starts negotiations when inbound traffic is detected. **Yes** is selected in this example.
Pre-Shared Key	Enter a pre-shared key. If you do not enter a value, the system generates a random 16-bit string as the pre-shared key. **Notice** Make sure that the on-premises device and the IPsec-VPN connection use the same pre-shared key. In this example, *fddsFF123***** is used.
Advanced Configuration	In this example, **ikev2** is selected for the **Version** parameter in the **IKE Configurations** section. The default values are used for the other parameters.

Parameter	Description
BGP Configuration	In this example, BGP Configuration is enabled. The following content describes the parameters. ■ **Tunnel CIDR Block**: Enter the CIDR block of the IPsec tunnel. The CIDR block must fall within 169.254.0.0/16. The subnet mask of the CIDR block must be 30 bits in length. In this example, *169.254.10.0/30* is entered. ■ **Local BGP IP address**: Enter the BGP IP address on the VPN gateway side. This IP address must fall within the CIDR block of the IPsec tunnel. In this example, *169.254.10.1* is entered. The BGP IP address on the data center side is *169.254.10.2*. ■ **Local ASN**: Enter the ASN on the VPN gateway side. In this example, *65531* is entered. **Note** We recommend that you use a private ASN to establish a connection to the data center over BGP. Refer to the relevant documentation for the valid range of a private ASN.
Health Check	In this example, the default settings are used.

iv. After you create an IPsec-VPN connection, click **OK** in the **Established** dialog box.

4. Enable automatic BGP advertising for the VPN gateway.

   After automatic BGP advertising is enabled and a peering connection is established between the VPN gateway and the on-premises gateway device, the VPN gateway learns and advertises the CIDR block of the data center to VPC1. The VPN gateway also advertises the routes in the system route table of VPC1 to the on-premises gateway device.

   i. In the left-side navigation pane, choose **Interconnections > VPN > VPN Gateways**.

   ii. On the **VPN Gateways** page, find VPNGateway1 and select ⋮ **> Enable Automatic BGP Propagation** in the **Actions** column.

   iii. In the **Enable Automatic BGP Propagation** message, click **OK**.

5. Download the IPsec configurations of the on-premises gateway device.

   i.

   ii. On the **IPsec Connections** page, find IPsecConnection1. In the **Actions** column, choose ⋮ > **Download Configuration**.

   Save the downloaded IPsec configurations on your client.

6. Add VPN configurations, BGP configurations, and static routes to the on-premises gateway device.

   Add VPN configurations, BGP configurations, and static routes to the on-premises gateway device based on the IPsec configurations that you downloaded.

The following configurations are used for reference only. The commands may vary based on the network device vendor. Contact the vendor to obtain the information about specific commands.

i. Open the CLI of the on-premises gateway device.

ii. Run the following commands to configure the IKEv2 proposal and policy:

```
crypto ikev2 proposal alicloud
encryption aes-cbc-128          //Configure the encryption algorithm. In this example, aes-cbc-128 is used.
integrity sha1                  //Configure the authentication algorithm. In this example, sha1 is used.
group 2                         //Configure the DH group. In this example, group 2 is used.
exit
!
crypto ikev2 policy Pureport_Pol_ikev2
proposal Pureport_prop
exit
!
```

iii. Run the following commands to configure the IKEv2 keyring:

```
crypto ikev2 keyring alicloud
peer alicloud
address 10.0.0.167               //Configure the private IP address of the VPN gateway. In this example, 10.0.0.167 is used.
pre-shared-key fddsFF123****     //Configure the pre-shared key. In this example, fddsFF123**** is used.
exit
!
```

iv. Run the following commands to configure the IKEv2 profile:

```
crypto ikev2 profile alicloud
match identity remote address 10.0.0.167 255.255.255.255    //Configure the private IP address of the VPN gateway. In this example, 10.0.0.167 is used.
identity local address 192.168.0.251    //Configure the VPN IP address of the data center. In this example, 192.168.0.251 is used.
authentication remote pre-share   //Set the authentication mode for the VPC to PSK (pre-shared key).
authentication local pre-share    //Set the authentication mode for the data center to PSK.
keyring local alicloud            //Invoke the IKEv2 keyring.
exit
!
```

v. Run the following commands to configure transform:

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
mode tunnel
exit
!
```

vi. Run the following commands to configure the IPsec profile and invoke the transform, PFS, and IKEv2 profiles:

```
crypto ipsec profile alicloud
set transform-set TSET
set pfs group2
set ikev2-profile alicloud
exit
!
```

vii. Run the following commands to configure the IPsec tunnel:

```
interface Tunnel100
ip address 169.254.10.2 255.255.255.252    //Configure the tunnel address for the data center. In this example, 169.254.10.2 is used.
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 10.0.0.167              //Configure the private IP address of the VPN gateway. In this example, 10.0.0.167 is used.
tunnel protection ipsec profile alicloud
no shutdown
exit
!
interface GigabitEthernet1                 //Configure the IP address of the interface that is used to connect to the VPN gateway.
ip address 192.168.0.251 255.255.255.0
negotiation auto
!
```

viii. Run the following commands to configure BGP:

> **Notice** To ensure that traffic from the VPC to the data center is routed to the encrypted tunnel of the VPN gateway, you must advertise a CIDR block that is smaller than the CIDR block of the data center in the BGP configurations of the on-premises gateway device.
>
> In this example, the CIDR block of the data center is 192.168.0.0/16. Therefore, you must advertise a CIDR block that is smaller than 192.168.0.0/16 in the BGP configurations of the on-premises gateway device. In this example, *192.168.1.0/24* is advertised.

```
router bgp 65530                         //Enable BGP and configure the BGP ASN of
the data center. In this example, 65530 is used.
bgp router-id 169.254.10.2               //Configure the ID of the BGP router. In t
his example, 169.254.10.2 is used.
bgp log-neighbor-changes
neighbor 169.254.10.1 remote-as 65531    //Configure the ASN of the BGP peer. In th
is example, the BGP ASN of the VPN gateway 65531 is used.
neighbor 169.254.10.1 ebgp-multihop 10   //Set the EBGP hop-count to 10.
!
address-family ipv4
network 192.168.1.0 mask 255.255.255.0   //Advertise the CIDR block of the data cen
ter. In this example, 192.168.1.0/24 is advertised.
neighbor 169.254.10.1 activate           //Activate the BGP peer.
exit-address-family
!
```

ix. Run the following command to configure a static route:

```
ip route 10.0.0.167 255.255.255.255 10.0.0.2  //Route traffic from the data center
to the VPN gateway to the Express Connect circuit.
```

Step 4: Configure routes for the VPC and the VBR

After you complete the preceding steps, an encrypted tunnel can be established between the on-premises gateway device and the VPN gateway. You must configure routes for the VPC and the VBR to route traffic to the encrypted tunnel when the data center communicates with Alibaba Cloud.

1. Add custom routes for VPC1.

   i. Log on to the VPC console.

   ii. In the left-side navigation pane, click **Route Tables**.

   iii. In the top navigation bar, select the region to which the route table belongs.

   In this example, the **China (Hangzhou)** region is selected.

   iv. On the **Route Tables** page, find and click the ID of the route table that you want to manage.

   In this example, the ID of the system route table of VPC1 is clicked.

   v. On the **Route Entry List** tab, click **Custom Route** and then click **Add Route Entry**.

vi. In the **Add Route Entry** panel, set the following parameters and click **OK**.

Parameter	Description
Name	Enter a name for the custom route.
Destination CIDR Block	Enter the destination CIDR block of the custom route. In this example, **IPv4 CIDR Block** is selected and the VPN IP address of the on-premises gateway device is used, which is *192 .168.0.251/32*.
Next Hop Type	Select the type of the next hop. In this example, **Transit Router** is selected.
Transit Router	Select the next hop of the custom route. In this example, VPC1-test is selected.

2. Add a custom route for the VBR.

   i. Log on to the Express Connect console.

   ii. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.

   iii. In the top navigation bar, select the region where the VBR is deployed.

   In this example, the **China (Hangzhou)** region is selected.

   iv. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to manage.

   v. Click the **Routes** tab and click **Add Route**.

   vi. In the **Add Route** panel, set the following parameters and click **OK**.

Parameter	Description
Next Hop Type	Select **Physical Connection Interface**.
Destination CIDR Block	Enter the VPN IP address of the on-premises gateway device. In this example, *192.168.0.251/32* is used.
Next Hop	Select the Express Connect circuit created in Step .

Step 5: Check the network connectivity

After you complete the preceding steps, the data center can communicate with VPC1 over private and encrypted connections. The following content describes how to test the connectivity between the data center and VPC1, and check whether the private connection is encrypted by the VPN gateway.

1. Test the network connectivity.

   i. Log on to ECS1. For more information, see Connect to an ECS instance.

ii. Run the **ping** command to ping a client in the data center to test the network connectivity between the data center and VPC1.

```
ping <the IP address of a client in the data center>
```

If an echo reply packet is returned, it indicates that the data center is connected to VPC1.

2. Check whether the private connection is encrypted.

If you can view the monitoring data of data transfer on the details page of the IPsec-VPN connection, it indicates that the private connection is encrypted.

i.

ii. In the top navigation bar, select the region where the VPN gateway is deployed.

In this example, the **China (Hangzhou)** region is selected.

iii.

iv. On the **IPsec Connections** page, find the IPsec-VPN connection created in Step and click its ID.
Go to the details page of the IPsec-VPN connection to view the monitoring data of data transfer.

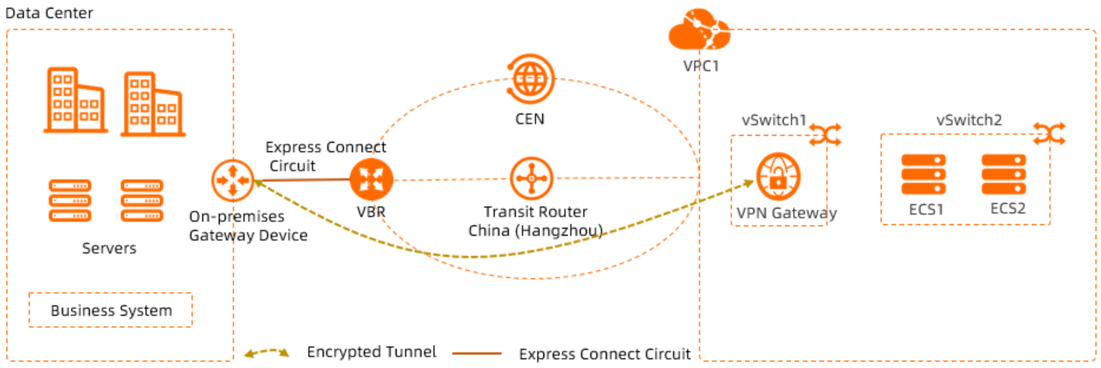
9.4. Encrypt private connections by using BGP routing

This topic describes how to encrypt the private connection between a data center and a virtual private cloud (VPC) by using a private VPN gateway (hereafter referred to as "VPN gateway"). To encrypt the private connection between a data center and a VPC, you can configure BGP routing for the VPN gateway and the virtual border router (VBR) that connects the data center to the VPC.

Background information

Before you start, we recommend that you understand how private connections are encrypted and the configuration methods. For more information, see Overview of configuration methods.

Scenarios



The preceding scenario is used as an example in this topic. An enterprise owns a data center in Hangzhou and has a VPC (VPC1) deployed in the China (Hangzhou) region. Applications are deployed on Elastic Compute Service (ECS) instances in VPC1. Due to business growth, the enterprise wants to connect VPC1 to the data center through an Express Connect circuit and CEN. In addition, the enterprise wants to encrypt the connection between VPC1 and the data center due to security concerns.

After VPC1 is connected to the data center through CEN and an Express Connect circuit, the enterprise can create a VPN gateway in VPC1 and establish an IPsec-VPN connection between the VPN gateway and an on-premises gateway device. Then, the enterprise can configure BGP routing for both the VBR and VPN gateway to encrypt the private connection.

Preparations

- Private VPN gateways are in invitational preview. Make sure that you have applied for the required permissions from your sales manager or to apply for the required permissions.
- You must plan networks for the data center and network instances. Make sure that the CIDR block of the data center does not overlap with those of the network instances. The following table describes the CIDR blocks in this example.

Item	CIDR block	IP address
VPC1	○ Primary CIDR block: 10.0.0.0/16 ○ CIDR block to which vSwitch1 belongs: 10.0.0.0/24 ○ CIDR block to which vSwitch2 belongs: 10.0.1.0/24	○ ECS1: 10.0.1.1 ○ ECS2: 10.0.1.2
VBR	10.0.0.0/30	○ VLAN ID: 201 ○ IPv4 address on the Alibaba Cloud side: 10.0.0.2/30 ○ IPv4 address on the user side: 10.0.0.1/30 In this example, the IPv4 address on the user side is the IPv4 address of the gateway device in the data center. ○ Autonomous system number (ASN): 45104 By default, the ASN of the VBR is 45104. You cannot change the ASN.
Data center	○ Primary CIDR block: 192.168.0.0/16 ○ Subnet1: 192.168.0.0/24 ○ Subnet2: 192.168.1.0/24	Client: 192.168.1.1

Item	CIDR block	IP address
On-premises gateway device	○ 10.0.0.0/30 ○ 192.168.0.0/24	○ VPN IP address: 192.168.0.251 The VPN IP address refers to the IP address of the interface of the on-premises gateway device to be connected to the VPN gateway. ○ IP address of the interface connected to the Express Connect circuit: 10.0.0.1 ○ ASN: 65530

- VPC1 is deployed in the China (Hangzhou) region and applications are deployed on the ECS instances in VPC1. For more information, see Create and manage a VPC.

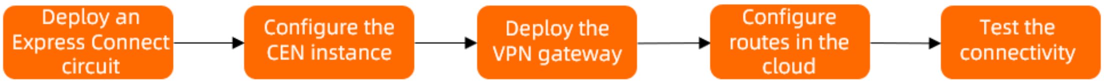
  Make sure that VPC1 in the China (Hangzhou) region contains at least one vSwitch in a zone that supports Enterprise Edition transit routers. In addition, each vSwitch must have at least one idle IP address so that VPC1 can be attached to the CEN instance. For more information, see Create a VPC connection.

  In this example, VPC1 contains two vSwitches (vSwitch1 and vSwitch2). vSwitch1 is deployed in Zone H and vSwitch2 is deployed in Zone I. ECS instances are deployed on vSwitch2. vSwitch1 is used only to associate with the VPN gateway.

  > **Note** When you create a VPC, we recommend that you create a dedicated vSwitch in the VPC for the VPN gateway. This way, the vSwitch can allocate a private IP address to the VPN gateway.

- Check the gateway device in the data center. Make sure that it supports standard IKEv1 and IKEv2 protocols. To check whether the gateway device supports the IKEv1 and IKEv2 protocols, contact the gateway vendor.
- Take note of the security group rules that apply to ECS instances in VPC1 and access control list (ACL) rules that apply to the client in the data center. Make sure that these rules allow ECS instances in VPC1 to communicate with the client in the data center. For more information, see Query security group rules and Add a security group rule.

Procedure


Deploy an Express Connect circuit
Configure the CEN instance
Deploy the VPN gateway
Configure routes in the cloud
Test the connectivity

Step 1: Deploy an Express Connect circuit

You must deploy an Express Connect circuit to connect the data center to Alibaba Cloud.

1. Create a connection over an Express Connect circuit.

   You must apply for an Express Connect circuit in the China (Hangzhou) region. For more information, see Create a dedicated connection over an Express Connect circuit or Overview.

In this example, a dedicated connection over an Express Connect circuit is created.

2. Create a VBR.
    i. Log on to the Express Connect console.
    ii. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.
    iii. In the top navigation bar, select the region where you want to create the VBR.

        In this example, the **China (Hangzhou)** region is selected.
    iv. On the **Virtual Border Routers (VBRs)** page, click **Create VBR**.
    v. In the **Create VBR** panel, set the following parameters and click **OK**.

        The following table describes only the key parameters. For more information about the other parameters, see Create a VBR.

Parameter	Description
Account	In this example, **Current account** is selected.
Name	In this example, *VBR* is used.
Physical Connection Interface	In this example, **Dedicated Physical Connection** is selected, and the Express Connect circuit created in Step is selected.
VLAN ID	In this example, *201* is used. **Note** Make sure that the VLAN ID of the VBR is the same as the VLAN ID of the interface that the on-premises gateway device uses to connect to the Express Connect circuit.
Set VBR Bandwidth Value	Specify a maximum bandwidth value for the VBR.
Peer IPv4 Address of Gateway at Alibaba Cloud Side	In this example, *10.0.0.2* is used.
Peer IPv4 Address of Gateway at Customer Side	In this example, *10.0.0.1* is used.
Subnet Mask (IPv4 Address)	In this example, *255.255.255.252* is used.

3. Configure a BGP group for the VBR.
    i. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to manage.
    ii. On the details page, click the **BGP Groups** tab.

   iii. On the **BGP Groups** tab, click **Create BGP Group**, set the following parameters, and click **OK**.

   The following section describes only the key parameters. For more information about the other parameters, see Configure BGP.

   - **Name**: Enter a name for the BGP group. In this example, *VBR-BGP* is entered.
   - **Peer ASN**: Enter the ASN of the on-premises gateway device. In this example, *65530* is used.

4. Configure a BGP peer for the VBR.

   i. On the VBR details page, click the **BGP Peers** tab.

   ii. On the **BGP Peers** tab, click **Create BGP Peer**.

   iii. In the **Create BGP Peer** panel, set the following parameters and click **OK**:

   - **BGP Group**: Select a BGP group.

     In this example, VBR-BGP is selected.

   - **BGP Peer IP Address**: Enter the IP address of the BGP peer.

     In this example, the IP address *10.0.0.1* is entered. This is the IP address of the interface that the on-premises gateway device uses to connect to the Express Connect circuit.

5. Configure BGP routing for the on-premises gateway device.

   The following configurations are used for reference only. The commands may vary based on the network device vendor. Contact the vendor to obtain the information about specific commands.

```
router bgp 65530                         //Enable BGP and configure the ASN of the data
center. In this example, 65530 is used.
bgp router-id 10.0.0.1                   //Enter the ID of the BGP router. In this exam
ple, 10.0.0.1 is used.
bgp log-neighbor-changes
neighbor 10.0.0.2 remote-as 45104        //Establish a peering connection to the VBR.
!
address-family ipv4
network 192.168.0.0 mask 255.255.0.0     //Advertise the CIDR block of the data center.

neighbor 10.0.0.2 activate               //Activate the BGP peer.
exit-address-family
!
```

Step 2: Configure a CEN instance

You must attach VPC1 and the VBR to a CEN instance. Then, the data center and VPC1 can communicate with each other through CEN.

1. Create a CEN instance.

   i. Log on to the CEN console.

   ii. On the **Instances** page, click **Create CEN Instance**.

   iii. In the **Create CEN Instance** panel, set the following parameters and click **OK**.

   - **Name**: Enter a name for the CEN instance.

     In this example, *CEN* is used.

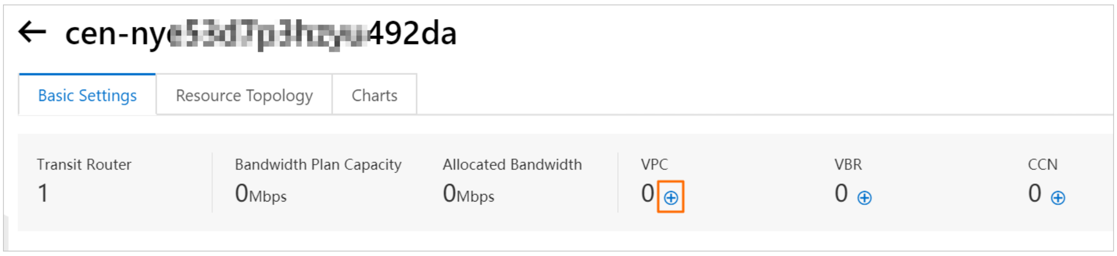
   - **Description**: Enter a description for the CEN instance.

     In this example, *CEN-for-test-private-VPN-Gateway* is used.

2. Attach VPC1 to the CEN instance

   i. On the **Instances** page, click the ID of the CEN instance created in Step .

   ii. On the **Basic Settings** tab, click ⊕ in the **VPC** section.



cen-ny[redacted]492da

Transit Router	Bandwidth Plan Capacity	Allocated Bandwidth	VPC	VBR	CCN
1	0Mbps	0Mbps	0 ⊕	0 ⊕	0 ⊕

   iii. On the **Connection with Peer Network Instance** page, set the following parameters and click **OK**.

Parameter	Description
Network Type	Select the type of network instance that you want to attach. In this example, **VPC** is selected.
Region	Select the region where the network instance is deployed. In this example, the **China (Hangzhou)** region is selected.
Transit Router	The system automatically creates a transit router in the selected region.
Select the primary and secondary zones for the transit router	Select the primary and secondary zones for the transit router. The following configurations are used in this example: ■ **Primary Zone**: **Hangzhou Zone H** ■ **Secondary Zone**: **Hangzhou Zone I**
Resource Owner ID	Select the Alibaba Cloud account to which the network instance belongs. In this example, **Your Account** is selected.
Billing Method	In this example, the default value **Pay-As-You-Go** is selected. For more information about billing rules, see Billing.
Attachment Name	Enter a name for the network connection. In this example, *VPC1-test* is used.
Networks	Select the ID of the network instance that you want to attach. In this example, VPC1 is selected.

Parameter	Description
VSwitch	Select a vSwitch from the primary zone and a vSwitch from the secondary zone. In this example, the following vSwitches are selected: ■ **Hangzhou Zone H (Primary)**: vSwitch1 ■ **Hangzhou Zone I (Secondary)**: vSwitch2
Advanced Settings	By default, the system automatically enables the following advanced features. The default settings are used in this example.

3. Attach the VBR to the CEN instance.

   i. On the **Connection with Peer Network Instance** page, set the following parameters and click **OK**.

Parameter	Description
Network Type	Select the type of network instance that you want to attach. In this example, **Virtual Border Router (VBR)** is selected.
Region	Select the region where the network instance is deployed. In this example, the **China (Hangzhou)** region is selected.
Transit Router	The system automatically displays the transit router in the current region.
Resource Owner ID	Select the Alibaba Cloud account to which the network instance belongs. In this example, **Your Account** is selected.
Attachment Name	Enter a name for the network connection. In this example, *VBR-test* is used.
Networks	Select the ID of the network instance that you want to attach. In this example, the VBR created in Step 1 is selected.

Parameter	Description
Advanced Settings	By default, the system automatically enables the following advanced features. ▪ **Associate with Default Route Table of Transit Router** After this feature is enabled, the VBR connection is automatically associated with the default route table of the transit router. The transit router forwards the traffic of the VBR based on the default route table. ▪ **Propagate System Routes to Default Route Table of Transit Router** After this feature is enabled, the system routes of the VBR are automatically advertised to the default route table of the transit router. ▪ **Propagate Routes to VBR** After this feature is enabled, the system automatically advertises the routes in the route table that is associated with the VBR connection to the VBR. The default settings are used in this example.

Step 3: Deploy a VPN gateway

After you complete the preceding steps, the data center is connected to VPC1 over a private connection. However, the private connection is not encrypted. To encrypt the private connection, you must deploy a VPN gateway in VPC1.

1. Create a VPN gateway.

   i.

   ii. In the top navigation bar, select the region where you want to create the VPN gateway.

   The VPN gateway and the VPC to be associated must belong to the same region. In this example, the **China (Hangzhou)** region is selected.

   iii.

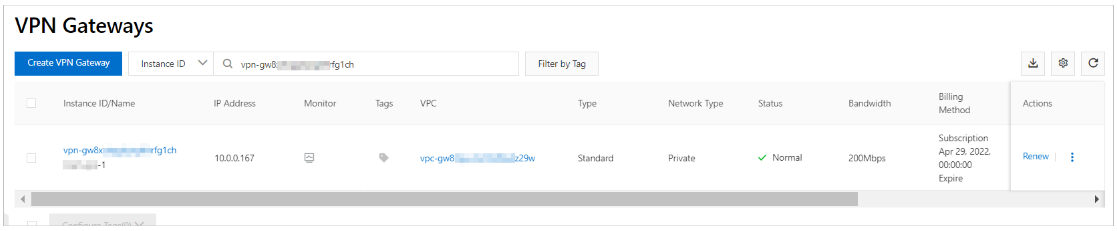
   iv. On the buy page, set the following parameters, click **Buy Now**, and then complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway. In this example, *VPNGateway1* is entered.
Region	Select the region where you want to deploy the VPN gateway. In this example, the **China (Hangzhou)** region is selected.

Parameter	Description
Network Type	Select the network type of the VPN gateway. **Private** is selected in this example.
VPC	Select the VPC with which you want to associate the VPN gateway. In this example, VPC1 is selected.
Specify VSwitch	Select whether to deploy the VPN gateway in a specified vSwitch of the VPC. **Yes** is selected in this example.
VSwitch	Select the vSwitch where you want to deploy the VPN gateway. vSwitch1 is selected in this example.
Maximum Bandwidth	Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
Traffic	The billing method of the VPN gateway. Default value: **Pay-by-data-transfer**. For more information, see Pay-as-you-go.
IPsec-VPN	Private VPN gateways support only the IPsec-VPN feature. In this example, the default value **Enable** is selected for the IPsec-VPN feature.
Duration	Specify the billing cycle. Default value: **By Hour**.
Service-linked Role	Click **Create Service-linked Role** and the system automatically creates the service-linked role AliyunServiceRoleForVpn. For more information about how a VPN gateway assumes the role to access other cloud resources, see AliyunServiceRoleForVpn. If **Created** is displayed, the service-linked role is created and you do not need to create it again.

v. Return to the **VPN Gateways** page, check and record the private IP address of the VPN gateway that you created. This IP address is used when you configure IPsec-VPN connections.

A newly created VPN gateway is in the **Preparing** state. After about 1 to 5 minutes, it enters the **Normal** state. The **Normal** state indicates that the VPN gateway is initialized and ready for use.



VPN Gateways

vpn-gw8[redacted]rfg1ch

	Instance ID/Name	IP Address	Monitor	Tags	VPC	Type	Network Type	Status	Bandwidth	Billing Method	Actions
□	vpn-gw8x[redacted]rfg1ch [redacted]-1	10.0.0.167			vpc-gw8[redacted]z29w	Standard	Private	✓ Normal	200Mbps	Subscription Apr 29, 2022, 00:00:00 Expire	Renew ⋮

2. Create a customer gateway.

   i.

   ii.

   iii. In the **Create Customer Gateway** panel, set the following parameters and click **OK**.

   The following content describes only the key parameters. For more information about the other parameters, see Create a customer gateway.

   - **Name**: Enter a name for the customer gateway.

     In this example, *Customer-Gateway* is used.

   - **IP Address**: Enter the VPN IP address of the on-premises device to be connected to the VPN gateway.

     In this example, *192.168.0.251* is used.

   - **ASN**: Enter the ASN of the on-premises gateway device.

     In this example, *65530* is used.

3. Create an IPsec-VPN connection.

   i.

   ii.

   iii. On the **Create IPsec Connection** page, configure the IPsec-VPN connection based on the following information and click **OK**.

   The following table describes only the key parameters. For more information about the other parameters, see Create an IPsec-VPN connection.

Parameter	Description
Name	Enter a name for the IPsec-VPN connection. In this example, *IPsecConnection1* is used.
VPN Gateway	Select the VPN gateway that you created. In this example, VPNGateway1 is selected.

Parameter	Description
Customer Gateway	Select the customer gateway that you created. In this example, Customer-Gateway is selected.
Routing Mode	Select a routing mode. In this example, **Destination Routing Mode** is selected.
Effective Immediately	Specify whether to immediately start negotiations. ▪ **Yes**: starts connection negotiations after the configuration is completed. ▪ **No**: starts negotiations when inbound traffic is detected. **Yes** is selected in this example.
Pre-Shared Key	Enter a pre-shared key. If you do not enter a value, the system generates a random 16-bit string as the pre-shared key. **Notice** Make sure that the on-premises device and the IPsec-VPN connection use the same pre-shared key. In this example, *fddsFF123***** is used.
Advanced Configuration	In this example, **ikev2** is selected for the **Version** parameter in the **IKE Configurations** section. The default values are used for the other parameters.

Parameter	Description
BGP Configuration	In this example, BGP Configuration is enabled. The following content describes the parameters. ■ **Tunnel CIDR Block**: Enter the CIDR block of the IPsec tunnel. The CIDR block must fall within 169.254.0.0/16. The subnet mask of the CIDR block must be 30 bits in length. In this example, *169.254.10.0/30* is entered. ■ **Local BGP IP address**: Enter the BGP IP address on the VPN gateway side. This IP address must fall within the CIDR block of the IPsec tunnel. In this example, *169.254.10.1* is entered. The BGP IP address on the data center side is *169.254.10.2*. ■ **Local ASN**: Enter the ASN on the VPN gateway side. Default value: 45104. In this example, the default value 45104 is used. **Notice** If you configure BGP routing for both the VBR and the VPN gateway, make sure that the ASN on the VPN gateway side is the same as the ASN of the VBR. This facilitates route management.
Health Check	In this example, the default settings are used.

iv. After you create an IPsec-VPN connection, click **OK** in the **Established** dialog box.

4. Enable automatic BGP advertising for the VPN gateway.

   After automatic BGP advertising is enabled and a peering connection is established between the VPN gateway and the on-premises gateway device, the VPN gateway learns and advertises the CIDR block of the data center to VPC1. The VPN gateway also advertises the routes in the system route table of VPC1 to the on-premises gateway device.

   i. In the left-side navigation pane, choose **Interconnections > VPN > VPN Gateways**.

   ii. On the **VPN Gateways** page, find VPNGateway1 and select ⋮ **> Enable Automatic BGP Propagation** in the **Actions** column.

   iii. In the **Enable Automatic BGP Propagation** message, click **OK**.

5. Download the IPsec configurations of the on-premises gateway device.

   i.

ii. On the **IPsec Connections** page, find IPsecConnection1. In the **Actions** column, choose ⋮ > **Download Configuration**.

Save the downloaded IPsec configurations on your client.

6. Add VPN configurations, BGP configurations, and static routes to the on-premises gateway device.

   Add VPN configurations, BGP configurations, and static routes to the on-premises gateway device based on the configurations of the IPsec-VPN connection that you downloaded.

   The following configurations are used for reference only. The commands may vary based on the network device vendor. Contact the vendor to obtain the information about specific commands.

   i. Open the CLI of the on-premises gateway device.

   ii. Run the following commands to set the IKEv2 proposal and policy:

```
crypto ikev2 proposal alicloud
encryption aes-cbc-128          //Configure the encryption algorithm. In this example, aes-cbc-128 is used.
integrity sha1                  //Configure the authentication algorithm. In this example, sha1 is used.
group 2                         //Configure the DH group. In this example, group 2 is used.
exit
!
crypto ikev2 policy Pureport_Pol_ikev2
proposal Pureport_prop
exit
!
```

   iii. Run the following commands to set the IKEv2 keyring:

```
crypto ikev2 keyring alicloud
peer alicloud
address 10.0.0.167               //Configure the private IP address of the VPN gateway. In this example, 10.0.0.167 is used.
pre-shared-key fddsFF123****     //Configure the pre-shared key. In this example, fddsFF123**** is used.
exit
!
```

   iv. Run the following commands to set the IKEv2 profile:

```
crypto ikev2 profile alicloud
match identity remote address 10.0.0.167 255.255.255.255    //Configure the private IP address of the VPN gateway. In this example, 10.0.0.167 is used.
identity local address 192.168.0.251    //Configure the VPN IP address of the data center. In this example, 192.168.0.251 is used.
authentication remote pre-share   //Set the authentication mode for the VPC to PSK (pre-shared key).
authentication local pre-share    //Set the authentication mode for the data center to PSK.
keyring local alicloud            //Invoke the IKEv2 keyring.
exit
!
```

v. Run the following commands to set transform:

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
mode tunnel
exit
!
```

vi. Run the following commands to configure the IPsec profile and invoke the transform, PFS, and IKEv2 profiles:

```
crypto ipsec profile alicloud
set transform-set TSET
set pfs group2
set ikev2-profile alicloud
exit
!
```

vii. Run the following commands to configure the IPsec tunnel:

```
interface Tunnel100
ip address 169.254.10.2 255.255.255.252    //Configure the tunnel address for the data center. In this example, 169.254.10.2 is used.
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 10.0.0.167              //Configure the private IP address of the VPN gateway. In this example, 10.0.0.167 is used.
tunnel protection ipsec profile alicloud
no shutdown
exit
!
interface GigabitEthernet1                 //Configure the IP address of the interface that is used to connect to the VPN gateway.
ip address 192.168.0.251 255.255.255.0
negotiation auto
!
```

viii. Run the following commands to set the BGP routing protocol:

> **Notice** To ensure that traffic from the VPC to the data center is routed to the encrypted tunnel of the VPN gateway, you must advertise a CIDR block that is smaller than the CIDR block of the data center in the BGP configurations of the on-premises gateway device.
>
> In this example, the CIDR block of the data center is 192.168.0.0/16. Therefore, you must advertise a CIDR block that is smaller than 192.168.0.0/16 in the BGP configurations of the on-premises gateway device. In this example, *192.168.1.0/24* is advertised.

```
router bgp 65530                          //Enable BGP and configure the ASN of the data center. In this example, 65530 is used.
neighbor 169.254.10.1 remote-as 45104     //Configure the ASN of the BGP peer. In this example, the ASN of the VPN gateway 45104 is used.
neighbor 169.254.10.1 ebgp-multihop 10    //Set the EBGP hop-count to 10.
!
address-family ipv4
network 192.168.1.0 mask 255.255.255.0    //Advertise the CIDR block of the data center. In this example, 192.168.1.0/24 is advertised.
neighbor 169.254.10.1 activate            //Activate the BGP peer.
exit-address-family
!
```

ix. Run the following command to configure a static route:

```
ip route 10.0.0.167 255.255.255.255 10.0.0.2  //Route traffic from the data center to the VPN gateway to the Express Connect circuit.
```

Step 4: Configure routes and routing policies for the VPC, VBR, and CEN instance

After you complete the preceding steps, an encrypted tunnel can be established between the on-premises gateway device and the VPN gateway. You must configure routes and routing policies for the VPC, VBR, and CEN instance to route traffic to the encrypted tunnel when the data center communicates with Alibaba Cloud.

1. Add custom routes for VPC1.
   i. Log on to the VPC console.
   ii. In the left-side navigation pane, click **Route Tables**.
   iii. In the top navigation bar, select the region to which the route table belongs.

      In this example, the **China (Hangzhou)** region is selected.
   iv. On the **Route Tables** page, find and click the ID of the route table that you want to manage.

      In this example, the ID of the system route table of VPC1 is clicked.
   v. On the **Route Entry List** tab, click **Custom Route** and then click **Add Route Entry**.

vi. In the **Add Route Entry** panel, set the following parameters and click **OK**.

Parameter	Description
Name	Enter a name for the custom route.
Destination CIDR Block	Enter the destination CIDR block of the custom route. In this example, **IPv4 CIDR Block** is selected and the VPN IP address of the on-premises gateway device is used, which is *192.168.0.251/32*.
Next Hop Type	Select the type of the next hop. In this example, **Transit Router** is selected.
Transit Router	Select the next hop of the custom route. In this example, VPC1-test is selected.

2. Add a custom route for the VBR.

   i. Log on to the Express Connect console.

   ii. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.

   iii. In the top navigation bar, select the region where the VBR is deployed.

   In this example, the **China (Hangzhou)** region is selected.

   iv. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to manage.

   v. Click the **Routes** tab and click **Add Route**.

   vi. In the **Add Route** panel, set the following parameters and click **OK**.

Parameter	Description
Next Hop Type	Select **Physical Connection Interface**.
Destination CIDR Block	Enter the VPN IP address of the on-premises gateway device. In this example, *192.168.0.251/32* is used.
Next Hop	Select the Express Connect circuit created in Step .

3. Configure a routing policy for the CEN instance.

   After you complete the preceding configurations, the data center learns the CIDR block of VPC1 from both the VBR and the VPN gateway. To ensure that traffic from Alibaba Cloud to the data center is preferentially routed to VPC1 through the encrypted tunnel of the VPN gateway, you must configure a routing policy for the CEN instance. The routing policy is used to ensure that the priority of the VPC CIDR block advertised by the VBR to the data center is lower than the priority of the VPC CIDR block advertised by the VPN gateway to the data center.

   i. Log on to the CEN console.

   ii. On the **Instances** page, click the ID of the CEN instance created in Step .

iii. Choose **Basic Settings > Transit Router**, find and click the ID of the transit router that you want to manage.

iv. On the details page of the transit router, click the **Route Table** tab and click **Route Maps**.

v. On the **Route Maps** tab, click **Add Route Map**. In the **Add Route Map** panel, set the following parameters and click **OK**.

The following table describes only the key parameters. For more information about the other parameters, see 路由策略概述.

Parameter	Description
Routing Policy Priority	Enter a priority value for the routing policy. In this example, *5* is entered.
Region	Select the region in which the routing policy applies. In this example, the **China (Hangzhou)** region is selected.
Associated Route Table	Select a route table to associate with the routing policy. In this example, the default route table of the current transit router is selected.
Direction	Select the direction in which the routing policy applies. In this example, **Import to Regional Gateway** is selected.
Match Condition	Configure match conditions for the routing policy. In this example, the following match conditions are used: ■ **Source Instance IDs**: Enter the ID of VPC1. ■ **Destination Instance IDs**: Enter the ID of the VBR. ■ **Route Prefix**: Enter *10.0.1.0/24* and *10.0.0.0/24*.
Routing Policy Action	Select an action for the routing policy. In this example, **Permit** is selected.
Add Policy Entry	Specify a priority for the routes that are permitted. In this example, **Appended AS Path** is selected and *65525*, *65526*, and *65527* are entered. This reduces the priority of the VPC CIDR block that the VBR advertises to the data center.

Step 5: Check the network connectivity

After you complete the preceding steps, the data center can communicate with VPC1 over private and encrypted connections. The following content describes how to test the connectivity between the data center and VPC1, and check whether the private connection is encrypted by the VPN gateway.

1. Test the network connectivity.

   i. Log on to ECS1. For more information, see Connect to an ECS instance.

ii. Run the **ping** command to ping a client in the data center to test the network connectivity between the data center and VPC1.

```
ping <the IP address of a client in the data center>
```

If an echo reply packet is returned, it indicates that the data center is connected to VPC1.

2. Check whether the private connection is encrypted.

   If you can view monitoring data of data transfer on the details page of the IPsec-VPN connection, it indicates that the private connection is encrypted.

   i.

   ii. In the top navigation bar, select the region where the VPN gateway is deployed.

   In this example, the **China (Hangzhou)** region is selected.

   iii.

   iv. On the **IPsec Connections** page, find the IPsec-VPN connection created in Step and click its ID.
   Go to the details page of the IPsec-VPN connection to view monitoring data of data transfer.