ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

VPN Gateway

User Guide

Product Version: v3.16.2

Document Version: 20220913

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

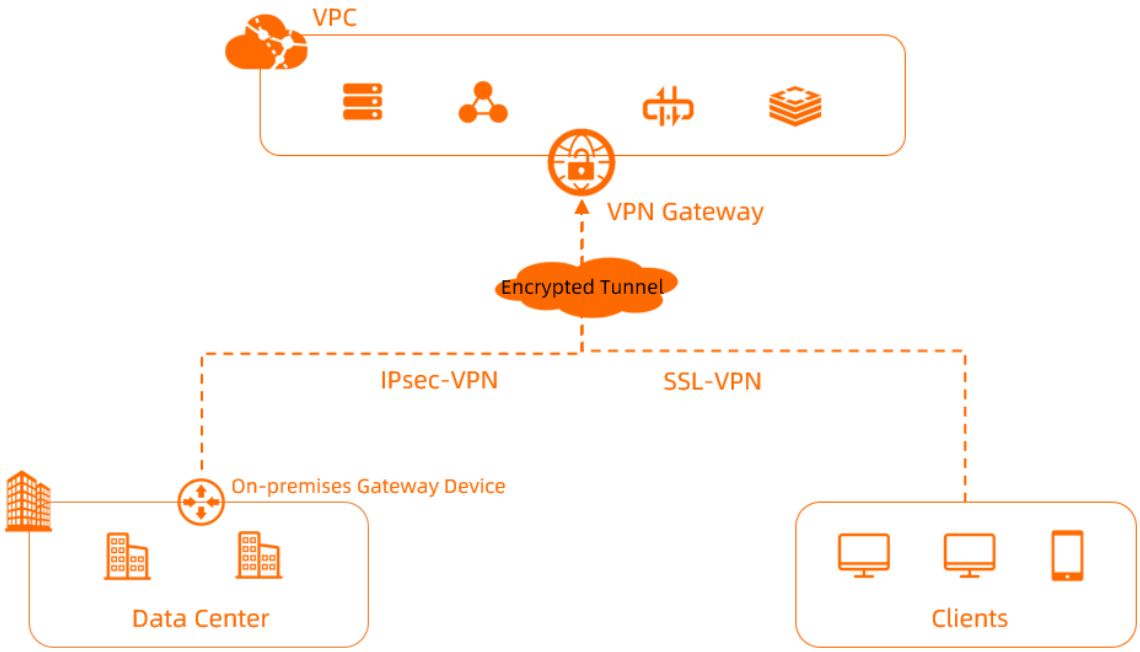
Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major 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.What is VPN Gateway?

VPN Gateway is an Internet-based service that securely and reliably connects enterprise data centers, office networks, and Internet terminals to virtual private clouds (VPCs) through encrypted tunnels.

> **Note** To comply with the relevant national regulations and policies, Alibaba Cloud VPN Gateway does not provide Internet access services.



Features

VPN Gateway supports both IPsec-VPN connections and SSL-VPN connections.

- IPsec-VPN

  IPsec-VPN connects networks based on routes. It facilitates the configuration and maintenance of VPN policies, and provides flexible traffic routing methods.

  You can use IPsec-VPN to connect a data center to a VPC or connect two VPCs. IPsec-VPN supports the IKEv1 and IKEv2 protocols. All on-premises gateway devices that support these two protocols can connect to VPN gateways on Alibaba Cloud.

- SSL-VPN

  SSL-VPN is based on OpenVPN. After you deploy the required resources, you can load the SSL client certificate on your client and initiate an SSL-VPN connection between the client and a VPC. This way, your client can access applications and services in the VPC.

Benefits

- **Security**

  VPN Gateway uses the IKE and IPsec protocols in data transmission to ensure data security.

- **Stability**

VPN Gateway adopts the hot-standby architecture to implement failover within a few seconds, session persistence, and zero service downtime.

- **Ease of use**

  VPN gateway is ready-to-use and its configurations immediately take effect. You can deploy VPN gateways in a fast manner.

- **Cost savings**

  The encrypted and Internet-based connections provided by VPN Gateway are more cost-effective than Express Connect circuits.

2.Log on to the VPN Gateway console

This topic describes how to log on to the Apsara Uni-manager Management Console.

Prerequisites

- Before you log on to the Apsara Uni-manager Management Console, the endpoint of the console is obtained from the deployment staff.
- We recommend that you use Google Chrome.

Procedure

1. Enter the URL of the Apsara Uni-manager Management Console in the address bar and press the Enter key.
2. Enter your username and password.

   Obtain the username and password that you use to log on to the Apsara Uni-manager Management Console from the operations administrator.

   > **Note** The first time that you log on to the Apsara Uni-manager Management Console, you must change the password of your account. For security purposes, your password must meet the minimum complexity requirements. The password must be 10 to 32 characters in length and must contain at least two of the following character types:
   >
   > - Uppercase or lowercase letters
   > - Digits
   > - Special characters, including exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%)

3. Click **Log On**.
4. If your account has multi-factor authentication (MFA) enabled, perform corresponding operations in the following scenarios:
   - You log on to the Apsara Uni-manager Management Console for the first time after MFA is enabled by the administrator:
     a. On the Bind Virtual MFA Device page, bind an MFA device.
     b. Enter the username and password again as in Step 2 and click **Log On**.
     c. Enter a six-digit MFA verification code and click **Authenticate**.
   - You have enabled MFA and bound an MFA device:

     Enter a six-digit MFA verification code and click **Authenticate**.

     > **Note** For more information, see the *Bind a virtual MFA device to enable MFA* topic in *Apsara Uni-manager Management Console User Guide*.

5. In the top navigation bar, choose **Products > Networking > Virtual Private Cloud**.

3.Get started with IPsec-VPN

3.1. IPsec-VPN overview

You can connect a data center to a virtual private cloud (VPC) by establishing an IPsec-VPN connection. This topic describes how to configure IPsec-VPN.

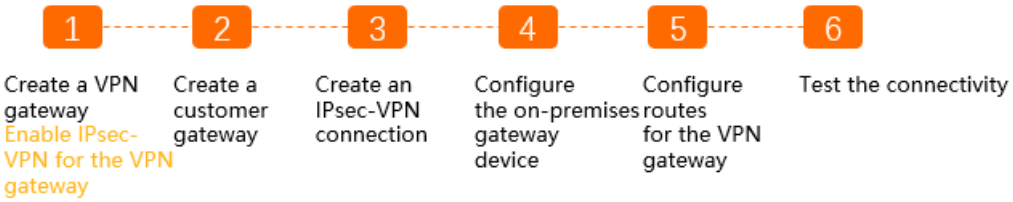
Prerequisites

Before you use IPsec-VPN to connect a data center to a VPC, make sure that the following requirements are met:

- The gateway device in the data center supports the IKEv1 and IKEv2 protocols.

  IPsec-VPN supports the IKEv1 and IKEv2 protocols. All gateway devices that support the two protocols can connect to VPN gateways on Alibaba Cloud.
- A static public IP address is assigned to the gateway device in the data center.
- The CIDR block of the data center does not overlap with the CIDR block of the VPC.
- You must make sure that the security group rules applied to the Elastic Compute Service (ECS) instances in the VPC allow gateway devices in the data center to access cloud resources.

Procedure



1. Create a VPN gateway

   You must enable the IPsec-VPN feature after you create the VPN gateway. You can establish more than one IPsec-VPN connection to each VPN gateway.
2. Create a customer gateway

   You must load the configuration of the gateway device in the data center to a customer gateway on Alibaba Cloud.
3. Create an IPsec-VPN connection

   An IPsec-VPN connection is a VPN tunnel between the VPN gateway and the gateway device in the data center. The data center can exchange encrypted data with Alibaba Cloud only after an IPsec-VPN connection is established.
4. Configure the gateway device in the data center

   You must load the configuration of the VPN gateway on Alibaba Cloud to the gateway device in the data center.
5. Add routes to the VPN gateway

You must add routes to the VPN gateway and advertise these routes to the VPC route table. Then, the VPC and the data center can communicate with each other. For more information, see Route overview.

6. Verify the connectivity

   Log on to an ECS instance that is not assigned a public IP address in the VPC. Then, run the **ping** command to **ping** the private IP address of a server that resides in the data center.

Common scenarios

Connect a data center to a VPC

3.2. Connect a data center to a VPC

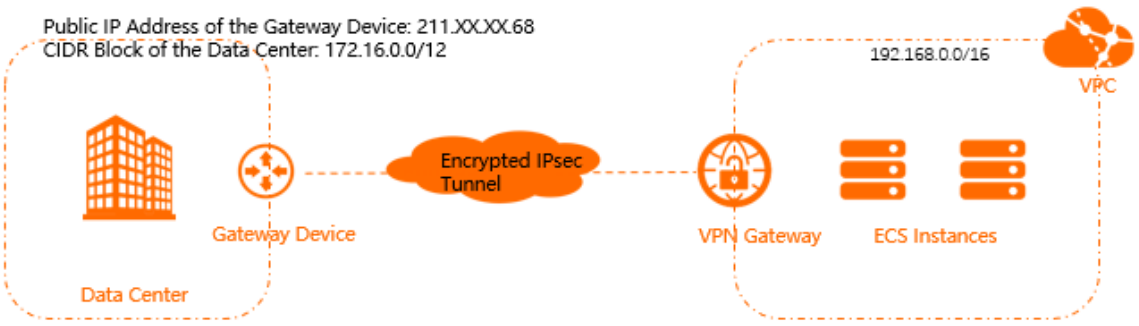
This topic describes how to use IPsec-VPN to connect a data center to a virtual private cloud (VPC). After you establish an IPsec-VPN connection, the data center and the VPC can communicate with each other.

Prerequisites

- The gateway device in the data center supports the IKEv1 and IKEv2 protocols. All gateway devices that support these protocols can connect to a VPN gateway.
- A static public IP address is assigned to the gateway device in the data center.
- The CIDR block of the data center does not overlap with the CIDR block of the VPC.
- You have read and understand the security group rules that apply to the ECS instances in VPCs, and the security group rules allow gateway devices in the data center to access cloud resources.

Context

The following scenario is used as an example. An enterprise has created a VPC on Apsara Stack. The CIDR block of the VPC is 192.168.0.0/16. The CIDR block of the data center is 172.16.0.0/16. The static public IP address of the gateway device in the data center is 211.XX.XX.68. To meet business requirements, the enterprise needs to connect the data center to the VPC. You can establish an IPsec-VPN connection between the data center and the VPC, as shown in the following figure. This way, the data center and the VPC can share resources with each other.



Step 1: 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 **Create VPN** page, set the following parameters and click **Submit**:
   - **Organization**: Select the organization to which the VPN gateway belongs.
   - **Resource Set**: Select the resource set to which the VPN gateway belongs.
   - **Region**: Select the region where you want to deploy the VPN gateway.

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

   - **Zone**: Select the zone where you want to deploy the VPN gateway.
   - **Instance Name**: Enter a name for the VPN gateway.

     The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
   - **VPC**: Select the VPC to be connected to the VPN gateway.
   - **VSwitch**: Select the vSwitch to be associated with the VPN gateway.
   - **Bandwidth**: Specify the maximum bandwidth of the VPN gateway. Unit: Mbit/s. The bandwidth is used for data transfer over the Internet.
   - **IPsec-VPN**: Specify whether to enable IPsec-VPN. In this example, **Enable** is elected.

     After IPsec-VPN is enabled, you can create IPsec-VPN connections between a data center and a VPC, or between two VPCs.
   - **SSL-VPN**: Specify whether to enable SSL-VPN. In this example, **Disable** is selected.

     SSL-VPN connections are point-to-site connections. SSL-VPN allows you to connect a client to Apsara Stack without the need to configure a customer gateway.
5. Return to the VPN Gateways page to view the VPN gateway.

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

Step 2: Create a customer gateway

1. In the left-side navigation pane, choose **VPN > Customer Gateways**.
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. On the **Create Customer Gateway** page, set the following parameters and click **Submit**:
   - **Organization**: Select the organization to which the customer gateway belongs.
   - **Resource Set**: Select the resource set to which the customer gateway belongs.
   - **Region**: Select the region where you want to deploy the customer gateway.

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

- **Zone**: Select the zone where you want to deploy the customer gateway.
- **Name**: Enter a name for the customer gateway.

  The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
- **IP Address**: Enter the public IP address of the gateway device in the data center that you want to connect to the VPC. In this example, 211.XX.XX.68 is used.
- **Description**: Enter a description for the customer gateway.

  The description must be 2 to 100 characters in length and must start with a letter. The description can contain digits, hyphens (-), underscores (_), full-width periods (。), full-width commas (，), and full-width colons (：).

Step 3: Create an IPsec-VPN connection

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. In the top navigation bar, select the region where you want to create the IPsec-VPN connection.

   > **Note** Make sure that the IPsec-VPN connection and the VPN gateway to be connected are deployed in the same region.
3. On the **IPsec Connections** page, click **Create an IPsec connection**.
4. On the **Create IPsec Connection** page, configure the IPsec-VPN connection based on the following information and click **Submit**:
   - **Organization**: Select the organization to which the IPsec-VPN connection belongs.
   - **Resource Set**: Select the resource set to which the IPsec-VPN connection belongs.
   - **Region**: Select the region to which the IPsec-VPN connection belongs.
   - **Zone**: Select the zone to which the IPsec-VPN connection belongs.
   - **Name**: Enter a name for the IPsec-VPN connection.
   - **VPN Gateway**: Select the created VPN gateway.
   - **Customer Gateway**: Select the customer gateway to be connected.
   - **Local CIDR Block**: Enter the CIDR block of the VPC where the VPN gateway is deployed. 192.168.0.0/16 is used in this example.
   - **Peer CIDR Block**: Enter the CIDR block of the data center. In this example, 172.16.0.0/16 is used.
   - **Effective Immediately**: Select whether to immediately start negotiations.
     - **Yes**: starts negotiations after the configuration is completed.
     - **No**: starts negotiations when inbound traffic is detected.
   - **Advanced Settings**: Select **Default**.

     By default, a pre-shared key is automatically generated.

Step 4: Load the configuration of the IPsec-VPN connection to the gateway device in the data center

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. On the **IPsec Connections** page, find the IPsec-VPN connection and click **Download peer configuration** in the **Operation** column.
3. In the **IPsec connection configuration** message, copy and save the configuration to an on-premises device.
4. Load the configuration of the IPsec-VPN connection to the gateway device in the data center. For more information, consult the vendor of your gateway device.

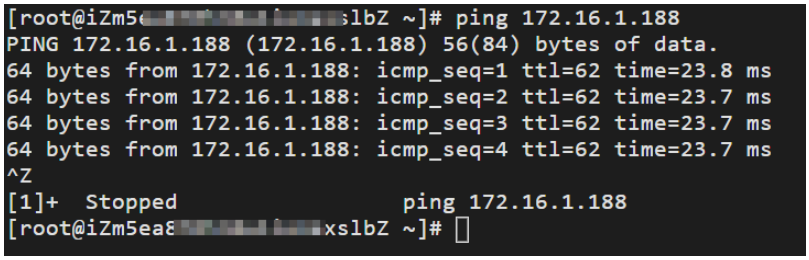
Step 5: Configure routes for the VPN gateway

1. In the left-side navigation pane, choose **VPN > VPN Gateways**.
2. On the **VPN Gateway** page, find the VPN gateway that you want to manage and click its ID.
3. On the **Destination-based Routing** tab, click **Add route entry**.
4. In the **Add route entry** dialog box, set the following parameters and click **OK**:
   - **Target network segment**: Enter the private CIDR block of the data center. In this example, 172.16.0.0/16 is used.
   - **Next hop type**: Select **IPsec connection**.
   - **Next hop**: Select the IPsec-VPN connection that you created.
   - **Publish to VPC**: Specify whether to automatically advertise the route to the VPC route table. In this example, **Yes** is selected.
   - **Weight**: Select a weight for the route. In this example, **100** is selected.
     - **100**: specifies a high priority for the route.
     - **0**: specifies a low priority for the route.

> **Note** If two routes are configured with the same destination CIDR block, you cannot set the weights of both routes to 100.

Step 6: Test the network connectivity

1. Log on to an Elastic Compute Service (ECS) instance that is not assigned a public address in the VPC.
2. Run the **ping** command to ping a server in the data center to test the network connectivity.



4.Get started with SSL-VPN

4.1. SSL-VPN overview

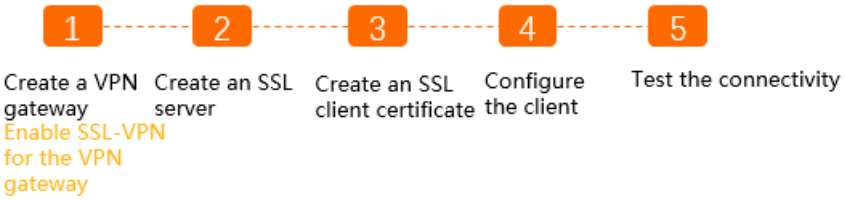
SSL-VPN allows clients to connect to a virtual private cloud (VPC) and access applications and services that are deployed in the VPC in a secure manner. This topic describes how to use SSL-VPN.

Prerequisites

Before you use SSL-VPN to establish a connection between a client and a VPC, make sure that the following requirements are met:

- The private CIDR block of the client does not overlap with the private CIDR block of the VPC. Otherwise, the client and the VPC cannot communicate with each other.
- The client can access the Internet.
- You have read and understand the security group rules that apply to the Elastic Compute Service (ECS) instances in the VPC, and make sure that the security rules allow the client to access the ECS instances.

Procedure



1. Create a VPN gateway.

   Create a VPN gateway and enable the SSL-VPN feature.

2. Create an SSL server.

   On the SSL server, specify the private CIDR block that the client needs to access and the CIDR block that is used by the client.

3. Create an SSL client certificate.

   Create and download a client certificate based on the SSL server configuration.

4. Configure the client.

   Download and install VPN software on the client, load the SSL client certificate, and then initiate an SSL-VPN connection.

5. Verify the connectivity.

   Open the CLI on the client, and run the **ping** command to ping an ECS instance in the VPC.

Basic scenarios

Connect a client to a VPC

4.2. Connect a client to a VPC

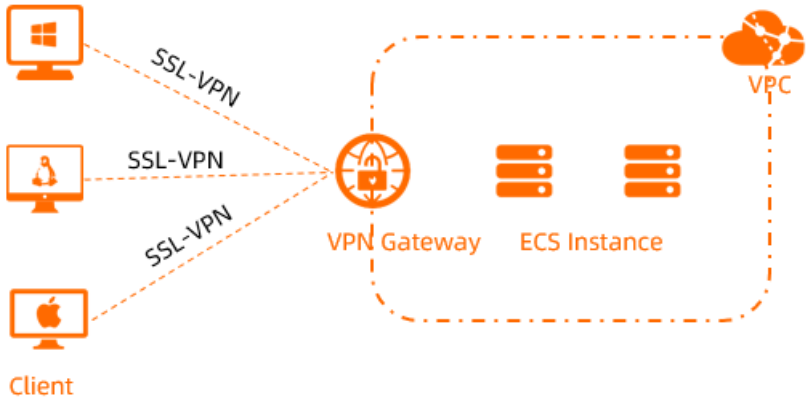
This topic describes how to connect a client to a virtual private cloud (VPC) by using SSL-VPN.

Prerequisites

- The private CIDR block of the client does not overlap with the private CIDR block of the VPC. Otherwise, the client and the VPC cannot communicate with each other.
- The client can access the Internet.
- You have read and understand the security group rules that apply to the ECS instances in VPCs, and the security group rules allow gateway devices in the data center to access cloud resources.

Context

The scenario in the following figure is used as an example to describe how to connect Linux, Windows, and Mac clients to a VPC by using SSL-VPN.



Step 1: 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 **Create VPN** page, set the following parameters and click **Submit**:
   - **Organization**: Select the organization to which the VPN gateway belongs.
   - **Resource Set**: Select the resource set to which the VPN gateway belongs.
   - **Region**: Select the region where you want to deploy the VPN gateway.

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

   - **Zone**: Select the zone where you want to deploy the VPN gateway.
   - **Instance Name**: Enter a name for the VPN gateway.

The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.

- **VPC**: Select the VPC to be connected to the VPN gateway.
- **VSwitch**: Select the vSwitch to be associated with the VPN gateway.
- **Bandwidth**: Specify the maximum bandwidth of the VPN gateway. The bandwidth is used for data transfer over the Internet.
- **IPsec-VPN**: Specify whether to enable IPsec-VPN. In this example, **Disable** is selected.
- **SSL-VPN**: Specify whether to enable SSL-VPN. In this example, **Enable** is selected.

  SSL-VPN connections are point-to-site connections. SSL-VPN allows you to connect a client to Apsara Stack without the need to configure a customer gateway.
- **SSL-VPN Connections**: Specify the maximum number of concurrent SSL connections that the VPN gateway supports.

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

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

Step 2: Create an SSL server

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

   > **Note** Make sure that the SSL server and the VPN gateway that you created are deployed in the same region.

3. On the **SSL Server** page, click **Create SSL Server**.
4. On the **Create SSL Server** page, set the following parameters and click **Submit**:
   - **Organization**: Select the organization to which the SSL server belongs.
   - **Resource Set**: Select the resource set to which the SSL server belongs.
   - **Region**: Select the region where you want to deploy the SSL server.
   - **Zone**: Select the zone where you want to deploy the SSL server.
   - **Name**: Enter a name for the SSL server.
   - **VPN Gateway**: Select the VPN gateway that you created.
   - **Local CIDR Block**: Enter the CIDR block of the network to which you want to connect. You can enter multiple local CIDR blocks. Separate multiple local CIDR blocks with commas (,). The local CIDR block can be the CIDR block of a VPC, a vSwitch, or an on-premises network.
   - **Client CIDR Block**: Enter the CIDR block that the client uses to connect to the SSL server. Example: 192.168.10.0/24.
   - **Advanced Settings**: Select **Default**.

Step 3: Create and download an SSL client certificate

1. In the left-side navigation pane, choose **VPN > SSL Clients** .
2. On the **SSL Client** page, click **Create SSL client**.

3. On the **Create SSL Client Certificate** page, set the following parameters for the SSL client, and then click **Submit**.
   - **Organization**: Select the organization to which the SSL client certificate belongs.
   - **Resource Set**: Select the resource set to which the SSL client certificate belongs.
   - **Region**: Select the region where you want to create the SSL client certificate.
   - **Zone**: Select the zone where you want to create the SSL client certificate.
   - **Name**: Enter a name for the SSL client certificate.
   - **VPN Gateway**: Select the VPN gateway with which you want to associate the SSL client certificate.
   - **SSL Server**: Select the SSL server with which you want to associate the SSL client certificate.
4. On the **SSL Client** page, find the created SSL client certificate and click **Download** in the **Operation** column.

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

Step 4: Configure the client

The following section describes how to configure Linux, Mac, and Windows clients.

- Configure a client that runs Linux
  i. Run the following command to install OpenVPN:

  ```
  yum install -y openvpn
  ```

  ii. Decompress the SSL client certificate package that you downloaded and copy the SSL client certificate to the */etc/openvpn/conf/* directory.

  iii. Go to the */etc/openvpn/conf/* directory and run the following command to start OpenVPN:

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

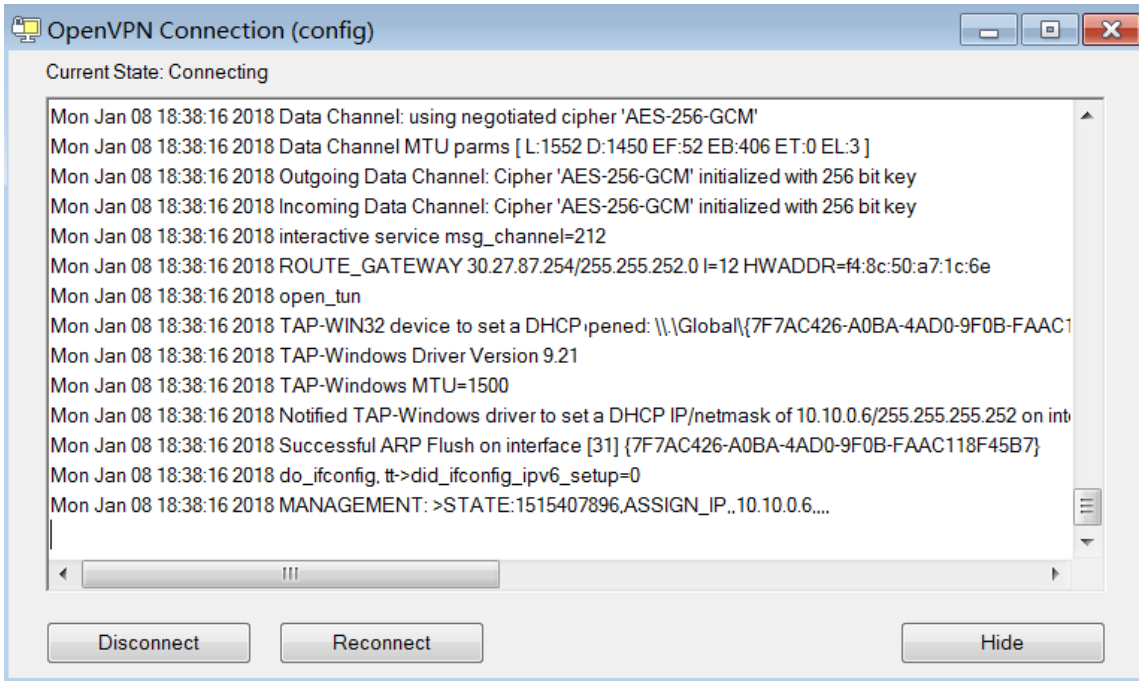
- Configure a client that runs Windows
  i. Download and install OpenVPN.

  Download OpenVPN.

  ii. Decompress the downloaded SSL client certificate package and copy the SSL client certificate to the *OpenVPN\config* directory.

  In this example, the certificate is copied to *C:\Program Files\OpenVPN\config*. You must copy the certificate to the directory where OpenVPN is installed.

  iii. Start OpenVPN and click **Connect** to initiate a connection.



- Configure a client that runs macOS
  i. Run the following command to install OpenVPN:

```
brew install openvpn
```

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

  ii. Copy the SSL client certificate package that you downloaded in Step 3 to the configuration directory of OpenVPN and decompress the package. Then, initiate an SSL-VPN connection.
    a. Back up all configuration files in the */usr/local/etc/openvpn* folder.
    b. Run the following command to delete the configuration files of OpenVPN:

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

    c. Run the following command to copy the downloaded SSL client certificate package to the configuration directory of OpenVPN:

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

`cert_location` specifies the path to which the SSL client certificate package is downloaded in Step 3. Example: */Users/example/Downloads/certs6.zip*.

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

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

    e. Run the following command to initiate a connection:

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

Step 5: Test the network connectivity

1. Open the CLI on the client.
2. Run the **ping** command to ping an Elastic Compute Service (ECS) instance in the VPC.

5.Manage a VPN Gateway

5.1. Create a VPN gateway

This topic describes how to create a VPN gateway. You must create a VPN gateway before you can use the IPsec-VPN and SSL-VPN features. After you create a VPN gateway, a public IP address is assigned to the VPN gateway.

Procedure

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 **Create VPN** page, set the following parameters and click **Submit**.

Parameter	Description
Organization	Select the organization to which the VPN gateway belongs.
Resource Set	Select the resource set to which the VPN gateway belongs.
Region	Select the region where you want to deploy the VPN gateway. You can create IPsec-VPN connections on VPN gateways to connect a data center to a virtual private cloud (VPC) or connect two VPCs. Make sure that the VPC and the VPN gateway associated with the VPC are deployed in the same region.
Zone	Select the zone to which the VPN gateway belongs.
Instance Name	Enter a name for the VPN gateway. The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
VPC	Select the VPC to be associated with the VPN gateway.
VSwitch	Select the vSwitch to be associated with the VPN gateway.
Bandwidth	Specify the maximum bandwidth value of the VPN gateway. Unit: Mbit/s. The bandwidth is used for data transfer over the Internet.
IPsec-VPN	Specify whether to enable the IPsec-VPN feature. Default value: **Enable IPsec**. After IPsec-VPN is enabled, you can create IPsec-VPN connections between a data center and a VPC, or between two VPCs.

Parameter	Description
SSL-VPN	Specify whether to enable the SSL-VPN feature. Default value: **Disable**. SSL-VPN connections are point-to-site connections. SSL-VPN allows you to connect a client to Apsara Stack without the need to configure a customer gateway.
SSL-VPN Connections	Select the maximum number of concurrent SSL-VPN connections that the VPN gateway supports. **Note** This parameter is available only if you enable SSL-VPN.

5.2. Modify a VPN gateway

This topic describes how to modify the name and description of a VPN gateway.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway that you want to modify, and click the icon below the instance ID. In the dialog box that appears, enter a new name and click **OK**.

   The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
5. Click in the **Description** column. In the dialog box that appears, enter a new description and click **OK**.

   The description must be 2 to 100 characters in length, and cannot start with `http://` or `https://`.

5.3. Configure routes of a VPN Gateway

5.3.1. Overview of gateway routes

After you create an IPsec-VPN connection by using a VPN gateway, you must add a route to the VPN gateway.

Route-based IPsec-VPN allows you to route network traffic in multiple ways, and facilitates the configuration and maintenance of VPN policies.

You can add the following two types of route to a VPN gateway:

- Policy-based routes.
- Destination-based routes.

Policy-based routing

Policy-based routes forward traffic based on source and destination IP addresses.

For more information, see Manage a policy-based route.

> **Note** Policy-based routes take precedence over destination-based routes.

Destination-based routes

Destination-based routes forward traffic to specified destination IP addresses.

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

5.3.2. Manage a policy-based route

A policy-based route forwards traffic based on source and destination IP addresses. This topic describes how to create, advertise, modify, and delete a policy-based route.

Prerequisites

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

Create a policy-based route

After you create an IPsec-VPN connection, you can create a policy-based route for the IPsec-VPN connection.

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway and click its ID.
5. Click the **Policy-based Routing** tab, and then click **Add Route Entry**.
6. In the **Add Route Entry** dialog box, set the following parameters and click **OK**.

Parameter	Description
Destination CIDR Block	Enter the private CIDR block that you want to access.
Source CIDR Block	Enter the private CIDR block on the virtual private cloud (VPC) side.
Next Hop Type	Select IPsec Connection.
Next Hop	Select the IPsec-VPN connection for which you want to create a policy-based route.

Parameter	Description
Publish to VPC	Specify whether to advertise the route to the VPC route table. ○ **Yes**(default): advertises the route to the VPC route table. ○ **No**: does not advertise the route to the VPC route table. **Note** If you select **No**, you must manually advertise the route to the VPC route table.
Weight	Select a weight: ○ **100** (default): specifies a high priority for the route. ○ **0**: specifies a low priority for the route. **Note** If a route table contains multiple policy-based routes that have the same source CIDR block, destination CIDR block, and weight, a policy-based route is randomly selected to forward traffic.

Advertise a policy-based route

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway and click its ID.
5. On the **Policy-based Routing** tab, find the policy-based route that you want to advertise and click **Publish** in the **Actions** column.
6. In the **Publish Route Entry** message, click **OK**.

   If you want to withdraw the policy-based route, click **Unpublish**.

Modify a policy-based route

You can change the weight of a policy-based route.

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway and click its ID.
5. On the **Policy-based Routing** tab, find the policy-based route that you want to modify and click **Edit** in the **Actions** column.
6. In the **Edit route entry** dialog box, enter a new weight and click **OK**.

Delete a policy-based route

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

4. On the **VPN Gateways** page, find the VPN gateway and click its ID.
5. On the **Policy-based Routing** tab, find the policy-based route that you want to delete and click **Delete** in the **Actions** column.
6. In the **Delete Route Entry** message, click **OK**.

5.3.3. Manage a destination-based route

A destination-based route forwards traffic based on destination IP addresses. This topic describes how to create, advertise, modify, and delete a destination-based route.

Prerequisites

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

Create a destination-based route

After you create an IPsec-VPN connection, you can create a destination-based route for the IPsec-VPN connection.

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway that you want to manage and click its ID.
5. On the **Destination routing table** tab, click **Add route entry**.
6. In the **Add route entry** dialog box, set the following parameters and click **OK**.

Parameter	Description
Target network segment	Enter the private CIDR block that you want to access.
Next hop type	Select IPsec connection.
Next hop	Select the IPsec-VPN connection for which you want to create a destination-based route.
Publish to VPC	Specify whether to advertise the route to the virtual private cloud (VPC) route table. ○ **Yes**(default): advertises the route to the VPC route table. ○ **No**: does not advertise the destination-based route to the VPC route table. **Note** If you select **No**, you must manually advertise the destination-based route to the VPC route table.

Parameter	Description
Weight	Select a weight. Valid values: ○ **100**: specifies a high priority for the destination-based route. ○ **0**: specifies a low priority for the destination-based route. **Note** If a route table contains multiple destination-based routes that have the same destination CIDR block and weight, a destination-based route is randomly selected to forward traffic.

Advertise a destination-based route

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway that you want to manage and click its ID.
5. On the **Destination routing table** tab, find the destination-based route that you want to manage and click **Publish** in the **Operation** column.
6. In the **Publish Route Entry** message, click **OK**.

   If you want to withdraw an advertised destination-based route, click **Unpublish**.

Modify the destination-based route

You can change the weight of a destination-based route.

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway that you want to manage and click its ID.
5. On the **Destination routing table** tab, find the destination-based route that you want to manage and click **Edit** in the **Operation** column.
6. In the **Edit route entry** dialog box, select a new weight and click **OK**.

Delete a destination-based route

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway that you want to manage and click its ID.
5. On the **Destination routing table** tab, find the destination-based route that you want to delete and click **Delete** in the **Operation** column.
6. In the **Delete Route Entry** message, click **OK**.

5.4. Delete a VPN gateway

This topic describes how to delete a VPN gateway that you no longer need. After you delete a VPN gateway, you can no longer establish IPsec-VPN or SSL-VPN connections to the VPN gateway.

Prerequisites

Before you delete a VPN gateway, make sure that the following conditions are met:

- The IPsec-VPN connections established to the VPN gateway are deleted. For more information, see Delete an IPsec-VPN connection.
- The SSL server associated with the VPN gateway is deleted. For more information, see Delete an SSL server.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. In the top navigation bar, select the region of the VPN gateway.
4. On the **VPN Gateways** page, find the VPN gateway that you want to delete and click **Delete** in the **Actions** column.
5. In the **Delete VPN Gateway** message, click **OK**.

6.Manage a customer gateway

6.1. Create a customer gateway

This topic describes how to create a customer gateway. You can use a customer gateway to establish an IPsec-VPN connection between a virtual private cloud (VPC) and a data center or between two VPCs. After you create a customer gateway, you can update the information about a gateway device in the data center to Alibaba Cloud. Then, you can connect the customer gateway to a VPN gateway. A customer gateway can connect to multiple VPN gateways.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > Customer Gateways**.
3. On the **Customer Gateways** page, click **Create Customer Gateway**.
4. On the **Create Customer Gateway** page, set the following parameters and click **Submit**.

Parameter	Description
Organization	Select the organization to which the customer gateway belongs.
Resource Set	Select the resource set to which the customer gateway belongs.
Region	Select the region where you want to deploy the customer gateway. **Note** Make sure that the customer gateway and the VPN gateway to be connected are deployed in the same region.
Zone	Select the zone where you want to deploy the customer gateway.
Name	Enter a name for the customer gateway. The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
IP Address	Enter the static public IP address of the gateway device in the data center.
Description	Enter a description for the customer gateway. The description must be 2 to 100 characters in length and must start with a letter. The description can contain digits, hyphens (-), underscores (_), full-width periods (。), full-width commas (，), and full-width colons (：).

6.2. Modify a customer gateway

This topic describes how to modify the name and description of a customer gateway.

Procedure

1. Log on to the VPN Gateway console.

2. In the left-side navigation pane, choose **VPN > Customer Gateways**.
3. In the top navigation bar, select the region of the customer gateway.
4. On the **Customer Gateways** page, find the customer gateway that you want to modify, and click the icon below the instance ID. In the dialog box that appears, modify the name, and then click **OK**.

   The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter..
5. Click in the **Description** column. In the dialog box that appears, enter a new description and click **OK**.

   The description must be 2 to 100 characters in length and must start with a letter. The description can contain digits, hyphens (-), underscores (_), full-width periods (。), full-width commas (，), and full-width colons (：).

6.3. Delete a customer gateway

This topic describes how to delete a customer gateway.

Prerequisites

The IPsec-VPN connections established to the VPN gateway are deleted. For more information, see Delete an IPsec-VPN connection.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > Customer Gateways**.
3. In the top navigation bar, select the region of the customer gateway.
4. On the **Customer Gateways** page, find the customer gateway that you want to delete, and then click **Delete** in the **Actions** column.
5. In the **Delete Customer Gateway** message, click **OK**.

7.Configure IPsec-VPN connections

7.1. Manage an IPsec-VPN connection

7.1.1. Create an IPsec-VPN connection

This topic describes how to create an IPsec-VPN connection. After you create a VPN gateway and a customer gateway, you can create an IPsec-VPN connection between the two gateways to encrypt data transmission.

Prerequisites

The IPsec-VPN feature is enabled when you create a VPN gateway. For more information, see Create a VPN gateway.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > IPsec Connections**.
3. On the **IPsec Connections** page, click **Create an IPsec connection**.
4. On the **Create IPsec-VPN Connection** page, configure the IPsec-VPN connection based on the following information and click **Submit**.

Parameter	Description
Organization	Select the organization to which the IPsec-VPN connection belongs.
Resource Set	Select the resource set to which the IPsec-VPN connection belongs.
Region	Select the region to which the IPsec-VPN connection belongs. **Note** Make sure that the IPsec-VPN connection and the VPN gateway to be connected are deployed in the same region.
Zone	Select the zone to which the IPsec-VPN connection belongs.
Name	Enter a name for the IPsec-VPN connection. The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
VPN Gateway	Select the VPN gateway to be connected through the IPsec-VPN connection.
Customer Gateway	Select the customer gateway to be connected through the IPsec-VPN connection.

Parameter	Description
Local CIDR Block	Enter the CIDR block on the virtual private cloud (VPC) side. The CIDR block is used in Phase 2 negotiations. If you use IKEv2, you can specify multiple local CIDR blocks. Separate CIDR blocks with commas (,).
Peer CIDR Block	Enter the CIDR block on the data center side. This CIDR block is used in Phase 2 negotiations. If you use IKEv2, you can specify multiple peer CIDR blocks. Separate CIDR blocks with commas (,).
Effective Immediately	Specify whether to immediately start negotiations for the connection. ○ **Yes**: starts negotiations after the configuration is complete. ○ **No** (default): starts negotiations when inbound traffic is detected.
Advanced Settings	Select the type of advanced settings. ○ **Default**: Use the default advanced settings. ○ **Configure**: Use custom settings.
Advanced Settings: IKE Settings	
Pre-shared Key	Enter the pre-shared key used for authentication between the VPN gateway and the customer gateway. You can specify a key, or use the key that is randomly generated by the system. By default, the system generates a 16-character string. To establish an IPsec-VPN connection, you must use the same key for the local side and the peer side.
Version	Select an IKE version. ○ **ikev1** (default) ○ **ikev2** IKEv1 and IKEv2 are supported. Compared with IKEv1, IKEv2 simplifies the security association (SA) negotiation process and provides better support for scenarios in which multiple CIDR blocks are used. We recommend that you select IKEv2.
Negotiation Mode	Select a negotiation mode. ○ **main** (default): This mode offers higher security during negotiations. ○ **aggressive**: This mode is faster and has a higher success rate. Connections negotiated in both modes ensure the same security level of data transmission.
Encryption Algorithm	Select the encryption algorithm that is used in Phase 1 negotiations. Supported algorithms are **aes** (default), **aes192**, **aes256**, **des**, and **3des**.

Parameter	Description
Authentication Algorithm	Select the authentication algorithm that is used in Phase 1 negotiations. Valid values: **sha1** and **md5** (default).
DH Group	Select the DH key exchange algorithm that is used in Phase 1 negotiations. ○ **group1**: DH group 1 ○ **group2**: DH group 2 (default) ○ **group5**: DH group 5 ○ **group14**: DH group 14
SA Life Cycle (Seconds)	Specify the SA lifecycle after Phase 1 negotiations succeed. Valid values: **0 to 86400**. Unit: seconds. Default value: **86400**.
LocalId	Specify the identifier of the VPN gateway. The identifier is used in Phase 1 negotiations. The default value is the public IP address of the VPN gateway. If you set LocalId to a value in the fully qualified domain name (FQDN) format, we recommend that you set Negotiation Mode to **aggressive**.
RemoteId	Specify the identifier of the customer gateway. The identifier is used in Phase 1 negotiations. The default value is the public IP address of the customer gateway. If you set RemoteId to a value in the FQDN format, we recommend that you set Negotiation Mode to **aggressive**.
Advanced Settings: IPsec Settings	
Encryption Algorithm	Select the encryption algorithm that is used in Phase 2 negotiations. Supported algorithms are **aes** (default), **aes192**, **aes256**, **des**, and **3des**.
Authentication Algorithm	Select the authentication algorithm that is used in Phase 2 negotiations. Valid values: **sha1** and **md5** (default).
DH Group	Select the DH key exchange algorithm that is used in Phase 2 negotiations. ○ **disabled**: does not use a DH key exchange algorithm. ■ For clients that do not support perfect forward secrecy (PFS), select **disabled**. ■ If you select a value other than **disabled**, the PFS feature is enabled by default, which requires a key update for every renegotiation. Therefore, you must also enable PFS for the client. ○ **group1**: DH group 1 ○ **group2**: DH group 2 (default) ○ **group5**: DH group 5 ○ **group14**: DH group 14
SA Life Cycle (Seconds)	Specify the SA lifecycle after Phase 2 negotiations succeed. Valid values: **0 to 86400**. Unit: seconds. Default value: **86400**.

7.1.2. Modify an IPsec-VPN connection

After you create an IPsec-VPN connection, you can modify its configurations.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > IPsec Connections**.
3. In the top navigation bar, select the region of the IPsec-VPN connection.
4. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to manage, and click **Edit** in the **Actions** column.
5. In the **Edit IPsec connection** dialog box, modify the name, advanced configurations, CIDR block, and then click **OK**.

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

7.1.3. Download the configuration of an IPsec-VPN connection

After you create an IPsec-VPN connection, you can download its configuration.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > IPsec Connections**.
3. In the top navigation bar, select the region of the IPsec-VPN connection.
4. On the **IPsec Connections** page, find the IPsec-VPN connection and click **Download peer configuration** in the **Actions** column.
5. In the **IPsec connection configuration** dialog box, copy and save the configuration.

> **Note** The values of RemoteSubnet and LocalSubnet in the configuration are opposite to the values that you specified when you create the IPsec-VPN connection. For a VPN gateway, RemoteSubnet refers to the CIDR block of the data center, whereas LocalSubnet refers to the CIDR block of the VPC. For a gateway device, LocalSubnet refers to the CIDR block of the data center, whereas RemoteSubnet refers to the CIDR block of the VPC.

7.1.4. Configure a security group

This topic describes how to configure a security group to control the inbound and outbound traffic of Elastic Compute Service (ECS) instances in the security group after an IPsec-VPN connection is created.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > IPsec Connections**.
3. In the top navigation bar, select the region of the IPsec-VPN connection.
4. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to manage and click **Configure routing security groups** in the **Operation** column.
5. In the **Configure routing security groups** dialog box, set the following parameters and click **OK**.

Parameter	Description
Security Group	Select the security group to which you want to add the security group rule.
Regular direction	Select the direction to which the security group rule applies. ○ **Out direction**: controls data transfer from the ECS instances in the security group to the Internet or other ECS instances. ○ **Inbound direction**: controls data transfer from the Internet or other ECS instances to the ECS instances in the security group.
Authorization policy	Specify the action to be performed on the requests that match the rule. ○ **Allow**: accepts requests. ○ **Deny**: denies requests without returning a response. If two security group rules use the same settings except for the action, the **Deny** action prevails over the **Allow** action.
Protocol type	Select a protocol for the security group rule.
Port range	Enter a port range for the security group rule. Valid values: -1 and 1 to 65535. You cannot enter only -1. Examples: ○ 1/200 specifies ports 1 to 200. ○ 80/80 specifies port 80. ○ -1/-1 specifies all ports.
Priority	Set the priority of the rule. Valid values: 1 to 100. The default value is 1, which indicates the highest priority.
Authorization Type	Specify the type of addresses that the security group rule allows or denies. Only **Address segment access** is supported.
NIC Type	Specify the type of data transfer that the security group rule controls. ○ **Internal**: controls data transfer within Apsara Stack. ○ **External**: controls data transfer over the Internet.
Authorization object	Specify the CIDR blocks that you want the security group rule to allow or deny. You can specify at most 10 CIDR blocks.
Automatic routing	Specify whether to automatically advertise routes. This feature is disabled by default.
Description	Enter a description for the security group rule. This parameter is optional. If you enter a description, the description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`.

7.1.5. Delete an IPsec-VPN connection

This topic describes how to delete an IPsec-VPN connection.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > IPsec Connections**.
3. In the top navigation bar, select the region of the IPsec-VPN connection.
4. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to delete, and click **Delete** in the **Operation** column.
5. In the **Delete IPsec connection** message, click **OK**.

7.2. MTU considerations

The maximum transmission unit (MTU) is the size of the largest packet that can be transmitted over a network layer protocol, such as TCP. Packets are measured in bytes. The MTU takes both the sizes of headers and data into account.

Segments transmitted over an IPsec tunnel are encrypted and then encapsulated into packets for routing purpose. The size of a segment must fit the MTU of the packet that carries the segment. Therefore, the MTU of the segment must be smaller than the MTU of the packet.

Gateway MTU

You must set the MTU of the local VPN gateway to a value no greater than 1,360 bytes. We recommend that you set the MTU to 1,360 bytes.

The TCP protocol negotiates the maximum segment length (MSS) of each packet segment between the sender and the receiver. We recommend that you set the TCP MSS of the on-premises VPN gateway to 1,359 bytes to facilitate the encapsulation and transfer of TCP packets.

8.Configure SSL-VPN

8.1. Manage an SSL server

8.1.1. Create an SSL server

This topic describes how to create an SSL server. Before you can create an SSL-VPN connection, you must create an SSL server.

Prerequisites

A VPN gateway is created and SSL-VPN is enabled for the VPN gateway. For more information, see Create a VPN gateway.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > SSL Servers**.
3. On the **SSL Servers** page, click **Create SSL Server**.
4. On the **Create SSL Server** page, set the following parameters and click **Submit**:

Parameter	Description
Organization	Select the organization to which the SSL server belongs.
Resource Set	Select the resource set to which the SSL server belongs.
Region	Select the region where you want to deploy the SSL server.
Zone	Select the zone where you want to deploy the SSL server.
Name	Enter a name for the SSL server. The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
VPN Gateway	Select the VPN gateway that you want to associate with the SSL server.
Local CIDR Block	Enter the CIDR block that the client needs to access through the SSL-VPN connection. It can be the CIDR block of a virtual private cloud (VPC), a vSwitch, a data center connected to a VPC through an Express Connect circuit, or a cloud service such as ApsaraDB RDS or Object Storage Service (OSS). You can enter multiple local CIDR blocks. Separate local CIDR blocks with commas (,). **Note** The subnet mask of the specified CIDR block must be 16 to 29 bits in length.

Parameter	Description
Client CIDR Block	Enter the CIDR block from which an IP address is allocated to the virtual network interface controller (NIC) of the client. Do not enter the private CIDR block of the client. When the client accesses the destination network through an SSL-VPN connection, the VPN gateway allocates an IP address from the client CIDR block to the client. **Note** Make sure that the local CIDR block and the client CIDR block do not overlap with each other.
Advanced Settings	Select the type of advanced settings. ○ **Default**: Use the default settings. ○ **Configure**: Use custom settings. You can set the following parameters: ■ **Protocol**: Select a protocol for the SSL-VPN connection. Valid values: **UDP** (default) and **TCP**. ■ **Port**: Specify the port used by the SSL-VPN connection. Default value: **1194**. You cannot use the following port numbers: 22, 2222, 22222, 9000, 9001, 9002, 7505, 80, 443, 53, 68, 123, 4510, 4560, 500, and 4500. ■ **Encryption Algorithm**: Select the encryption algorithm used by the SSL-VPN connection. Valid values: **AES-128-CBC** (default), **AES-192-CBC**, **AES-256-CBC**, and **none**. ■ **Compressed**: Specify whether to compress the data that is transmitted over the SSL-VPN connection. Default value: **No**.

8.1.2. Modify an SSL server

After you create an SSL server, you can modify its configurations.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > SSL Servers**.
3. In the top navigation bar, select the region of the SSL server.
4. On the **SSL Servers** page, find the SSL server that you want to manage and click **Edit** in the **Operation** column.
5. In the **Edit SSL Server** dialog box, modify the name, server CIDR block, client CIDR block, and advanced settings of the SSL server, and then click **OK**.

   For more information about the parameters, see Create an SSL server.

8.1.3. Configure a security group

This topic describes how to configure a security group to control the inbound and outbound traffic of Elastic Compute Service (ECS) instances in the security group after an IPsec-VPN connection is created.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > SSL Servers**.
3. In the top navigation bar, select the region of the SSL server.
4. On the **SSL Servers** page, find the SSL server that you want to manage and click **Configure routing security groups** in the **Operation** column.
5. In the **Configure routing security groups** dialog box, set the following parameters and click **OK**.

Parameter	Description
Security Group	Select the security group to which you want to add the security group rule.
Regular direction	Select the direction to which the security group rule applies. ○ **Out direction**: controls data transfer from the ECS instances in the security group to the Internet or other ECS instances. ○ **Inbound direction**: controls data transfer from the Internet or other ECS instances to the ECS instances in the security group.
Authorization policy	Specify the action to be performed on the requests that match the rule. ○ **Allow**: accepts requests. ○ **Deny**: denies requests without returning a response. If two security group rules use the same settings except for the action, the **Deny** action prevails over the **Allow** action.
Protocol type	Select a protocol for the security group rule.
Port range	Enter a port range for the security group rule. Valid values: -1 and 1 to 65535. You cannot enter only -1. Examples: ○ 1/200 specifies ports 1 to 200. ○ 80/80 specifies port 80. ○ -1/-1 specifies all ports.
Priority	Set the priority of the rule. Valid values: 1 to 100. The default value is 1, which indicates the highest priority.
Authorization Type	Specify the type of addresses that the security group rule allows or denies. Only **Address segment access** is supported.
NIC Type	Specify the type of data transfer that the security group rule controls. ○ **Internal**: controls data transfer within Apsara Stack. ○ **External**: controls data transfer over the Internet.

Parameter	Description
Authorization Object	Specify the CIDR blocks that you want the security group rule to allow or deny. You can specify at most 10 CIDR blocks.
Description	Enter a description for the security group rule. The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`. You can leave this parameter empty.

8.1.4. Delete an SSL server

This topic describes how to delete an SSL server. After you delete an SSL server, the system also deletes the SSL clients associated with the SSL server.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > SSL Servers**.
3. In the top navigation bar, select the region of the SSL server.
4. On the **SSL Servers** page, find the SSL server that you want to delete and click **Delete** in the **Operation** column.
5. In the **SSL Servers** dialog box, click **OK**.

8.2. Manage an SSL client certificate

8.2.1. 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.

Prerequisites

An SSL server is created. For more information, see Create an SSL server.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > SSL Clients** .
3. In the top navigation bar, select the region of the SSL client.
4. On the **SSL Clients** page, click **Create SSL Client**.
5. On the **Create SSL Client Certificate** page, set the following parameters and click **Submit**.

Parameter	Description
Organization	Select the organization to which the SSL client belongs.

Parameter	Description
Resource Set	Select the resource set to which the SSL client belongs.
Region	Select the region to which the SSL client belongs.
Zone	Select the zone to which the SSL client belongs.
Name	Enter a name for the SSL client certificate. The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
VPN Gateway	Select the VPN gateway that you want to associate with the SSL client certificate.
SSL Server	Select the SSL server that you want to associate with the SSL client certificate.

8.2.2. Download an SSL client certificate

This topic describes how to download an SSL client certificate. You can download an SSL client certificate in the VPN Gateway console.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > SSL Clients** .
3. In the top navigation bar, select the region of the SSL client.
4. On the **SSL Clients** page, find the SSL client certificate that you want to download and click **Download** in the **Operation** column.

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

8.2.3. Delete an SSL client certificate

This topic describes how to delete an SSL client certificate.

Procedure

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **VPN > SSL Clients** .
3. In the top navigation bar, select the region of the SSL client.
4. On the **SSL Clients** page, find the SSL client certificate that you want to delete, and click **Delete** in the **Operation** column.
5. In the **Delete Client Certificate** message, click **OK**.