

ALIBABA CLOUD

# 阿里云

## 专有云企业版

VPN网关  
用户指南

产品版本：v3.16.2

文档版本：20220915

 阿里云

## 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

# 目录


1.什么是VPN网关	06
2.登录VPN网关管理控制台	08
3.IPsec-VPN入门	09
3.1. IPsec-VPN入门概述	09
3.2. 建立VPC到本地数据中心的连接	10
4.SSL-VPN入门	14
4.1. SSL-VPN入门概述	14
4.2. 客户端远程连接VPC	14
5.管理VPN网关	19
5.1. 创建VPN网关	19
5.2. 修改VPN网关	20
5.3. 配置VPN网关路由	20
5.3.1. 网关路由概述	20
5.3.2. 使用策略路由	20
5.3.3. 使用目的路由	22
5.4. 删除VPN网关	24
6.管理用户网关	25
6.1. 创建用户网关	25
6.2. 修改用户网关	25
6.3. 删除用户网关	26
7.配置IPsec-VPN	27
7.1. 管理IPsec连接	27
7.1.1. 创建IPsec连接	27
7.1.2. 修改IPsec连接	29
7.1.3. 下载IPsec连接配置	29
7.1.4. 配置路由安全组	30

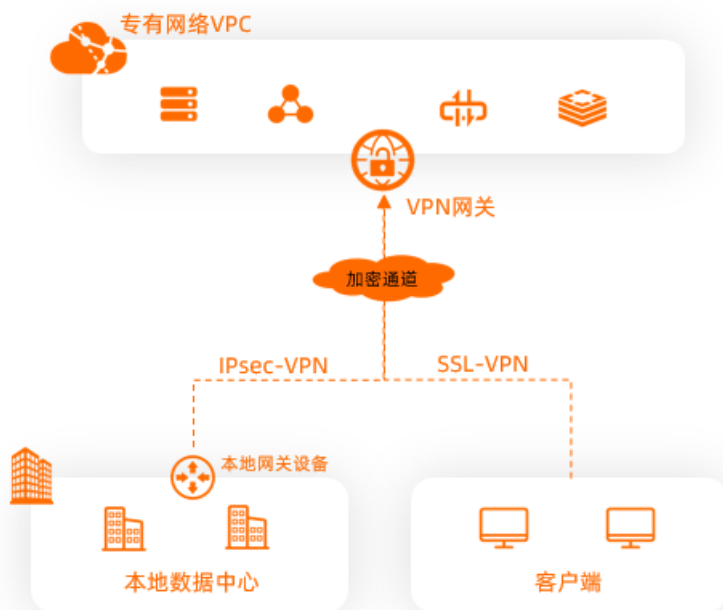
---

7.1.5. 删除IPsec连接	31
7.2. MTU注意事项	31
8.配置SSL-VPN	32
8.1. 管理SSL服务端	32
8.1.1. 创建SSL服务端	32
8.1.2. 修改SSL服务端	33
8.1.3. 配置路由安全组	33
8.1.4. 删除SSL服务端	34
8.2. 管理SSL客户端	35
8.2.1. 创建SSL客户端证书	35
8.2.2. 下载SSL客户端证书	35
8.2.3. 删除SSL客户端证书	36

# 1.什么是VPN网关

VPN网关是一款基于互联网的网络连接服务，通过建立加密通道的方式实现企业本地数据中心、企业办公网络或互联网终端与阿里云专有网络VPC（Virtual Private Cloud）之间安全可靠的私网互联。

 **说明** 阿里云VPN网关在国家相关政策法规内提供服务，不提供访问互联网的功能。



## 功能特性

VPN网关提供IPsec-VPN和SSL-VPN两种连接方式：

- IPsec-VPN

IPsec-VPN是一种基于路由的网络连接技术，不仅可以让您更方便地配置和维护VPN策略，而且还为您提供了灵活的流量路由方式。

您可以使用IPsec-VPN建立本地数据中心与VPC之间或不同的VPC之间的连接。IPsec-VPN支持IKEv1和IKEv2协议，只要支持这两种协议的本地网关设备均可以和阿里云VPN网关互连。

- SSL-VPN

SSL-VPN是一种基于OpenVPN架构的网络连接技术。部署完成后，您仅需要在客户端中加载证书并发起连接，便可通过SSL-VPN功能从客户端远程访问VPC中部署的应用和服务。

## 产品优势

- 安全

使用IKE和IPsec协议对传输数据进行加密，保证数据安全可信。

- 稳定

底层采用双机热备架构，故障时秒级切换，保证会话不中断，业务不受影响。

- 简单

功能开通即用，配置实时生效，实现快速部署。

- **低成本**

基于互联网建立加密通道，相比使用专线成本更低。

## 2. 登录VPN网关管理控制台

本文主要向您介绍如何登录Apsara Uni-manager运营控制台。


### 前提条件

- 登录Apsara Uni-manager运营控制台前，确认您已从部署人员处获取Apsara Uni-manager运营控制台的服务域名地址。
- 推荐使用Chrome浏览器。

### 操作步骤

1. 在浏览器地址栏中，输入Apsara Uni-manager运营控制台的服务域名地址，按回车键。
2. 输入正确的用户名及密码。


请向运营管理员获取登录控制台的用户名和密码。

 **说明** 首次登录Apsara Uni-manager运营控制台时，需要修改登录用户名的密码，请按照提示完成密码修改。为提高安全性，密码长度必须为10~32位，且至少包含以下两种类型：

- 英文大写或小写字母（A~Z、a~z）
- 阿拉伯数字（0~9）
- 特殊符号（感叹号（!）、at（@）、井号（#）、美元符号（\$）、百分号（%）等）

3. 单击**账号登录**。
4. 如果账号已激活MFA多因素认证，请根据以下两种情况进行操作：
  - 管理员强制开启MFA后的首次登录：
    - a. 在绑定虚拟MFA设备页面中，按页面提示步骤绑定MFA设备。
    - b. 按照步骤2重新输入账号和密码，单击**账号登录**。
    - c. 输入6位MFA码后单击**认证**。
  - 您已开启并绑定MFA：

输入6位MFA码后单击**认证**。

 **说明** 绑定并开启MFA的操作请参见Apsara Uni-manager运营控制台用户指南中的**绑定并开启虚拟MFA设备**章节。

5. 在页面顶部的菜单栏中，选择**产品 > 网络 > 专有网络 VPC**。



## 3.IPsec-VPN入门

### 3.1. IPsec-VPN入门概述

通过IPsec-VPN可建立专有网络VPC（Virtual Private Cloud）与本地数据中心间的VPN连接。本文为您介绍IPsec-VPN的使用流程。

#### 环境要求

使用IPsec-VPN功能建立VPC与本地数据中心的VPN连接前，请确保您的环境满足以下条件：

- 本地数据中心的网关设备必须支持IKEv1和IKEv2协议。  
IPsec-VPN支持IKEv1和IKEv2协议，只要支持这两种协议的设备均可以和阿里云VPN网关互连。
- 本地数据中心的网关设备必须配置静态公网IP地址。
- 本地数据中心和VPC间互通的网段没有重叠。
- 您已了解VPC中所应用的安全组规则，并确保安全组规则允许本地数据中心的网关设备访问云上资源。

#### 使用流程



##### 1. 创建VPN网关

VPN网关开启IPsec-VPN功能，一个VPN网关可以建立多条IPsec连接。

##### 2. 创建用户网关

通过创建用户网关，您可以将本地数据中心网关设备的信息注册到阿里云上。

##### 3. 创建IPsec连接

IPsec连接是指VPN网关和本地数据中心网关设备建立连接后的VPN通道。只有建立IPsec连接后，本地数据中心才能使用VPN网关进行加密通信。

##### 4. 配置本地网关

您需要在本地数据中心的网关设备中加载阿里云上VPN网关的配置。

##### 5. 配置VPN网关路由

您需要在VPN网关中配置路由，并发布路由到VPC路由表以实现本地数据中心和VPC的通信。更多信息，请参见[网关路由概述](#)。

##### 6. 测试连通性

登录到阿里云VPC内一台无公网IP的ECS实例，通过ping命令，ping本地数据中心内一台服务器的私网IP地址，验证通信是否正常。

#### 入门场景

[建立VPC到本地数据中心的连接](#)

## 3.2. 建立VPC到本地数据中心的连接

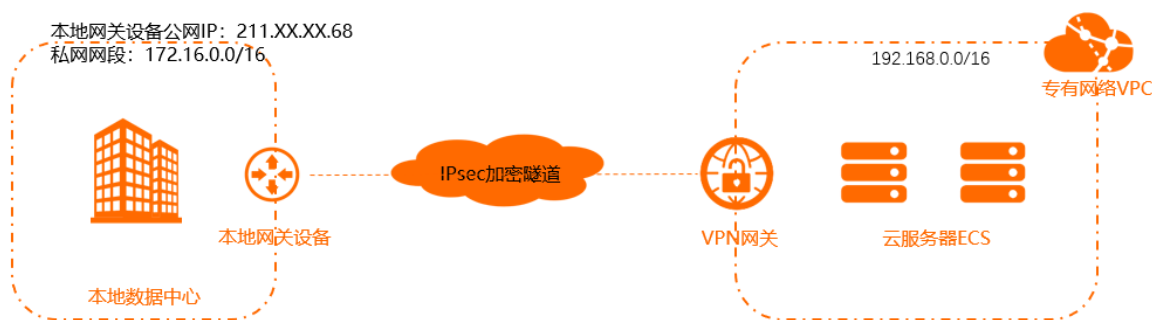
本文介绍如何使用IPsec-VPN建立专有网络VPC（Virtual Private Cloud）到本地数据中心的VPN连接，实现本地数据中心与VPC的互通。

### 前提条件

- 确保本地数据中心的网关设备支持IKEv1和IKEv2协议，只要支持这两种协议的本地网关设备均可以和云上VPN网关互连。
- 本地数据中心的网关设备已经配置了静态公网IP。
- 本地数据中心和VPC互通的网段没有重叠。
- 您已经了解VPC中的ECS实例所应用的安全组规则，并确保安全组规则允许本地数据中心的网关设备访问云上资源。

### 背景信息

本文以下图场景为例。某公司在阿里云创建了VPC，网段为192.168.0.0/16。本地数据中心的网段为172.16.0.0/16，本地网关设备的公网IP为211.XX.XX.68。公司因业务发展，需要本地数据中心与云上VPC互通。您可以通过IPsec-VPN，建立本地数据中心与云上VPC的连接，实现云上和云下的互通。



### 步骤一：创建VPN网关

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > VPN网关。
3. 在VPN网关页面，单击创建VPN网关。
4. 在创建VPN页面，根据以下信息配置VPN网关，然后单击提交。
  - 组织：选择VPN网关所属的组织。
  - 资源集：选择VPN网关所属的资源集。
  - 地域：选择VPN网关的地域。

说明 确保VPC的地域和VPN网关的地域相同。

- 可用区：选择VPN网关所属的可用区。
- 实例名称：输入VPN网关的实例名称。  
长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（\_）和短划线（-）。
- VPC：选择VPN网关要连接的VPC。
- VSwitch：选择VPN网关所关联的交换机。


- **带宽规格**：选择VPN网关的带宽规格。单位为Mbps。带宽规格是VPN网关所具备的公网带宽。
- **IPsec-VPN**：选择是否开启IPsec-VPN功能。本示例选择开启。  
您可以通过创建IPsec隧道，建立本地数据中心到VPC、VPC到VPC的安全连接。
- **SSL-VPN**：选择是否开启SSL-VPN功能。本示例选择关闭。  
提供点到站点的VPN连接，不需要配置客户网关，终端直接接入。

5. 返回VPN网关页面，查看创建的VPN网关。

刚创建好的VPN网关的状态是**准备中**，约1~5分钟左右会变成**正常状态**。**正常状态**表明VPN网关已经完成了初始化，可以正常使用。


## 步骤二：创建用户网关

1. 在左侧导航栏，选择**VPN > 用户网关**。
2. 在顶部菜单栏，选择用户网关的地域。

 **说明** 用户网关的地域必须和要连接的VPN网关的地域相同。

3. 在**用户网关**页面，单击**创建用户网关**。
4. 在**创建用户网关**页面，根据以下信息配置用户网关，然后单击**提交**。

- **组织**：选择用户网关所属的组织。
- **资源集**：选择用户网关所属的资源集。
- **地域**：选择用户网关所属的地域。

 **说明** 用户网关的地域必须和要连接的VPN网关的地域相同。

- **可用区**：选择用户网关所属的可用区。
- **名称**：输入用户网关的名称。  
长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（\_）和短划线（-）。
- **IP地址**：输入VPC要连接的本地数据中心网关设备的公网IP地址。本示例输入211.XX.XX.68。
- **描述**：输入用户网关的描述信息。  
长度为2~100个字符，以大小写字母或中文开始，可包含数字、短划线（-）、下划线（\_）、全角句号（。）、全角逗号（，）和全角冒号（：）。

## 步骤三：创建IPsec连接

1. 在左侧导航栏，选择**VPN > IPsec连接**。
2. 在顶部菜单栏，选择IPsec连接实例的地域。

 **说明** IPsec连接实例的地域必须和要连接的VPN网关的地域相同。

3. 在**IPsec连接**页面，单击**创建IPsec连接**。
4. 在**创建IPsec连接**页面，根据以下信息配置IPsec连接，然后单击**提交**。
  - **组织**：选择IPsec连接所属的组织。
  - **资源集**：选择IPsec连接所属的资源集。

- **地域**：选择IPsec连接所属的地域。
- **可用区**：选择IPsec连接所属的可用区。
- **名称**：输入IPsec连接的名称。
- **VPN网关**：选择已创建的VPN网关。
- **用户网关**：选择要连接的用户网关。
- **本端网段**：输入已选VPN网关所属VPC的网段。本示例输入192.168.0.0/16。
- **对端网段**：输入本地数据中心的网段。本示例输入172.16.0.0/16。
- **立即生效**：选择是否立即生效。
  - **是**：配置完成后立即进行协商。
  - **否**：当有流量进入时进行协商。
- **高级配置**：选择**默认**高级配置。

默认配置下，自动生成预共享密钥。

## 步骤四：在本地网关设备中加载VPN配置

1. 在左侧导航栏，选择**VPN > IPsec连接**。
2. 在IPsec连接页面，找到目标IPsec连接实例，在操作列单击**下载对端配置**。
3. 在IPsec连接配置对话框，复制并保存配置信息至您本地。
4. 根据本地网关设备的配置要求，将下载的配置添加到本地网关设备中。详细配置，请咨询本地网关设备的厂家。

## 步骤五：配置VPN网关路由

1. 在左侧导航栏，选择**VPN > VPN网关**。
2. 在VPN网关页面，找到目标VPN网关实例，单击实例ID。
3. 在目的路由表页签，单击**添加路由条目**。
4. 在添加路由条目对话框，根据以下信息配置目的路由，然后单击**确定**。
  - **目标网段**：输入本地数据中心的私网网段。本示例输入172.16.0.0/16。
  - **下一跳类型**：选择**IPsec连接**。
  - **下一跳**：选择IPsec连接实例。
  - **发布到VPC**：选择是否将新添加的路由发布到VPC路由表。本示例选择**是**。
  - **权重**：选择路由的权重值。本示例选择**100**。
    - **100**：高优先级。
    - **0**：低优先级。

 **说明** 相同目标网段的目的路由，不支持同时设置权重值为100。

## 步骤六：测试连通性

1. 登录到VPC内一台无公网IP的ECS实例。
2. 通过**ping**命令，访问本地数据中心内的一台服务器，验证通信是否正常。

```
[root@iZm5e...slbZ ~]# ping 172.16.1.188
PING 172.16.1.188 (172.16.1.188) 56(84) bytes of data.
64 bytes from 172.16.1.188: icmp_seq=1 ttl=62 time=23.8 ms
64 bytes from 172.16.1.188: icmp_seq=2 ttl=62 time=23.7 ms
64 bytes from 172.16.1.188: icmp_seq=3 ttl=62 time=23.7 ms
64 bytes from 172.16.1.188: icmp_seq=4 ttl=62 time=23.7 ms
^Z
[1]+  Stopped                  ping 172.16.1.188
[root@iZm5ea8...xslbZ ~]#
```

## 4.SSL-VPN入门

### 4.1. SSL-VPN入门概述

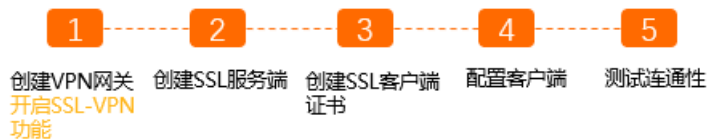
通过SSL-VPN可使客户端远程接入专有网络VPC（Virtual Private Cloud），安全地访问VPC中部署的应用和服务。本文为您介绍SSL-VPN的使用流程。

#### 环境要求

使用SSL-VPN功能建立客户端与VPC的连接前，请确保满足以下条件：

- 客户端的私网网段和VPC的私网网段没有重叠，否则无法通信。
- 客户端可以访问互联网。
- 您已了解VPC中所应用的安全组规则，并确保安全组规则允许客户端访问云上资源。

#### 使用流程



##### 1. 创建VPN网关。

创建VPN网关并开启SSL-VPN功能。

##### 2. 创建SSL服务端。

在SSL服务端中指定客户端要访问的私网网段和客户端访问时使用的网段。

##### 3. 创建SSL客户端证书。

根据SSL服务端配置，创建并下载客户端证书。

##### 4. 配置客户端。

在客户端中下载安装VPN软件、加载客户端证书，然后发起VPN连接。

##### 5. 测试连通性。

打开客户端的命令行窗口，通过ping命令，访问VPC内一台ECS实例，验证通信是否正常。

#### 入门场景

客户端远程连接VPC

### 4.2. 客户端远程连接VPC

本文为您介绍客户端如何通过SSL-VPN连接专有网络VPC（Virtual Private Cloud）。

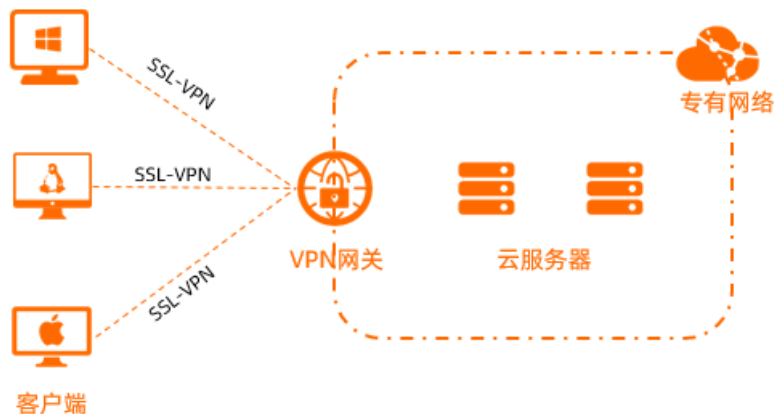
#### 前提条件

- 客户端的私网网段和VPC的私网网段没有重叠，否则无法通信。
- 您的客户端可以访问互联网。

- 您已经了解VPC中的ECS实例所应用的安全组规则，并确保安全组规则允许本地数据中心的网关设备访问云上资源。

## 背景信息

本文以下图场景为例，为您介绍Linux、Windows和Mac客户端如何通过SSL-VPN连接到VPC。



## 步骤一：创建VPN网关

- 登录VPN网关管理控制台。
- 在左侧导航栏，选择VPN > VPN网关。
- 在VPN网关页面，单击创建VPN网关。
- 在创建VPN页面，根据以下信息配置VPN网关，然后单击提交。
  - 组织：选择VPN网关所属的组织。
  - 资源集：选择VPN网关所属的资源集。
  - 地域：选择VPN网关的地域。

说明 确保VPC的地域和VPN网关的地域相同。

- 可用区：选择VPN网关所属的可用区。
  - 实例名称：输入VPN网关的实例名称。  
长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（\_）和短划线（-）。
  - VPC：选择VPN网关要连接的VPC。
  - VSwitch：选择VPN网关所关联的交换机。
  - 带宽规格：选择VPN网关的带宽规格。带宽规格是VPN网关所具备的公网带宽。
  - IPsec-VPN：选择是否开启IPsec-VPN功能。本示例选择关闭。
  - SSL-VPN：选择是否开启SSL-VPN功能。本示例选择开启。  
SSL-VPN提供点到站点的VPN连接，不需要配置客户网关，终端直接接入。
  - SSL连接数：选择您需要同时连接的客户端最大数量。
- 返回VPN网关页面，查看创建的VPN网关。

刚创建好的VPN网关的状态是**准备中**，约1~5分钟左右会变成**正常**状态。**正常**状态就表明VPN网关完成了初始化，可以正常使用了。

## 步骤二：创建SSL服务端

1. 在左侧导航栏，选择**VPN > SSL服务端**。
2. 在顶部菜单栏，选择SSL服务端的地域。

 **说明** 请确保SSL服务端的地域和已创建的VPN网关的地域相同。

3. 在**SSL服务端**页面，单击**创建SSL服务端**。
4. 在**创建SSL服务端**页面，根据以下信息配置SSL服务端，然后单击**提交**。
  - **组织**：选择SSL服务端所属的组织。
  - **资源集**：选择SSL服务端所属的资源集。
  - **地域**：选择SSL服务端的地域。
  - **可用区**：选择SSL服务端所属的可用区。
  - **名称**：输入SSL服务端的名称。
  - **VPN网关**：选择已创建的VPN网关。
  - **本端网段**：以CIDR地址块的形式输入要连接的网络。支持输入多个本端网段，本端网段之间使用半角逗号（,）分隔。本端网段可以是任何VPC或交换机的网段，也可以是本地网络的网段。
  - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。例如：192.168.10.0/24。
  - **高级配置**：使用**默认**高级配置。

## 步骤三：创建并下载SSL客户端证书

1. 在左侧导航栏，选择**VPN > SSL客户端**。
2. 在**SSL客户端**页面，单击**创建SSL客户端**。
3. 在**创建SSL客户端证书**页面，根据以下信息创建SSL客户端证书，然后单击**提交**。
  - **组织**：选择SSL客户端证书所属的组织。
  - **资源集**：选择SSL客户端证书所属的资源集。
  - **地域**：选择SSL客户端证书的地域。
  - **可用区**：选择SSL客户端证书的可用区。
  - **名称**：输入SSL客户端证书的名称。
  - **VPN网关**：选择SSL客户端证书关联的VPN网关。
  - **SSL服务端**：选择SSL客户端证书关联的SSL服务端。
4. 在**SSL客户端**页面，找到已创建的客户端证书，然后在**操作列**单击**下载**。

SSL客户端证书会下载到您本地。

## 步骤四：配置客户端

以下内容为您介绍如何配置Linux、Mac和Windows客户端。

- Linux客户端
  - i. 执行以下命令安装OpenVPN客户端。



```
yum install -y openvpn
```

- ii. 将已下载的证书解压拷贝到 `/etc/openvpn/conf/` 目录。
- iii. 进入到 `/etc/openvpn/conf/` 目录下，执行以下命令启动OpenVPN客户端软件。

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

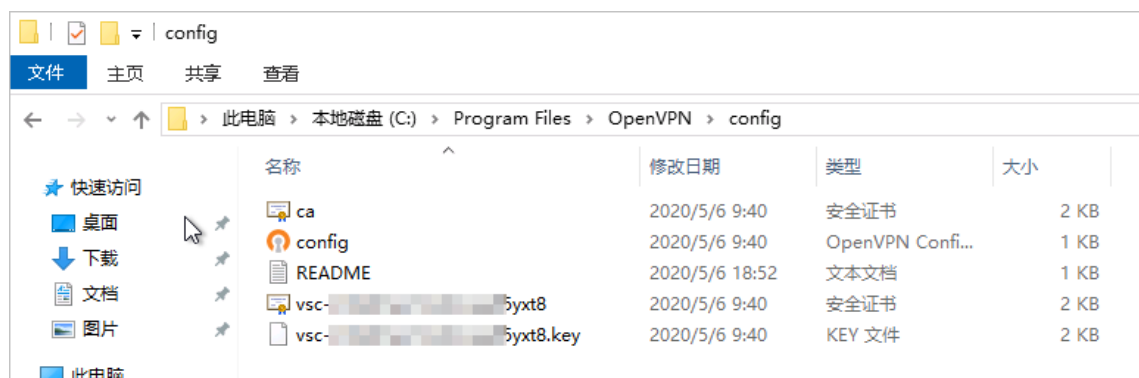
- Windows客户端

- i. 下载并安装OpenVPN客户端。

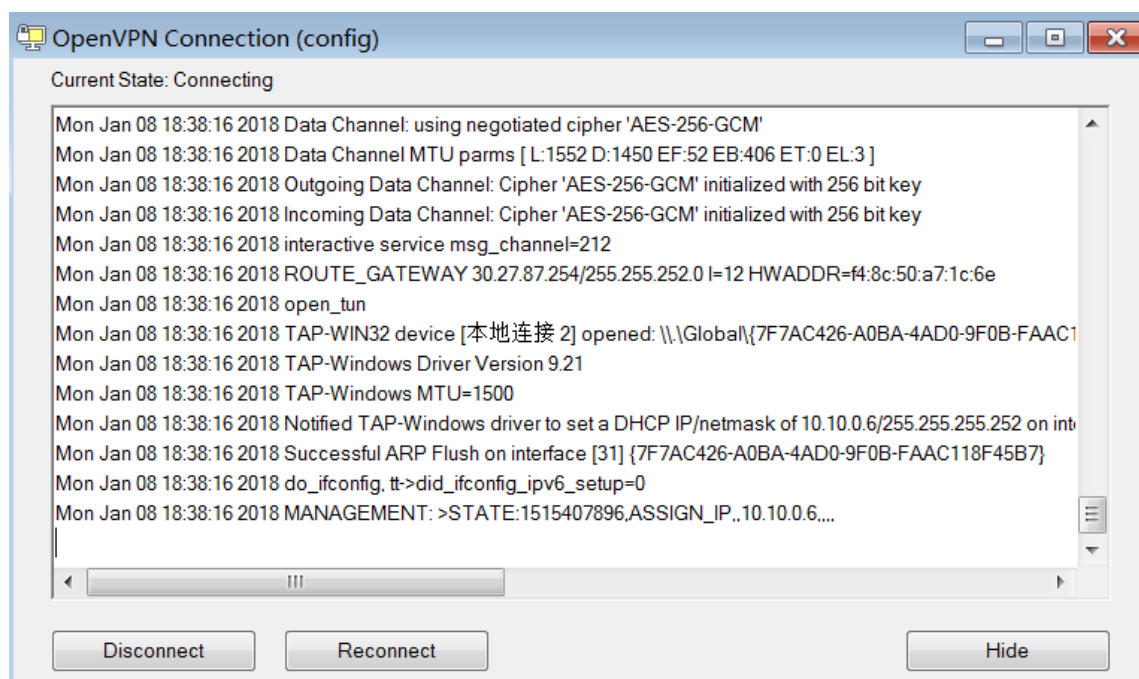
下载[OpenVPN](#)。

- ii. 将已经下载的SSL客户端证书解压拷贝到 `OpenVPN\config` 目录。

本示例将证书解压拷贝到 `C:\Program Files\OpenVPN\config` 目录，请您根据安装路径将证书解压拷贝到实际的目录。



- iii. 启动Openvpn客户端软件，单击Connect发起连接。



- Mac客户端

- i. 执行以下命令安装OpenVPN客户端。

```
brew install openvpn
```

❓ 说明 如果尚未安装homebrew，先安装homebrew。

ii. 将步骤三中下载的证书解压拷贝到配置目录并建立连接：

a. 备份 `/usr/local/etc/openvpn` 文件夹下的所有配置文件。

b. 执行以下命令删除OpenVPN的配置文件：

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

c. 执行以下命令将已经下载的SSL客户端证书拷贝到配置目录：

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

`cert_location` 是步骤三中下载的SSL客户端证书的路径。例如：`/Users/example/Downloads/certs6.zip`。

d. 执行以下命令解压证书：

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

e. 执行以下命令发起连接：

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

## 步骤五：测试连通性

1. 打开客户端命令行窗口。
2. 执行ping命令，访问VPC内的任意一台ECS实例，测试网络连通性。

# 5.管理VPN网关

## 5.1. 创建VPN网关

在使用IPsec-VPN和SSL-VPN功能前，您必须创建一个VPN网关。成功创建VPN网关后，系统会为VPN网关分配一个公网IP地址。

### 操作步骤



1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > VPN网关。
3. 在VPN网关页面，单击创建VPN网关。
4. 在创建VPN页面，根据以下信息配置进行配置，然后单击提交。

配置	说明
组织	选择VPN网关所属的组织。
资源集	选择VPN网关所属的资源集。
地域	选择VPN网关所属的地域。 如果使用VPN网关的IPsec-VPN功能建立VPC到本地数据中心或VPC到VPC的VPN连接，必须确保VPN网关的地域和VPC的地域相同。
可用区	选择VPN网关所属的可用区。
实例名称	输入VPN网关的实例名称。 长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。
VPC	选择VPN网关所关联的VPC。
VSwitch	选择VPN网关所关联的交换机。
带宽规格	选择VPN网关的带宽规格。单位：Mbps。 带宽规格是指VPN网关所具备的公网带宽。
IPsec-VPN	选择是否开启IPsec-VPN功能。默认值：开启。 您可以通过创建IPsec隧道，建立本地数据中心到VPC、VPC到VPC的安全连接。
SSL-VPN	选择是否开启SSL-VPN功能。默认值：关闭。 提供点到站点的VPN连接，不需要配置客户网关，终端直接接入。
SSL连接数	选择您需要同时连接的客户端的数量。 <div> 说明 本选项只有在选择开启了SSL-VPN功能后才可配置。</div>

## 5.2. 修改VPN网关

创建VPN网关实例后，您可以修改VPN网关实例的名称和描述信息。

### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择VPN > VPN网关。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在VPN网关页面，找到目标VPN网关实例，在实例ID下面找到并单击图标，在弹出的对话框中修改实例的名称，然后单击**确定**。  
名称长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（\_）和短划线（-）。
5. 在描述列找到并单击图标，在弹出的对话框中修改实例的描述信息，然后单击**确定**。

描述信息长度为2~100个字符，不能以 `http://` 和 `https://` 开始。

## 5.3. 配置VPN网关路由

### 5.3.1. 网关路由概述

创建IPsec连接后，您需要手动添加VPN网关路由。

基于路由的IPsec-VPN，不仅可以更方便地配置和维护VPN策略，而且还提供了灵活的流量路由方式。

您可以为VPN网关添加如下两种路由：

- 策略路由。
- 目的路由。

#### 策略路由

策略路由基于源IP和目的IP进行更精确的路由转发。

添加策略路由的详细信息，请参见[使用策略路由](#)。

 **说明** 策略路由比目的路由的优先级高。

#### 目的路由

目的路由仅基于目的IP进行路由转发。

添加目的路由的详细信息，请参见[使用目的路由](#)。

### 5.3.2. 使用策略路由

策略路由会基于流量的源IP和目的IP进行更精确的路由转发。本文为您介绍如何添加、发布、修改以及删除策略路由。

#### 前提条件

您已经创建了IPsec连接。具体操作，请参见[创建IPsec连接](#)。

## 添加策略路由

创建IPsec连接后，您可以为IPsec连接添加策略路由。

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 单击**策略路由**表页签，然后单击**添加路由条目**。
6. 在**添加路由条目**对话框，根据以下信息配置进行配置，然后单击**确定**。

配置	说明
目标网段	输入要访问的私网网段。
源网段	输入VPC侧的私网网段。
下一跳类型	选择IPsec连接。
下一跳	选择需要建立VPN连接的IPsec连接实例。
发布到VPC	<p>选择是否将新添加的路由发布到VPC路由表。</p> <ul style="list-style-type: none"> <li>是（默认值）：将新添加的路由发布到VPC路由表。</li> <li>否：不发布新添加的路由到VPC路由表。</li> </ul> <p> <b>说明</b> 如果您选择否，添加策略路由后，您还需在策略路由表中发布路由。</p>
权重	<p>选择权重值：</p> <ul style="list-style-type: none"> <li>100（默认值）：高优先级。</li> <li>0：低优先级。</li> </ul> <p> <b>说明</b> 如果策略路由表中存在多条源网段、目标网段、权重值均相同的路由条目，则系统将随机选择一条路由条目转发流量。</p>

## 发布策略路由

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 单击**策略路由**表页签，找到目标路由条目，在**操作**列单击**发布**。
6. 在**发布路由**对话框，单击**确定**。

目标路由发布后，您可以单击**撤销发布**，撤销已经发布的路由。

## 编辑策略路由

在您创建策略路由后，您可以修改策略路由的权重值。

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 单击**策略路由**表页签，找到目标路由条目，在操作列单击**编辑**。
6. 在**编辑路由条目**对话框，修改策略路由的权重值，然后单击**确定**。

## 删除策略路由

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 单击**策略路由**表页签，找到目标路由条目，在操作列单击**删除**。
6. 在**删除路由条目**对话框，单击**确定**。

## 5.3.3. 使用目的路由

目的路由基于流量的目的IP进行路由转发。本文为您介绍如何添加、发布、修改以及删除目的路由。

### 前提条件


您已经创建了IPsec连接。具体操作，请参见[创建IPsec连接](#)。

### 添加目的路由

创建IPsec连接后，您可以为IPsec连接添加目的路由。

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 在**目的路由**表页签，单击**添加路由条目**。
6. 在**添加路由条目**对话框，根据以下信息进行配置，然后单击**确定**。

配置	说明
目标网段	输入要访问的私网网段。
下一跳类型	选择IPsec连接。
下一跳	选择需要建立VPN连接的IPsec连接实例。

配置	说明
发布到VPC	<p>选择是否将新添加的路由发布到VPC路由表。</p> <ul style="list-style-type: none"> <li>是（默认值）：将新添加的路由发布到VPC路由表。</li> <li>否：不发布新添加的路由到VPC路由表。</li> </ul> <p> <b>说明</b> 如果您选择否，添加目的路由后，您还需在目的路由表中发布路由。</p>
权重	<p>选择权重值：</p> <ul style="list-style-type: none"> <li>100：优先级高。</li> <li>0：优先级低。</li> </ul> <p> <b>说明</b> 如果目的路由表中存在多条目标网段、权重值均相同的路由条目，则系统将随机选择一条路由条目转发流量。</p>

## 发布目的路由

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 在目的路由表页签，找到目标路由条目，在操作列单击**发布**。
6. 在发布路由对话框，单击**确定**。

目标路由发布后，您可以单击**撤销发布**，撤销已经发布的路由。

## 编辑目的路由

在您创建目的路由后，您可以修改目的路由的权重值。

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 在目的路由表页签，找到目标路由条目，在操作列单击**编辑**。
6. 在编辑路由条目对话框，修改目的路由的权重值，然后单击**确定**。

## 删除目的路由

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > VPN网关**。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在**VPN网关**页面，单击目标VPN网关实例ID。
5. 在目的路由表页签，找到目标路由条目，在操作列单击**删除**。

6. 在删除路由条目对话框，单击确定。

## 5.4. 删除VPN网关

您可以删除一个不需要的VPN网关实例。删除后，该VPN网关实例将不再提供IPsec-VPN和SSL-VPN连接服务。

### 前提条件

删除VPN网关实例前，请确保满足以下条件：

- 已经删除了VPN网关实例关联的IPsec连接。具体操作，请参见[删除IPsec连接](#)。
- 已经删除了VPN网关实例关联的SSL服务端。具体操作，请参见[删除SSL服务端](#)。

### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择VPN > VPN网关。
3. 在顶部菜单栏，选择VPN网关实例的地域。
4. 在VPN网关页面，找到目标VPN网关实例，在操作列单击删除。
5. 在删除VPN网关对话框，单击确定。



# 6.管理用户网关

## 6.1. 创建用户网关

当使用IPsec-VPN在本地数据中心与VPC或不同的VPC之间建立连接时，需要创建用户网关。通过创建用户网关，您可以将本地网关的信息注册到云上，然后将用户网关和VPN网关连接起来。一个用户网关可以连接多个VPN网关。

### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择VPN > 用户网关。
3. 在用户网关页面，单击创建用户网关。
4. 在创建用户网关页面，根据以下信息配置用户网关，然后单击提交。


配置	说明
组织	选择用户网关所属的组织。
资源集	选择用户网关所属的资源集。
地域	选择用户网关所属的地域。 <div>② 说明 用户网关的地域必须和要连接的VPN网关的地域相同。</div>
可用区	选择用户网关所属的可用区。
名称	输入用户网关的名称。 长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。
IP地址	本地数据中心网关设备的静态公网IP地址。
描述	输入用户网关的描述。 长度为2~100个字符，以大小写字母或中文开始，可包含数字、短划线（-）、下划线（_）、全角句号（。）、全角逗号（，）和全角冒号（：）。

## 6.2. 修改用户网关


创建用户网关实例后，您可以修改用户网关实例的名称和描述信息。

### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择VPN > 用户网关。
3. 在顶部菜单栏，选择用户网关实例的地域。

4. 在**用户网关**页面，找到目标用户网关实例，在实例ID下面找到并单击  图标，在弹出的对话框中修改实例名称，然后单击**确定**。

名称长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（\_）和短划线（-）。

5. 在**描述**列找到并单击  图标，在弹出的对话框中修改用户网关实例的描述信息，然后单击**确定**。

描述信息长度为2~100个字符，以大小写字母或中文开始，可包含数字、短划线（-）、下划线（\_）、全角句号（。）、全角逗号（，）和全角冒号（：）。

## 6.3. 删除用户网关

您可以删除一个不需要的用户网关。

### 前提条件

已删除了用户网关实例关联的IPsec连接。具体操作，请参见[删除IPsec连接](#)。

### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择**VPN > 用户网关**。
3. 在顶部菜单栏，选择用户网关实例的地域。
4. 在**用户网关**页面，找到目标用户网关，在**操作**列单击**删除**。
5. 在**删除用户网关**对话框中，单击**确定**。

# 7.配置IPsec-VPN

## 7.1. 管理IPsec连接

### 7.1.1. 创建IPsec连接

创建VPN网关和用户网关后，您可以创建IPsec连接建立加密通信通道。

#### 前提条件

创建VPN网关时已经开启了IPsec功能。具体操作，请参见[创建VPN网关](#)。

#### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择VPN > IPsec连接。
3. 在IPsec连接页面，单击创建IPsec连接。
4. 在创建IPsec连接页面，根据以下信息配置IPsec连接，然后单击提交。

配置	说明
组织	选择IPsec连接所属的组织。
资源集	选择IPsec连接所属的资源集。
地域	选择IPsec连接所属的地域。 <div> 说明 IPsec连接所属的地域需和待连接的VPN网关的地域相同。</div>
可用区	选择IPsec连接所属的可用区。
名称	输入IPsec连接的名称。 长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。
VPN网关	选择待连接的VPN网关。
用户网关	选择待连接的用户网关。
本端网段	输入需要和本地数据中心互连的VPC侧的网段，用于第二阶段协商。 IKEv2版本下支持添加多个本端网段，多个本端网段之间使用半角逗号（,）分隔。
对端网段	输入需要和VPC互连的本地数据中心侧的网段，用于第二阶段协商。 IKEv2版本下支持添加多个对端网段，多个对端网段之间使用半角逗号（,）分隔。

配置	说明
立即生效	选择是否立即生效。 <ul style="list-style-type: none"> <li>是：配置完成后立即进行协商。</li> <li>否（默认值）：当流量进入时进行协商。</li> </ul>
高级配置	选择高级配置的类型。 <ul style="list-style-type: none"> <li>默认（默认值）：使用默认的高级配置。</li> <li>配置：自定义高级配置。</li> </ul>
高级配置：IKE配置	
预共享密钥	用于VPN网关与用户网关之间的身份认证。默认情况下会随机生成，也可以手动指定密钥。 默认会随机生成一个16位的字符串。建立IPsec连接要求本端和对端的密钥必须一致。
版本	选择IKE协议的版本。 <ul style="list-style-type: none"> <li>ikev1（默认值）</li> <li>ikev2</li> </ul> <p>目前系统支持IKEv1和IKEv2，相对于IKEv1版本，IKEv2版本简化了SA的协商过程并且对于多网段的场景提供了更好的支持，所以建议选择IKEv2版本。</p>
协商模式	选择协商模式。 <ul style="list-style-type: none"> <li>main（默认值）：主模式，协商过程安全性高。</li> <li>aggressive：野蛮模式，协商快速且协商成功率高。</li> </ul> <p>协商成功后两种模式的信息传输安全性相同。</p>
加密算法	选择第一阶段协商使用的加密算法。支持aes（默认值）、aes192、aes256、des和3des。
认证算法	选择第一阶段协商使用的认证算法。支持sha1和md5（默认值）。
DH分组	选择第一阶段协商的Diffie-Hellman密钥交换算法。 <ul style="list-style-type: none"> <li>group1：表示DH分组中的DH1。</li> <li>group2（默认值）：表示DH分组中的DH2。</li> <li>group5：表示DH分组中的DH5。</li> <li>group14：表示DH分组中的DH14。</li> </ul>
SA生存周期（秒）	设置第一阶段协商的SA的生存周期。取值范围：0~86400。单位：秒。默认值：86400。
LocalId	设置VPN网关的标识，用于第一阶段的协商。默认值为VPN网关的公网IP地址。如果手动设置LocalId为FQDN格式，建议将协商模式改为野蛮模式（aggressive）。

配置	说明
Remoteld	设置用户网关的标识，用于第一阶段的协商。默认值为用户网关的公网IP地址。如果手动设置Remoteld为FQDN格式，建议将协商模式改为野蛮模式（aggressive）。
高级配置：IPsec配置	
加密算法	选择第二阶段协商的加密算法。支持aes（默认值）、aes192、aes256、des和3des。
认证算法	选择第二阶段协商的认证算法。支持sha1和md5（默认值）。
DH分组	<p>选择第二阶段协商的Diffie-Hellman密钥交换算法。</p> <ul style="list-style-type: none"> <li>◦ disabled：表示不使用DH密钥交换算法。 <ul style="list-style-type: none"> <li>■ 对于不支持PFS的客户端请选择disabled。</li> <li>■ 如果选择为非disabled的任何一个组，会默认开启PFS功能（完美向前加密），使得每次重协商都要更新密钥，因此，相应的客户端也要开启PFS功能。</li> </ul> </li> <li>◦ group1：表示DH分组中的DH1。</li> <li>◦ group2（默认值）：表示DH分组中的DH2。</li> <li>◦ group5：表示DH分组中的DH5。</li> <li>◦ group14：表示DH分组中的DH14。</li> </ul>
SA生存周期（秒）	设置第二阶段协商的SA的生存周期。取值范围：0~86400。单位：秒。默认值：86400。

## 7.1.2. 修改IPsec连接

创建IPsec连接后，您可以修改IPsec连接的配置。

### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择VPN > IPsec连接。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，在操作列单击编辑。
5. 在编辑IPsec连接对话框，修改IPsec连接的名称、高级配置、互通网段等配置，然后单击确定。


关于参数的详细说明，请参见[创建IPsec连接](#)。

## 7.1.3. 下载IPsec连接配置

创建IPsec连接后，您可以下载IPsec连接的配置。

### 操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > IPsec连接。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，在操作列单击下载对端配置。
5. 在IPsec连接配置对话框，复制并保存配置信息。

 **说明** 下载配置中的RemoteSubnet和LocalSubnet与创建IPsec连接时的本端网段和对端网段正好是相反的。因为从阿里云VPN网关的角度看，对端是本地数据中心的网段，本端是阿里云侧的VPC网段；而从本地数据中心的网关设备角度看，LocalSubnet就是指本地数据中心的网段，RemoteSubnet则是指阿里云VPC的网段。

## 7.1.4. 配置路由安全组

创建IPsec连接后，您可以配置路由安全组，来控制安全组内ECS实例的入方向流量和出方向流量。

### 操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > IPsec连接。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，在操作列单击配置路由安全组。
5. 在配置路由安全组对话框，根据以下信息进行配置，然后单击确定。

配置	说明
安全组	选择要配置安全组规则的安全组。
规则方向	选择安全组规则的规则方向。 <ul style="list-style-type: none"> <li>出方向：指ECS实例访问内网中其他ECS实例或者公网上的资源。</li> <li>入方向：指内网中的其他ECS实例或公网上的资源访问ECS实例。</li> </ul>
授权策略	选择安全组规则的授权策略。 <ul style="list-style-type: none"> <li>允许：放行相应的访问请求。</li> <li>拒绝：直接丢弃数据包，不会返回任何回应信息。</li> </ul> <p>如果两个安全组规则其他都相同，只有授权策略不同，则拒绝策略生效，允许策略不生效。</p>
协议类型	选择安全组规则的协议类型。
端口范围	输入安全组规则的端口范围。端口取值范围：-1，1~65535，其中-1无法单独设置。 端口输入格式示例： <ul style="list-style-type: none"> <li>1/200表示端口范围1~200。</li> <li>80/80表示单个端口80。</li> <li>-1/-1表示不限制端口。</li> </ul>

配置	说明
优先级	设置优先级。默认值为1，即最高优先级，可设置范围1~100。
授权类型	选择安全组规则的授权类型。 目前，仅支持地址段访问。
网卡类型	选择网卡类型。 <ul style="list-style-type: none"> <li>内网：安全组规则仅对内网生效。</li> <li>公网：安全组规则仅对公网生效。</li> </ul>
授权对象	选择安全组规则的授权对象。 支持多组授权对象，最多支持10组授权对象。
自动下发路由	打开或关闭自动下发路由。默认为关闭状态。
描述	输入安全组规则的描述信息。 描述可以为空，或输入2~256个中英文字符，不能以 <code>http://</code> 和 <code>https://</code> 开始。

## 7.1.5. 删除IPsec连接

您可以删除一个不需要的IPsec连接。

### 操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > IPsec连接。
3. 在顶部菜单栏，选择IPsec连接的地域。
4. 在IPsec连接页面，找到目标IPsec连接，在操作列单击删除。
5. 在删除IPsec连接对话框，单击确定。

## 7.2. MTU注意事项

最大传输单元 (MTU) 是网络层协议（如 TCP）支持的最大数据包的大小（以字节为单位），标头和数据均包括在内。

通过IPsec隧道发送的网络数据包经过加密，然后封装在外部数据包中，以便进行路由。因为封装的内部数据包本身必须适合外部数据包的MTU，所以其MTU必须更小。

### 网关MTU

您必须配置本地VPN网关，将其使用的MTU限制在1360字节之内，建议MTU设置为1360字节。

对于TCP流量，在TCP协议收发双方通信数据时，会协商每一个报文段所能承载的最大数据长度（MSS）。我们建议您将本地VPN网关的TCP MSS设置为1359字节，便于TCP数据包的封装和传输。

# 8.配置SSL-VPN

## 8.1. 管理SSL服务端

### 8.1.1. 创建SSL服务端

开启SSL-VPN功能建立点到站点连接时，您必须先创建SSL服务端。

#### 前提条件

您已经创建了VPN网关并开启了SSL-VPN。具体操作，请参见[创建VPN网关](#)。

#### 操作步骤

1. [登录VPN网关管理控制台](#)。
2. 在左侧导航栏，选择VPN > SSL服务端。
3. 在SSL服务端页面，单击创建SSL服务端。
4. 在创建SSL服务端页面，根据以下信息配置SSL服务端，然后单击提交。

配置	说明
组织	选择SSL服务端所属的组织。
资源集	选择SSL服务端所属的资源集。
地域	选择SSL服务端所属的地域。
可用区	选择SSL服务端所属的可用区。
名称	输入SSL服务端的名称。 长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。
VPN网关	选择要关联的VPN网关。
本端网段	本端网段是客户端通过SSL-VPN连接要访问的地址段。本端网段可以是VPC的网段、交换机的网段、通过物理专线和VPC互连的IDC的网段、云服务如RDS、OSS等的网段。 支持输入多个本端网段，本端网段之间使用半角逗号（,）分隔。 <div>🔍 说明 本端网段的子网掩码在16到29位之间。</div>
客户端网段	客户端网段是给客户端虚拟网卡分配访问地址的地址段，不是指客户端已有的内网网段。当客户端通过SSL-VPN连接访问本端时，VPN网关会从指定的客户端网段中分配一个IP地址给客户端使用。 <div>🔍 说明 请确保客户端网段和本端网段不冲突。</div>



配置	说明
高级配置	<p>选择高级配置的类型。</p> <ul style="list-style-type: none"> <li>默认：使用默认高级配置。</li> <li>配置：自定义高级配置，自定义高级配置包括以下参数： <ul style="list-style-type: none"> <li>协议：SSL连接使用的协议。支持UDP（默认值）或TCP。</li> <li>端口：SSL连接使用的端口。默认值：1194。 不支持使用以下端口：22、2222、22222、9000、9001、9002、7505、80、443、53、68、123、4510、4560、500、4500。</li> <li>加密算法：SSL连接使用的加密算法，支持AES-128-CBC（默认值）、AES-192-CBC、AES-256-CBC和none。</li> <li>是否压缩：是否对传输数据进行压缩处理。默认值：否。</li> </ul> </li> </ul>

## 8.1.2. 修改SSL服务端

创建SSL服务端后，您可以修改SSL服务端的配置。

### 操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > SSL服务端。
3. 在顶部菜单栏，选择SSL服务端的地域。
4. 在SSL服务端页面，找到目标SSL服务端，在操作列单击编辑。
5. 在编辑SSL服务端对话框，修改SSL服务端的名称、本端网段、客户端网段、高级配置等信息，然后单击确定。

关于参数的详细说明，请参见[创建SSL服务端](#)。

## 8.1.3. 配置路由安全组

创建IPsec连接后，您可以配置路由安全组，来控制安全组内ECS实例的入方向流量和出方向流量。

### 操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > SSL服务端。
3. 在顶部菜单栏，选择SSL服务端的地域。
4. 在SSL服务端页面，找到目标SSL服务端，在操作列单击配置路由安全组。
5. 在配置路由安全组对话框，根据以下信息进行配置，然后单击确定。

配置	说明
安全组	选择要配置安全组规则的安全组。

配置	说明
规则方向	<p>选择安全组规则的规则方向。</p> <ul style="list-style-type: none"> <li>出方向：指ECS实例访问内网中其他ECS实例或者公网上的资源。</li> <li>入方向：指内网中的其他ECS实例或公网上的资源访问ECS实例。</li> </ul>
授权策略	<p>选择安全组规则的授权策略。</p> <ul style="list-style-type: none"> <li>允许：放行相应的访问请求。</li> <li>拒绝：直接丢弃数据包，不会返回任何响应信息。</li> </ul> <p>如果两个安全组规则其他都相同，只有授权策略不同，则拒绝策略生效，允许策略不生效。</p>
协议类型	选择安全组规则的协议类型。
端口范围	<p>输入安全组规则的端口范围。端口取值范围：-1，1~65535，其中-1无法单独设置。</p> <p>端口输入格式示例：</p> <ul style="list-style-type: none"> <li>1/200表示端口范围1~200。</li> <li>80/80表示一个端口80。</li> <li>-1/-1表示不限制端口。</li> </ul>
优先级	设置优先级。默认值为1，即最高优先级，可设置范围1~100。
授权类型	<p>选择安全组规则的授权类型。</p> <p>目前，仅支持地址段访问。</p>
网卡类型	<p>选择网卡类型。</p> <ul style="list-style-type: none"> <li>内网：安全组规则仅对内网生效。</li> <li>公网：安全组规则仅对公网生效。</li> </ul>
授权对象	<p>选择安全组规则的授权对象。</p> <p>支持多组授权对象，最多支持10组授权对象。</p>
描述	<p>输入安全组规则的描述信息。</p> <p>描述可以为空，或输入2~256个中英文字符，不能以 <code>http://</code> 和 <code>https://</code> 开头。</p>

## 8.1.4. 删除SSL服务端

您可以删除一个不需要的SSL服务端。删除SSL服务端时，系统会一并删除SSL服务端关联的SSL客户端。

### 操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > SSL服务端。

- 3. 在顶部菜单栏，选择SSL服务端的地域。
- 4. 在SSL服务端页面，找到目标SSL服务端，在操作列单击删除。
- 5. 在SSL服务端对话框，单击确定。

## 8.2. 管理SSL客户端

### 8.2.1. 创建SSL客户端证书

创建SSL服务端后，您还需根据SSL服务端创建SSL客户端证书。

#### 前提条件

您已经创建了SSL服务端。具体操作，请参见[创建SSL服务端](#)。

#### 操作步骤

- 1. [登录VPN网关管理控制台](#)。
- 2. 在左侧导航栏，选择VPN > SSL客户端。
- 3. 在顶部菜单栏，选择SSL客户端的地域。
- 4. 在SSL客户端页面，单击创建SSL客户端。
- 5. 在创建SSL客户端证书页面，根据以下信息进行配置，然后单击提交。

配置	说明
组织	选择SSL客户端所属的组织。
资源集	选择SSL客户端所属的资源集。
地域	选择SSL客户端所属的地域。
可用区	选择SSL客户端所属的可用区。
名称	输入SSL客户端证书的名称。 长度为2~100个字符，以大小写字母或中文开始，可包含数字、下划线（_）和短划线（-）。
VPN网关	选择要关联的VPN网关。
SSL服务端	选择要关联的SSL服务端。

### 8.2.2. 下载SSL客户端证书

SSL客户端连接SSL-VPN，需要加载SSL客户端证书。您可以在VPN网关管理控制台下载SSL客户端证书。

#### 操作步骤

- 1. [登录VPN网关管理控制台](#)。
- 2. 在左侧导航栏，选择VPN > SSL客户端。
- 3. 在顶部菜单栏，选择SSL客户端的地域。

4. 在SSL客户端页面，找到目标SSL客户端证书，在操作列单击下载。

SSL客户端证书会下载至您本地。

### 8.2.3. 删除SSL客户端证书

您可以删除一个不需要的SSL客户端证书。

#### 操作步骤

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择VPN > SSL客户端。
3. 在顶部菜单栏，选择SSL客户端的地域。
4. 在SSL客户端页面，找到目标SSL客户端证书，在操作列单击删除。
5. 在删除SSL客户端证书对话框，单击确定。