ALIBABA CLOUD

阿里云

VPN网关

IPsec-VPN入门

文档版本：20220527

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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

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。

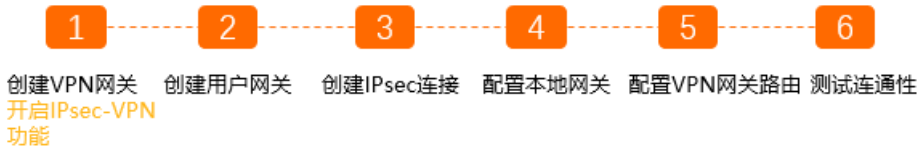
环境要求

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。具体操作，请参见查询安全组规则。

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。具体操作，请参见本地网关配置。
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
- 建立VPC到本地数据中心的连接（BGP动态路由）

2.建立VPC到本地数据中心的连接

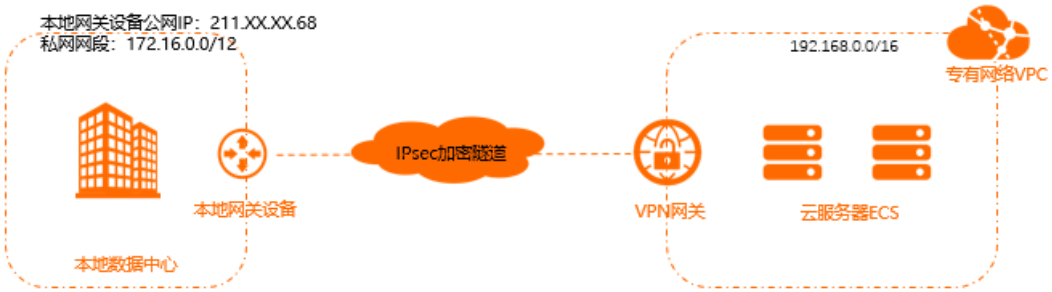
本文介绍如何使用IPsec-VPN建立专有网络VPC（Virtual Private Cloud）到本地数据中心的VPN连接，实现本地数据中心与VPC的互通。

前提条件

- 您已经注册了阿里云账号。如未注册，请先完成账号注册。
- 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。具体操作，请参见查询安全组规则和添加安全组规则。

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172.16.0.0/12，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.
2. 在**VPN网关**页面，单击**创建VPN网关**。
3. 在购买页面，根据以下信息配置VPN网关，然后单击**立即购买**并完成支付。
   - **实例名称**：输入VPN网关的实例名称。
   - **地域和可用区**：选择VPN网关所属的地域。

     > **说明** 确保VPC的地域和VPN网关的地域相同。

   - **网关类型**：选择要创建的VPN网关类型。本示例选择**普通型**。
   - **VPC**：选择要连接的VPC。
   - **指定交换机**：是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。

     如果您选择了**是**，您还需要指定具体的**虚拟交换机**。
   - **带宽规格**：选择VPN网关的公网带宽峰值。单位为Mbps。
   - **IPsec-VPN**：选择是否开启IPsec-VPN功能。本示例选择**开启**。

- **SSL-VPN**：选择是否开启SSL-VPN功能。本示例选择**关闭**。
- **计费周期**：选择购买时长。关于计费的更多信息， 请参见计费说明。

4. 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**网间互联 > 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**面板，根据以下信息配置用户网关，然后单击**确定**。
   - **名称**：输入用户网关的名称。
   - **IP地址**：输入VPC要连接的本地数据中心的网关设备的公网IP。本示例输入211.XX.XX.68。
   - **描述**：输入用户网关的描述信息。

   更多参数信息，请参见创建用户网关。

步骤三：创建IPsec连接

1. 在左侧导航栏，选择**网间互联 > 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**确定**。
   - **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**：选择已创建的用户网关。
   - **路由模式**：选择路由模式。本示例选择**目的路由模式**。
   - **立即生效**：选择是否立即生效。本示例选择**否**。
     - **是**：配置完成后立即进行协商。
     - **否**：当有流量进入时进行协商。
   - **预共享密钥**：输入共享密钥。建立IPsec连接需保证该值与本地网关设备的预共享密钥一致。

     如果不输入该值，系统默认生成一个16位的随机字符串。

   其他选项使用默认配置。更多信息，请参见创建IPsec连接。

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**网间互联 > VPN > IPsec连接**。

2. 在**IPsec连接**页面，找到目标IPsec连接实例，然后在**操作**列下选择 ⋮ > **下载对端配置**。
3. 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。具体操作，请参见本地网关配置。

步骤五：配置VPN网关路由

1. 在左侧导航栏，选择**网间互联 > 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**面板，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172.16.0.0/12。
   - **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。关于如何登录ECS实例，请参见连接方式概述。
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@iZm5[redacted]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@iZm5ea[redacted]xslbZ ~]#
```

3.建立VPC到本地数据中心的连接（BGP动态路由）

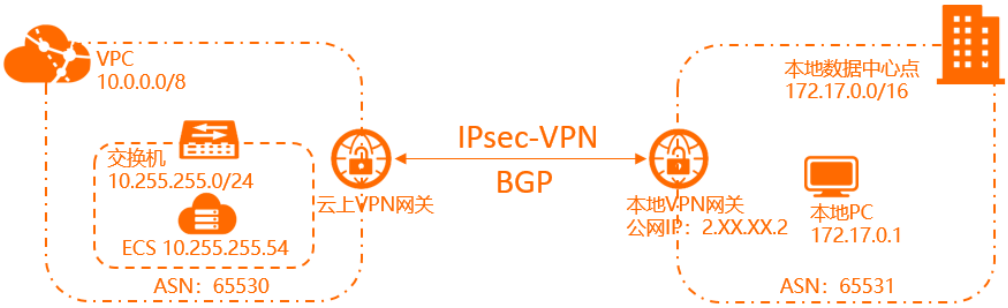
本文介绍如何使用IPsec-VPN建立专有网络VPC（Virtual Private Cloud）到本地数据中心的VPN连接，并通过BGP动态路由协议自动学习路由实现VPC与本地数据中心间的资源互通，降低网络维护成本和网络配置风险。

场景示例

本文以下图场景为例。某公司已在德国（法兰克福）地域创建了一个VPC，私网网段为10.0.0.0/8，自治系统号ASN（Autonomous System Number）为65530。该公司在法兰克福拥有本地数据中心，公网IP为2.XX.XX.2，私网网段为172.17.0.0/16，ASN为65531。因业务发展，需要云上VPC与本地数据中心互通。

您可以通过IPsec-VPN建立VPC到本地数据中心的VPN连接，并配置BGP动态路由。配置成功后，VPC和本地数据中心通过BGP动态路由协议自动学习路由实现资源互通，降低网络维护成本和网络配置风险。

> **说明** 在互联网中，一个自治系统AS（Autonomous System）是一个有权自主决定在本系统中应采用何种路由协议的小型单位。这个网络单位可以是一个简单的网络也可以是一个或多个普通的网络管理员来控制的网络群体，它是一个单独的可管理的网络单元。一个自治系统将会分配一个全局的唯一的号码，这个号码叫做自治系统号（ASN）。



BGP动态路由支持的地域

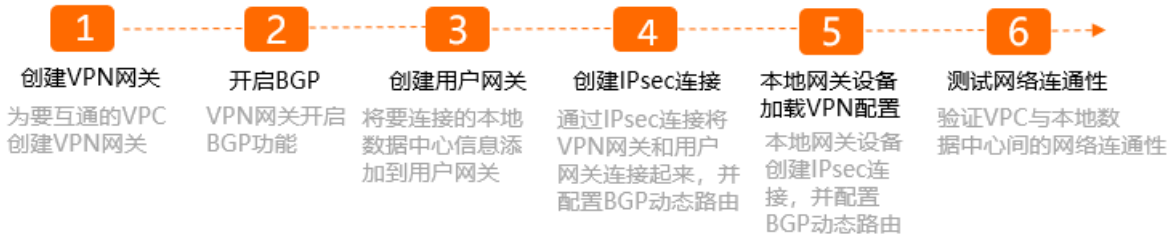
区域	地域
亚太	华东1（杭州）、华东2（上海）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华南1（深圳）、中国（香港）、日本（东京）、新加坡、澳大利亚（悉尼）、马来西亚（吉隆坡）、印度尼西亚（雅加达）、印度（孟买）
欧洲与美洲	德国（法兰克福）、英国（伦敦）、美国（弗吉尼亚）、美国（硅谷）
中东与印度	阿联酋（迪拜）

前提条件

- 您已经注册了阿里云账号。如未注册，请先完成账号注册。
- 您已经在德国（法兰克福）地域创建了VPC并部署了云服务。具体操作，请参见搭建IPv4专有网络。
- 确保本地数据中心的网关设备支持IKEv1和IKEv2协议，支持这两种协议的设备均可以和云上VPN网关互连。

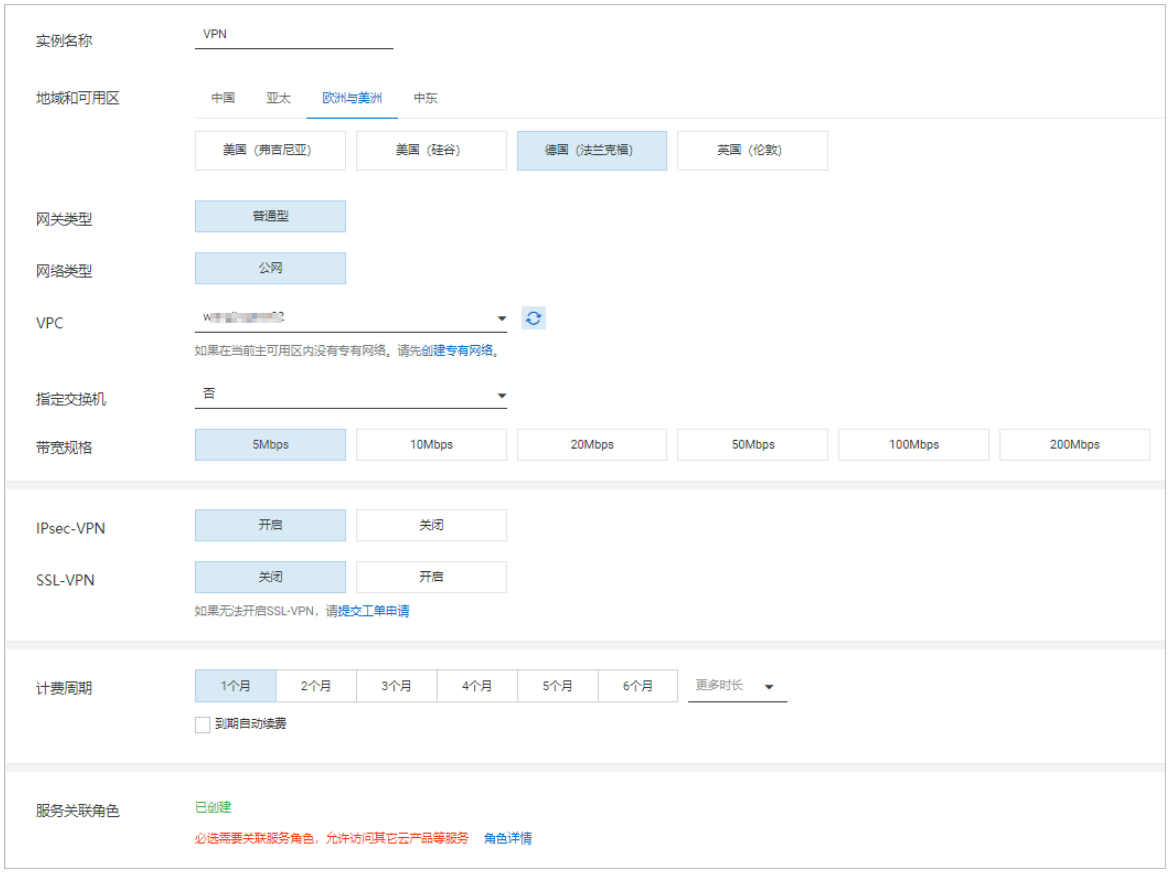
- 本地数据中心的网关设备已经配置了静态公网IP。
- 本地数据中心和VPC互通的网段没有重叠。
- 您已经了解VPC中的ECS实例所应用的安全组规则，并确保安全组规则允许本地数据中心的网关设备访问云上资源。具体操作，请参见查询安全组规则和添加安全组规则。

配置步骤



步骤一：创建VPN网关

1.
2. 在**VPN网关**页面，单击**创建VPN网关**。
3. 在购买页面，根据以下信息创建VPN网关，然后单击**立即购买**并完成支付。



配置	说明
实例名称	输入VPN网关的实例名称。本示例输入*VPN*。

配置	说明
地域和可用区	选择VPN网关的地域。 确保VPC的地域和VPN网关的地域相同。本示例选择**德国（法兰克福）**。
网关类型	选择要创建的VPN网关类型。本示例选择**普通型**。
网络类型	选择实例的网络类型。本示例默认显示**公网**。
VPC	选择要连接的VPC。本示例选择德国（法兰克福）地域创建的VPC。
指定交换机	选择是否为VPN网关指定所属的交换机。本示例选择**否**。 如果您选择了**是**，您还需要指定具体的**虚拟交换机**。
带宽规格	选择带宽规格。 单位：Mpbs。 带宽规格是VPN网关所具备的公网带宽峰值。本示例选择**5 Mbps**。
IPsec-VPN	选择是否开启IPsec-VPN功能。 本示例选择**开启**。
SSL-VPN	选择是否开启SSL-VPN功能。 本示例选择**关闭**。
计费周期	选择购买时长。关于计费的更多信息， 请参见计费说明。
服务关联角色	单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。 已创建若本配置项显示为**已创建**，则表示您的账号下已创建了该角色，无需重复创建。

创建好的VPN网关的状态是**准备中**，约1~5分钟左右会变更为**正常**。**正常**状态表明VPN网关已经完成了初始化，可以正常使用。VPN网关创建后，系统会为VPN网关自动分配一个公网IP地址用于建立VPN连接。

说明 如果您没有创建新的VPN网关，计划使用存量的VPN网关实现本文场景，请确保您存量的VPN网关已升级至最新版本。如果您存量VPN网关不是最新版本，默认您无法使用BGP动态路由功能。

您可以在**升级**按钮处查看VPN网关是否是最新版本，如果不是最新版本，您可以通过**升级**按钮进行升级。具体操作，请参见升级VPN网关。

步骤二：开启BGP

BGP用于在不同的自治系统（AS）之间交换路由信息。使用BGP动态路由功能前，您需要为VPN网关开启BGP功能。

> **说明** VPN网关开启BGP动态路由功能后，不支持关闭。

1. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，找到已创建的VPN网关，在**操作**列下选择 ⋮ **> 开启路由自动传播**。

4. 在**开启路由自动传播**对话框，单击**确定**。

   开启后，VPN网关会将BGP路由条目自动传播到VPC中。

步骤三：创建用户网关

您可以通过创建用户网关，将本地数据中心的网络信息注册到云上，然后将用户网关和VPN网关连接起来。

1. 在左侧导航栏，选择**网间互联 > 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**面板，根据以下信息配置用户网关，然后单击**确定**。

配置	说明
名称	输入用户网关的名称。本示例输入*CGW*。
IP地址	输入本地数据中心网关设备的公网IP地址。本示例输入*2.XX.XX.2*。
自治系统号	输入本地数据中心网络的自治系统号。本示例输入*65531*。
描述	输入用户网关的描述信息。

关于参数的更多信息，请参见创建用户网关。

创建完成后，返回用户网关页面，您可以看到已创建的用户网关。系统会为用户网关自动分配一个公网IP地址用于和VPN网关建立连接。

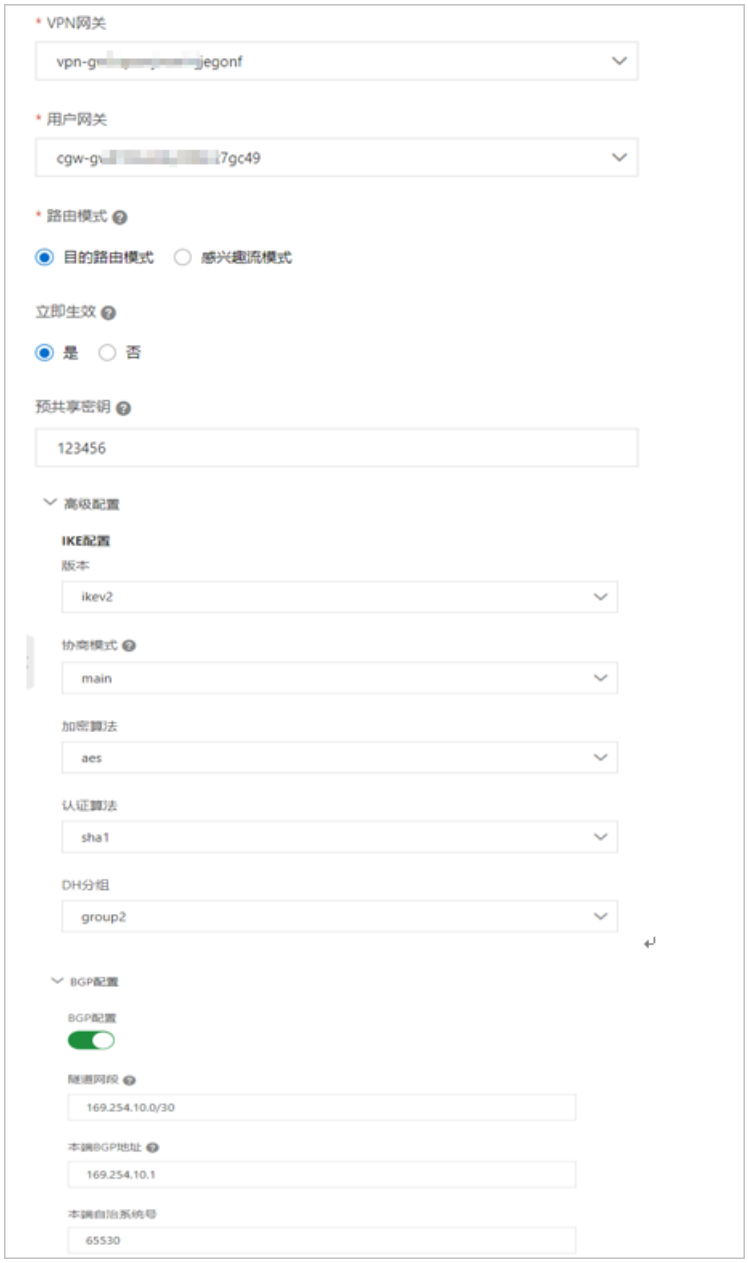
步骤四：创建IPsec连接

1. 在左侧导航栏，选择**网间互联 > 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，根据以下信息创建IPsec连接，然后单击**确定**。

   本示例只提供与创建VPC到本地数据中心间的IPsec连接强相关的配置参数，其他选项使用默认配置。更多信息，请参见创建IPsec连接。



配置	说明
名称	输入IPsec连接的名称。本示例输入*VPCTOIDC*。
VPN网关	选择要连接的VPN网关。 选择步骤一中创建的VPN网关。
用户网关	选择要连接的用户网关。 选择步骤三中创建的用户网关。
路由模式	选择路由模式。本示例选择**目的路由模式**。

配置	说明
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。 本示例选择**是**。
预共享密钥	输入预共享密钥。 请确保要建立的IPsec连接VPC侧和本地数据中心侧的预共享密钥一致。本示例输入*123456*。
版本	选择IKE的版本。本示例选择**ikev2**。
加密算法	选择加密算法。本示例选择**aes**。
认证算法	选择认证算法。本示例选择**sha1**。
DH分组	选择DH分组。本示例选择**group2**。
隧道网段	输入IPsec隧道的网段，该网段在169.254.0.0/16内的掩码长度为30的网段。本示例输入*169.254.10.0/30*。
本端BGP地址	输入本端BGP地址，该地址为隧道网段内的一个IP地址。本示例输入*169.254.10.1*。 **说明** 请确保IPsec隧道两端的BGP地址不冲突。
本端自治系统号	输入VPC侧的自治系统号。本示例输入*65530*。

步骤五：在本地网关设备中加载VPN配置

云上创建IPsec连接后，您还需要在本地网关设备中加载VPN配置，才能建立VPC到本地数据中心的VPN连接。

本示例以思科IOSXE系统的防火墙为例，介绍如何在本地网关设备中加载VPN配置。

1. 登录思科防火墙设备的命令行配置界面。
2. 执行以下命令，配置ikev2 proposal和policy 。

```
crypto ikev2 proposal alicloud
encryption aes-cbc-128          //配置加密算法，本示例配置为aes-cbc-128。
integrity sha1                  //配置认证算法，本示例配置为sha1。
group 2                         //配置DH分组，本示例配置为group2。
exit
!
crypto ikev2 policy Pureport_Pol_ikev2
proposal Pureport_prop
exit
!
```

3. 执行以下命令，配置ikev2 keyring。

```
crypto ikev2 keyring alicloud
peer alicloud
address 1.XX.XX.1                //配置VPC侧VPN网关的公网IP地址，本示例配置为1.XX.XX.1。
pre-shared-key 123456           //配置钥匙串，本示例配置为123456。
exit
!
```

4. 执行以下命令，配置ikev2 profile。

```
crypto ikev2 profile alicloud
match identity remote address 1.XX.XX.1 255.255.255.255     //匹配VPC侧VPN网关的公网IP，本示例匹配的地址为1.XX.XX.1。
identity local address 2.XX.XX.2     //本地数据中心的公网IP，本示例配置为2.XX.XX.2。
authentication remote pre-share    //认证对端的方式为PSK。
authentication local pre-share     //认证本端的方式为PSK。
keyring local alicloud             //调用密钥串。
exit
!
```

5. 执行以下命令，配置transform。

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
mode tunnel
exit
!
```

6. 执行以下命令，配置IPsec Profile，并调用transoform、pfs和ikev2 profile。

```
crypto ipsec profile alicloud
set transform-set TSET
set pfs group2
set ikev2-profile alicloud
exit
!
```

7. 执行以下命令，配置IPsec隧道。

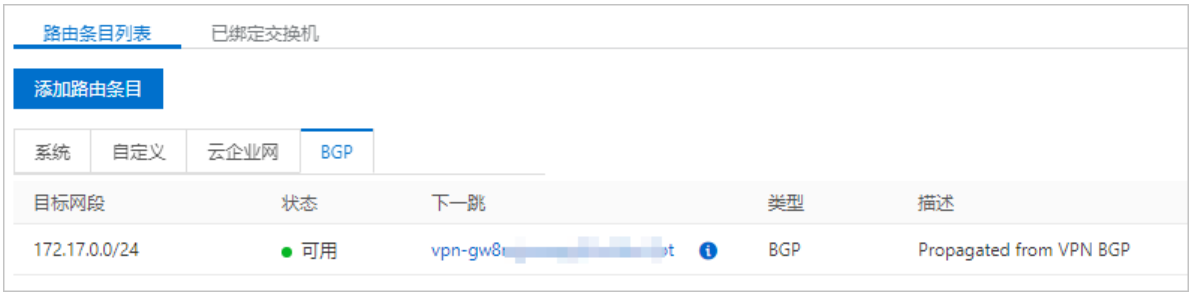
```
interface Tunnel100
ip address 169.254.10.2 255.255.255.252     //配置本端（本地数据中心）隧道地址，本示例配置为169.254.10.2。
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 1.XX.XX.1                  //隧道对端（云上VPN网关）公网IP地址，本示例配置为1.XX.XX.1。
tunnel protection ipsec profile alicloud
no shutdown
exit
!
interface GigabitEthernet1
ip address 2.XX.XX.2 255.255.255.0
negotiation auto
!
```

8. 执行以下命令，配置BGP路由协议。

```
router bgp 65531                          //开启bgp路由协议，并配置本端（本地数据中心）ASN。本示例配置ASN为65531。
bgp router-id 169.254.10.2                //bgp路由器id，本示例设置为169.254.10.2。
bgp log-neighbor-changes
neighbor 169.254.10.1 remote-as 65530     //配置bgp邻居的ASN。
neighbor 169.254.10.1 ebgp-multihop 10    //配置ebgp跳数为10。
!
address-family ipv4
network 172.17.0.0 mask 255.255.0.0       //宣告本端（本地数据中心）网段，本示例配置为172.17.0.0/16。
neighbor 169.254.10.1 activate            //激活bgp邻居。
exit-address-family
!
```

IPsec连接建立成功后，云上云下VPN网关会进行以下路由宣告：

- 本地数据中心VPN网关通过BGP动态路由协议自动学习本地数据中心网段路由，并自动宣告给云上VPN网关。云上VPN网关会将学习到的BGP路由自动传播到VPC的系统路由表中。



- 云上VPN网关通过BGP路由协议自动学习VPC系统路由表中的路由，并自动宣告给本地数据中心侧VPN网关设备。

步骤六：测试连通性

1. 登录到VPC内一台无公网IP的ECS实例。关于如何登录ECS实例，请参见连接方式概述。
2. 通过 `ping` 命令，访问本地数据中心的客户端，验证通信是否正常。

   经验证，VPC ECS实例可以正常访问本地数据中心的客户端。

```
[root@iZ[redacted]ednm7ocZ ~]# ping 172.17.0.1
PING 172.17.0.48 (172.17.0.48) 56(84) bytes of data.
64 bytes from 172.17.0.1: icmp_seq=1 ttl=64 time=193 ms
64 bytes from 172.17.0.1: icmp_seq=2 ttl=64 time=134 ms
64 bytes from 172.17.0.1: icmp_seq=3 ttl=64 time=142 ms
64 bytes from 172.17.0.1: icmp_seq=4 ttl=64 time=294 ms
64 bytes from 172.17.0.1: icmp_seq=5 ttl=64 time=111 ms
^C
```

3. 登录本地数据中心客户端。
4. 通过 `ping` 命令，访问VPC下的ECS实例，验证通信是否正常。

   经验证，本地数据中心客户端可以正常访问VPC ECS实例。

```
Router#ping 10.255.255.54 source 172.17.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.54, timeout is 2 seconds:
Packet sent with a source address of 172.17.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 154/154/155 ms
```

4.使用手机（iOS系统）自带的VPN软件建立远程连接

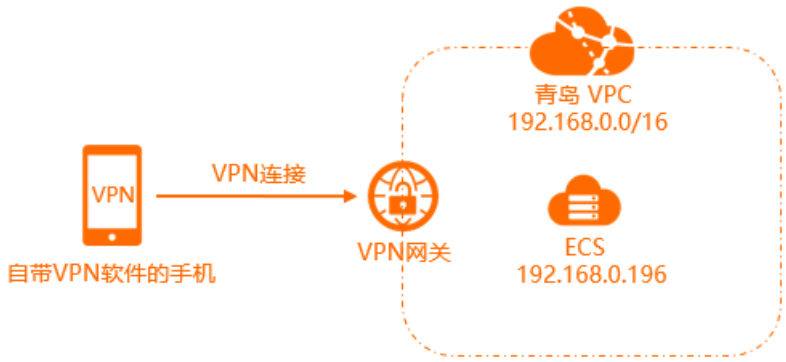
本文介绍如何使用手机（iOS系统）自带的VPN软件建立与云上VPN网关的连接，实现手机远程访问云上资源。

前提条件

- 您已经注册了阿里云账号。如未注册，请先完成账号注册。
- 您的手机端的系统为iOS。
- 您已经在IPsec服务端支持的地域创建了专有网络。具体操作，请参见搭建IPv4专有网络。

> 说明
>
> - 目前，仅以下地域支持IPsec服务端功能：华东1（杭州）、华东2（上海）、华东5（南京-本地地域）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华北6（乌兰察布）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）、日本（东京）、韩国（首尔）、新加坡、澳大利亚（悉尼）、马来西亚（吉隆坡）、印度尼西亚（雅加达）、菲律宾（马尼拉）、泰国（曼谷）、印度（孟买）、德国（法兰克福）、英国（伦敦）、美国（弗吉尼亚）、美国（硅谷）、阿联酋（迪拜）。
> - 当前仅支持iOS系统的手机使用自带的VPN软件建立与云上VPN网关的连接。

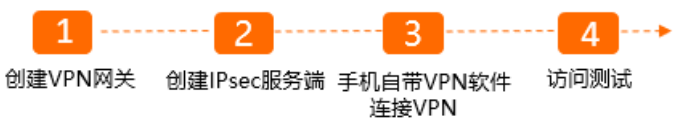
场景说明



某公司在华北1（青岛）地域创建了ECS实例，并部署了企业应用。因公司业务发展，需要出差员工可以通过手机远程访问部署在云上的企业应用。

您可以创建VPN网关，并在VPN网关中创建IPsec服务端，然后通过手机自带的VPN软件与云上VPN网关建立连接。连接成功后，手机可以远程访问云上企业应用。

配置步骤



步骤一：创建VPN网关

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关要关联的VPC实例的地域。本示例选择**华北1（青岛）**。
3. 在**VPN网关**页面，单击**创建VPN网关**。
4. 在购买页面，根据以下信息配置VPN网关，然后单击**立即购买**并完成支付。
   - **实例名称**：输入VPN网关的实例名称。

     名称长度为2~128个字符，以英文字母或中文开始，可包含数字、短划线（-）和下划线（_）。
   - **地域和可用区**：选择VPN网关的地域。

     本示例选择**华北1（青岛）**。
   - **网关类型**：选择要创建的VPN网关类型。本示例选择**普通型**。
   - **VPC**：选择VPN网关要关联的VPC。
   - **指定交换机**：选择是否为VPN网关指定所属的交换机。
     - **否**：不为VPN网关指定所属的交换机，系统会在指定VPC下的任意一个交换机内创建VPN网关。
     - **是**：为VPN网关指定所属的交换机，系统会在指定的交换机下创建VPN网关。
   - **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。

     本示例选择5 Mbps。
   - **IPsec-VPN**：选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以实现本地数据中心与VPC之间的连接。

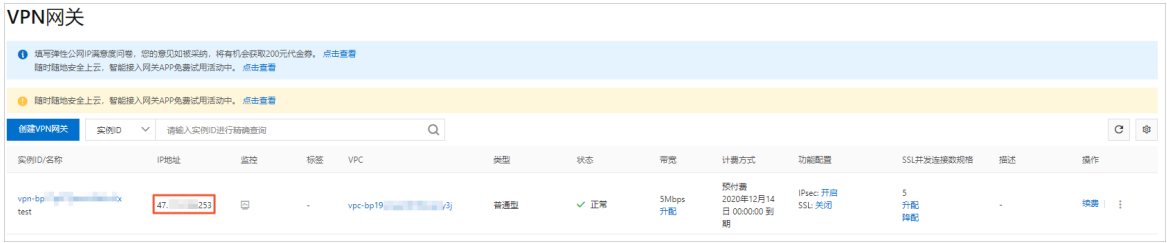
     本示例选择**关闭**。
   - **SSL-VPN**：选择开启或关闭SSL-VPN功能。SSL-VPN功能允许您从任何位置的单台计算机连接到VPC。

     使用手机自带的VPN软件建立与云上VPC的VPN连接需要开启SSL-VPN功能，本示例选择**开启**。
   - **SSL连接数**：选择支持同时连接的最大客户端数量。

     本示例选择5。

     > **说明** SSL-VPN与IPsec服务端共享SSL连接数。例如，SSL连接数为5，您已经有3个SSL客户端连接了SSL-VPN，则您还能使用2个手机客户端连接IPsec服务端。
   - **计费周期**：选择购买时长。关于计费的更多信息，请参见计费说明。
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**，约两分钟左右会变成**正常**状态。正常状态表明VPN网关完成了初始化，可以正常使用。系统会为VPN网关分配一个公网IP，用于手机客户端与云上VPN网关建立连接。



> **说明** 如果您没有创建新的VPN网关，计划使用存量的VPN网关实现本文场景，请确保您存量的VPN网关已升级至最新版本。如果您存量VPN网关不是最新版本，默认您无法使用IPsec服务端。
>
> 您可以在**升级**按钮处查看VPN网关是否是最新版本，如果不是最新版本，您可以通过**升级**按钮进行升级。具体操作，请参见升级VPN网关。

步骤二：创建IPsec服务端

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > IPsec服务端**。
3. 在顶部菜单栏，选择IPsec服务端的地域。
4. 在**IPsec服务端**页面，单击**创建IPsec服务端**。
5. 在**创建IPsec服务端**页面，根据以下信息配置IPsec服务端。
   - **名称**：输入IPsec服务端的名称。

     名称长度为2~128个字符之间，以英文字母或中文开始，可包含数字、短划线（-）和下划线（_）。
   - **VPN网关**：选择手机自带的VPN软件要连接的VPN网关。

     本示例选择步骤一中创建的VPN网关。
   - **本端网段**：输入手机要远程访问的VPC的网段。

     本示例输入192.168.0.0/16。
   - **客户端网段**：输入IPsec隧道客户端的私网网段。

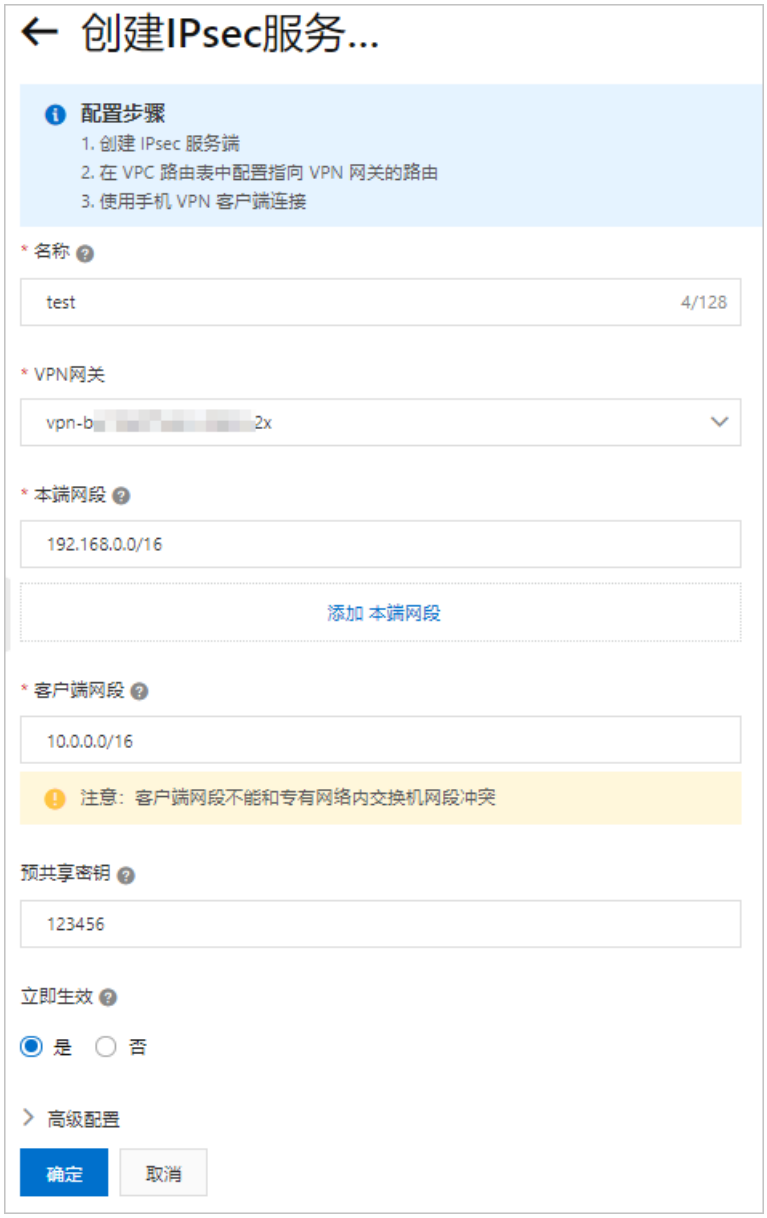
     客户端网段是给手机客户端虚拟网卡分配的私网网段，不是指手机客户端的私网网段。当手机客户端通过VPN连接访问云上VPC时，VPN网关会从指定的客户端网段中分配一个IP地址给客户端使用。

     > **说明** 客户端网段不能与VPC内交换机网段冲突。

     本示例输入10.0.0.0/16。
   - **预共享密钥**：用于IPsec服务端与手机客户端之间的身份认证，建立IPsec要求两端密钥必须一致。默认情况下会随机生成，您也可以手动指定密钥。

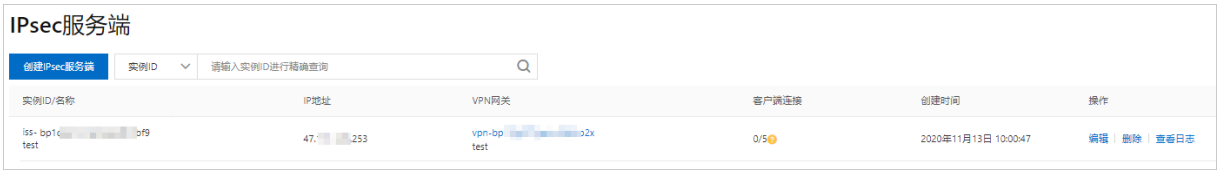
     本示例输入123456。
   - **立即生效**：选择是否立即生效。
     - **是**：配置完成后立即进行协商。
     - **否**：当有流量进入时进行协商。

     本示例选择**是**。
   - **高级配置**：使用默认高级配置。



6. 单击**确定**。

IPsec服务端创建成功后，您可以在**IPsec服务端**页面查看创建的IPsec服务端。



步骤三：手机自带VPN软件连接VPN

以下内容以iOS 14系统为例，介绍如何使用手机自带的VPN软件与云上VPN网关建立连接。

1. 打开手机的**设置**。
2. 选择**通用** > **VPN** > **添加VPN配置**。
3. 在**添加配置**页面，根据以下信息配置VPN。
   - **类型**：选择VPN的类型。

本示例选择**IKEv2**。

- **描述**：输入VPN的描述信息。
- **服务器**：输入手机客户端要连接的云上VPN网关的公网IP地址。

  本示例输入步骤一中创建的VPN网关的公网IP地址。
- **远程ID**：输入手机客户端要连接的云上VPN网关的公网IP地址。

  本示例输入步骤一中创建的VPN网关的公网IP地址。
- **本地ID**：本示例不填。
- **用户鉴定**：选择VPN网关用户鉴定类型。

  本示例选择**无**。
- **使用证书**：本示例关闭。
- **密钥**：用于IPsec服务端与手机客户端之间的身份认证，IPsec建立要求两端密钥必须一致。

  本示例输入**123456**。

4. 单击**完成**。
5. 在**VPN**页面，选中目标VPN配置，打开**状态**开关。

待VPN状态显示**已连接**表示VPN连接成功。

步骤四：访问测试

完成以下操作，测试手机客户端与云上VPC资源的连通性。

1. 打开手机浏览器。
2. 在地址栏输入ECS实例的私网IP地址。

   本示例输入**192.168.0.196**。

经测试，手机客户端可以远程访问云上VPC资源。