阿里云
VPN网关

IPsec-VPN入门

文档版本：20190627

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 教程概览

本教程为您介绍如何通过IPsec-VPN，建立VPC到本地数据中心的VPN连接。

前提条件

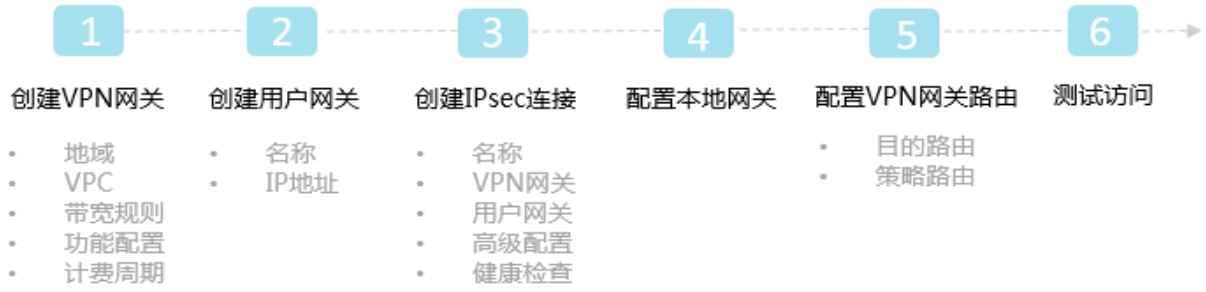
使用IPsec-VPN功能建立VPC到本地数据中心的VPN连接，确保满足以下条件：

- 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都可以和阿里云VPN网关互连，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和Ixia等。
- 本地数据中心的网关必须配置静态公网IP。
- 本地数据中心的网段和专有网络的网段不能重叠。

配置流程说明

建立VPC到本地数据中心的VPN连接的流程图如下：



1. 创建VPN网关

   VPN网关开启IPsec-VPN功能，一个VPN网关最多可以建立10个IPsec连接。
2. 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。
3. 创建IPsec连接

   IPsec连接是指VPN网关和用户网关建立连接后的VPN通道。只有IPsec连接建立后，用户侧企业数据中心才能使用VPN网关进行加密通信。
4. 配置本地网关

   您需要在本地VPN网关设备中加载阿里云VPN网关的配置。详细信息，请参见本地CPE配置。

5. 配置VPN网关路由

   您需要在VPN网关中配置路由，并发布到VPC路由表中。详细信息，请参见网关路由概述。

6. 测试访问

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

详细配置信息，请参见建立VPC到本地数据中心的连接。

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VPC到本地数据中心的VPN连接，从而实现本地数据中心与VPC的互通。

前提条件

使用IPsec-VPN功能建立VPC到本地数据中心的VPN连接，确保满足以下条件：

- 检查本地数据中心的网关设备。阿里云VPN网关支持标准的IKEv1和IKEv2协议。因此，只要支持这两种协议的设备都可以和云上VPN网关互连，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和 Ixia等。
- 本地数据中心的网关已经配置了静态公网IP。
- 本地数据中心的网段和专有网络的网段不能重叠。

步骤一 创建VPN网关

完成以下操作，创建VPN网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关。
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，然后单击立即购买完成支付。
   - 实例名称：输入VPN网关的实例名称。
   - 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。

- VPC： 选择要连接的VPC。
- 带宽规格：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
- IPsec-VPN： 选择开启IPsec-VPN功能。
- SSL-VPN： 选择是否开启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专有网络。
- SSL连接数： 选择您需要同时连接的客户端最大规格。

> 说明:
> 本选项只有在选择开启了SSL-VPN功能后才可配置。

- 计费周期：选择购买时长。

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，可以正常使用了。

> 说明:
> VPN网关的创建一般需要1-5分钟。

步骤二 创建用户网关

完成以下操作，创建用户网关。

1. 在左侧导航栏，单击VPN > 用户网关。
2. 选择用户网关的地域。
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网关设备的公网IP。
   - 描述：输入用户网关的描述信息。

步骤三 创建IPsec连接

完成以下操作，创建IPsec连接。

1. 在左侧导航栏，单击VPN > IPsec连接。
2. 选择创建IPsec连接的地域。
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。
   - 对端网段：输入本地数据中心的网段。
   - 是否立即生效：选择是否立即协商。
     - 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，该值必须与本地网关设备的预共享密钥一致。

     其他选项使用默认配置。

步骤四 在本地网关设备中加载VPN配置

完成以下操作，在本地网关设备中加载VPN配置。

1. 在左侧导航栏，单击VPN > IPsec连接。
2. 选择IPsec连接的地域。
3. 在IPsec连接页面，找到目标IPsec连接，然后单击操作列下的下载对端配置。
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。详细信息，请参见本地网关配置。

   下载配置中的RemotSubnet和LocalSubnet与创建IPsec连接时的本端网段和对端网段是相反的。因为从阿里云VPN网关的角度看，对端是用户IDC的网段，本端是VPC网段；而从本地网关设备的角度看，LocalSubnet就是指本地IDC的网段，RemotSubnet则是指阿里云VPC的网段。

步骤五 配置VPN网关路由

完成以下操作，配置VPN网关路由。

1. 在左侧导航栏，单击VPN > VPN网关。
2. 选择VPN网关的地域。
3. 在VPN网关页面，找到目标VPN网关，单击实例ID/名称列下的实例ID。
4. 在目的路由表页签，单击添加路由条目。

5. 在添加路由条目页面，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IDC侧的私网网段。
- 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。本例选择是。
- 权重：选择权重值。本例选择100。

步骤六 测试访问

登录到阿里云VPC内一台无公网IP的ECS实例，并通过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。