阿里云
VPN网关

产品简介

文档版本：20190626

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

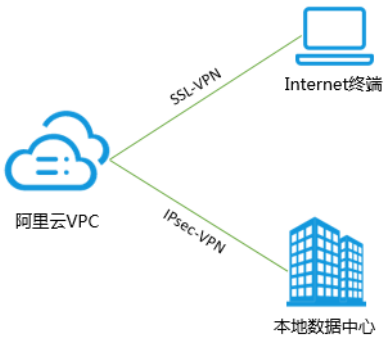
格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier 字体`	命令。	执行 `cd /d C:/windows` 命令，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 什么是VPN网关

VPN网关是一款基于Internet的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络（VPC）安全可靠的连接。VPN网关提供IPsec-VPN连接和SSL-VPN连接。

> **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Internet功能。



功能

VPN网关提供IPsec-VPN和SSL-VPN功能：

- IPsec-VPN

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

  您可以使用IPsec-VPN功能将本地数据中心与VPC或不同的VPC之间进行连接。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。

  详细信息，请参见建立VPC到本地数据中心的连接和建立VPC到VPC的连接。

- SSL-VPN

  您可以使用SSL-VPN功能从客户端远程接入VPC中部署的应用和服务。部署完成后，您仅需要在客户端中加载证书发起连接，即可实现远程接入。

  详细信息，请参见Linux客户端远程连接、Windows客户端远程连接和Mac客户端远程连接。

产品优势

VPN网关有以下优势：

- 安全：使用IKE和IPsec协议对传输数据进行加密，保证数据安全可靠。

- **高可用：采用双机热备架构，故障时秒级切换，保证会话不中断，业务无感知。**
- **成本低：基于Internet建立加密通道，比建立专线的成本更低。**
- **配置简单：开通即用，配置实时生效，快速完成部署。**

2 使用场景

VPN网关是一款基于Internet的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络（VPC）安全可靠的连接。VPN网关配置灵活，可满足不同的应用场景。

VPC到本地数据中心的连接

您可以通过IPsec-VPN将本地数据中心和VPC快速连接起来，构建混合云。

IPsec-VPN基于路由，不仅可以更方便的配置和维护VPN策略，而且还提供了灵活的流量路由方式。详细信息，请参见建立VPC到本地数据中心的连接。

> 说明:
> 建立VPC到本地数据中心的VPN连接要求本地数据中心的网络地址和VPC的网络地址不能冲突，并且本地数据中心的VPN网关必须配置一个静态公网IP。

VPC到VPC的连接

您可以通过IPsec-VPN将两个VPC快速连接起来，实现云上资源共享。

IPsec-VPN基于路由，不仅可以更方便的配置和维护VPN策略，而且还提供了灵活的流量路由方式。详细信息，请参见建立VPC到VPC的连接。

> 说明:
> 互连的两个VPC内的交换机的IP地址段不能冲突。

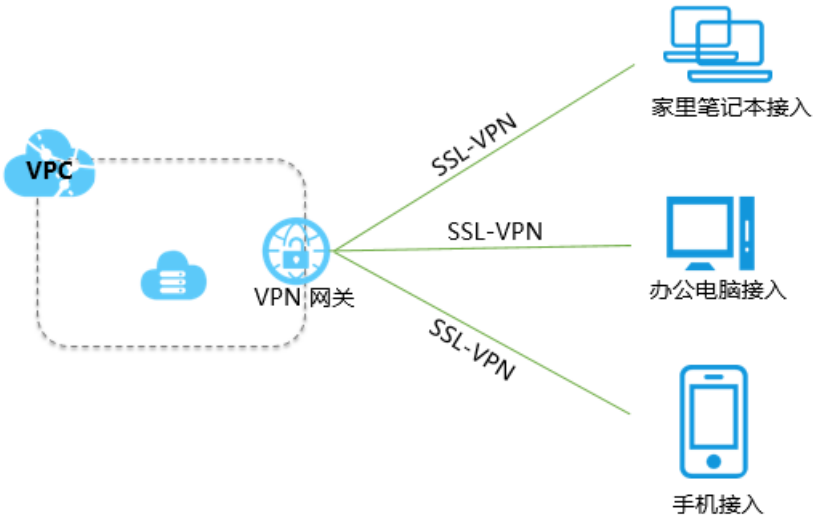
VPC到移动客户端的连接

您可以通过建立SSL-VPN隧道将单个移动客户端和VPC连接起来，满足远程办公的需要。无论何时何地，只要有Internet就可以安全地接入VPC。

SSL连接支持Windows、Linux、Mac、IOS和Android等操作系统多终端接入。

详细信息，请参见*Linux*客户端远程连接、*Windows*客户端远程连接和*Mac*客户端远程连接。

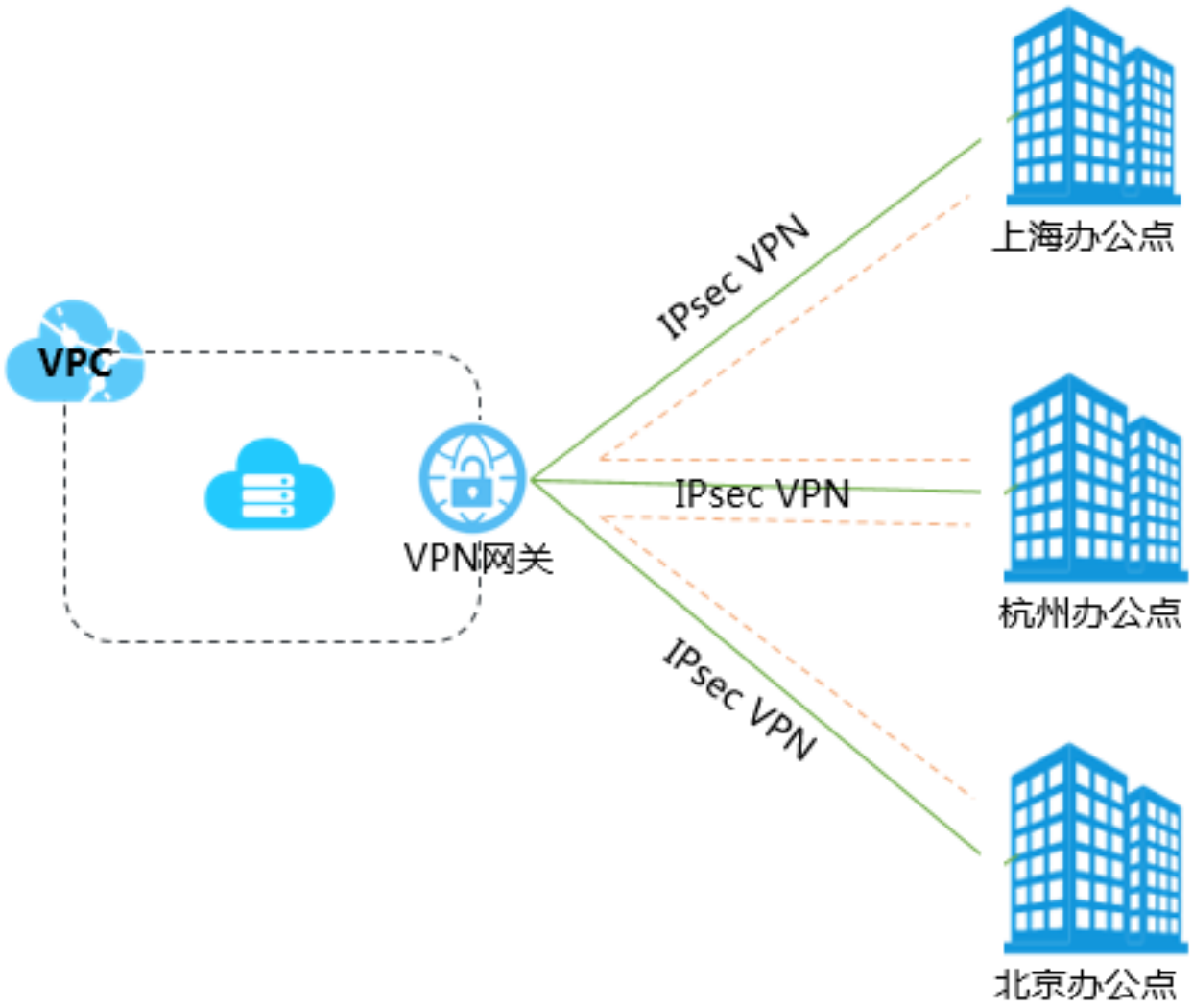
> **说明:**
> 分配给终端的IP地址段和专有网络交换机的地址段不能冲突。



Hub Spoke连接

您可以通过Hub Spoke功能在多个站点之间建立安全通信，使各个站点通过VPC网关实现互连。Hub Spoke可满足大型企业在各个办公点之间建立内网通信的需求。

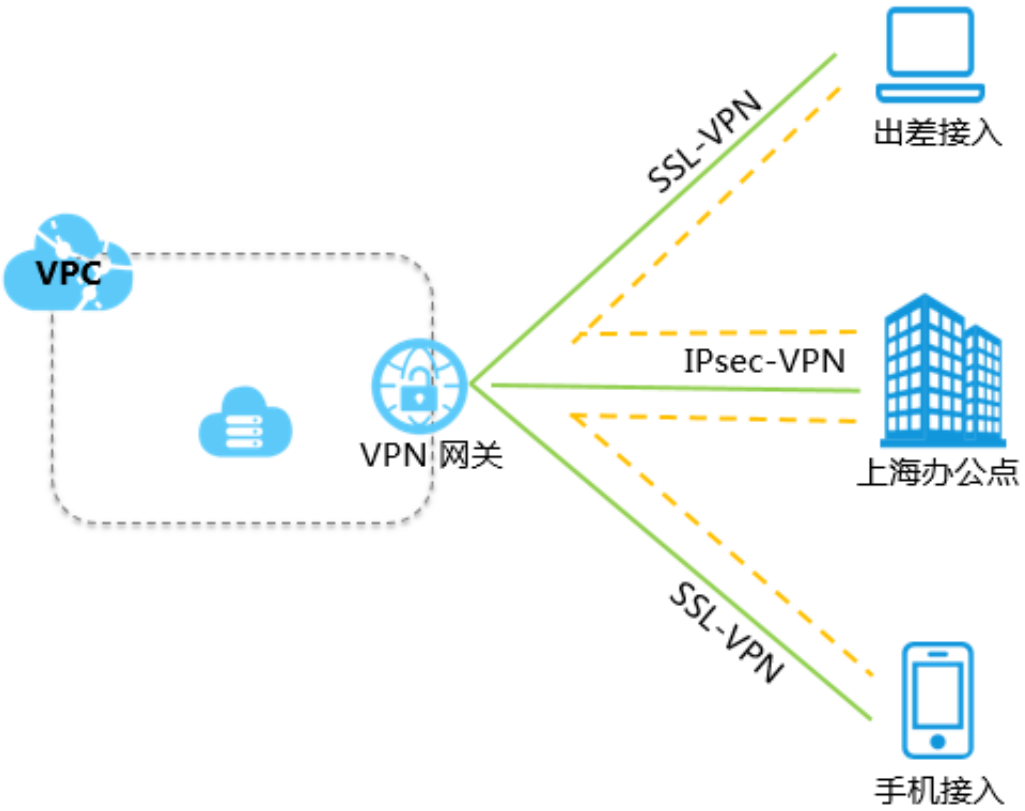
详细信息，请参见*Hub Spoke*连接。



IPsec-VPN和SSL-VPN组合使用

您可以组合使用IPsec-VPN和SSL-VPN，扩展网络拓扑。客户端接入后，不仅可以访问VPC，还可以访问接入的办公网络。

说明:
所有需要互通的私网IP地址段不能冲突。


VPC
VPN 网关
SSL-VPN
出差接入
IPsec-VPN
上海办公点
SSL-VPN
手机接入

3 使用限制

在使用VPN网关前，您需要了解以下限制。

资源	默认限制	提升配额
每个账号可创建的VPN网关数量	30	提交工单
每个账号可保有的SSL客户端证书的数量	50	提交工单
每个地域可创建的用户网关数量	100	无法调整
一个VPN网关可创建的IPsec连接的数量	10	提交工单
一个VPN网关可创建的策略路由的数量	20	提交工单
一个VPN网关可创建的目的路由的数量	20	提交工单
一个VPN网关可关联的SSL服务端的数量	1	无法调整
SSL服务端端口	不能使用以下端口： 22, 2222, 22222, 9000, 9001, 9002, 7505, 80, 443, 53, 68, 123, 4510, 4560, 500, 4500	无法调整
SSL客户端证书的有效期	三年	无法调整