

Alibaba Cloud

VPN网关 产品简介

文档版本：20211202

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> <code>Instance_ID</code>
[] 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>

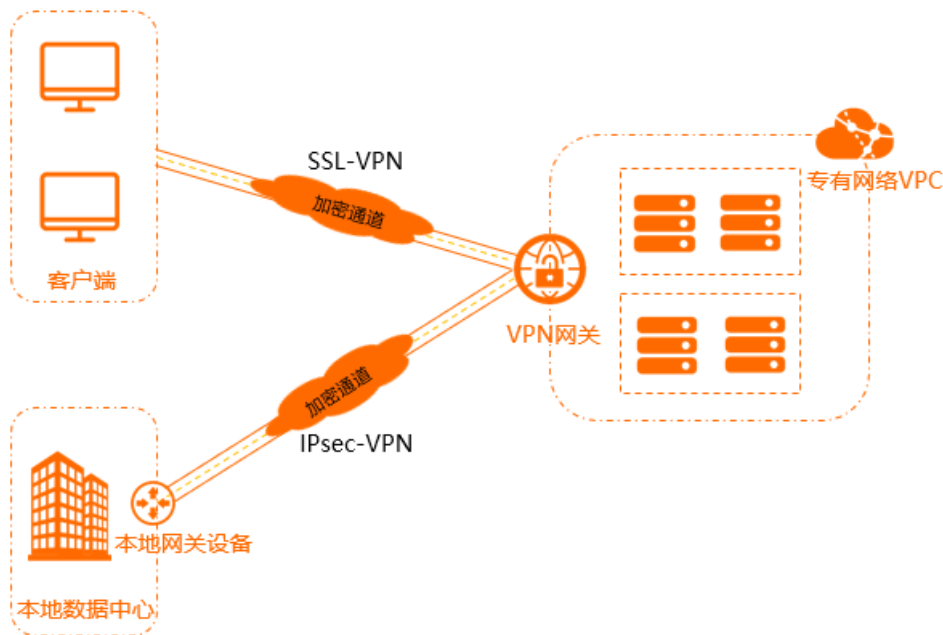
目录

1.什么是VPN网关	05
2.应用场景	07
3.使用限制	10

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，不提供访问互联网的功能。



功能特性

VPN网关提供IPsec-VPN连接和SSL-VPN连接：

- 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。

更多信息，请参见[IPsec-VPN入门概述](#)。

- 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。

更多信息，请参见[SSL-VPN入门概述](#)。

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，业务不受影响。
- 成本低：基于互联网建立加密通道，比建立专线的成本更低。

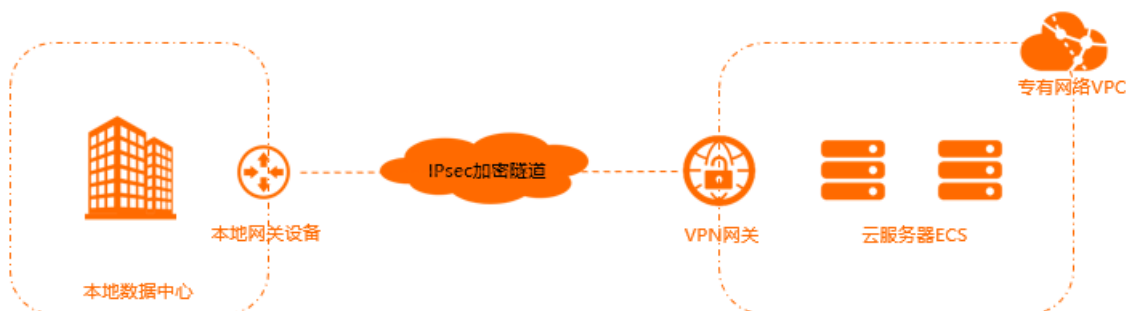
- 配置简单：开通即用，配置实时生效，快速完成部署。

2.应用场景

VPN网关是一款基于互联网的网络连接服务，通过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）之间安全可靠的连接。本文为您介绍VPN网关常见应用场景。

建立VPC与本地数据中心之间的连接

您可以通过IPsec-VPN将本地数据中心和VPC连接起来，构建混合云网络。具体操作，请参见[建立VPC到本地数据中心的连接](#)。



建立VPC与VPC之间的连接

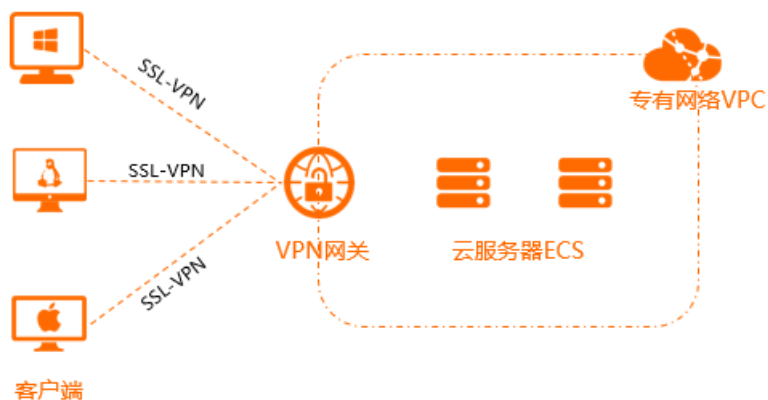
您可以通过IPsec-VPN将两个VPC快速连接起来，实现云上资源共享。具体操作，请参见[建立VPC到VPC的连接](#)。



建立VPC与客户端之间的连接

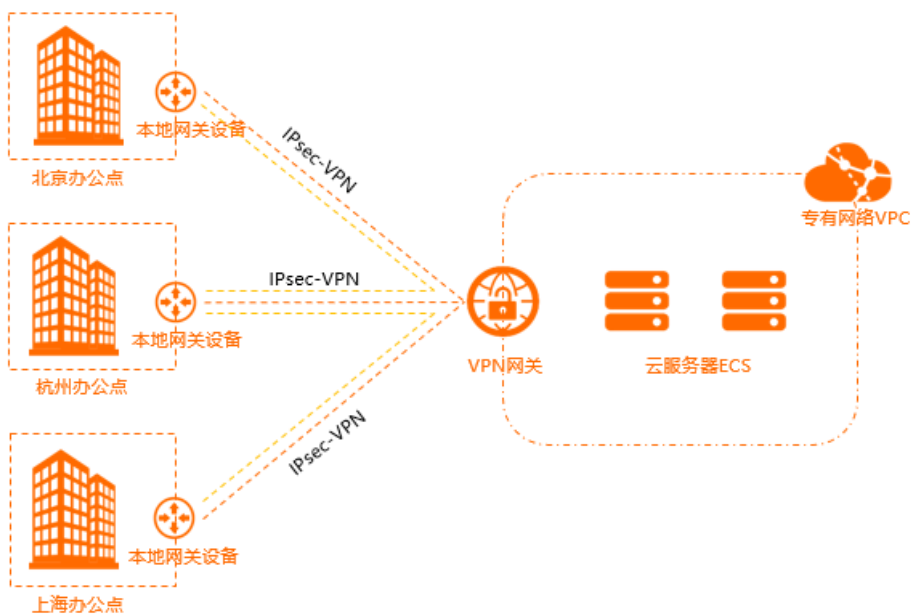
您可以通过SSL-VPN将客户端和VPC连接起来，客户端通过互联网可随时随地安全地连接VPC，满足您远程办公的需要。

SSL-VPN支持Windows、Linux、Mac、iOS和Android操作系统类型的客户端接入。具体操作，请参见[客户端远程连接VPC](#)。



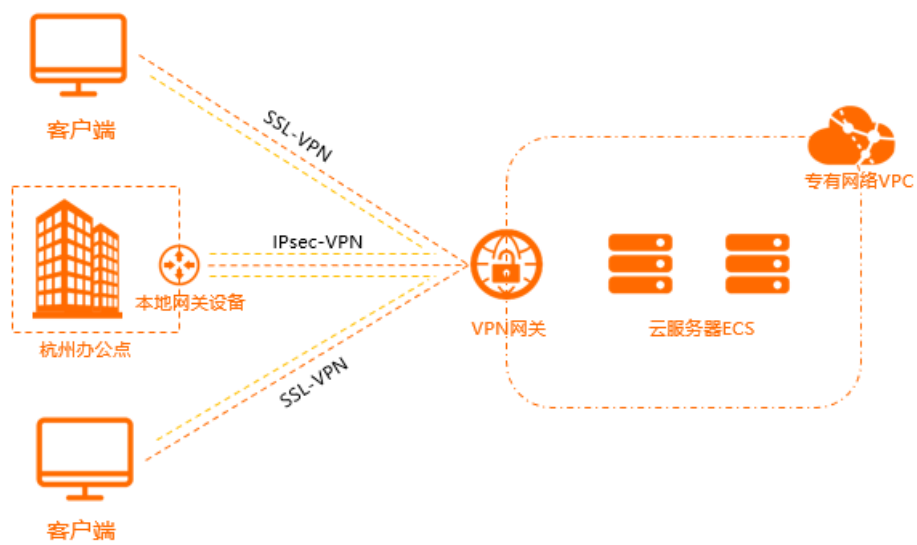
建立多个站点之间的连接

您可以使用IPsec-VPN将多个办公网络同时连接到VPN网关中，并通过VPN网关的Hub Spoke功能实现多个办公网络之间内网互通。具体操作，请参见[Hub Spoke连接](#)。



建立客户端和站点之间的连接

您可以组合使用IPsec-VPN和SSL-VPN同时连接办公网络和客户端。连接建立后，客户端和办公网络均可以访问VPC，且客户端和办公网络之间可以互相通信。



3.使用限制

本文介绍VPN网关产品的资源限制，以及如何申请更高配额。

实例限制

资源	默认限制	提升配额
一个阿里云账号支持创建的VPN网关实例个数	30  说明 VPN网关实例的个数仅受限于阿里云账号，与地域和专有网络VPC（Virtual Private Cloud）实例无关。 例如，在同一个阿里云账号下： - 如果您仅为一个地域下的一个VPC实例创建VPN网关，则默认您可以为该VPC实例创建最多30个VPN网关。 - 如果您需要为多个地域下的多个VPC实例创建VPN网关，则默认所有地域下VPC实例的VPN网关数量之和不能超过30个。	您可以前往 配额管理页面 自助提升配额。具体操作，请参见 管理配额 。
一个VPN网关实例支持创建的策略路由条目个数	20	
一个VPN网关实例支持创建的目的路由条目个数	20	
一个VPC实例支持添加的指向VPN网关实例的自定义路由条目个数	50	提交工单
一个VPN网关实例的BGP路由表支持的路由条目个数	50	提交工单

用户网关限制

资源	默认限制	提升配额
一个地域支持创建的用户网关实例个数	100	无法调整。

IPsec-VPN限制

资源	默认限制	提升配额
一个VPN网关实例支持创建的IPsec连接的个数	10	您可以前往 配额管理页面 自助提升配额。具体操作，请参见 管理配额 。
一个IPsec连接支持的最大带宽峰值	200 Mbps  说明 如果您的VPN网关实例的带宽峰值大于200 Mbps，您可以通过创建多个IPsec连接充分利用VPN网关实例的带宽。更多信息，请参见如何充分利用VPN网关带宽。	无法调整。
一个IPsec连接支持添加的本端网段个数	5	
一个IPsec连接支持添加的对端网段个数	5	

SSL-VPN限制

资源	默认限制	提升配额
一个阿里云账号支持创建的SSL客户端证书个数	50	您可以前往 配额管理页面 自助提升配额。具体操作，请参见 管理配额 。
一个VPN网关实例支持创建的SSL服务端的个数	1	无法调整。
一个SSL服务端支持添加的本端网段个数	5	
一个SSL服务端支持添加的对端网段个数	1	
SSL服务端不支持使用的端口	22、2222、22222、9000、9001、9002、7505、80、443、53、68、123、4510、4560、500、4500	
SSL客户端证书的有效期限	3年	