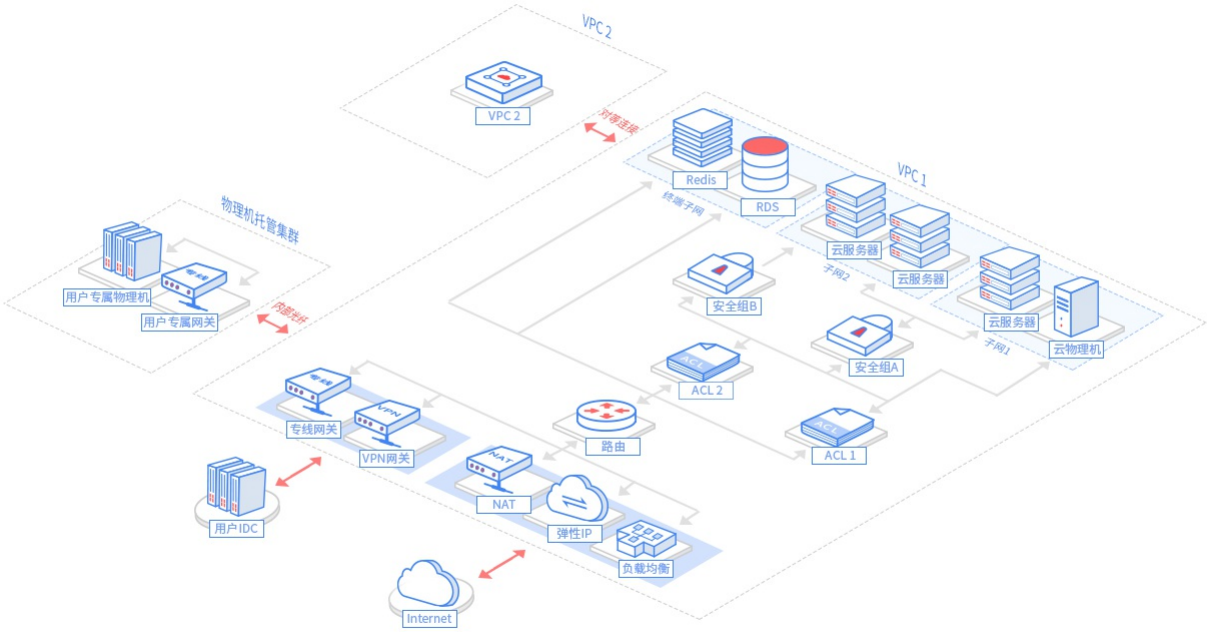
目录

产品概述

虚拟私有网络（Virtual Private Cloud，简称VPC）能帮助您在金山云中构建完全逻辑隔离，可自主掌控的专有网络，让您在自定义的虚拟网络中部署金山云各种服务，包括云服务器、裸金属服务器、负载均衡、云数据库等云服务资源。此外，您也可以通过专线/IPsec VPN等连接方式将VPC和您的已有数据中心一起构建混合云解决方案，实现平滑迁移上云。

产品架构



产品组成

虚拟私有网络至少由1个私网网段、路由、子网组成；

- **私网网段**：在创建虚拟私有网络和子网之前，需要指定虚拟私有网络使用的私网网段；推荐使用192.168.0.0/16、172.16.0.0/12、10.0.0.0/8等作为私网网段；

网段	说明
192.168.0.0/16~28	可用IP数量最多为65,532
10.0.0.0/8~28	可用IP数量最多为1,048,572
172.16.0.0/12~28	可用IP数量最多为16,777,212
自定义网段	除198.18.0.0/15，100.64.0.0/10，240.0.0.0/4，11.255.0.0/16，35.0.0.0/8，33.0.0.0/8及其子网外的自定义网段

- **子网**：一个虚拟私有网络由至少一个子网组成，虚拟私有网络内的云资源必须部署在子网内，子网的网段必须在虚拟私有网络的私有网段范围内。
  目前金山云子网有3种类型，不同类型的子网用于部署不同资源；
  - 云服务器子网：用于部署云服务器资源；
  - 裸金属服务器子网：用于部署裸金属服务器资源；
  - 终端子网：用户部署负载均衡、数据库、文件存储；
- **路由（路由表）**：用户在创建虚拟私有网络时，会默认创建子网相关的路由，以保证同一个虚拟私有网络下的所有子网互通。

高性能互联网访问

金山云VPC为您提供灵活、高性能的互联网连接方式，包括弹性IP、公网NAT。

连接方式	详述
弹性IP(EIP)	弹性IP（Elastic IP，简称EIP）是与用户账户相关联的IP地址，可以绑定到用户的任何一台云服务器、物理机或负载均衡上；拥有多种灵活的计费方式，可以满足各种业务场景的需求。
公网NAT	NAT（Network Address Translation)网络地址转换是一种将虚拟私有网络中内网IP 地址和公网IP地址进行转换的网关，能够让虚拟私有网络内无公网IP的云服务器或云物理主机访问互联网。NAT支持最大满足15Gbps流量。通过多机热备实现高可用，单机出故障自动切换，业务无感知。

稳定、可靠的用户数据中心连接

如果您希望构建企业的混合云部署，那么可以使用公网VPN/专线接入连接您的云上计算资源及本地数据中心。

- **VPN连接**是一种通过公网加密通道连接您IDC和金山云私有网络的方式。您可以在控制台创建私有网络的VPN网关、对端网关和支持IPsec加密协议的VPN通道，快速实现私有网络和您本地数据中心的安全通信，助力您快速部署混合云。
- **专线接入**是一种通过物理专线打通您的数据中心和虚拟私有网络，帮助您建立灵活、可靠的混合云网络连接。

云上资源灵活互通

您可以通过对等连接和基础网络互通实现私有网络内的资源与其它云资源的互通。

- **对等连接**是一种用于跨VPC网络数据同步的互联服务，打通对等连接的两个VPC之间就像同一个VPC网络一样。您可以实现同地域或跨地域的相同/不同账号的VPC互联，通过在两端配置路由策略，可以实现不同VPC的流量互通。对等连接不依赖某个独立硬件，因而不存在单点故障或带宽瓶颈。
- **基础网络互通**是指将基础网络内的云服务器关联至指定私有网络的服务，可以打通基础网络中的云服务器与私有网络之间的网络通信，实现内网资源平滑连接。

安全控制

您可以通过网络访问控制列表和安全组实现端口和实例维度的资源访问控制。帮助您提高云资源的安全性。

- **网络访问控制列表**（Access Control List，ACL）是一个子网级别的无状态安全规则，是一个可选安全层，可作为防火墙，以控制进出子网的数据流，可以精确到协议和端口维度。您可以设置网络 ACL，使其规则与您的安全组相似，以便为您的 VPC 添加额外安全层。
- **安全组**是一个实例级别的包过滤功能的虚拟防火墙，它用于设置单台或多台实例的网络访问控制。您可以将同一地域内具有相同网络安全隔离需求的云服务器实例加到同一个安全组内，通过网络策略对云服务器的出入流量进行安全过滤。

产品优势

软件定义

按需灵活自定义网络配置，自由定义网络划分、IP地址和路由策略，部署云主机、满足各种应用场景。以软件定义网络，节省设备及运维成本。

安全隔离

基于VXLAN隔离的私有网络，多租户间互不影响，通过网络ACL和安全组分别从子网和服务器维度控制网络访问，可以精确到协议和端口级粒度，多维度、全方位满足您网络安全需求。

高性能Internet访问

支持15Gbps带宽的多机热备NAT、弹性IP、负载均衡轻松帮您打破网络性能瓶颈。

互联互通

通过对等连接服务，您可以在一分钟内互联多地云资源，轻松实现两地三中心容灾部署。同时，通过跨账号对等连接，您还可与金山云上的其它合作伙伴实现数据互通，快速构建开放式云端生态。

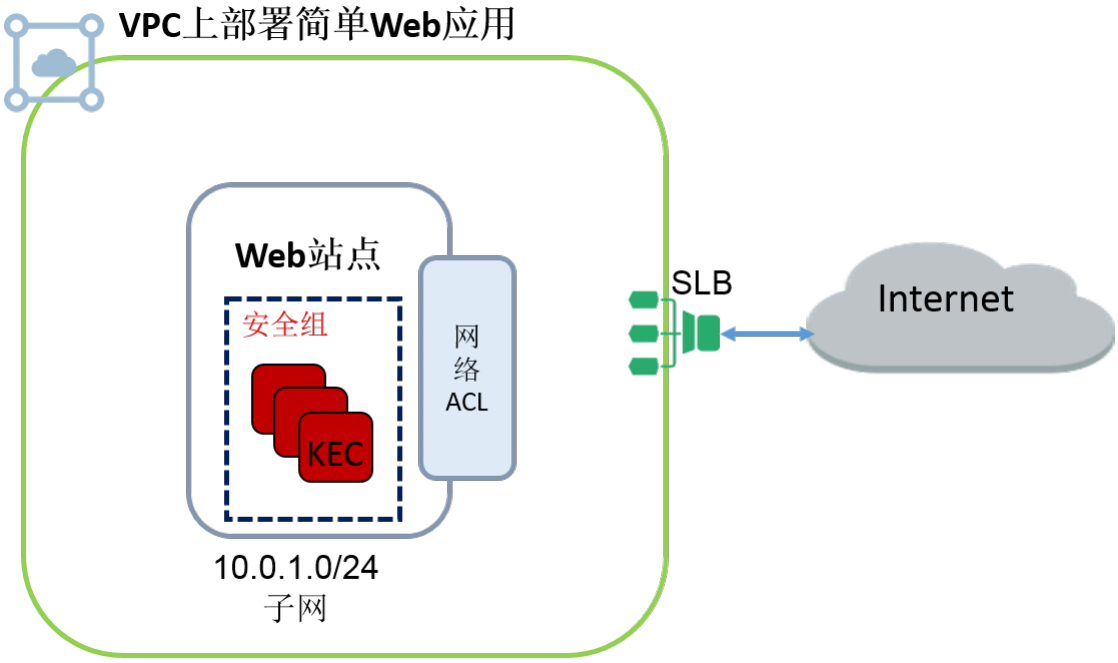
轻松构建混合云

稳定可靠的IPsec VPN/专线连接虚拟私有网络至您的数据中心，您可根据业务量弹性扩展应用程序的云服务器等资源，同时还支持物理机直接接入VPC，既降低了企业IT运维成本，又不用担心企业核心数据的扩散，轻松构建混合云。

使用场景

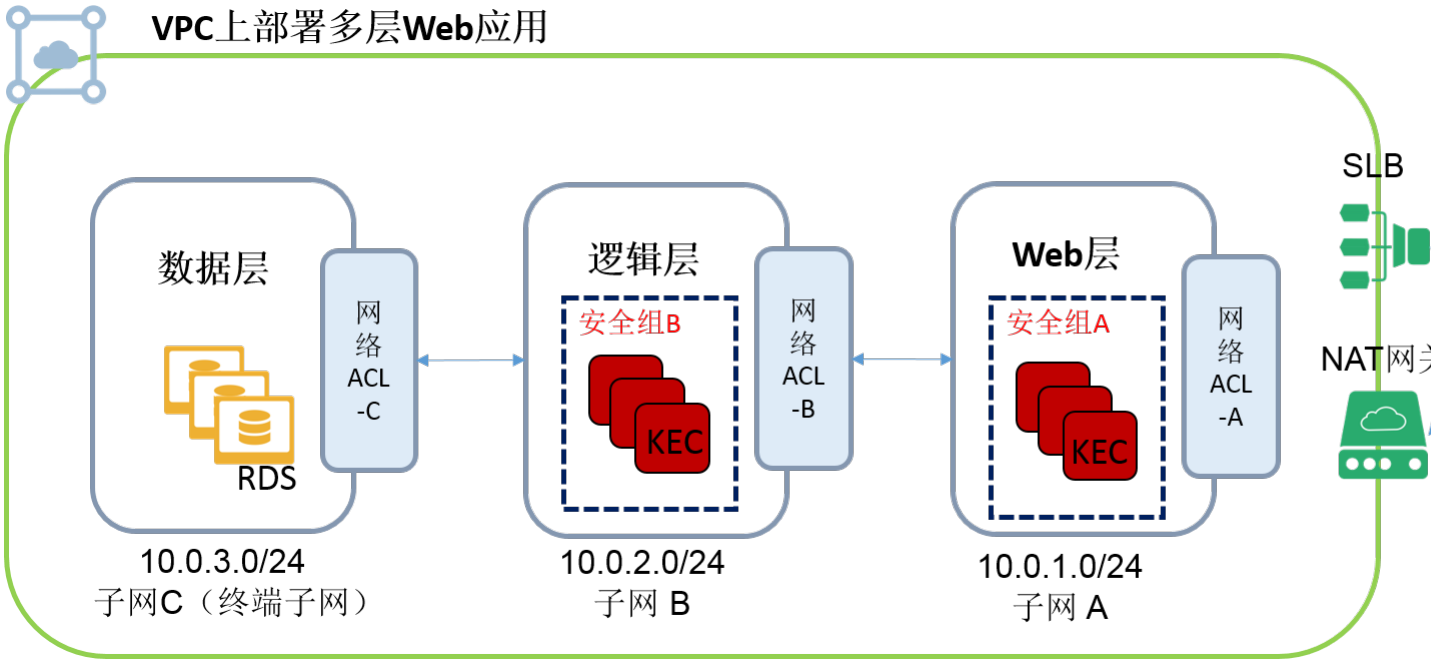
场景1 - 部署简单Web应用

私有网络可以用来部署简单Web应用网站，如博客,门户网站等。通过安全组和网络ACL等安全功能，您可以使web应用仅响应HTTP等请求，但拒绝web应用访问Internet，从而保证web应用的安全。另外在业务增长时，您还可以在VPC中启用负载均衡，部署数据库，缓存服务等，架构轻松平滑升级。



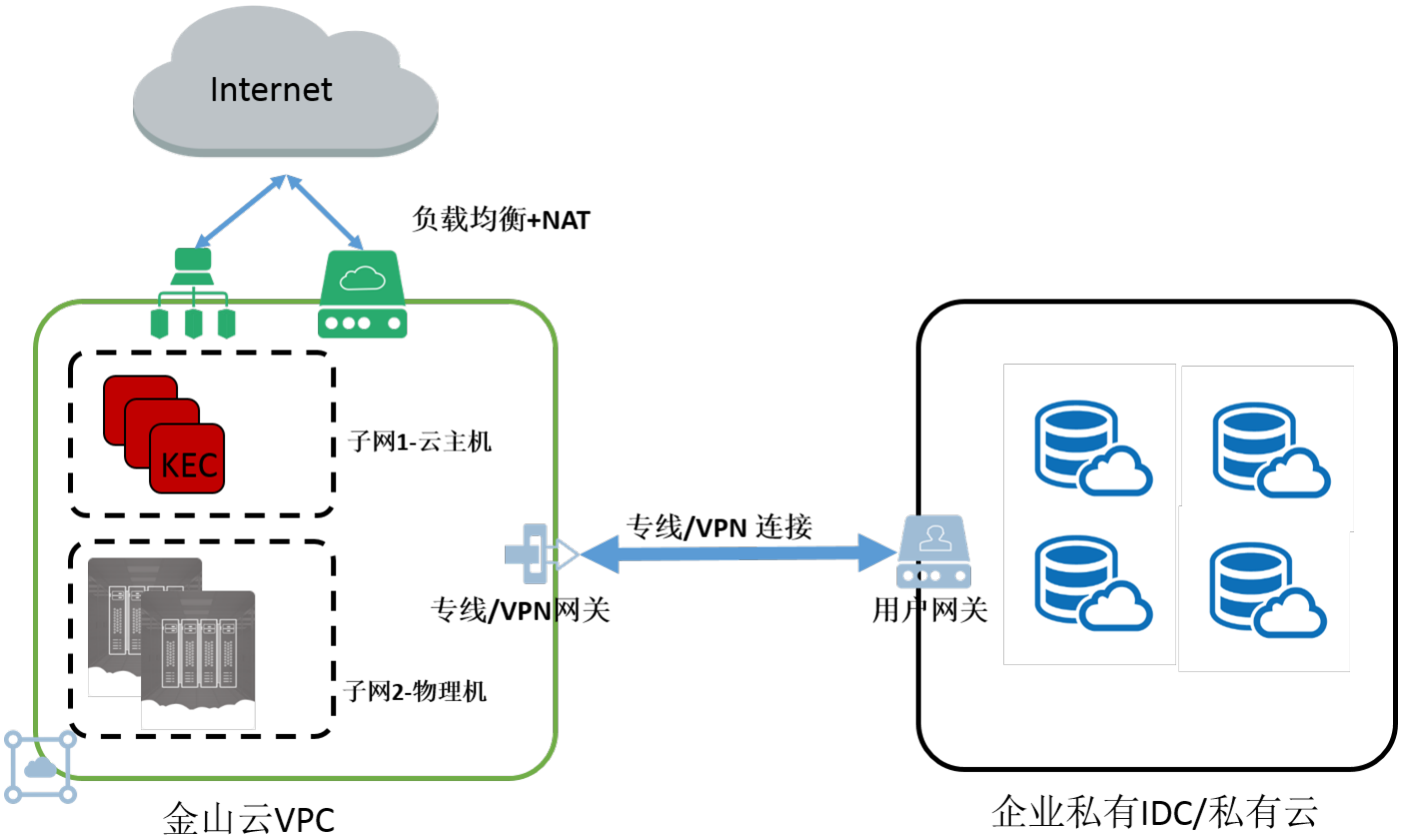
场景2 - 部署多层Web应用

您可以在私有网络内创建不同子网，Web层放在一个子网，通过配置负载均衡提供公网接入访问，通过配置NAT网关对公网出向访问；逻辑层单独放在一个子网，只能和Web层及数据层通信，数据层放在另外一个子网，只能和逻辑层通信，子网和子网之间的流量通过网络ACL进行控制。私有网络可以在给您的应用提供Internet服务的同时，又保障数据库服务器的安全，让您可以安全灵活地在VPC中部署多层Web应用程序。



场景3 - 部署混合云

您可以在私有网络内部署您的应用程序，在您的企业数据中心部署数据库服务器。金山云私有网络提供稳定安全的IPsec VPN 或者 专线接入 帮您打通企业数据中心与云端资源。通过云上资源的弹性扩展特性帮助您降低企业IT运维成本，同时又不用担心企业核心数据安全，轻松实现弹性灵活混合云部署。



名词解释

- 虚拟私有网络与子网
  - 地域（Region）
  - 可用区（Availability Zone）
  - 虚拟私有网络
  - 基础网络
  - 子网
  - 网段
  - 内网IP
  - 公网IP
  - 路由
- 访问互联网
  - 弹性IP
  - NAT（网络地址转换）
- 连接您的数据中心

虚拟私有网络与子网

地域（Region）

金山云不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。金山云会逐步增加区域和可用区供应以满足更多节点的覆盖。建议用户选择靠近您客户的地域，可降低访问时延、提高下载速度。

可用区（Availability Zone）

可用区（Availability Zone）是指金山云在同一地域内电力，网络，机房互相独立的物理数据中心。目标是能够保证可用区间故障相互隔离（大型灾害或者大型电力故障除外），不出现故障扩散，使得用户的业务持续在线服务。通过在多个可用区启动不同实例，用户可以保护应用程序不受单一位置故障的影响，实现同地域下高可用服务。

虚拟私有网络

虚拟私有网络（Virtual Private Cloud）能帮助您在金山云中构建完全逻辑隔离的网络空间，通过软件自定义网络，灵活的自定义网络、IP地址、路由、安全策略等。您在自定义的虚拟网络中可以部署金山云各种服务。包括：云服务器、物理机、负载均衡、云数据库等。您可以通过弹性IP、NAT灵活访问互联网，您也可以通过专线/VPN等连接方式将VPC和您的已有数据中心一起构建完美的混合云解决方案，实现平滑迁移上云。

基础网络

基础网络是金山云上所有用户的公共网络资源池，该资源池内云服务器内网 IP 地址由金山云统一分配。

子网

子网是从虚拟私有网络中划分的一块地址空间，您可以在子网中关联金山云的各种云服务，金山云子网分为三种。

- 云服务器子网 您可以在普通子网中关联云服务器。
- 终端子网 您可以在终端子网中关联RDS等业务。
- 裸金属服务器子网 您可以在物理机子网中关联裸金属服务器。

网段

网段由您指定的独立网络空间地址块，通过IP和掩码结合，实现对网络的整体划分。以10.1.0.0/16为例，斜杠左边为网络块的IP，斜杠右边为网络块的掩码。通过设定掩码的大小，可以调整网络块的大小设定。网络块包括的IP数 = 2^(32-掩码)，因而10.1.0.0/16网络块最多包含65536个IP地址。

内网IP

内网IP无法访问互联网，可以用于VPC内实例之间的通讯。

公网IP

公网IP地址可以访问互联网，全球唯一的IP地址。

路由

路由是网络流量所经过的途径规则，每条路由包含了三个参数：

- 目标网段：目的网段
- 下一跳类型：虚拟私有网络下一跳类型支持“互联网网关”、“主机路由”、“对等连接”、“专线网关”、“VPN通道”
- 下一跳：指定关联到该路由的流量具体跳转至哪个下一跳。

访问互联网

弹性IP

弹性IP（Elastic IP，EIP）是有带宽的公网IP地址，支持绑定和解绑。您可以与云服务器、物理机、负载均衡等进行绑定。实现云资源访问互联网。

NAT（网络地址转换）

NAT是通过网络地址转换，实现虚拟私有网络内的云服务器或物理机访问互联网功能。NAT支持最大满足15Gbps流量。通过多机热备实现高可用，单机出故障自动切换，业务无感知。

连接您的数据中心

用户IDC

用户数据中心(Internet Data Center，IDC)，是用户部署在金山云外的一整套IT设施。

IPsec

IPsec 是一个协议套件，通过验证和加密数据流的每个 IP 数据包来保护 互联网 协议 (IP) 通信安全。

IPsec VPN

IPsec VPN是一种通过公网加密通道连接您的IDC和虚拟私有网络的方式。

专线

专线是从用户IDC接入一条物理专线到金山云机房，实现IDC和虚拟私有网络的互通。

对等连接

对等连接是不同虚拟私有网络之间互通的连接，建立对等连接的虚拟私有网络内的云服务器、物理机等资源可以实现互通。

安全

网络ACL

网络访问控制列表（Access Control List，ACL）是一个子网级别的无状态安全规则。

安全组

安全组是一个云服务器级别的有状态安全规则。

VPC内可部署的服务

金山云 VPC 可以许多其他 金山云 服务集成，它们之间的关系如下表所示：

计算与网络服务

产品	与VPC的关系
云服务器 KEC	您可将云服务器部署在VPC中
裸金属服务器（星曜）	您可将裸金属服务器（星曜）部署在VPC中
专属宿主机 KDH	您可将专属宿主机部署在VPC中
GPU云服务器 GPUVM	您可将GPU云服务器部署在VPC中
GPU裸金属服务器 GPU	您可将GPU物理服务器部署在VPC中
负载均衡 SLB	您可以在虚拟私有网络内部署私网SLB或者公网SLB
网络地址转换 NAT	可用于虚拟私有网络内流量访问Internet
对等连接	可用于连接同地域/跨地域的私有网络
告警服务	为VPC内某些服务的关键指标提供异常告警

数据库服务

产品	与VPC的关系
云数据库Redis	您可在虚拟私有网络通过终端子网连接云数据库服务，该服务将占用终端子网IP
云数据库MongoDB	同上
关系型数据库KRDS	同上
云数据库Memcached	同上
金山云分布式数据库服务KDRDS	同上
分布式事务服务（KDTX）	同上