目录

第一步：新建VPN网关

1. 登录VPN网关控制台。
2. 选择对应的虚拟私有网络和需要的配置后，点击**立即购买**按钮进行后续支付操作。新建VPN网关成功后，系统会分配两个公网IP，用于VPN互联。

第二步：新建客户网关

1. 登录客户网关控制台。
2. 填写客户侧相关信息，客户侧公网IP用于和VPN网关的公网IP互联。

第三步：新建VPN通道

1. 登录VPN通道控制台。
2. 选择对应的VPN网关和客户网关，填写预共享密钥用于用于VPN两侧校验。

基本信息	配置项	说明
VPN网关	选择已创建的VPN网关，如果没有可新建。 北京、上海、广州机房支持VPN2.0网关；其他机房只支持VPN1.0网关。	
客户网关	选择已创建的客户网关，如果没有可新建。	
路由模式	VPN2.0网关，支持感兴趣流和目的路由；VPN1.0网关，默认只支持感兴趣流。	
高可用模式	一条VPN通道下两条VPN隧道的工作模式，包括负载和主备。负载模式下，两条隧道同时工作；主备模式下，主隧道发生故障，流量会自动切换至备用隧道。 - 目的路由：支持负载和主备。 - 感兴趣流：只支持负载。	
预共享密钥	预共享密钥是用于验证IPsec连接的Unicode 字符串，金山云侧和客户侧必须使用相同的预共享密钥。	
健康检查	用于检测主备VPN隧道健康情况，将流量切换至健康的通道。 说明：目的路由支持健康检查，感兴趣流不支持健康检查。	
健康检查方式	检查方式为NQA。	
重试间隔	3s	
重试次数	3次	
金山侧互联IP	目的路由模式下需要填写互联IP，感兴趣流模式无需填写。	
客户侧互联IP	目的路由模式下需要填写互联IP，感兴趣流模式无需填写。	

IKE配置

配置项	说明
版本	IKE V1
加密算法	身份加密算法 支持3des、aes、aes-cbc-192、aes-cbc-256、des、sm1-cbc-128
认证算法	身份认证算法 支持md5和sha
DH分组	指定IKE交换密钥时使用的DH组 支持DHGroup1、DHGroup2、DHGroup5、DHGroup14、DHGroup24，密钥交换的安全性随着DH组的扩大而增加，但交换的时间也会增加。

IPsec配置

配置项	说明
加密算法	身份加密算法 支持esp-3des、esp-aes、aes-cbc-192、aes-cbc-256、esp-des、esp-null

认证算法	身份认证算法 支持esp-sha-hmac、esp-md5-hmac、sha256、sha384、sha512、sm3
生存周期(s)	单位：秒
生存周期(KB)	单位：KB

第四步：配置本地网关设备

通过前面三步完成金山云侧的IPsec相关配置后，需要对客户侧本地网关设备进行配置。注意相关的配置信息要与金山侧VPN通道的配置保持一致。

第五步：配置VPN路由

VPN1.0网关

1. 登录路由控制台，点击新建路由。
2. 填写路由信息。
   - 虚拟私有网络：选择VPN网关关联的VPC。
   - 目标网段：填写客户侧的网段。
   - 下一跳：选择VPN通道。
   - VPN通道：选择创建的VPN通道。

VPN2.0网关

1. 登录路由控制台，点击新建路由。
2. 填写路由信息。
   - 虚拟私有网络：选择VPN网关关联的VPC。
   - 目标网段：填写客户侧的网段。
   - 下一跳：选择VPN网关
   - VPN网关：选择创建的VPN网关。
3. 填写VPN网关路由
   - 进入VPN控制台，点击VPN网关名称。
   - 点击路由页签。
   - 点击新建路由，填写路由信息
   - IP版本：支持IPv4。
   - 目标网段：如果下一跳类型为VPC，填写VPC的目标网段；如果下一跳类型为VPN通道，填写客户侧数据中心的目标网段。
   - 下一跳类型：选择VPN通道或VPC。
   - 下一跳：如果下一跳类型是VPN通道，选择对应的VPN通道；如果下一跳类型是VPC，下一跳置灰无需填写。

第六步：验证连通性

使用金山侧VPC 内的云服务器 ping 客户网关的公网IP，如果可以ping通代表VPC和客户数据中心间可正常通信。