

目 录

目录	1
产品简介	2
产品概述	2
组成部分	2
VPN网关	2
客户网关	2
VPN通道	2

产品简介

产品概述

VPN连接（VPN Connections）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。

组成部分

VPN连接由三个部分组成：VPN网关、客户网关、VPN通道

VPN网关

VPN网关是虚拟私有网络建立VPN连接的出口网关，与客户网关（客户IDC侧的IPsecVPN服务网关）配合使用，主要用于金山云虚拟私有网络和金山云外IDC之间建立安全可靠的加密网络通信。金山云VPN网关采用双机热备策略，单台故障时自动切换，不影响业务正常运行。

VPN网关根据带宽上限分为5种设置，分别为：5M、10M、20M、50M、100M、200M。您可以随时调整 VPN 网关带宽设置，即时生效。

VPN网关区分1.0和2.0版本。VPN2.0网关支持高可用，一台VPN网关设备发生故障，可以快速切换到另一台VPN网关设备。（感兴趣流不支持VPN网关高可用，目的路由支持VPN网关高可用，推荐使用目的路由模式）当前北京、上海、广州机房支持创建VPN2.0网关，其他机房仍只支持VPN1.0网关。

客户网关

客户网关是指客户IDC机房的IPsecVPN服务网关，客户网关需与金山云VPN网关配合使用，一个VPN网关可与多个客户网关建立加密的VPN网络通道。

VPN通道

VPN网关和客户网关建立后，即可建立VPN通道，用于虚拟私有网络和金山云外IDC之间的加密通信。当前VPN通道支持 IPsec和GreOverIPsec加密协议，可满足绝大多数 VPN 连接的需求。

每个 VPN 通道包括两条 VPN 隧道，两条VPN隧道互为负载和主备模式。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。

VPN 通道在运营商公网中运行，公网的网络阻塞、抖动会对VPN网络质量有影响，因此也无法提供 SLA 服务协议保障。如果业务对延时、抖动敏感，建议通过专线接入私有网络，更多内容可以查看专线接入服务。

金山云上的 VPN 通道在实现 IPsec 中使用 IKE（Internet Key Exchange，因特网密钥交换）协议来建立会话。IKE 具有一套自保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPsec 会话。