天翼云 3.0 • VPN

用户使用指南

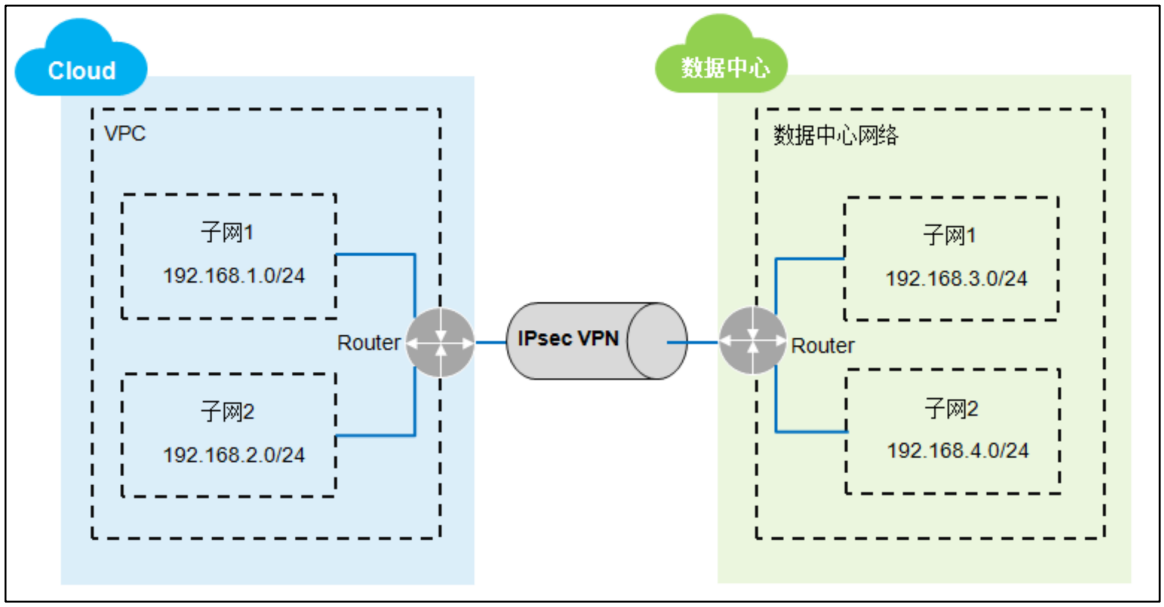
中国电信股份有限公司云计算分公司

目 录

1 产品定义

VPN 即虚拟专用网络，业务用于在远端用户和 VPC 之间建立一条安全加密的通信隧道，使远端用户通过 VPN 直接使用 VPC 中的业务资源。默认情况下，在 VPC 中的弹性云主机无法与您自己的数据中心或私有网络进行通信。如果您需要将 VPC 中的弹性云主机和您的数据中心或私有网络连通，可以启用 VPN 功能，目前支持 IPSec VPN。

IPSec VPN 是一种加密的隧道技术，通过使用加密的安全服务在不同的网络之间建立保密而安全的通讯隧道。假设您在云中已经申请了 VPC，并申请了 2 个子网（192.168.1.0/24, 192.168.2.0/24),您在自己的数据中心 Router 下也有 2 个子网(192.168.3.0/24, 192.168.4.0/24)。您可以通过 VPN 使 VPC 内的子网与数据中心的子网互相通信。



2 VPN 管理指南

2.1 申请 VPN

1. 注册并登录控制中心。
2. 在系统首页，单击【网络 > 虚拟私有云】，选择【VPN】选项。
3. 在【VPN】界面，单击【申请 VPN】。
4. 根据界面提示设置 VPN 相关信息，并单击【确定】。

图 2-1 申请 VPN

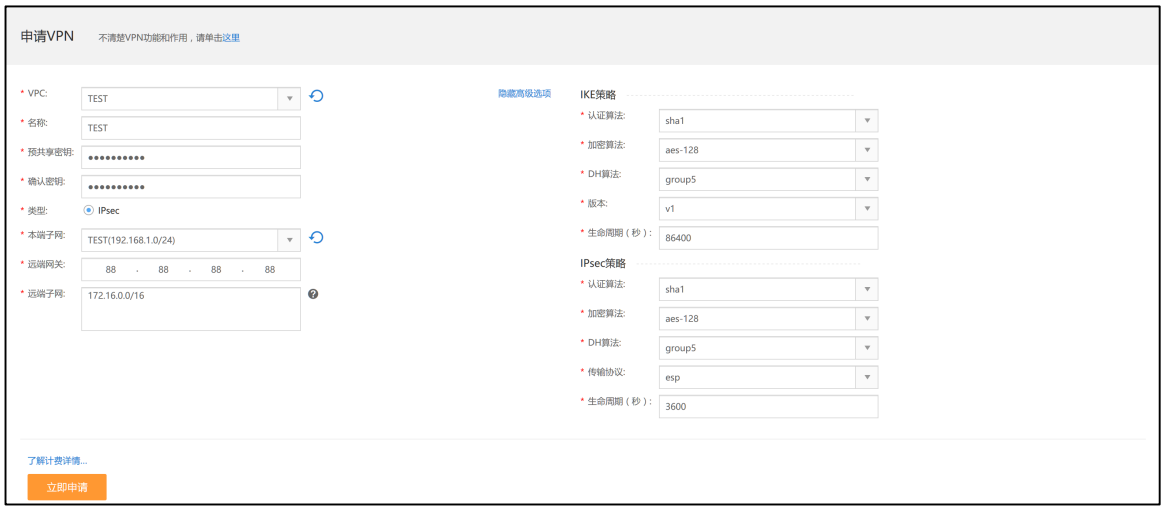


表 2-1 参数说明

参数	说明	取值样例
VPC	VPN 本端所属的 VPC。	TEST
名称	VPN 的名称。	TEST
预共享密钥/确认密钥	预共享密钥（Pre Shared Key），取值范围为 6～128 位。此项配置在本端 VPC 的 VPN 和对端的 VPN 中，配置需要完全一致。	-

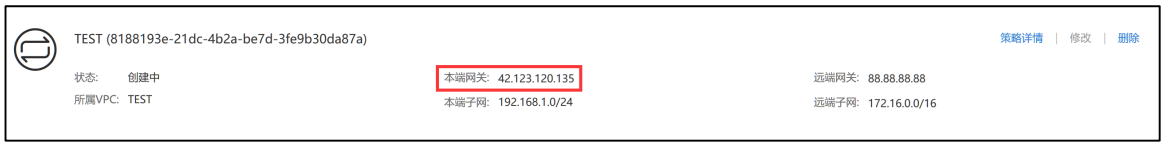
参数	说明	取值样例
类型	VPN 的类型，目前支持 IPSec。	IPSec
本端子网	本端 VPC 内需要与对端的网络互通的子网。需输入子网和掩码，多个子网使用逗号隔开。	TEST(192.168.1.0/24)
远端网关	对端网络中 VPN 的公网 IP 地址,用于与本端 VPC 内的 VPN 建立连接。	88.88.88.88
远端子网	对端网络中需要与本端 VPC 通信的子网地址。	172.16.0.0/16
认证算法（IKE 策略）	认证哈希算法，支持的算法：SHA1。	sha1
加密算法（IKE 策略）	支持的算法:AES-128,AES-192,AES-256,3DES。	aes-128
DH 算法（IKE 策略）	Diffie-Hellman 密钥交换算法，支持的算法：group2，group5，group14。	group5
版本（IKE 策略）	IKE 密钥交换协议版本，支持的版本：v1，v2。	v1
生命周期（IKE 策略）	安全联盟（SA—Secuity Associations）的生存时间，单位：秒。在超过生存时间后，安全联盟将被重新协商。	86400
认证算法（IPSec 策略）	认证算法，支持的算法：SHA1。	sha1
加密算法（IPSec 策略）	支持的算法:AES-128,AES-192,AES-256,3DES。	aes-128
DH 算法（IPSec 策略）	Diffie-Hellman 密钥交换算法，支持的算法：group2，group5，group14。	group5
传输协议（IPSec 策略）	IPSec 传输和封装用户数据时使用的安全协议，目前支持的协议：AH，ESP，AH-ESP。	esp
生命周期（IPSec 策略）	安全联盟（SA—Secuity Associations）的生存时间，单位：秒。在超过生存时间后，安全联盟将被重新协商。	3600

说明：IKE 策略指定了 IPSec 隧道在协商阶段的加密和认证算法，IPSec 策略指定了 IPSec 在数据传输阶段所使用的协议，加密以及认证算法；这些参数在本端 VPC 的 VPN 和对端网络的 VPN 中需要进行相同的配置，否则会导致 VPN 无法建立连接。

5. VPN 参数配置完成后，单击【立即申请】，确认资源详情配置无误后，阅读并勾选同意《虚拟私有云服务协议》，单击【确认申请】。VPN 创建成功后，该 VPN 会被分配一个公网 IP，如下图中

标红的参数，在对端网络 VPN 配置隧道时，远端网关需要配置为该 IP 地址（示例为 42.123.120.135）。

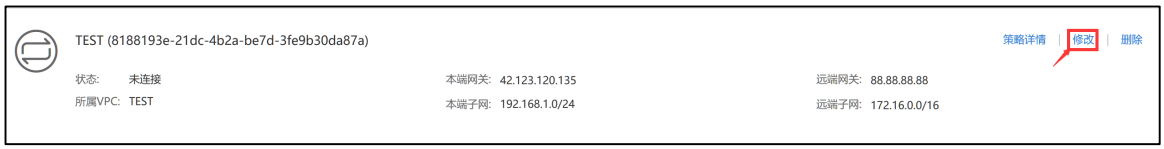
图 2-2 本端 VPN 公网 IP



2.2 修改 VPN 配置信息

1. 在【VPN】界面找到所需修改的 VPN，单击其所在行右侧的【修改】。

图 2-3 修改 VPN



2. 在修改界面对 VPN 参数进行修改，修改完成后单击【确定】。

图 2-4 修改 VPN 参数

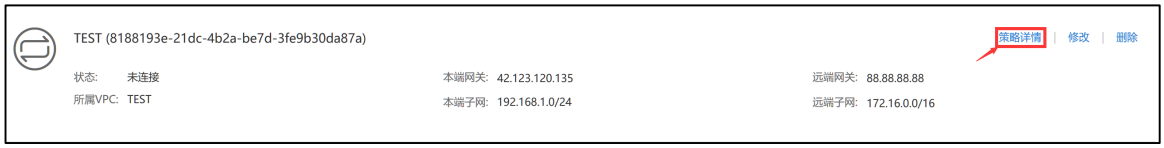
表 2-2 参数说明

参数	说明	取值样例
VPC	VPN 本端所属的 VPC（不可修改）。	TEST
名称	修改后的 VPN 名称。	TEST-1
本端网关	本端 VPN 网关的公网 IP（不可修改）。	42.123.120.135
本端子网	本端 VPC 内需要与对端的网络互通的子网。通过下拉菜单选择修改本端子网（可多选）。	subnet-ca92(192.168.0.0/24)
类型	VPN 的类型，目前支持 IPSec。	IPSec
远端网关	对端网络中 VPN 的公网 IP 地址，用于与本端 VPC 内的 VPN 建立连接，在对端更换其网关公网 IP 地址后，需要本端手动配置修改。	8.8.8.8
远端子网	对端网络中需要与本端 VPC 通信的子网地址，在对端需要通信的子网发生变更后，需要本端手动修改子网和掩码，多个子网使用逗号隔开。	192.168.10.0/24
预共享密钥/确认密钥	勾选预共享密钥选择框后，可对密钥进行修改。	-

2.3 查看 VPN 策略详情

1. 在【VPN】界面找到所需查看的 VPN，单击其所在行右侧的【策略详情】。

图 2-5 删除 VPN



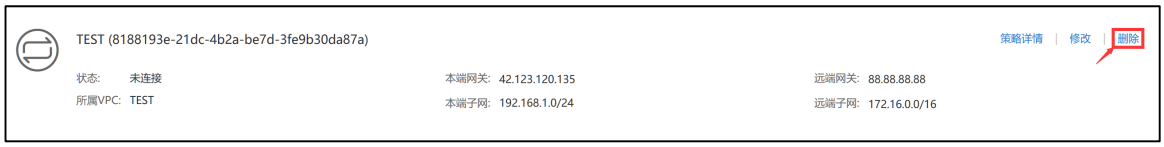
2. 在【策略详情】界面可以查看已配置的 IKE 策略和 IPSec 策略，不可对这些策略修改，可作为对端 VPN 网关配置相关策略的参考。

图 2-6VPN 策略详情

2.4 删除 VPN

1. 在【VPN】界面找到所需删除的 VPN，单击其所在行右侧的【删除】。

图 2-7 删除 VPN



2. 在删除界面确认删除信息，并单击【确定】。

图 2-8 确定删除 VPN

3 常见问题

3.1 每个用户可申请多少个 VPN？

在默认情况下，每个用户最多可申请 5 个 VPN，如果无法满足需求，可以提工单申请扩大配额。

3.2 VPN 是否收费？

目前处于公测阶段，提供免费服务。

3.3 使用 VPN 时，两端的子网网段可以相同吗？

不可以。

3.4 VPN 能否支持跨地域的 VPC 内网互通？

不支持。

3.5 是否可以通过 VPN 网关访问 Internet？

不可以，VPN 网关仅提供私网接入 VPC 功能，不提供 Internet 访问。