



虚拟专用网络

用户使用指南

天翼云科技有限公司

目录

1 简介	3
1.1 什么是虚拟专用网络	3
1.2 应用场景	4
1.3 参考标准和协议	5
1.4 基本概念	6
1.4.1 IPSec VPN	6
2 入门	7
2.1 流程简介	7
2.2 创建虚拟私有云基本信息及默认子网（可选）	8
2.3 为虚拟私有云创建新的子网（可选）	11
2.4 申请 VPN	13
2.5 创建 VPN 网关	19
2.6 创建 VPN 连接	20
2.7 配置安全组策略（可选）	23
2.7.1 创建安全组	23
2.7.2 添加安全组规则	24
3 管理	26
3.1 查看已申请 VPN	26
3.2 修改已申请 VPN	27
3.3 删除 VPN	27
3.4 关于配额	27
4 最佳实践	28
4.1 通过 VPN 连接 VPC.....	28
5 常见问题	30
5.1 一个用户下支持多少个 IPSec VPN?	30
5.2 IPSec VPN 是否会自动进行协商?	30
5.3 如何解决无法建立连接问题?	30
5.4 VPN 建立后您的数据中心或局域网无法访问弹性云服务器?	31
5.5 VPN 连接建立后，弹性云服务器无法访问您的数据中心或局域网?	31
5.6 VPN 支持将两个 VPC 互连吗?	31
5.7 VPN 本端子网和远端子网数量有什么限制?	31
5.8 为什么 VPN 创建成功后状态显示未连接?	31
5.9 VPN 配置下发后，多久能够生效?	32
5.10 如何配置 VPN 对端设备?（HUAWEI USG6600 配置示例）	32
5.11 对端 VPN 设备支持列表?.....	34

5.12 无法连接或网速慢如何排查?	34
5.13 虚拟专用网络是否支持 SSL VPN?	34
A 修订记录	35

1 简介

1.1 什么是虚拟专用网络

产品概述

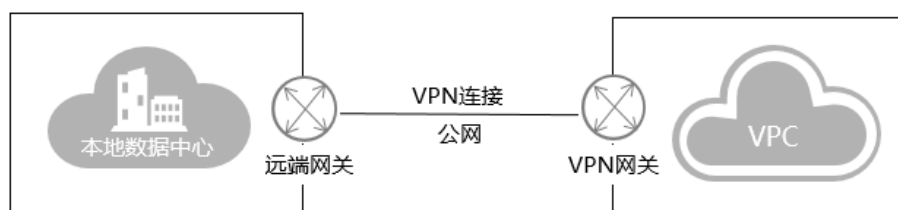
虚拟专用网络（Virtual Private Network，以下简称 VPN），用于在远端用户和虚拟私有云（Virtual Private Cloud，以下简称 VPC）之间建立一条安全加密的公网通信隧道。当您作为远端用户需要访问 VPC 的业务资源时，您可以通过 VPN 连通 VPC。

默认情况下，在虚拟私有云(VPC) 中的弹性云服务器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 中的弹性云服务器和您的数据中心或私有网络连通，可以启用 VPN 功能。

VPN 由 VPN 网关和 VPN 连接组成，VPN 网关提供了虚拟私有云的公网出口，与用户本地数据中心侧的远端网关对应。VPN 连接则通过公网加密技术，将 VPN 网关与远端网关关联，使本地数据中心与虚拟私有云通信，更快速、安全的构建混合云环境。

VPN 组网图如图 1-1 所示。

图1-1 VPN 组网图



组成部分

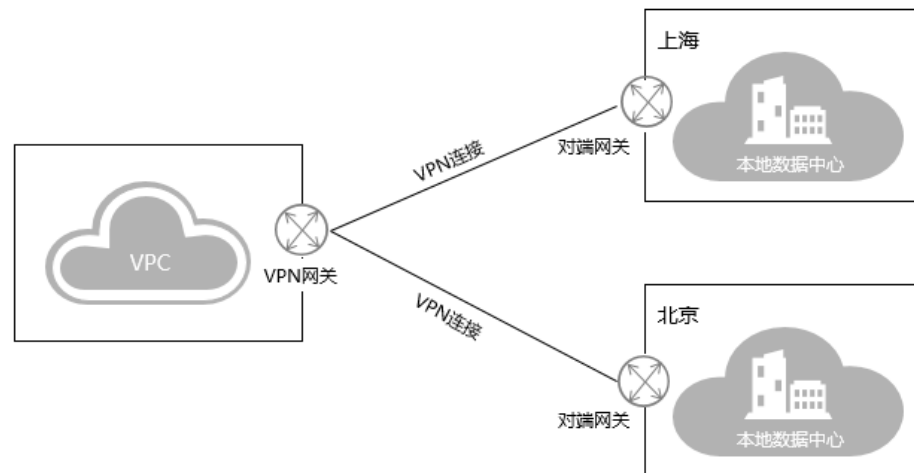
- **VPN 网关**

VPN 网关是虚拟私有云中建立的出口网关设备，通过 VPN 网关可建立虚拟私有云和企业数据中心或其它区域 VPC 之间的安全可靠的加密通信。

VPN 网关需要与用户本地数据中心的远端网关配合使用，一个本地数据中心绑定一个远端网关，一个虚拟私有云绑定一个 VPN 网关。VPN 支持点到点或点到多点连接，所以，VPN 网关与远端网关为一对一或一对多的关系。

VPN 网关如图 1-2 所示。

图1-2 组网拓扑



- **VPN 连接**

VPN 连接是一种基于 Internet 的 IPsec 加密技术，帮您快速构建 VPN 网关和用户本地数据中心的远端网关之间的安全、可靠的加密通道。当前 VPN 连接支持 IPsec VPN 协议。

VPN 连接使用 IKE 和 IPsec 协议对传输数据进行加密，保证数据安全可靠，并且 VPN 连接使用的是公网技术，更加节约成本。

1.2 应用场景

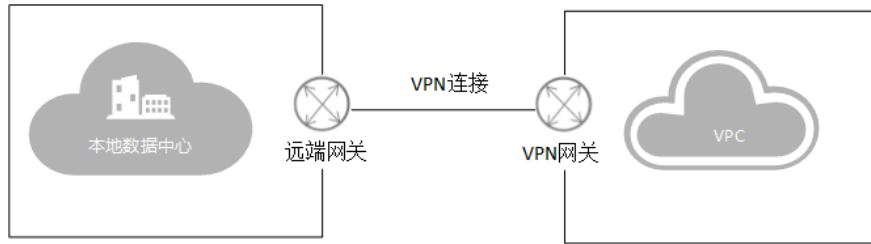
通过 VPN 在传统数据中心与 VPC 之间建立通信隧道，您可方便地使用云平台的云服务器、块存储等资源；应用程序转移到云中、启动额外的 Web 服务器、增加网络的计算容量，从而实现企业的混合云架构，既降低了企业 IT 运维成本，又不用担心企业核心数据的扩散。

VPN 支持站点到站点的连接和多站点连接。

单站点 VPN 连接

您可以通过建立 VPN 将本地数据中心和 VPC 快速连接起来，构建混合云。如图 1-3 所示。

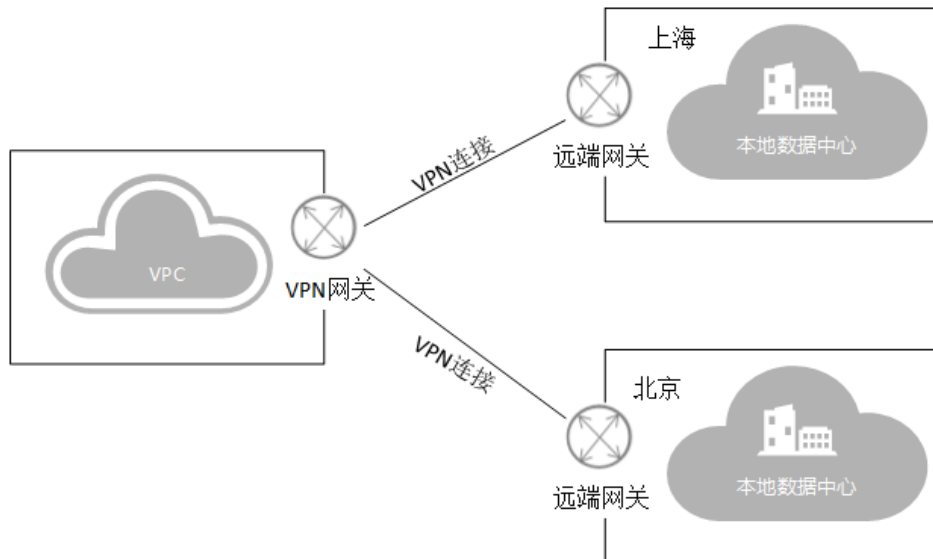
图1-3 单站点连接



多站点 VPN 连接

您可以通过建立 VPN 将多个本地数据中心和 VPC 快速连接起来，构建混合云。如图 1-4 所示。

图1-4 多站点连接



说明

建立多站点 VPN 连接要求各个站点之间的子网网段不能冲突。

1.3 参考标准和协议

与 IPSec 特性相关的参考标准与协议如下：

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2857: The Use of HMAC-RIPEND-160-96 within ESP and AH

- RFC 3566: The AES-XCBC-MAC-96 Algorithm and its use with IPsec
- RFC 3625: More Modular Exponential (MODP)Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748: Extensible Authentication Protocol(EAP)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2)Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4322: Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4359: The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2)
- RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2)

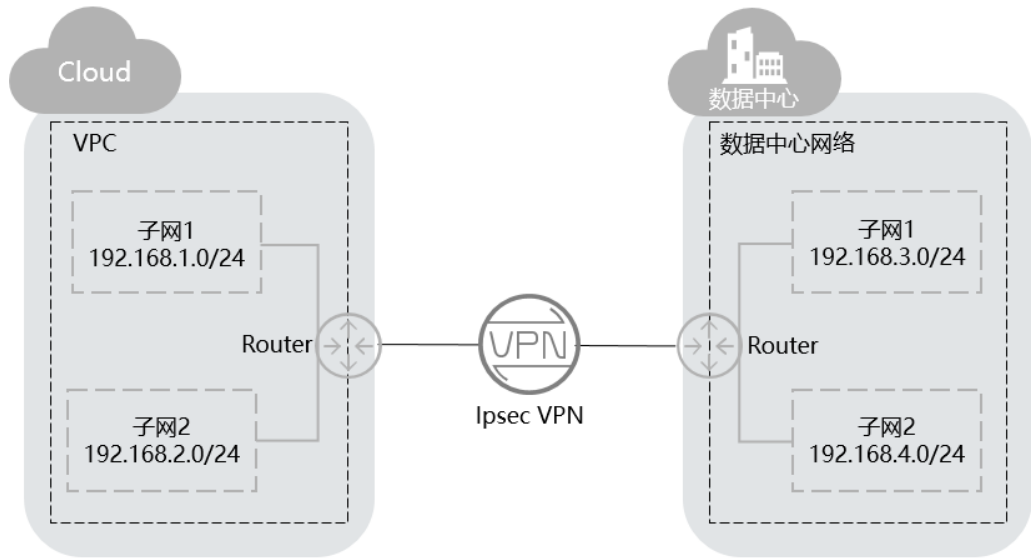
1.4 基本概念

1.4.1 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。

如图 1-5 所示，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。

图1-5 IPsec VPN



目前我们支持点到点 VPN（Site-to-Site VPN）和点到多点 VPN（Hub-Spoke VPN），需要您在自己的数据中心内也搭建 VPN。

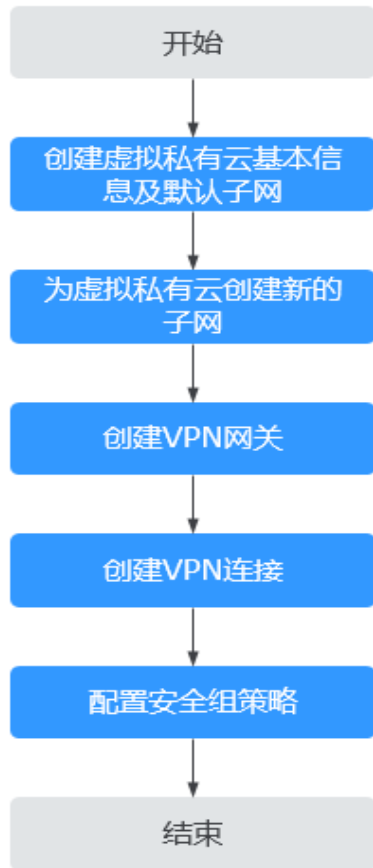
VPC 内的 VPN 和您搭建的 VPN，需要保证 IKE 策略以及 IPsec 策略配置一致。在配置前，请确认您的设备满足 IPsec 的相关标准协议。

2 入门

2.1 流程简介

默认情况下，在 Virtual Private Cloud (VPC) 中的弹性云服务器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 中的弹性云服务器和您的数据中心或私有网络连通，可以启用虚拟专用网络（VPN）功能。

图2-1 虚拟专用网络入门流程图



2.2 创建虚拟私有云基本信息及默认子网（可选）

操作场景

虚拟私有云可以为您的弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。

要拥有一个完整的虚拟私有云，第一步请参考本章节任务创建虚拟私有云的基本信息及默认子网；然后再根据您的实际网络需求，参考后续章节继续创建子网、申请弹性IP、安全组等网络资源。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 单击“创建虚拟私有云”。
4. 在“创建虚拟私有云”页面，根据界面提示配置虚拟私有云参数。

创建虚拟私有云时会同时创建一个默认子网，您还可以单击“添加子网”创建多个子网。

单击“自定义配置”，配置子网的高级参数。

表2-1 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
名称	VPC 名称。 名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。	VPC-001
网段（IPv4 网段）	VPC 的地址范围，VPC 内的子网地址必须在 VPC 的地址范围内。 目前支持网段范围： 10.0.0.0/8~24 172.16.0.0/12~24 192.168.0.0/16~24	192.168.0.0/16
标签	虚拟私有云的标识，包括键和值。可以为虚拟私有云创建 10 个标签。 标签的命名规则请参见表 2-3。	<ul style="list-style-type: none"> • 键：vpc_key1 • 值：vpc-01

表2-2 子网参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。	Subnet
子网网段	子网的地址范围，需要在 VPC 的地址范围内。	192.168.0.0/24
子网 IPv4 网段	子网的地址范围，需要在 VPC 的地址范围内。 已申请 IPv6 公测的用户显示此配置项。	192.168.0.0/24

参数	说明	取值样例
子网 IPv6 网段	选择是否勾选开启 IPv6。 已申请 IPv6 公测的用户显示此配置项。开启 IPv6 功能后，将自动为子网分配 IPv6 网段，暂不支持自定义设置 IPv6 网段。该功能一旦开启，将不能关闭。	-
高级配置	单击下拉箭头，可配置子网的高级参数，包括网关、DNS 服务器地址等。	默认配置
网关	子网的网关。 通向其他子网的 IP 地址，用于实现与其他子网的通信。	192.168.0.1
DNS 服务器地址	默认配置了 2 个 DNS 服务器地址，您可以根据需要修改。多个 IP 地址以英文逗号隔开。	100.125.x.x
DHCP 租约时间	DHCP 租约时间是指 DHCP 服务器自动分配给客户端的 IP 地址的使用期限。超过租约时间，IP 地址将被收回，需要重新分配。单位：天。 DHCP 租约时间改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。	365
标签	子网的标识，包括键和值。可以为子网创建 10 个标签。 标签的命名规则请参见表 2-4。	<ul style="list-style-type: none"> • 键：subnet_key1 • 值：subnet-01

表2-3 虚拟私有云标签命名规则

参数	规则	样例
键	<ul style="list-style-type: none"> • 不能为空。 • 对于同一虚拟私有云键值唯一。 • 长度不超过 36 个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。 	vpc_key1
值	<ul style="list-style-type: none"> • 长度不超过 43 个字符。 • 由英文字母、数字、下划线、点、中划线、中文字符组 	vpc-01

参数	规则	样例
	成。	

表2-4 子网标签命名规则

参数	规则	样例
键	<ul style="list-style-type: none"> 不能为空。 对于同一子网键值唯一。 长度不超过 36 个字符。 由英文字母、数字、下划线、中划线、中文字符组成。 	subnet_key1
值	<ul style="list-style-type: none"> 长度不超过 43 个字符。 由英文字母、数字、下划线、点、中划线、中文字符组成。 	subnet-01

5. 检查当前配置，单击“立即创建”。

2.3 为虚拟私有云创建新的子网（可选）

操作场景

申请 VPC 时会创建默认子网，当默认子网不能满足需求时，您可以创建新的子网。

子网默认配置 DHCP 协议，即使用该 VPC 的弹性云服务器启动后，会通过 DHCP 协议自动获取到 IP 地址。

说明

当前在部分区域中，子网与虚拟私有云已解耦，解耦后子网入口迁移，目前存在以下两种入口。

- 在虚拟私有云详情页的“子网”页签，可对子网进行操作。本小节的操作步骤指导以此入口为例。
- 在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“子网”，可对子网进行操作。

操作步骤

- 登录管理控制台。
- 在系统首页，选择“网络 > 虚拟私有云”。
- 在左侧导航栏选择“虚拟私有云”。
- 在虚拟私有云列表中，单击需要创建子网的虚拟私有云名称。
- 在“子网”页签中，单击“创建子网”。

6. 根据界面提示配置参数。

表2-5 参数说明

参数	说明	取值样例
虚拟私有云	选择待创建子网的 VPC。 当“子网”独立存在于导航栏时，本参数可见。	-
名称	子网的名称。 名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。	Subnet
子网网段	子网的地址范围，需要在 VPC 的地址范围内。	192.168.0.0/24
子网 IPv4 网段	子网的地址范围，需要在 VPC 的地址范围内。 已申请 IPv6 公测的用户显示此配置项。	192.168.0.0/24
子网 IPv6 网段	选择是否勾选开启 IPv6。 已申请 IPv6 公测的用户显示此配置项。开启 IPv6 功能后，将自动为子网分配 IPv6 网段，暂不支持自定义设置 IPv6 网段。该功能一旦开启，将不能关闭。	-
高级配置	单击下拉箭头，可配置子网的高级参数，包括网关、DNS 服务器地址等。	默认配置
网关	子网的网关。	192.168.0.1
DNS 服务器地址	默认配置了 2 个 DNS 服务器地址，您可以根据需要修改。多个 IP 地址以英文逗号隔开。	100.125.x.x
DHCP 租约时间	DHCP 租约时间是指 DHCP 服务器自动分配给客户端的 IP 地址的使用期限。超过租约时间，IP 地址将被收回，需要重新分配。单位：天。 DHCP 租约时间改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。	365
标签	子网的标识，包括键和值。可以为子网创建 10 个标签。 标签的命名规则请参考表 2-6。	<ul style="list-style-type: none"> • 键：subnet_key1 • 值：subnet-01
描述	子网的描述信息，非必填项。 描述信息内容不能超过 255 个字符，且不能包	-

参数	说明	取值样例
	含“<”和“>”。	

表2-6 子网标签命名规则

参数	规则	样例
键	<ul style="list-style-type: none"> 不能为空。 对于同一子网键值唯一。 长度不超过 36 个字符。 由英文字母、数字、下划线、中划线、中文字符组成。 	subnet_key1
值	<ul style="list-style-type: none"> 长度不超过 43 个字符。 由英文字母、数字、下划线、点、中划线、中文字符组成。 	subnet-01

7. 单击“确定”。

注意事项

子网创建成功后，有 5 个系统保留地址您不能使用。以 192.168.0.0/24 的子网为例，默认的系统保留地址如下：

- 192.168.0.0：网络标识符，私有 IP 地址范围开始，不作分配
- 192.168.0.1：网关地址
- 192.168.0.253：系统接口，用于 VPC 对外通信
- 192.168.0.254：DHCP 服务地址
- 192.168.0.255：广播地址

如果您在创建子网时选择了自定义配置，系统保留地址可能与上面默认的不同，系统会根据您的配置进行自动分配。

2.4 申请 VPN

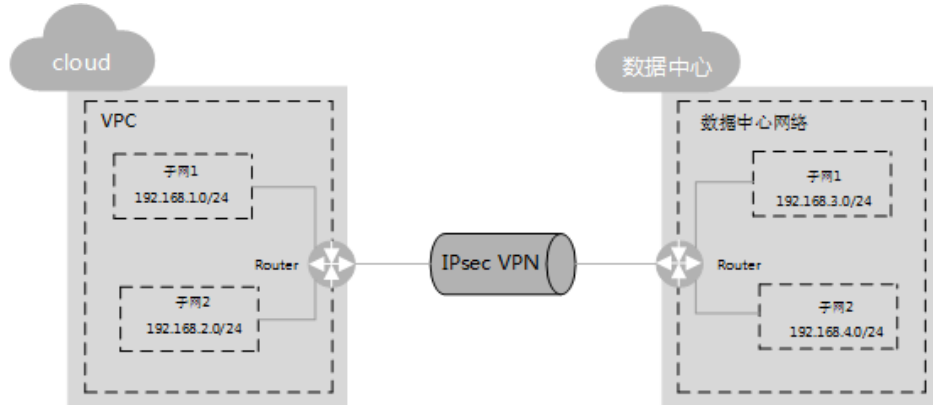
简介

默认情况下，在 Virtual Private Cloud (VPC) 中的弹性云服务器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 中的弹性云服务器和您的数据中心或私有网络连通，可以启用虚拟专用网络功能。此操作您需要在 VPC 中创建 VPN 并更新安全组规则。

简单的 IPsecVPN 内网对连拓扑说明

如图 2-2 所示，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。

图2-2 IPSec VPN



目前我们支持点到点 VPN（Site-to-Site VPN）和点到多点 VPN（Hub-Spoke VPN），除了在 VPC 中搭建 VPN，您还需在自己的数据中心内也搭建 VPN。

VPC 内的 VPN 和您搭建的 VPN，需要保证 IKE 策略以及 IPsec 策略配置一致。在配置前，请参考表 2-7 了解相关术语，并确认您的设备满足以下协议，以及相关配置的约束。

表2-7 术语解释

参数	说明	限制
RFC 2409	定义了 Internet 密钥交换（IKE）协议，它是用于协商和验证密钥信息来保护连接的。	<ul style="list-style-type: none"> 使用预共享密钥进行 IKE 协议的建立。 使用主模式和野蛮模式进行协商。
RFC 4301	定义了 IPsec 的架构，IPsec 能够提供的安全服务，以及各个组件之间如何配置工作的。	请使用 IPsec 隧道模式建立 VPN 连接。

操作场景

通过执行该任务，您可以创建 VPN，以便在您的数据中心与云服务之间建立一条保密而安全的通信隧道。需要先申请 VPN 网关，再申请 VPN 连接，一个 VPN 网关可以对应多个 VPN 连接。

申请 VPN 网关

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟专用网络”。
3. 在左侧导航栏选择“虚拟专用网络 > VPN 网关”。
4. 在“VPN 网关”界面，单击“购买 VPN 网关”。
5. 根据界面提示配置参数，并单击“立即购买”。

表2-8 VPN 网关参数说明

参数	说明	取值样例
计费模式	VPN 网关支持按需计费。 网关费用分为网关配置费用以及带宽使用费用。	按需计费
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	哈尔滨节点
虚拟私有云	VPN 接入的 VPC 名称。	vpc-001
名称	VPN 网关名称。	vpngw-001
类型	VPN 类型。默认为选择“IPsec”。	IPsec
带宽大小	本地 VPN 网关的带宽大小（单位 Mbit/s），为所有基于该网关创建的 VPN 连接共享的带宽，VPN 连接带宽总和不超过 VPN 网关的带宽。 在 VPN 使用过程中，当网络流量超过 VPN 带宽时有可能造成网络拥塞导致 VPN 连接中断，请用户提前做好带宽规划。 可以在 CES 监控中配置告警规则对带宽进行监控。	100
可靠性	可靠性分为“单活”和“双活”两种。	双活
计费方式	支持两种计费方式：按带宽计费/按流量计费	按流量计费

6. 确认信息正确后，单击“提交”。

📖 说明

- VPN 网关创建完成后，VPN 网关的状态为“未连接”。当有 VPN 连接使用该 VPN 网关时，VPN 网关的状态更新为“正常”
- 目前 VPN 处于公测状态，如需要使用，请提交工单申请公测权限。

- 目前仅有乌鲁木齐、哈尔滨、中卫、郑州、南宁节点支持先创建 VPN 网关、再创建 VPN 连接的业务模式。其它节点，需要先创建本端 VPC 的 VPN 连接，针对本端 VPC 的 VPN 连接中内容，创建对端 VPC 的 VPN 网关/连接内容，再修改、更新本端 VPC 的 VPN 连接信息。

申请 VPN 连接

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟专用网络”。
3. 在左侧导航栏选择“虚拟专用网络> VPN 连接”。
4. 在“VPN 连接”页面，单击“购买 VPN 连接”。
5. 根据界面提示配置参数，并单击“立即购买”。

表2-9 VPN 连接参数说明

参数	说明	取值样例
计费模式	VPN 连接支持按需计费	按需计费
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	哈尔滨节点
VPN 网关	VPN 连接挂载的 VPN 网关名称。	vpcgw-001
名称	VPN 连接名称。	vpn-001
预共享密钥	预共享密钥（Pre Shared Key），取值范围为 6~128 位。此项配置在 VPC 的 VPN 和您的数据中心的 VPN 中，配置需要一致。	Test@123
确认密钥	再次输入预共享密钥。	Test@123
本端子网	本端子网指需要通过 VPN 访问用户本地网络的 VPC 子网。支持以下方式设置本端子网。 <ul style="list-style-type: none"> • 选择子网 • 手动输入网段 	192.168.1.0/24, 192.168.2.0/24
远端网关	您的数据中心或私有网络中 VPN 的公网 IP 地址，用于与 VPC 内的 VPN 互通。在双活网关下支持输入 2 个远端网关 IP 地址。	-
远端子网	远端子网指需要通过 VPN 访问 VPC 的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端 VPC 已有的对等连接网段重合。	192.168.3.0/24, 192.168.4.0/24
高级配置	<ul style="list-style-type: none"> • 默认配置 	自定义配置

参数	说明	取值样例
	<ul style="list-style-type: none"> • 已有配置 • 自定义配置：自定义配置 IKE 策略和 IPsec 策略。相关配置说明请参考表 2-10 和表 2-11。 	

表2-10 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、MD5。 默认配置为：SHA1。	SHA1
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐）。 默认配置为：AES-128。	aes-128
DH 算法	Diffie-Hellman 密钥交换算法，支持的算法：Group2、Group5、Group14。 默认配置为：Group5。	Group5
版本	IKE 密钥交换协议版本，支持的版本：v1、v2。 默认配置为：v1。	v1
生命周期（秒）	安全联盟（SA—Security 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。 默认配置为：86400。	86400
协商模式	选择 IKE 策略版本为“v1”时，可以配置协商模式，取值支持 Main、Aggressive。 默认配置为：Main	Main

表2-11 IPsec Policy 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、	SHA1

参数	说明	取值样例
	MD5。 默认配置为：SHA1。	
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置 IPSec 隧道协商时使用。 支持的算法：DH Group2、DH Group5、DH Group14。 默认配置为：DH Group5。	DH Group5
传输协议	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。 默认配置为：ESP。	ESP
生命周期（秒）	安全联盟（SA—Security 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。 默认配置为：3600。	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 VPC 上的 VPN 连接和您数据中心的 VPN 中需要进行相同的配置，否则会导致 VPN 无法建立连接。

6. 单击“提交”。

创建成功后云为该 IPSec VPN 分配一个公网出口 IP 地址。该地址为 VPN 页面中，已创建的 VPN 的本端网关地址。在您自己数据中心配置对端隧道时，远端网关需要配置为该 IP 地址。

图2-3 网关出口 IP 地址

VPN名称/ID	状态	所属VPC	本端网关	本端子网	远端网关	远端子网	操作
vpn-6e6c	未连接	vpc-c04	192.168.1.1	172.16.0.0/24	192.168.1.1	172.16.0.0/24	策略详情 修改 删除

7. 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行 IPSecVPN 隧道配置。

- VPN 配置样例请参考 5.10 如何配置 VPN 对端设备？（HUAWEI USG6600 配置示例）
- VPN 连接支持的协议参考 1.3 参考标准和协议。
- VPN 设备支持列表请参考 5.11 对端 VPN 设备支持列表？

2.5 创建 VPN 网关

操作场景

您需要将 VPC 中的弹性云服务器和您的数据中心或私有网络连通，需要先创建 VPN 网关。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟专用网络”。
3. 在左侧导航栏选择“虚拟专用网络 > VPN 网关”。
4. 在“VPN 网关”界面，单击“创建 VPN 网关”。
5. 根据界面提示配置参数，并单击“立即购买”。VPN 网关参数请参考表 2-12

表2-12 VPN 网关参数说明

参数	说明	取值样例
计费模式	VPN 网关支持按需计费的计费模式。	按需计费
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	哈尔滨节点
名称	VPN 网关名称。	vpngw-001
虚拟私有云	VPN 接入的 VPC 名称。	vpc-001
类型	VPN 类型。默认为选择“IPsec”。	IPsec
可靠性	可靠性分为“单活”和“双活”两种。	双活
计费方式	按需计费支持两种计费方式：按带宽计费/按流量计费。 <ul style="list-style-type: none"> • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。 	按流量计费
带宽大小	本地 VPN 网关的带宽大小（单位 Mbit/s），为所有基于该网关创建的	100

参数	说明	取值样例
	VPN 连接共享的带宽，VPN 连接带宽总和不超过 VPN 网关的带宽。	
描述	VPN 网关的描述信息。	-

2.6 创建 VPN 连接

操作场景

您需要将 VPC 中的弹性云服务器和您的数据中心或私有网络连通，创建 VPN 网关后需要创建 VPN 连接。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟专用网络”。
3. 在左侧导航栏选择“虚拟专用网络 > VPN 连接”。
4. 在“VPN 连接”页面，单击“创建 VPN 连接”。
5. 根据界面提示配置参数，并单击“立即购买”。VPN 连接参数请参考表 2-13。

表2-13 VPN 连接参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	华北-北京一
计费模式	VPN 连接支持按需计费。	按需计费
名称	VPN 连接名称。	vpn-001
VPN 网关	VPN 连接挂载的 VPN 网关名称。	vpcgw-001
本端子网	本端子网指需要通过 VPN 访问用户本地网络的 VPC 子网。支持以下方式设置本端子网： <ul style="list-style-type: none"> • 选择子网 • 手动输入网段 说明 多个本端子网不支持子网网段重叠。	192.168.1.0/24, 192.168.2.0/24
远端网关	您的数据中心或私有网络中 VPN 的公网 IP 地址，用于与 VPC 内的 VPN 互	-

参数	说明	取值样例
	通。	
远端子网	远端子网指需要通过 VPN 访问 VPC 的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端 VPC 已有的对等连接网段、专线/云连接的远端子网网段重复。 说明 多个远端子网不支持子网网段重叠。	192.168.3.0/24, 192.168.4.0/24
预共享密钥	预共享密钥（Pre Shared Key），指配置在云上 VPN 连接的密钥，需要与本地网络 VPN 设备配置的密钥一致。此密钥用于 VPN 连接协商。 取值范围：6~128 位。	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	<ul style="list-style-type: none"> 默认配置 已有配置 自定义配置：包含 IKE 策略和 IPsec 策略，用于指定 VPN 隧道加密算法。相关配置说明请参考表 2-14 和表 2-15。 	自定义配置

表2-14 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、MD5。 默认配置为：SHA1。	SHA1
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐）。 默认配置为：AES-128。	AES-128
DH 算法	Diffie-Hellman 密钥交换算法，支持的算法：Group 2、Group 5、Group 14。 默认配置为：Group 5。	Group 5
版本	IKE 密钥交换协议版本，支持的版本：v1、v2。	v1

参数	说明	取值样例
	默认配置为：v1。	
生命周期（秒）	安全联盟（SA—Security 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。 默认配置为：86400。	86400
协商模式	选择 IKE 策略版本为“v1”时，可以配置协商模式，选择只支持 Main。 默认配置为：Main	Main

表2-15 IPsec Policy 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：SHA1、SHA2-256、SHA2-384、SHA2-512、MD5。 默认配置为：SHA1。	SHA1
加密算法	加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置 IPsec 隧道协商时使用。 PFS 组支持的算法：DH group 2、DH group 5、DH group 14。 默认配置为：DH group 5。	DH group 5
传输协议	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。 默认配置为：ESP。	ESP
生命周期（秒）	安全联盟（SA—Security 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

参数	说明	取值样例
	默认配置为：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 VPC 上的 VPN 连接和您数据中心的 VPN 中需要进行相同的配置，否则会导致 VPN 无法建立连接。

6. 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行 IPSecVPN 隧道配置。
 - VPN 配置样例请参考 5.10 如何配置 VPN 对端设备？（HUAWEI USG6600 配置示例）
 - VPN 连接支持的协议参考 1.3 参考标准和协议。
 - VPN 设备支持列表请参考 5.11 对端 VPN 设备支持列表？

2.7 配置安全组策略（可选）

2.7.1 创建安全组

操作场景

您可以创建安全组并定义安全组中的规则，将 VPC 中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。建议您将不同公网访问策略的弹性云服务器划分到不同的安全组。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击“创建安全组”。
5. 在“创建安全组”界面，根据界面提示配置参数，参数说明参考表 2-16。

表2-16 参数说明

参数	参数说明	取值样例
名称	安全组的名称，必填项。 安全组的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。 说明	sg-318b

参数	参数说明	取值样例
	安全组名称创建后可以修改，建议不要重名。	
描述	安全组的描述信息，非必填项。 描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。	-

6. 单击“确定”。

2.7.2 添加安全组规则

操作场景

安全组创建后，您可以在安全组中设置出方向、入方向规则，这些规则会对安全组内部的云服务器出入方向网络流量进行访问控制，当云服务器加入该安全组后，即受到这些访问规则的保护。

- 入方向：指从外部访问安全组规则下的弹性云服务器。
- 出方向：指安全组规则下的弹性云服务器访问安全组外的实例。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
5. 在入方向规则页签，单击“添加规则”，添加入方向规则。
单击“+”可以依次增加多条入方向规则。

表2-17 入方向参数说明

参数	说明	取值样例
协议/应用	网络协议。目前支持“ALL”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。	TCP
端口和源地址	端口：允许远端地址访问弹性云服务器指定端口，取值范围为：1~65535。	22 或 22-30
	源地址：可以是 IP 地址、安全组。例如： <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx/32 (IPv4 地址) • xxx.xxx.xxx.0/24 (子网) • 0.0.0.0/0 (任意地址) 	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过 255 个字符，且不能包含“<”	-

参数	说明	取值样例
	和“>”。	

6. 在出方向规则页签，单击“添加规则”，添加出方向规则。
单击“+”可以依次增加多条出方向规则。

表2-18 出方向参数说明

参数	说明	取值样例
协议/应用	网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。	TCP
端口和目的地址	端口：允许弹性云服务器访问远端地址的指定端口，取值范围为：1~65535。	22 或 22-30
	目的地址：可以是 IP 地址、安全组。例如： <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx/32（IPv4 地址） • xxx.xxx.xxx.0/24（子网） • 0.0.0.0/0（任意地址） 	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。	-

7. 单击“确定”。

3 管理

3.1 查看已申请 VPN

操作场景

用户申请 VPN 后，可以查看已申请的 VPN。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟专用网络”。
3. 在“虚拟专用网络”界面，即可看到已申请的 VPN。其中 VPN 的状态信息如表 3-1 所示。

表3-1 VPN 状态

状态	说明
正常	当 VPN 创建成功并已经和用户本地数据中心正常连接时，显示此状态。
未连接	当 VPN 创建成功，但未和用户本地数据中心连接时，显示此状态。
创建中	当系统正在创建 VPN 时，显示此状态。
更新中	当系统正在更新 VPN 信息时，显示此状态。
删除中	当系统正在删除 VPN 时，显示此状态。
异常	异常情况下，显示此状态。
冻结	VPN 资源被冻结时，显示此状态。

3.2 修改已申请 VPN

操作场景

当创建的 VPN 网络信息和 VPC 网络有冲突或需要根据最新网络环境调整时，可通过修改 VPN 信息的方式进行调整。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟专用网络”。
3. 在“虚拟专用网络”界面所需修改的 VPN 所在行，单击“修改”。
4. 根据界面提示配置参数。
5. 单击“确定”。

3.3 删除 VPN

操作场景

当无需使用 VPN 网络、需要释放网络资源时，可删除 VPN。

操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟专用网络”。
3. 在“虚拟专用网络”界面所需删除的 VPN 所在行，单击“删除”。
4. 单击“是”。


3.4 关于配额

什么是配额？

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额？

1. 登录管理控制台。
2. 单击页面右上角的“My Quota”图标 。
系统进入“服务配额”页面。

- 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额？

目前系统暂不支持在线调整配额大小。如您需要调整配额，请提交工单申请配额调整，客服将在工单中告知您实时进展。

4 最佳实践

4.1 通过 VPN 连接 VPC

操作场景

默认情况下，在 Virtual Private Cloud (VPC) 中的弹性云服务器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 中的弹性云服务器和您的数据中心或私有网络连通，可以启用 VPN 功能。申请 VPN 后，用户需要配置安全组并检查本端与对端网络的连通性，以确保 VPN 功能可用。主要场景分为两类：

- 点对点 VPN：本端为处于云服务平台上的一个 VPC，对端为一个数据中心，通过 VPN 建立用户数据中心与 VPC 之间的通信隧道。
- 点对多点 VPN：本端为处于云服务平台上的一个 VPC，对端为多个数据中心，通过 VPN 建立不同用户数据中心与 VPC 之间的通信隧道。

配置 VPN 时需要注意以下几点：

- 本端子网与对端子网不能重复。
- 本端子网网段不能重复。
- 本端和对端的 IKE 策略、IPSec 策略、PSK 相同。
- 本端和对端子网，网关等参数对称。
- VPC 内弹性云服务器安全组允许访问对端和被对端访问。
- VPN 对接成功后两端的服务器或者虚拟机之间需要进行通信，VPN 的状态才会刷新为正常。

前提条件

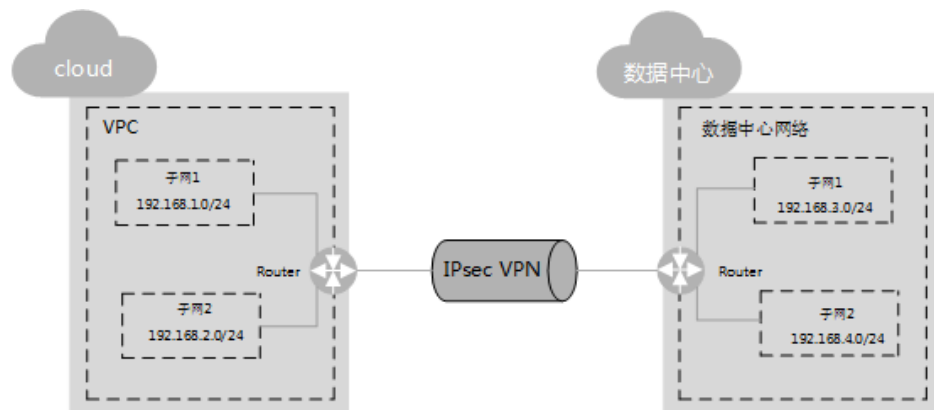
已创建 VPN 所需的虚拟私有云和子网。

操作步骤

1. 在管理控制台上，选择合适的 IKE 策略和 IPsec 策略申请 VPN。
2. 检查本端和对端子网的 IP 地址池。

如图 4-1 所示，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。

图4-1 IPsec VPN



本端和对端子网 IP 池不能重合。例如，本端 VPC 有两个子网，分别为：192.168.1.0/24 和 192.168.2.0/24，那么对端子网的 IP 地址池不能包含本端 VPC 的这两个子网。

3. 配置 VPC 的安全组策略。
4. 检查 VPC 安全组。
安全组必须放通来自 VPN 的报文。可以使用 ping 方法来检查 VPC 安全组是否放通。
5. 检查远端 LAN 配置（即对端数据中心网络配置）。
在远程 LAN（对端数据中心网络）配置中有可以将 VPN 流量转发到 LAN 中网络设备的路由。如果 VPN 流量无法正常通信，请检查远程 LAN 是否存在拒绝策略。

5 常见问题

5.1 一个用户下支持多少个 IPSec VPN?

IPSec VPN 目前处于公测状态，需要提交工单申请公测权限后，再针对不同节点，申请配额数量。

5.2 IPSec VPN 是否会自动进行协商?

IPSec VPN 隧道为被动模式，只有在本端有流量经过隧道时才会触发自动协商。

5.3 如何解决无法建立连接问题?

1. 检查云上 VPN 连接中的 IKE 策略和 IPsec 策略中的协商模式和加密算法是否与远端配置一致。
 - a. 如果第一阶段 IKE 策略已经建立，第二阶段的 IPsec 策略未开启，常见情况为 IPsec 策略与数据中心远端的配置不一致。
 - b. 如果客户本地侧使用的是 CISCO 的物理设备，建议客户使用 MD5 算法。同时将云上 VPN 连接端 IPSec 策略中的认证算法设置为 MD5。

2. 检查 ACL 是否配置正确。

假设您的数据中心的子网为 192.168.3.0/24 和 192.168.4.0/24，VPC 下的子网为 192.168.1.0/24 和 192.168.2.0/24，则您在数据中心或局域网中的 ACL 应对您的每一个数据中心子网配置允许 VPC 下的子网通信的规则，如下例：

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
```

3. 配置完成后检查 VPN 是否连接，ping 测试两端内网是否正常。

5.4 VPN 建立后您的数据中心或局域网无法访问弹性云服务器？

我们提供的安全组默认不允许任何源访问，请确认您的安全组是否配置允许对端的子网地址访问。

5.5 VPN 连接建立后，弹性云服务器无法访问您的数据中心或局域网？

需要确认是否已做好 VPN 公网 IP 到您的数据中心或局域网公网 IP 的防火墙策略，云上出口未做策略限制。

5.6 VPN 支持将两个 VPC 互连吗？

如果两个 VPC 位于同一区域内，可以使用 VPC 对等连接互连。

如果两个 VPC 位于不同区域，可以通过 VPN 连接，分别把这两个 VPC 的 CIDR 作为本端子网和远端子网。

5.7 VPN 本端子网和远端子网数量有什么限制？

VPN 本端子网和远端子网数量乘积最大支持到 225 的规模。

5.8 为什么 VPN 创建成功后状态显示未连接？

VPN 对接成功后两端的服务器或者虚拟机之间需要进行通信，VPN 的状态才会刷新为正常。

- **IKE v1 版本：**
如果 VPN 连接经历了一段无流量的空闲时间，则需要重新协商。协商时间取决于 IPsec Policy 策略中的“生命周期（秒）”取值。“生命周期（秒）”取值一般为 3600（1 小时），会在第 54 分钟时重新发起协商。若协商成功，则保持则保持连接状态至下一轮协商。若协商失败，则在 1 小时内将状态设置为未连接，需要 VPN 两端重新进行通信才能恢复为连接状态。可以使用网络监控工具（例如 IP SLA）生成保持连接的 Ping 信号来避免这种情况发生。
- **IKE v2 版本：**如果 VPN 连接经历了一段无流量的空闲时间，VPN 保持连接状态。

5.9 VPN 配置下发后，多久能够生效？

VPN 配置生效的时间与 VPN 配置中的本端子网数和对端子网数的乘积呈线性增长关系。

5.10 如何配置 VPN 对端设备？（HUAWEI USG6600 配置示例）

因为隧道的对称性，在云上的 VPN 参数和您的 VPN 中需要进行相同的配置，否则会导致 VPN 无法建立连接。

在您自己数据中心的路由器或者防火墙上需要进行 IPSec VPN 隧道配置，具体配置方法取决于您使用的网络设备，请查询对应设备厂商的指导书。

本文以 Huawei USG6600 系列 V100R001C30SPC300 版本的防火墙的配置过程为例进行说明，供参考。

假设数据中心的子网为 192.168.3.0/24 和 192.168.4.0/24，VPC 下的子网为 192.168.1.0/24 和 192.168.2.0/24，VPC 上 IPSec 隧道的出口公网 IP 为 XXX.XXX.XX.XX（从 VPC 上 IPSec VPN 的本端网关参数上获取）。

操作步骤

1. 登录防火墙设备的命令行配置界面。
2. 查看防火墙版本信息。

```
display version
17:20:502017/03/09
Huawei Versatile Security Platform Software
Software Version: USG6600 V100R001C30SPC300 (VRP (R) Software, Version 5.30)
```

3. 创建 ACL 并绑定到对应的 vpn-instance。

```
acl number 3065 vpn-instance vpn64
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
q
```

4. 创建 ike proposal。

```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```

5. 创建 ike peer，并引用之前创建的 ike proposal，其中对端 IP 地址是 x.x.x.x。

```
ike peer vpnikepeer_64
pre-shared-key *****（*****为您输入的预共享密码）
ike-proposal 64
undo version 2
```

```
remote-address vpn-instance vpn64 x.x.x.x
sa binding vpn-instance vpn64
q
```

6. 创建 IPSec 协议。

```
ipsec proposal ipsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. 创建 IPSec 策略，并引用 ike policy 和 ipsec proposal。

```
ipsec policy vpnipsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal ipsecpro64
local-address xx.xx.xx.xx
q
```

8. 将 IPSec 策略应用到相应的子接口上去。

```
interface GigabitEthernet0/0/2.64
ipsec policy vpnipsec64
q
```

9. 测试连通性。

在上述配置完成后，我们可以利用您在云中的主机和您数据中心的主机进行连通性测试，如下图所示：

```
root@i-psiwbqhh:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:7c:ba:bf:cc
          inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:7cff:feba:bfcc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2304 (2.3 KB)  TX bytes:3404 (3.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KB)  TX bytes:1296 (1.2 KB)

root@i-psiwbqhh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=62 time=1.27 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=62 time=1.25 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=62 time=0.871 ms
64 bytes from 192.168.1.2: icmp_req=5 ttl=62 time=0.886 ms
64 bytes from 192.168.1.2: icmp_req=6 ttl=62 time=0.676 ms
64 bytes from 192.168.1.2: icmp_req=7 ttl=62 time=1.06 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.676/1.510/4.554/1.258 ms
```

5.11 对端 VPN 设备支持列表?

满足 IPsec VPN 标准和协议的设备，大部分都可以对接 VPN。例如：Cisco ASA 防火墙、华为 USG6 系列防火墙、USG9 系列防火墙、山石网科防火墙、Cisco ISR 路由器等。对于华为 USG6 系列防火墙、USG9 系列防火墙具体设备列表如表 5-1 所示。

表5-1 华为 VPN 设备列表

对端支持列表	说明
HUAWEI USG6 系列	USG6320/6310/6510-SJJ USG6306/6308/6330/6350/6360/6370/6380/6390/6507/6530/6550/6570: 2048 USG6620/6630/6650/6660/6670/6680
HUAWEI USG9 系列	USG9520/USG9560/USG9580

其他满足的设备，也在支持列表中，但是可能会因为设备对协议的实现方式不一致，导致接入失败。如果发现不能建立连接，请参考 5.3 如何解决无法建立连接问题？，进行基本检查或联系技术支持人员。

5.12 无法连接或网速慢如何排查?

排查方法如下：

1. 查看云主机规格，云上 VPN 的入口流量不限速，与云主机规格有关。
2. 云上 VPN 的出口流量限速，查看用户的带宽是否已经达到或者超出上限。
3. 排查用户的本地网络，查看是否为用户侧数据中心网络速度的影响。
4. 排查云上与用户侧数据中心是否存在丢包现象。

5.13 虚拟专用网络是否支持 SSL VPN?

目前虚拟专用网络不支持 SSL VPN。

A 修订记录

发布日期	修改说明
2022-09-20	第六次正式发布。文档内容更新如下： 调整文档逻辑。
2017-11-30	第五次正式发布。文档内容更新如下： 新增 VPN 网关和 VPN 连接特性。
2017-07-30	第四次正式发布。文档内容更新如下： <ul style="list-style-type: none">新增“最佳实践”。
2017-03-30	第三次正式发布。文档内容更新如下： <ul style="list-style-type: none">新增对端 VPN 配置示例。
2017-02-28	第二次正式发布。文档内容更新如下： <ul style="list-style-type: none">支持不同 VPC 下多个本端网关与同一个远端网关建立 IPSec VPN 隧道。
2016-10-19	第一次正式发布。