



VPN 连接

用户使用指南

天翼云科技有限公司

目录

1	VPN 连接产品简介	4
1.1	什么是 VPN 连接	4
1.2	产品优势	6
1.3	功能特性	7
1.4	应用场景	9
1.4.1	IPsec VPN 应用场景	9
1.4.2	SSL VPN 应用场景	11
1.5	使用限制	11
1.6	VPN 网关功能支持的地域	12
2	VPN 连接快速入门	13
2.1	IPsec VPN 快速入门	14
2.1.1	IPsec VPN 入门概述	14
2.1.2	建立 VPC 到本地数据中心的连接	15
2.2	SSL VPN 快速入门	22
2.2.1	SSL VPN 入门概述	22
2.2.2	客户端远程连接 VPC	23
3	VPN 连接用户指南	34
3.1	管理 VPN 网关	34
3.1.1	创建和管理 VPN 网关实例	34
3.1.2	配置 VPN 网关路由	37
3.2	开启 IPsec VPN 和 SSL VPN	42
3.3	配置 IPsec VPN	43
3.3.1	IPsec VPN 配置概览	43
3.3.2	管理用户网关	45
3.3.3	管理 IPsec 连接	47
3.3.4	本地网关配置	57
3.4	配置 SSL VPN	82

3.4.1	SSL VPN 配置概览.....	82
3.4.2	管理 SSL 服务端.....	84
3.4.3	管理 SSL 客户端.....	88
3.4.4	修改 SSL 并发连接数.....	90
3.4.5	查看 SSL 客户端的连接信息.....	91
3.5	证书管理.....	91
3.5.1	证书类型概览.....	91
3.5.2	上传证书.....	92
3.5.3	删除证书.....	94
3.6	配额管理.....	95
3.7	MTU 配置说明.....	96
4	VPN 连接常见问题.....	99
4.1	IPsec VPN 连接常见问题.....	99
4.2	SSL VPN 连接常见问题.....	105
4.3	VPN 网关常见问题.....	108
4.4	如何配置本地网关设备.....	112
4.5	多网段互通配置建议及常见问题.....	112
4.6	其他问题.....	118

1 VPN 连接产品简介

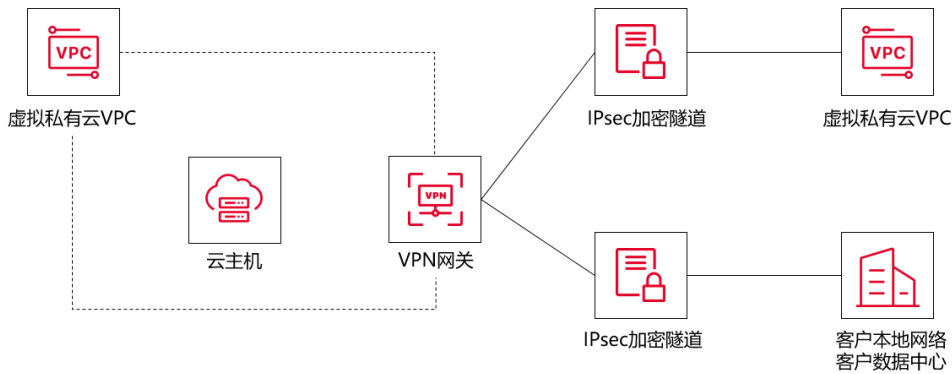
1.1 什么是 VPN 连接

天翼云 VPN 连接是一款基于 Internet 的 VPN 网络连接服务 ,VPN(Virtual Private Network) 即虚拟专用网络 ,用于在远端用户和 VPC (Virtual Private Cloud) 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。

根据使用的加密协议不同 ,VPN 连接可以提供 IPsec VPN 和 SSL VPN 两种连接方式。

IPsec VPN

IPsec (IP Security) 是一种 IP 层的隧道加密技术 ,通过使用加密算法在不同的网络之间建立加密的安全隧道。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 IPsec VPN 功能。

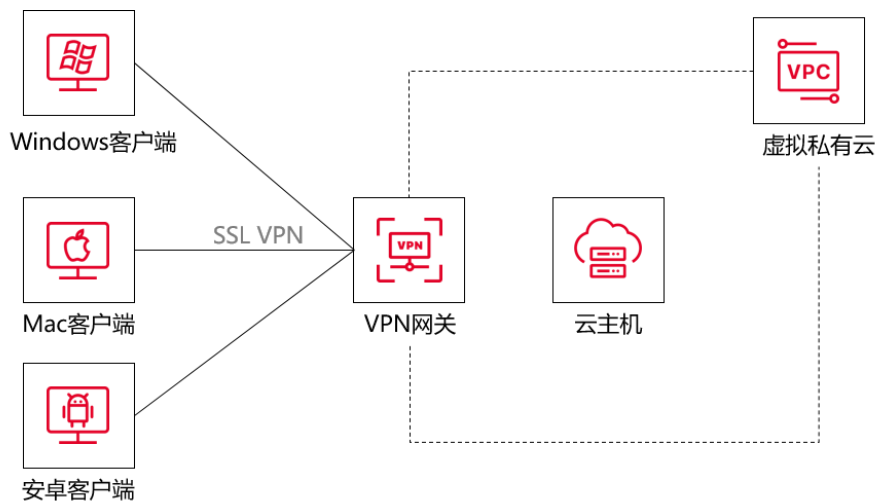


通过 IPsec VPN 连接可以实现企业数据中心、办公网络等与虚拟私有云 (VPC) 建立安全可靠的连接。假设您在天翼云中已经申请了 VPC ,并创建了 2 个子网 (192.168.1.0/24, 192.168.2.0/24) , 您在自己的数据中心网络中也有 2 个子网

(192.168.3.0/24, 192.168.4.0/24)。您可以通过 IPsec VPN 使 VPC 内的子网与数据中心的子网互相通信。

SSL VPN

SSL VPN (Secure Sockets Layer VPN) 是基于互联网线路，通过 SSL 加密通道将用户终端与天翼云 VPC 建立安全可靠连接的服务，满足客户便捷接入 VPC 的需求。



假设您在天翼云中已经申请了 VPC，并创建了 2 个子网 (192.168.1.0/24, 192.168.2.0/24)，当您有移动终端访问 VPC 业务的需求时，您可以通过 SSL VPN 实现便捷安全的网络接入。

相关术语解释

VPN 网关

VPN 网关是 VPN 连接的接入点。一个 VPN 网关仅能绑定一个 VPC，每个 VPN 网关可以创建多个 VPN 连接。每个 VPN 网关默认分配了一个公网 IP 地址，可以满足用户本地数据中心侧 VPN 设备或移动终端接入 VPC 的业务需求。

用户网关

用户企业侧的 VPN 网关，与 VPC 侧 VPN 网关互为本端、远端。用户侧数据中心 VPN 网关需具备固定公网 IP，动态拨号公网 IP 无法进行 IPsec VPN 对接。如果用户侧公网 IP 进行了变更，则需要尽快在天翼云上进行同步修改。否则，会导致 IPsec VPN 协商失败，流量转发不通。

IPsec 连接

IPsec 连接是一种基于 IP 协议的加密技术，用于构建 VPN 网关和用户本地数据中心远端网关之间的安全、可靠的加密通道。VPN 连接使用 IKE (Internet Key Exchange, 网络密钥交换协议) 和 IPsec 协议对传输数据进行加密，保证数据安全可靠，并且 IPsec VPN 连接基于互联网进行传输，更加节约成本。

SSL 服务端

SSL 服务端是 SSL VPN 连接的客户端网关，主要实现数据包的封装与解封装。需要在 VPN 网关中进行 SSL 服务端的相关配置，如配置本端子网、客户端地址池、传输协议及端口等。

SSL 客户端

SSL VPN 客户端是一种安全访问虚拟专用网络 (VPN) 的客户端应用程序，它使用安全套接层 (SSL) 协议来建立加密的远程连接，以确保数据在客户端和 VPN 服务器之间的传输安全。

1.2 产品优势

高性能

VPN 连接采用高端 VPN 网关设备，自动化配置，保证 VPN 业务性能。

高可用

采用双机热备架构，当单台网关设备发生故障时，可自动切换到备机，切换时间为秒级，会话不会中断，用户业务无感知。

安全可靠

IPsec VPN 采用 IKE 和 IPsec 协议对传输数据进行加密，SSL VPN 采用 TLS (Transport Layer Security, 传输层安全性协议) 协议对传输数据进行加密，数据传输安全可靠。

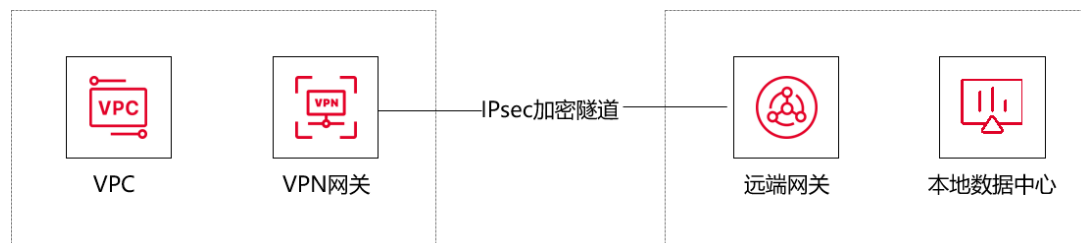
简单易用

即买即用，快速部署。在天翼云控制台配置相关参数，在数据中心网络或移动终端进行简单配置即可完成连接。

1.3 功能特性

VPC 到本地数据中心的连接

通过 VPN 网关将本地数据中心和云上 VPC 快速连接，以构建混合云。

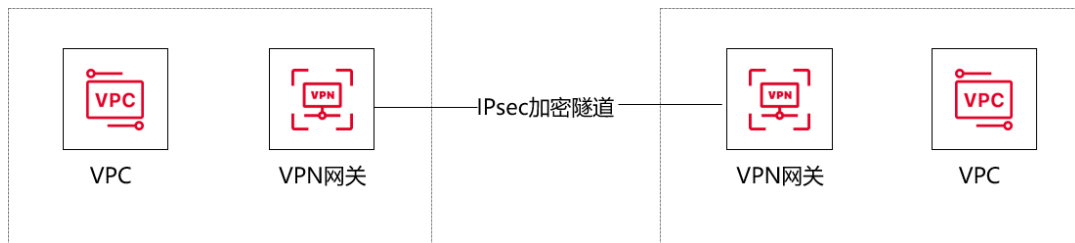


注意：VPC 内子网和本地数据中心子网不能重合。

例如，本端 VPC 有两个子网，分别为：192.168.1.0/24 和 192.168.2.0/24，那么对端子网中不能包含本端 VPC 的这两个子网。同时，本地数据中心网关要支持 IPsec VPN 功能。

VPC 到 VPC 的连接

通过 VPN 网关将两个或多个 VPC 快速连接以实现云上资源互通。与对等连接和云间高速不同，VPN 连接不仅可以实现天翼云不同区域 VPC 的互通，也可以实现与其他云服务商的 VPC 互联（前提是对方也具备 IPsec VPN 的接入能力）。



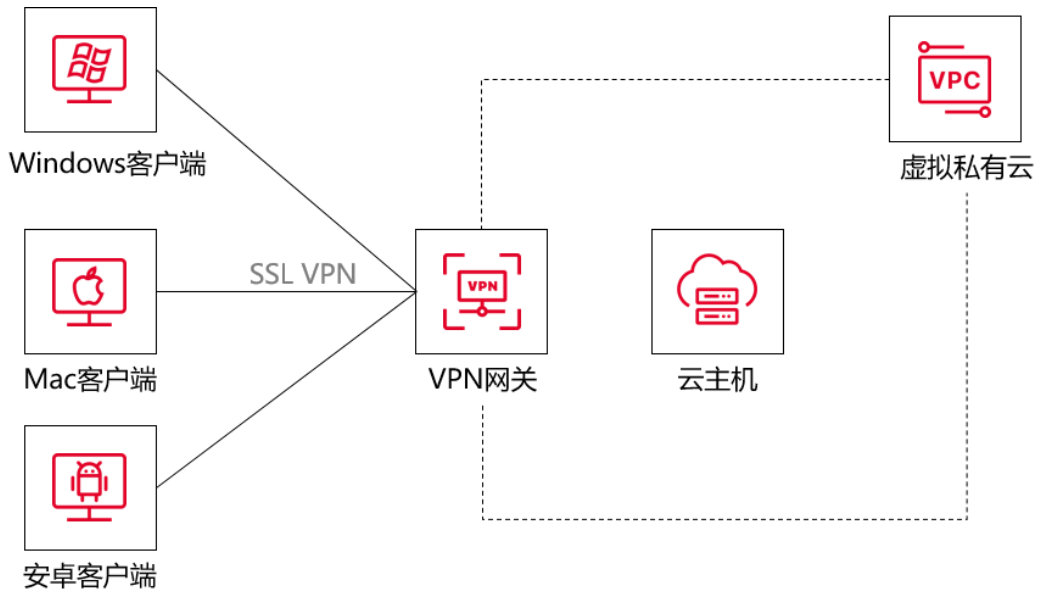
注意：互联的两个 VPC 内的子网不能重合。

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 VPC 子网中不能包含本端 VPC 的这两个子网。

客户端到 VPC 的连接

您可以通过 SSL VPN 将客户端和 VPC 连接起来，客户端可以通过互联网随时随地安全地连接 VPC，满足远程办公的需要。

SSL VPN 支持 Windows、Mac、Android 操作系统类型的客户端接入。



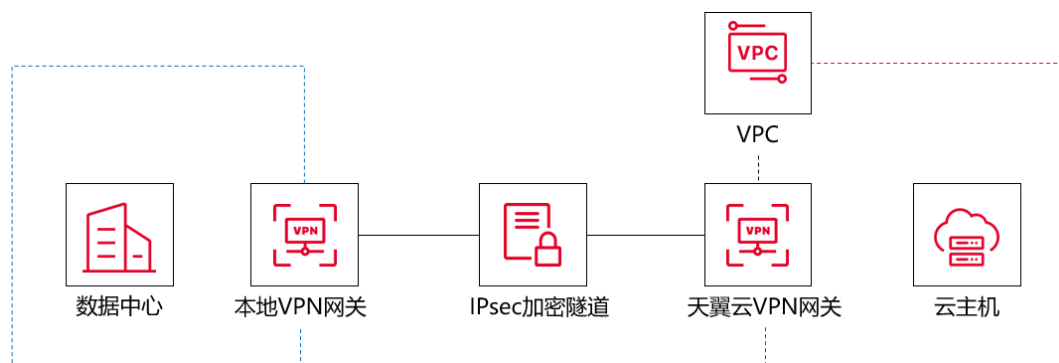
1.4 应用场景

1.4.1 IPsec VPN 应用场景

IPsec VPN 支持在企业本地数据中心或企业办公网络与天翼云 VPC (Virtual Private Cloud) 之间建立安全可靠的网络连接。

混合组网

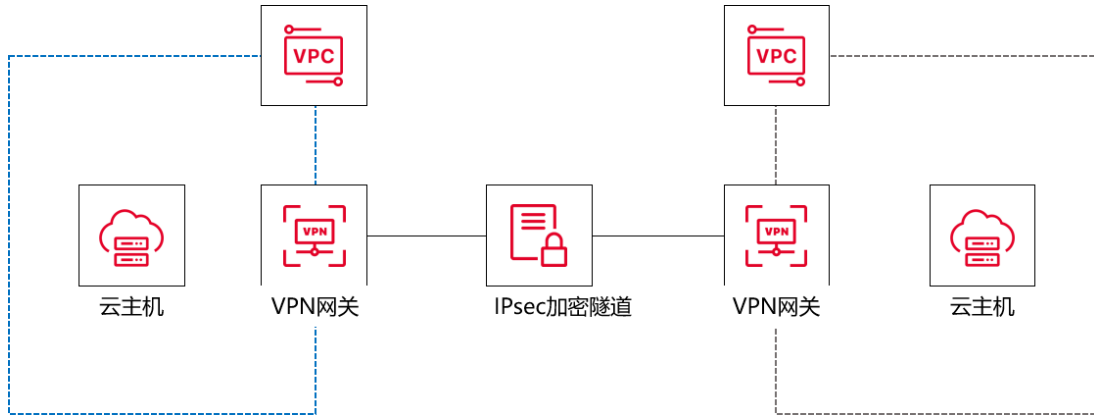
您可以通过 IPsec VPN 隧道连接用户的数据中心和天翼云资源池的 VPC 网络，快速便捷地利用云上的弹性资源。



通过采用加密的 IPsec VPN 隧道将用户本地网络和云上 VPC 互联，利用 VPC 的弹性伸缩功能，扩展应用计算能力。

云上网络互联

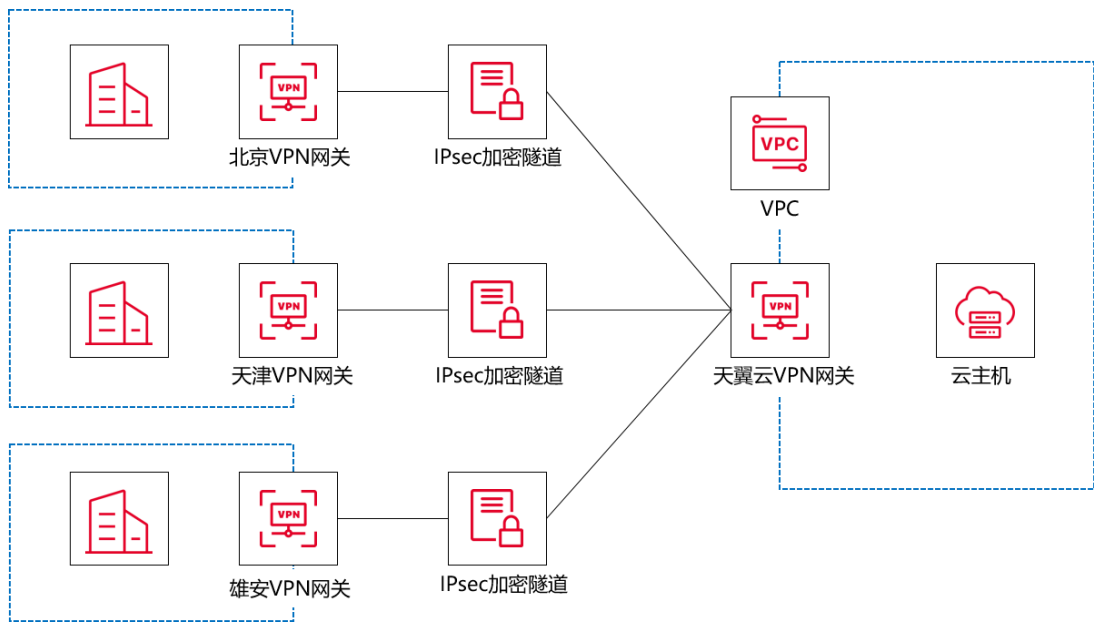
通过 IPsec VPN 连接不同区域的 VPC，使用户的数据和服务在不同地域能够互联互通。



您可以通过 IPsec VPN 连接天翼云不同区域资源池的 VPC，也可以连接天翼云与其他云服务商的网络（前提是对方也具备同等 IPsec VPN 能力）。

多站点互联

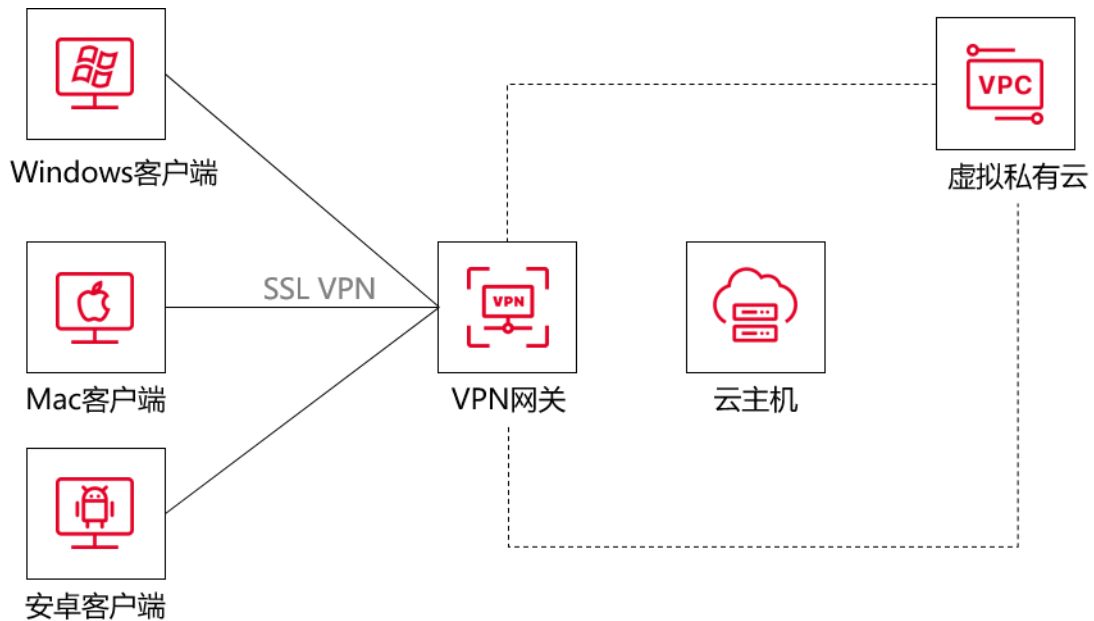
通过 IPsec VPN 连接，可将多个站点的流量进行汇聚和转发。



- 您可以通过 VPN 网关建立多个 IPsec 连接通道，与企业的多个站点进行连接。
- 每个站点都可以访问云上 VPC 资源，实现多站点上云流量的汇聚。
- 每个站点可以通过 VPN 网关实现多个站点网络之间的互通。

1.4.2 SSL VPN 应用场景

在移动互联网的背景下，SSL VPN 可以帮助客户随时随地建立一条安全隧道，直达客户云上 VPC。客户可以使用多种客户端（如个人电脑、手机、平板等），通过安装配置客户端软件，采用证书、密码等认证方式与 VPC 自由连接。



- 支持用户级限速。
- 配置简单，全程加密，保证数据传输安全。

1.5 使用限制

VPN 连接的使用限制如下表所示：

资源	限制	说明

单个 VPC 可创建的 VPN 网关数量	1	无法调整
单个用户可以创建 IPsec VPN 用户网关实例数	100	提交工单
单个用户可以创建 SSL VPN 服务端实例数	20	提交工单
单个用户可以创建 SSL VPN 客户端实例数	20	提交工单

1.6 VPN 网关功能支持的地域

下表中的“✓”表示该功能已在该地域支持，“x”表示该功能在该地域暂不支持。

VPN 类型	IPsec VPN		SSL VPN	SSL VPN 双因子认证
网关类型	普通型 VPN 网关	国密型 VPN 网关	普通型 VPN 网关	所有 VPN 网关类型均支持
主备模式资源池	✓	x	x	x
集群模式资源池	✓	✓	✓	✓

资源池架构分为主备模式和集群模式，具体资源池清单和区别如下：

对比项	主备模式资源池	集群模式资源池
资源池架构	单 AZ，虚拟网元	多 AZ，多活模式，物理网元
可扩展性	受虚拟网元规格限制，性能提升空间有限	易于扩展，通过扩展集群规模，提升产品性能

对比项	主备模式资源池	集群模式资源池
可用性	只能单虚拟网元部署，故障无法容灾	跨 AZ 容灾，集群内多主机互备，可用性比主备模式有质的提升
资源池清单	<p>华东：芜湖 2、南京 2、南京 3、南京 4、南京 5、九江、上海 7、杭州 2</p> <p>华南：福州 3、福州 4、佛山 3、广州 6、南宁 2、香港 1、武汉 3、武汉 4、长沙 3、郴州 2、海口 2</p> <p>西南：重庆 2、贵州 3、成都 4、拉萨 3、昆明 2</p> <p>北方：北京 5、兰州 2、石家庄 20、中卫 2、中卫 5、内蒙 6、西宁 2、西安 3、西安 4、西安 5、晋中</p>	<p>华东：上海 36、华东 1、南昌 5</p> <p>华南：武汉 41、长沙 42</p> <p>北方：青岛 20、青岛 21、石家庄 21、大连 7</p>

2 VPN 连接快速入门

2.1 IPsec VPN 快速入门

2.1.1 IPsec VPN 入门概述

环境要求

- 本地数据中心的网关设备必须配置公网 IP 地址。
- 本地数据中心的网关设备必须支持 IKEv1 或 IKEv2 协议，支持任何一种协议的设备均可以和 VPN 网关建立 IPsec VPN 连接。
- 本地数据中心和天翼云 VPC 间互通的网段没有重合。

使用流程



创建VPN网关 创建用户网关 创建IPsec连接 配置VPN网关路由（可选） 配置本地网关 测试连通性

1. 创建 VPN 网关

创建 VPN 网关并开启 IPsec VPN 功能，一个 VPN 网关可以建立多条 IPsec 连接。

2. 创建用户网关

通过创建用户网关，您可以将本地数据中心 VPN 网关设备的信息注册到天翼云上。

3. 创建 IPsec 连接

IPsec 连接是指 VPN 网关和本地数据中心 VPN 网关设备建立连接后的 VPN 隧道。只有在建立 IPsec 隧道后，本地数据中心才能使用 VPN 网关进行加密通信。

4. 配置 VPN 网关路由（可选）。

- 当创建的 IPsec 连接配置的路由模式为“目的路由”时，您需要在 VPN 网关中配置路由，并发布路由到 VPC 路由表以实现本地数据中心和 VPC 的通信。

- 当创建的 IPsec 连接配置的路由模式为“感兴趣路由”时，无需执行此操作。

5. 配置本地网关设备

您需要在本地数据中心的网关设备中添加 VPN 配置。

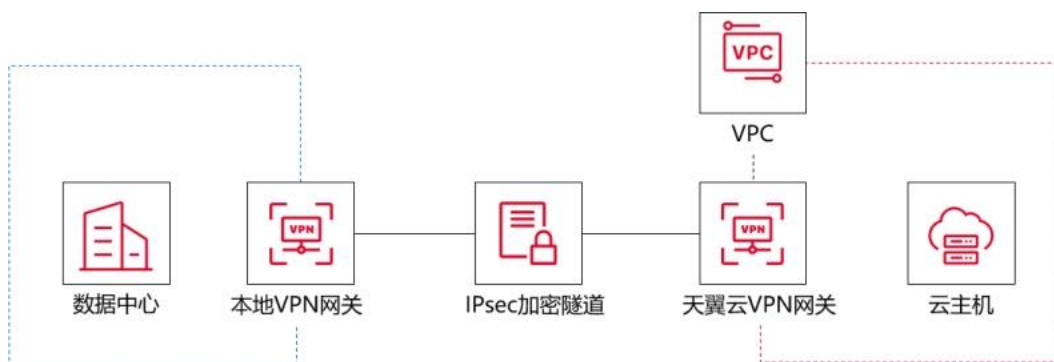
6. 测试连通性

登录到天翼云 VPC 内一台弹性云主机实例，通过 **ping** 命令，**ping** 本地数据中心内一台服务器的私网 IP 地址（未禁用 ping 探测），验证通信是否正常。

2.1.2 建立 VPC 到本地数据中心的连接

场景示例

以下图组网场景为例，某公司在天翼云创建了 VPC，子网网段为 192.168.1.0/24 和 192.168.2.0/24。本地数据中心的网段为 172.16.1.0/24，本地网关设备的公网 IP 为 121.XX.XX.113。公司因业务发展，需要本地数据中心与云上 VPC 互通。您可以通过 IPsec VPN，建立本地数据中心与云上 VPC 的连接，实现云上和云下的加密通信。



环境要求

- 本地数据中心网关设备必须配置公网 IP 地址。


- 本地数据中心的网关设备必须支持 IKEv1 或 IKEv2 协议，支持任何一种协议的设备均可以和 VPN 网关建立 IPsec VPN 连接。
- 本地数据中心和天翼云 VPC 间互通的网段没有重合。

准备工作

- 您已经在天翼云创建了 VPC，VPC 中使用云主机部署了相关业务。
- 您已经了解云主机实例所应用的安全组规则，并确保安全组规则允许本地数据中心网络中的终端设备访问云上资源。

操作步骤

步骤一：创建 VPN 网关


1. 登录控制中心。
2. 单击控制中心左上角的 ，选择目标资源池。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击“创建 VPN 网关”，进入订购页面，按照提示配置参数。

参数	说明	取值样例
地域	VPN 网关所在的资源池。	华东 1
名称	VPN 网关的名称。	vpn-gateway-f0e0
网关类型	选择 VPN 网关的类型。	普通

实例类型	选择 VPN 网关的实例类型。	IPsec
企业项目	选择当前 VPN 网关归属项目。	default
本端类型	通过 VPN 网关接入的资源类型。	虚拟私有云 VPC
虚拟私有云	选择要使用的 VPC 作为本端资源。	vpc-682f
子网	选择当前 VPC 中本端的子网资源。	<ul style="list-style-type: none"> subnet-682f (192.168.1.0/24)
IPsec 带宽	VPN 网关要通过弹性 IP 访问公网，这里选择对应的弹性 IP 带宽大小，单位 Mbps，5M 起售。	20M
IPsec 连接数	选择对应的 IPsec VPN 并发连接数。	20
购买时长	包年包月场景需要选择，购买 VPN 网关实例的时长。	6 个月
自动续订	资源到期后自动续订，按月购买时按月续订，按年购买时按年续订。	开启

- 单击“下一步”。
- 在购买确认页，勾选服务协议，点击“确认下单”，进入订单列表。
- 在订单页面，单击“立即支付”，支付成功后，VPN 网关创建成功。

步骤二：创建用户网关

1. 登录控制中心。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择 “VPN 连接” ，进入 VPN 连接页面。
4. 在左侧网络控制台，选择 “IPsec VPN” ，进入用户网关列表页面。
5. 单击 “创建用户网关” 。
6. 按照提示配置用户网关参数。

参数	说明	取值样例
名称	用户网关的名称。	user-gateway-5da3
IP 地址	对端 VPN 网关的静态公网 IP 地址，对端网关必须具有固定的公网 IP，不能是动态 IP。	121.229.145.113

7. 单击 “确定” ，创建成功。

步骤三：创建 IPsec 连接

1. 登录控制中心。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。

3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入 IPsec VPN 页面。
5. 单击“IPsec 连接”，进入“IPsec 连接”页签。
6. 单击“创建 IPsec 连接”，按照提示配置参数。

参数	说明	取值样例
名称	VPN 连接的名称。	connection-1
VPN 网关	选择已经创建的 VPN 网关。	vpn-gateway-46c1- ipsec
用户网关	选择已经创建的用户网关。	user-gateway-5da3
路由模式	支持目的路由和感兴趣路由两种路由模式。	感兴趣路由
本端子网	选择 VPC 侧哪个子网需要和企业侧进行联通。	subnet- b2a0(192.168.1.0/24)
对端网段	配置企业侧哪个网段需要和 VPC 侧进行联通。	172.16.1.0/24
协商生效	支持立即协商和流量触发两种协商方式。	立即生效
认证方式	支持密钥认证和证书认证两种认证方式。	密钥认证
预共享密钥	设置自定义密钥。	ctyun_test01

确认密钥	设置确认密钥。	ctyun_test01
LocalId	支持 FQDN 和 IP 格式	默认为当前选取的网关地址，如 11.XX.XX.11
Remoteld	支持 FQDN 和 IP 格式	默认选择用户网关的公网地址，如 121.XX.XX.113

7. 单击“确认”，完成 IPsec 连接创建。

步骤四：配置 VPN 网关路由（可选）

- 当创建的 IPsec 连接配置的路由模式为“目的路由”时，您需要在 VPN 网关中配置路由，并发布路由到 VPC 路由表以实现本地数据中心和 VPC 的通信。
- 当创建的 IPsec 连接配置的路由模式为“感兴趣路由”时，无需执行此操作。

1. 登录控制中心。

2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。

3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。

4. 在 VPN 网关页面，单击目标 VPN 网关实例。

5. 在 VPN 网关实例详情页面，在“策略路由”页签，单击“添加路由条目”。

6. 在添加路由条目页面，根据以下信息配置策略路由，单击“确定”。

配置	说明	取值样例
目标网段	输入要访问的本地数据中心的私网网段。	172.16.1.0/24
源网段	输入 VPN 网关实例关联的 VPC 侧的私网网段。	192.168.3.0/24

下一跳类型	选择 IPsec 连接。	IPsec 连接
下一跳	选择需要建立 IPsec VPN 连接的 IPsec 连接。	connection-2
是否发布	<p>选择是否将新添加的路由发布到 VPC 路由表。</p> <p>是（推荐）：将新添加的路由发布到 VPC 路由表。</p> <p>否：不发布新添加的路由到 VPC 路由表。</p> <p>说明 如果您选择否，添加策略路由后，您还需执行发布策略路由。</p>	是
权重	路由的优先级属性。	100（默认值）

步骤五：在本地网关设备中加载 VPN 配置

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入 IPsec VPN 页面。
5. 单击“IPsec 连接”，进入“IPsec 连接”页面。

6. 在 IPsec 连接页面，找到目标 IPsec 连接实例，在操作列选择“更多”，单击“下载对端配置”。
7. 根据本地网关设备的配置要求，将下载的配置添加到本地网关设备中。具体操作，请参见“用户指南 > 本地网关配置”。

步骤六：测试连通性

1. 登录到 VPC 内一台弹性云主机实例。
2. 执行 ping 命令，访问本地数据中心内的一台服务器，验证通信是否正常。
如果能够收到回复报文，则证明通信正常。

2.2 SSL VPN 快速入门

2.2.1 SSL VPN 入门概述

前提条件

- 客户端可以访问互联网。
- 客户端的私网网段和 VPC 的私网网段没有重合，否则无法访问 VPC 内的网络资源。
- 您已了解 VPC 中所应用的安全组规则，并确保安全组规则允许客户端访问云上资源。

使用流程



1. 创建 VPN 网关。

创建 VPN 网关并开启 SSL VPN 功能。

2. 创建 SSL 服务端。

创建相应的 SSL 服务端，用于接入用户侧连接 SSL VPN 服务。

3. 创建 SSL 客户端。

在控制台创建 SSL 客户端，用于生成客户端连接 SSL VPN 服务端的配置。

4. 下载客户端证书。

在控制台下载客户端证书，一共三个证书。

5. 配置客户端。

下载客户端软件，安装并配置客户端。

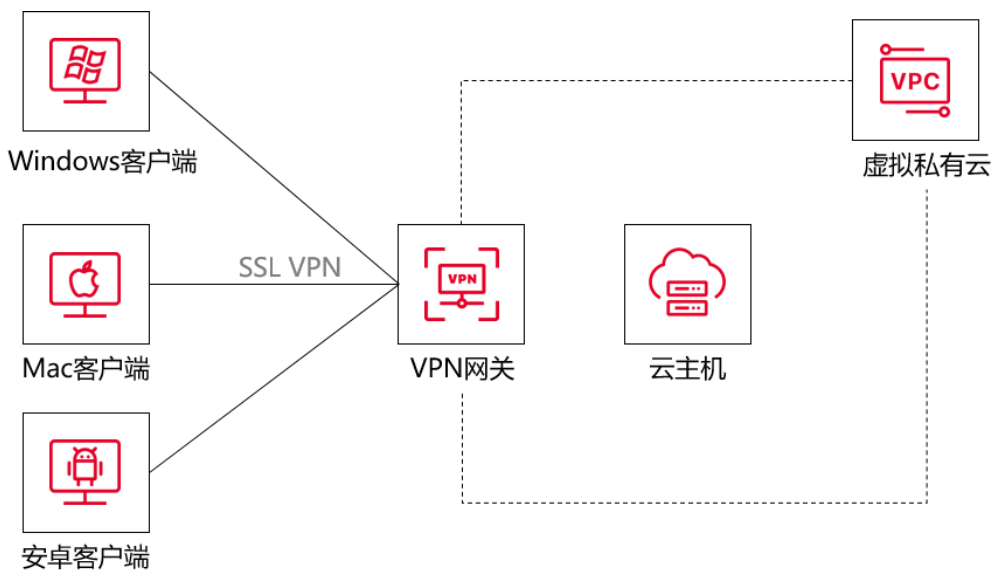
6. 测试连通性。

登录客户端，访问 VPC，测试网络连通性。

2.2.2 客户端远程连接 VPC

背景信息

客户端通过 SSL VPN 隧道远程接入 VPC，实现与 VPC 内资源的安全通信。



前提条件

- 客户端的地址池和 VPC 的子网网段没有重合。
- 客户端可以访问互联网。
- 您已经了解 VPC 中所应用的安全组规则，并确保安全组规则允许客户端访问云上资源。

操作步骤

步骤一：创建 VPN 网关

1. 登录[控制中心](#)。
2. 单击控制中心左上角的 ，选择目标资源池。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 连接页面，单击“创建 VPN 网关”，进入订购页面，按照提示配置参数。

参数	说明	取样
地域	VPN 网关所在的资源池。	华东 1
名称	VPN 网关的名称。	vpngw-1
网关类型	选择 VPN 网关的类型。	普通

参数	说明	取样
实例类型	选择 VPN 网关的实例类型。	SSL
企业项目	选择当前 VPN 网关归属项目。	default
本端类型	通过 VPN 网关接入的资源类型。	虚拟私有云 VPC
虚拟私有云	选择要使用的 VPC 作为本端资源。	vpc-682f
子网	选择当前 VPC 中本端的子网资源。	subnet-12345
SSL 带宽	VPN 网关要通过弹性 IP 访问公网，这里选择对应的弹性 IP 带宽大小。单位：Mbps，5M 起售。	20M
SSL 并发连接数	选择对应的 SSL VPN 并发连接数。	20
购买时长	包年包月场景需要选择，购买 VPN 网关实例的时长。	6 个月
自动续订	资源到期后自动续订，按月购买时按月续订，按年购买时按年续订。	开启

5. 单击“下一步”。
6. 在购买确认页，勾选服务协议，点击“确认下单”，进入订单列表。
7. 在订单页面，点击“立即支付”，支付成功后，VPN 网关创建成功。

说明：记录 VPN 网关的 IP 地址，步骤五配置客户端的时候使用。

步骤二：创建 SSL 服务端

创建 VPN 网关后，需要创建相应的 SSL 服务端，用于提供用户侧连接 SSL VPN 服务。服务端配置时需要注意，SSL 客户侧地址池与 VPC 的子网网段没有交集，否则无法通信。

1. 登录[控制中心](#)。
2. 单击控制中心左上角的，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 进入 SSL VPN 列表页面中，单击“创建 SSL 服务端”。
6. 按照提示配置用户网关参数。

参数	说明	取值样例
名称	SSL 服务端的名称。	SSL-server1
区域	VPN 网关所在的资源池。	华东 1


参数	说明	取值样例
VPN 网关	选择需要使用的 VPN 网关。	vpn-gateway-a5f1-ssl
虚拟私有云	选择要使用的 VPC 作为本端资源。	vpc-a7f3
本端子网	选择本端需要连接的子网网段信息（可以复选，最多 5 个网段）。	subnet-yl(192.168.0.0/24)
客户端地址池	配置客户端地址池范围。	10.0.0.0/24
协议	SSL VPN 使用的协议。 默认：TCP	TCP
端口	SSL VPN 使用的端口，端口可配置范围： 1024 ~ 49151。 默认：1194	1194
加密算法	SSL VPN 使用的加密算法。 默认：AES-256-GCM	AES-256-GCM
是否压缩	是否对传输数据进行压缩处理。 默认：否	否

参数	说明	取值样例
自定义 DNS	SSL VPN 需要配置的自定义 DNS 地址。	10.10.1.1
启用双因子认证	<ul style="list-style-type: none"> 启用双因子认证，客户端登录不仅需要证书，同时需要输入密码。 取消双因子认证，登录端登录只需要证书，无需密码。 	开启

7. 点击“确定”，创建成功。

步骤三：创建 SSL 客户端


创建 SSL 客户端时，需要选择绑定的 SSL 服务端，并指定账号名称。创建完成后，可以在该页面下载 SSL 证书和密码信息，用于服务端和客户端进行双向认证。

1. 登录[控制中心](#)。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 进入 SSL VPN 页面中，单击“SSL 客户端”，进入 SSL 客户端页面，单击“创建客户端”。
6. 按照提示配置用户网关参数，单击“确定”，创建成功。

参数	说明	取值样例
SSL 服务端	与当前创建客户端互联的 SSL 服务端。	SSL-server1
账号名称	用于客户端登陆的账号信息。	sslclient1
隧道限速	限速开关，选择是否对当前客户端的隧道进行限速。	关

7. 在操作列单击“查看账号密码”，记录该密码，客户端登录的时候使用。

步骤四：下载客户端证书

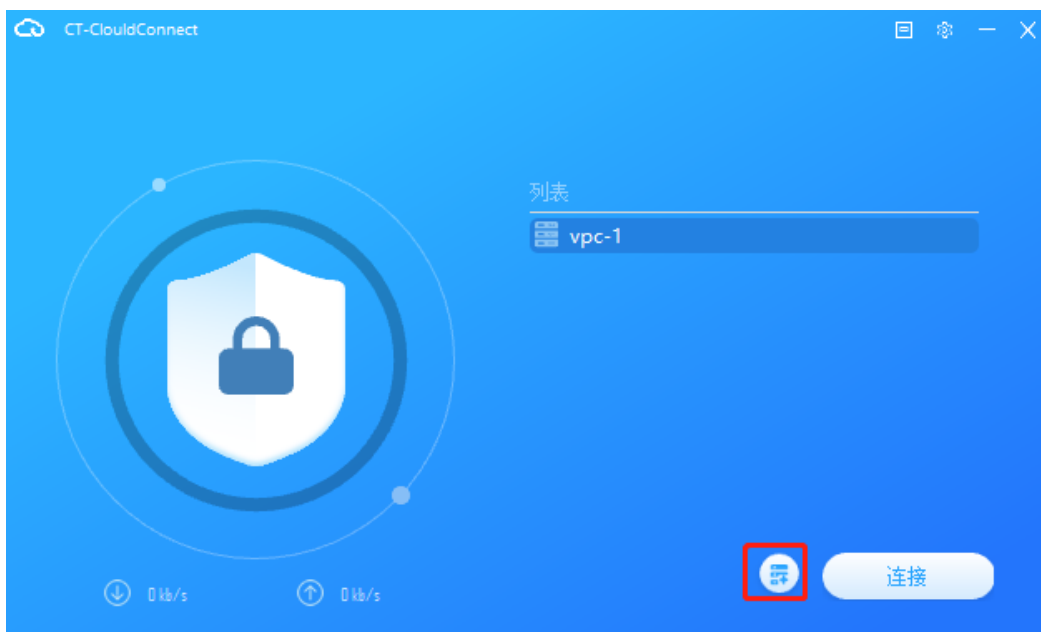
1. 登录[控制中心](#)。
2. 单击控制中心左上角的，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 进入 SSL VPN 页面中，单击“SSL 客户端”，进入 SSL 客户端页面。
6. 在 SSL 客户端页面，找到目标 SSL 客户端，在操作列单击“更多”，选择“证书下载”，一共三个证书。

步骤五：配置客户端

以 Windows 客户端为例进行操作说明，按照以下操作，安装并配置 Windows 客户

端。

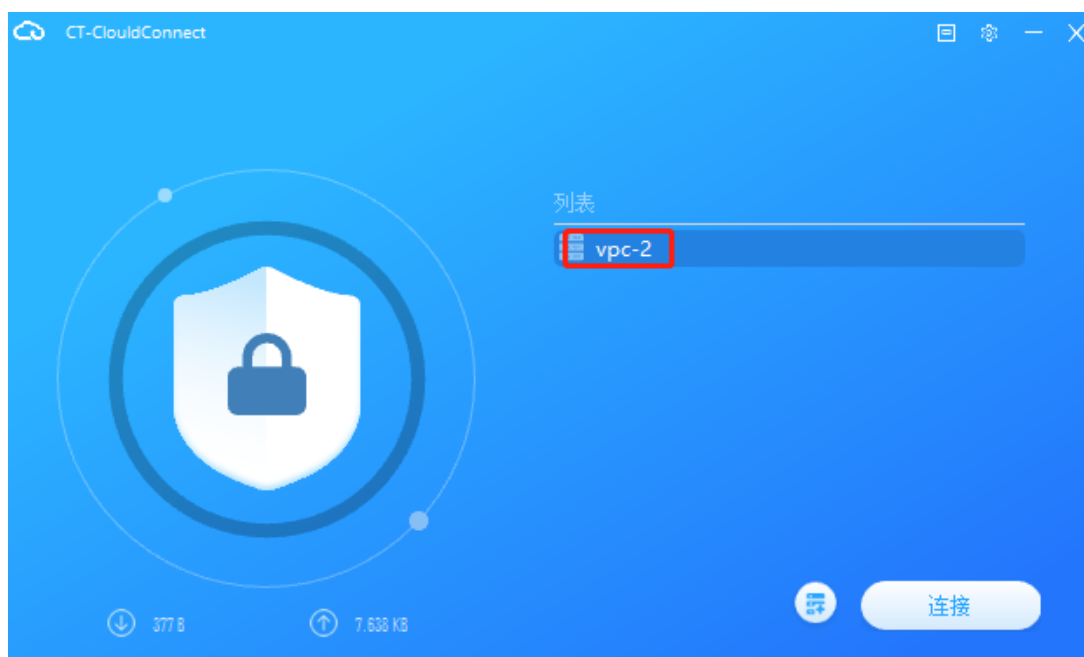
1. 下载[客户端](#)，选择“Windows 7 及以上版本”，单击“立即下载”，下载客户端软件并安装客户端软件。
2. 安装完成，打开 CT-CloudConnect 客户端软件，单击图中红色标识图标。



3. 单击“新增配置”，进入新增配置对话框。
4. 输入连接的名称，网关填写步骤一记录的 VPN 网关 IP 地址和步骤 2 配置的端口，这里以 121.229.145.113 : 1194 为例，单击“保存”，进入确认信息页面。



5. 在确认信息页面，单击“确认信息”。
6. 双击图中连接名称，如 vpc-2，进入新增配置（高级）页面。



7. 在新增配置（高级）页面，导入步骤四下载的三个证书，单击“保存”。

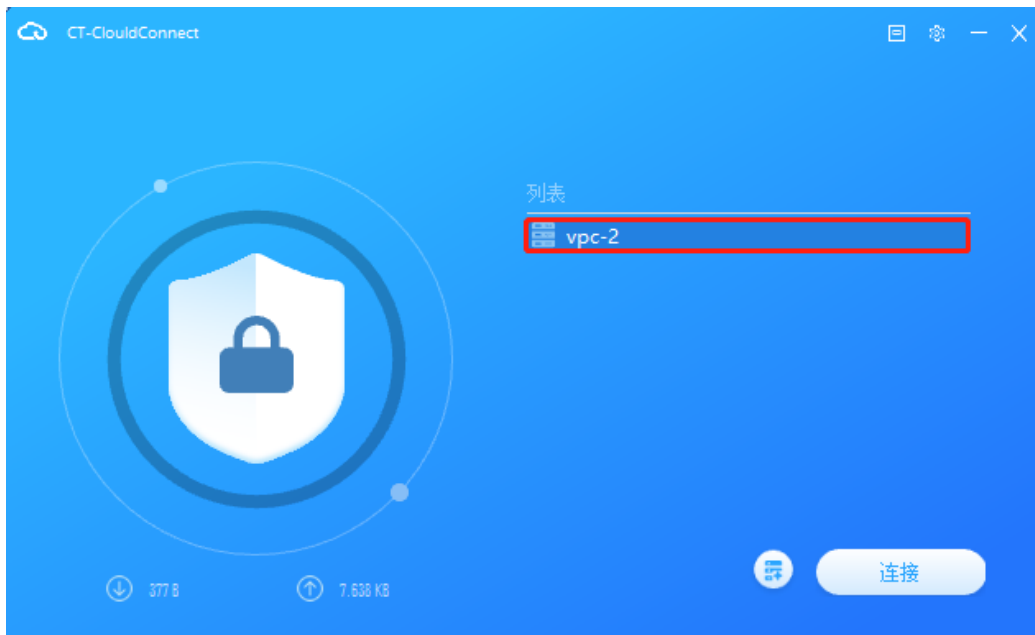
名称	<input type="text" value="vpc-2"/>
网关	<input type="text" value="121.229.145.113:1194"/>
用户名	<input type="text"/>
租户名称	<input type="text"/> 
CA 证书	<input type="text"/>  
	SHA1: fe45217e6d30dc008d282e100dc8f3a5dff42813
服务器证书	<input type="text"/> 
	SHA1: 573bafcc9bffb72f680ec39a0cbdb98e5d66fd2
OTP令牌	<input type="text" value="HOTP (RFC4226)"/> 
VPN协议	<input type="text" value="Cisco AnyConnect"/>
本地证书 <input type="radio"/> 系统存储区 <input type="radio"/>	
用户证书	<input type="text"/>  
	A1: cd116854158a6366d11762042dcd4e64cc39d23e
用户密钥	<input type="text"/>  
超时重连	<input type="text" value="60s"/>
DTLS尝试周期	<input type="text" value="16s"/>
<input type="checkbox"/> 连接时最小化	

步骤六：测试连通性

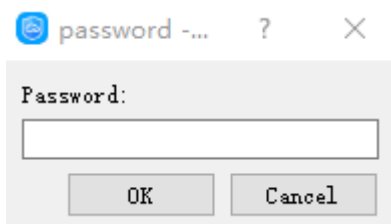
登录客户端，访问 VPC，测试网络连通性。

按照以下操作，测试 Windows 客户端与 VPC 的连通性。

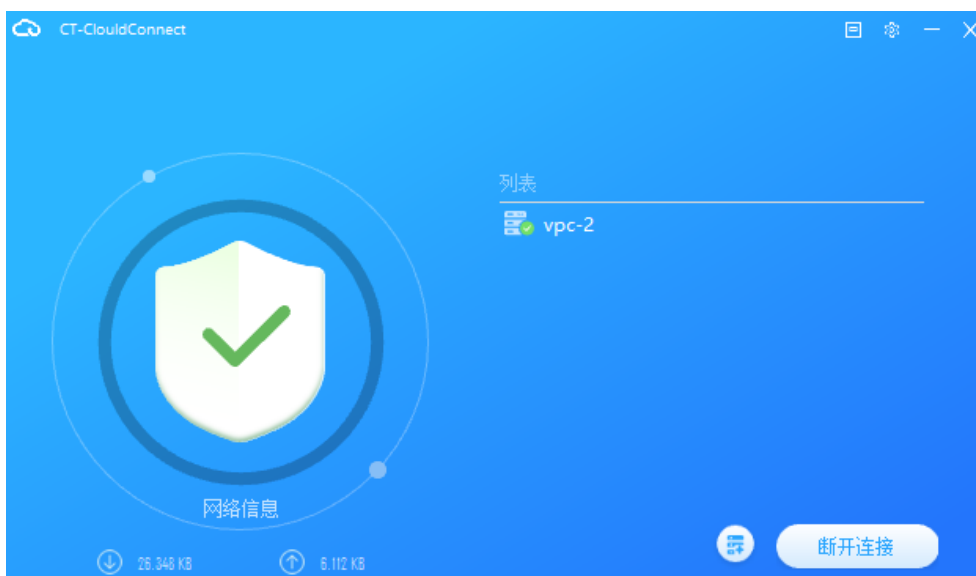
1. 单击图中的连接名称，如 vpc-2，单击“连接”，进入输入密码对话框。



2. 在输入密码对话框，输入步骤三记录的密码，单击“OK”



Windows 客户端上线成功。



经测试，Windows 客户端可以正常连接 VPC。

3 VPN 连接用户指南

3.1 管理 VPN 网关

3.1.1 创建和管理 VPN 网关实例

创建 VPN 网关

1. 登录[控制中心](#)。
2. 单击控制中心左上角的  ，选择目标资源池。
3. 在网络产品中选择“VPN 连接” ，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击“创建 VPN 网关” ，进入订购页面，按照提示配置参数。

参数	说明	取值样例
地域	VPN 网关所在的资源池。	华东 1
名称	VPN 网关的名称。	vpn-gateway-f0e0
网关类型	选择 VPN 网关的类型。	普通
实例类型	选择 VPN 网关的实例类型。	IPsec
企业项目	选择当前 VPN 网关归属项目。	default
本端类型	通过 VPN 网关接入的资源类型。	虚拟私有云 VPC
虚拟私有云	选择要使用的 VPC 作为本端资源。	vpc-682f

参数	说明	取值样例
子网	选择当前 VPC 中本端的子网资源。	subnet-682f (192.168.1.0/24)
IPsec 带宽	VPN 网关要通过弹性 IP 访问公网，这里选择对应的弹性 IP 带宽大小，单位 Mbps，5M 起售。	20M
IPsec 连接数	选择对应的 IPsec VPN 并发连接数。	20
购买时长	包年包月场景需要选择，购买 VPN 网关实例的时长。	6 个月
自动续订	资源到期后自动续订，按月购买时按月续订，按年购买时按年续订。	开启

5. 单击“下一步”。
6. 在购买确认页，勾选服务协议，点击“确认下单”，进入订单列表。
7. 在订单页面，单击“立即支付”，支付成功后，VPN 网关创建成功。

修改 VPN 网关

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。

3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，找到目标 VPN 网关实例，在操作列可以对 VPN 网关进行扩容、续订等操作。

删除 VPN 网关

- VPN 网关实例不支持删除，到期后将进入自动释放流程。
- 如果在 VPN 网关实例未到期前，您不需要再使用 VPN 网关实例，您可以申请退订，申请退订后系统会自动释放 VPN 网关实例。如果 VPN 网关下存在使用中的 IPsec 连接或 SSL 连接，则暂不支持退订，请删除相关连接配置后再申请退订。

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，找到目标 VPN 网关实例，在操作列单击“退订”。
5. 在退订 VPN 网关实例页面，单击“确定”，删除 VPN 网关实例。

查看 VPN 网关

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。

3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，找到目标 VPN 网关实例，单击目标 VPN 网关名称，进入 VPN 网关详情页。

3.1.2 配置 VPN 网关路由

3.1.2.1 网关路由概述

在创建目的路由模式的 IPsec 连接后，您还需要手动添加 VPN 网关路由。

基于路由的 IPsec VPN，不仅可以更方便地配置和维护 VPN 策略，而且还提供了灵活的流量路由方式。

您可以为 VPN 网关添加如下两种路由：

- 目的路由。
- 策略路由。

目的路由

目的路由仅基于目的 IP 进行路由转发。

添加目的路由的详细信息，请参见[使用目的路由](#)。

策略路由

策略路由基于源 IP 和目的 IP 进行更精确的路由转发。

添加策略路由的详细信息，请参见[使用策略路由](#)。

策略路由比目的路由的优先级高。

3.1.2.2 使用目的路由

- 当创建的 IPsec 连接配置的路由模式为“目的路由”时，您需要在 VPN 网关中配置路由，并发布路由到 VPC 路由表以实现本地数据中心和 VPC 的通信。
- 当创建的 IPsec 连接配置的路由模式为“感兴趣路由”时，无需执行此操作。


前提条件

您已经创建了 IPsec 连接，请参见[创建和管理 IPsec 连接](#)。

使用限制

不支持添加目标网段为 0.0.0.0/0 的目的路由。


添加目的路由

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击目标 VPN 网关名称。
5. 在目的路由页签，单击“添加路由条目”。
6. 在添加路由条目面板，根据以下信息配置目的路由，然后单击“确定”。


配置	说明	取值样例
目标网段	输入要访问的私网网段。	172.16.1.0/24
下一跳类型	选择 IPsec 连接。	IPsec 连接
下一跳	选择需要建立 IPsec VPN 连接的 IPsec 连接。	connection-2
是否发布	选择是否将新添加的路由发布到 VPC 路由表。	是

	<p>是（推荐）：将新添加的路由发布到 VPC 路由表。</p> <p>否：不发布新添加的路由到 VPC 路由表。</p> <p>说明 如果您选择否，添加目的路由后，您还需执行发布的操作。</p>	
权重	路由的优先级属性。	100（默认值）

撤回目的路由

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击目标 VPN 网关名称。
5. 在目的路由表页签，找到目标路由条目，在操作列单击“撤回”。
6. 在撤回路由对话框，单击“确定”，撤回已经发布的路由。

删除目的路由

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击目标 VPN 网关名称。

5. 在目的路由表页签，找到目标路由条目，先单击操作列的“撤回”，再单击“删除”。
6. 在删除路由条目对话框，单击“确定”，删除已经添加的路由。

3.1.2.3 使用策略路由

- 当创建的 IPsec 连接配置的路由模式为“目的路由”时，您需要在 VPN 网关中配置路由，并发布路由到 VPC 路由表以实现本地数据中心和 VPC 的通信。
- 当创建的 IPsec 连接配置的路由模式为“感兴趣路由”时，无需执行此操作。

前提条件

您已经创建了 IPsec 连接，请参见[创建和管理 IPsec 连接](#)。

使用限制

不支持添加目标网段为 0.0.0.0/0 的策略路由。


添加策略路由

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击目标 VPN 网关名称。
5. 在 VPN 网关实例详情页面，在“策略路由”页签，单击“添加路由条目”。
6. 在添加路由条目页面，根据以下信息配置策略路由，单击“确定”。

配置	说明	取值样例
目标网段	输入要访问的本地数据中心的私网	172.16.1.0/24


	网段。	
源网段	输入 VPN 网关实例关联的 VPC 侧的私网网段。	192.168.3.0/24
下一跳类型	选择 IPsec 连接。	IPsec 连接
下一跳	选择需要建立 IPsec VPN 连接的 IPsec 连接。	connection-2
是否发布	<p>选择是否将新添加的路由发布到 VPC 路由表。</p> <p>是（推荐）：将新添加的路由发布到 VPC 路由表。</p> <p>否：不发布新添加的路由到 VPC 路由表。</p> <p>说明 如果您选择否，添加策略路由后，您还需执行发布的操作。</p>	是
权重	路由的优先级属性。	100（默认值）

撤回策略路由

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击目标 VPN 网关名称。

5. 在 VPN 网关实例详情页面，单击“策略路由表”页签，找到目标路由条目，在操作列单击“撤回”。
6. 在撤回路由对话框，单击“确定”，撤回已经发布的路由。

删除策略路由

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，单击目标 VPN 网关名称。
5. 在 VPN 网关实例详情页面，单击“策略路由表”页签，找到目标路由条目，在操作列先单击“撤回”，再单击“删除”。
6. 在删除路由条目对话框，单击“确定”。

3.2 开启 IPsec VPN 和 SSL VPN


您可以在创建 VPN 网关时直接开启 IPsec VPN 和 SSL VPN 功能，也可以在创建 VPN 网关后根据需要再开启 IPsec VPN 或 SSL VPN 功能。

开启 IPsec VPN 功能

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，找到目标 VPN 网关实例，在功能配置列单击 IPsec 后的“开启”。

5. 在配置页面，选择“IPsec 带宽”、“IPsec 连接数”、“购买时长”，单击“下一步”。
6. 在购买确认页，勾选服务协议，单击“确认下单”，进入订单列表。
7. 在订单页面，单击“立即支付”，支付成功后，IPsec VPN 功能开启成功。

开启 SSL VPN 功能

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在 VPN 网关页面，找到目标 VPN 网关实例，在功能配置列单击 SSL 后的“开启”。
5. 在配置页面，选择“SSL 带宽”、“SSL 并发连接数”、“购买时长”，单击“下一步”。
6. 在购买确认页，勾选服务协议，单击“确认下单”，进入订单列表。
7. 在订单页面，单击“立即支付”，支付成功后，SSL VPN 功能开启成功。

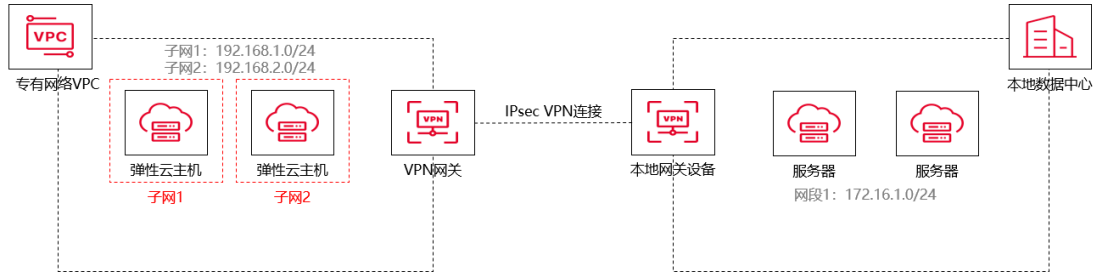
3.3 配置 IPsec VPN

3.3.1 IPsec VPN 配置概览

场景示例

以下图组网场景为例，某公司在天翼云创建了 VPC，子网网段为 192.168.1.0/24

和 192.168.2.0/24。本地数据中心的网段为 172.16.1.0/24，本地网关设备的公网 IP 为 121.XX.XX.113。公司因业务发展，需要将本地数据中心与云上 VPC 互通。您可以通过 IPsec VPN，建立本地数据中心与云上 VPC 的连接，实现云上和云下的加密通信。



环境要求

- 本地数据中心的 VPN 网关设备必须配置公网 IP 地址。
- 本地数据中心的 VPN 网关设备必须支持 IKEv1 或 IKEv2 协议，支持任何一种协议的设备均可以和天翼云 VPN 网关建立 IPsec VPN 连接。
- 本地数据中心和天翼云 VPC 间互通的网段没有重合。

使用流程



创建VPN网关 创建用户网关 创建IPsec连接 配置VPN网关路由（可选） 配置本地网关 测试连通性

1. 创建 VPN 网关

创建 VPN 网关并开启 IPsec VPN 功能，一个 VPN 网关可以建立多条 IPsec 连接。

2. 创建用户网关

通过创建用户网关，您可以将本地数据中心 VPN 网关设备的信息注册到天翼云上。

3. 创建 IPsec 连接

IPsec 连接是指 VPN 网关和本地数据中心 VPN 网关设备建立连接后的 VPN 隧道。只有在建立 IPsec 隧道后，本地数据中心才能使用 VPN 网关进行加密通信。

4. 配置 VPN 网关路由（可选）。

- 当创建的 IPsec 连接配置的路由模式为“目的路由”时，您需要在 VPN 网关中配置路由，并发布路由到 VPC 路由表以实现本地数据中心和 VPC 的通信。
- 当创建的 IPsec 连接配置的路由模式为“感兴趣路由”时，无需执行此操作。

5. 配置本地网关设备

您需要在本地数据中心的网关设备中添加 VPN 配置。

6. 测试连通性

登录到天翼云 VPC 内一台弹性云主机实例，通过 ping 命令，ping 本地数据中心内一台服务器的私网 IP 地址（未禁用 ping 探测），验证通信是否正常。

3.3.2 管理用户网关

3.3.2.1 创建用户网关

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入用户网关列表页面。


5. 单击“创建用户网关”。
6. 按照提示配置用户网关参数。

参数	说明	取值样例
名称	用户网关的名称。	user-gateway-5da3
IP 地址	对端 VPN 网关的静态公网 IP 地址，对端网关必须具有固定的公网 IP，不能是动态 IP。	121.XX.XX.113

7. 单击“确定”，创建成功。


3.3.2.2 修改用户网关

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入用户网关列表页面。
5. 在用户网关列表页，找到目标用户网关，在操作列单击“修改”，可以修改用户网关的名称和描述信息。

3.3.2.3 删除用户网关

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择 “VPN 连接” ，进入 VPN 连接页面。
4. 在左侧网络控制台，选择 “IPsec VPN” ，进入用户网关列表页面。
5. 在用户网关列表页，找到待删除的用户网关，在操作列单击 “删除” ，可以删除用户网关。

注意：如果用户网关上已经配置了 VPN 连接，则用户网关不允许删除。

3.3.3 管理 IPsec 连接

3.3.3.1 创建和管理 IPsec 连接

前提条件

- 在创建 IPsec 连接前，请先了解 IPsec VPN 连接的使用流程，并依据使用流程完成创建 IPsec 连接的所有前置操作步骤。
- 如果 IPsec 连接绑定了国密型的 VPN 网关实例，则在创建 IPsec 连接前，需要在证书管理中上传相关的国密证书。

创建 IPsec 连接（普通型-密钥认证）

1. 登录控制中心。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。


3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入 IPsec VPN 页面。
5. 单击“IPsec 连接”，进入“IPsec 连接”页签。
6. 单击“创建 IPsec 连接”，按照提示配置参数。

参数	说明	取值样例
名称	VPN 连接的名称。	connection-1
VPN 网关	选择已经创建的 VPN 网关。	vpn-gateway-46c1- ipsec
用户网关	选择已经创建的用户网关。	user-gateway-5da3
路由模式	支持目的路由和感兴趣路由两种路由模式。	感兴趣路由
本端子网	选择 VPC 侧哪个子网需要和企业侧进行联通。	subnet- b2a0(192.168.1.0/24)
对端网段	配置企业侧哪个网段需要和 VPC 侧进行联通。	172.16.1.0/24
协商生效	支持立即协商和流量触发两种协商方式。	立即生效
认证方式	支持密钥认证和证书认证两种认证方式。	密钥认证
预共享密钥	认证方式选择密钥认证时，用于设置自定义密钥。	ctyun***01

确认密钥	认证方式选择密钥认证时，用于设置确认密钥。	ctyun***01
LocalId	支持 FQDN 和 IP 格式	默认为当前选取的网关地址，如 11.XX.XX.11
RemoteId	支持 FQDN 和 IP 格式	默认选择用户网关的公网地址，如 121.XX.XX.113

7. 单击“确认”，完成 IPsec 连接创建。

创建 IPsec 连接（普通型-证书认证）

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入 IPsec VPN 页面。
5. 单击“IPsec 连接”，进入“IPsec 连接”页签。
6. 单击“创建 IPsec 连接”，按照提示配置参数。


参数	说明	取值样例
名称	VPN 连接的名称。	connection-1
VPN 网关	选择已经创建的 VPN 网关。	vpn-gateway-46c1- ipsec
用户网关	选择已经创建的用户网关。	user-gateway-5da3

路由模式	支持目的路由和感兴趣路由两种路由模式。	感兴趣路由
本端子网	选择 VPC 侧哪个子网需要和企业侧进行联通。	subnet-b2a0(192.168.1.0/24)
对端网段	配置企业侧哪个网段需要和 VPC 侧进行联通。	172.16.1.0/24
协商生效	支持立即协商和流量触发两种协商方式。	立即生效
认证方式	支持密钥认证和证书认证两种认证方式。	证书认证
认证选择	认证方式选择证书认证时，用于选择使用的加密证书。支持选择“自签（默认）”或自行上传的证书。	自签（默认）
LocalId	仅支持 DN 格式。	系统默认填充，不支持修改。
Remoteld	仅支持 DN 格式。	系统默认填充，不支持修改。

7. 单击“确认”，完成 IPsec 连接创建。

创建 IPsec 连接（国密型）

1. 登录控制中心。

2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择 “VPN 连接” ，进入 VPN 连接页面。
4. 在左侧网络控制台，选择 “IPsec VPN” ，进入 IPsec VPN 页面。
5. 单击 “IPsec 连接” ，进入 “IPsec 连接” 页签。
6. 单击 “创建 IPsec 连接” ，按照提示配置参数。

参数	说明	取值样例
名称	VPN 连接的名称。	connection-1
VPN 网关	选择已经创建的 VPN 网关。	vpn-gateway-46c1- ipsec
用户网关	选择已经创建的用户网关。	user-gateway-5da3
路由模式	支持目的路由和感兴趣路由两种路由模式。	感兴趣路由
本端子网	选择 VPC 侧哪个子网需要和企业侧进行联通。	subnet- b2a0(192.168.1.0/24)
对端网段	配置企业侧哪个网段需要和 VPC 侧进行联通。	172.16.1.0/24
协商生效	支持立即协商和流量触发两种协商方式。	立即生效
认证方式	支持证书认证。	证书认证

认证选择	认证方式选择证书认证时，用于选择使用的加密证书。需要先在证书管理中上传相关的国密证书。	cert-e437
LocalId	仅支持 DN 格式，非必填。	建议留空。
Remoteld	远端用户网关证书的名称，仅支持 DN 格式，名称需要从对端使用的证书中获取。	/CN=vpn2.home.gm.sig /OU=ctyun/O=ctyun/C =cn

7. 单击“确认”，完成 IPsec 连接创建。

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、SHA256、SHA384、SHA512、SM3（国密型网关使用）。 默认配置为：SHA1	SHA256
加密算法	加密算法，支持的算法： AES-128、AES-192、 AES-256、3DES、SM4	AES-128

	<p>(国密型网关使用)。</p> <p>默认配置为：AES-128</p>	
DH 算法	<p>Diffie-Hellman 密钥交换算法，支持的算法：</p> <p>Group 2、Group 5、Group 14。</p> <p>默认配置为：Group 5</p>	Group 14
版本	<p>IKE 密钥交换协议版本，支持的版本：v1、v2、国密 IKE。</p> <p>默认配置为：v1</p>	v2
生命周期 (秒)	<p>安全联盟 (SA—Security Associations) 的生存时间，单位：秒。</p> <p>在超过生存时间后，安全联盟将被重新协商。</p> <p>默认配置为：86400</p>	86400
协商模式	<p>支持 Main、Aggressive 两种模式。</p> <p>默认配置为：Main</p>	Main

IPsec 策略

参数	说明	取值样例
认证算法	<p>认证哈希算法，支持的算法：SHA1、SHA256、SHA384、SHA512、SM3（国密型网关使用）。</p> <p>默认配置为：SHA1</p>	SHA2-256
加密算法	<p>加密算法，支持的算法：AES-128、AES-192、AES-256、3DES、SM4（国密型网关使用）。</p> <p>默认配置为：AES-128</p>	AES-128
PFS	<p>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。</p> <p>PFS 组支持的算法：DH group 2、DH group 5、DH group 14。</p> <p>默认配置为：DH group 5</p>	DH group 14

DPD	选择开启或关闭对等体存活检测功能。 默认配置为：启用	启用
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：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

3.3.3.2 修改 IPsec 连接

创建 IPsec 连接后，您可以修改 IPsec 连接的配置信息。

操作步骤


1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入 IPsec VPN 页面。

5. 单击“IPsec 连接”，进入“IPsec 连接”页签。
6. 在 IPsec 连接页面，在操作列单击“修改”，进入修改 IPsec 连接页面。
7. 在修改 IPsec 连接页面，可以修改 IPsec 连接名称、本段子网、对端网段、协商生效、认证方式以及高级配置等信息，修改完成，单击“确认”。

3.3.3.3 下载证书

当创建的 IPsec 连接的认证方式为证书认证，且认证选择为自签时，天翼云 VPN 网关会自动为您生成认证证书，您需要在 IPsec 连接页面下载相关的证书，并导入您本地数据中心的设备。

操作步骤


1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“IPsec VPN”，进入 IPsec VPN 页面。
5. 单击“IPsec 连接”，进入“IPsec 连接”页签。
6. 在 IPsec 连接页面，在操作列单击“证书下载”，下载根证书、证书和密钥文件。

3.3.3.4 下载 IPsec 连接配置

创建 IPsec 连接后，您可以下载 IPsec 连接的配置。

操作步骤

1. 登录控制中心。

2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择 “VPN 连接” ，进入 VPN 连接页面。
4. 在左侧网络控制台，选择 “IPsec VPN” ，进入 IPsec VPN 页面。
5. 单击 “IPsec 连接” ，进入 “IPsec 连接” 页签。
6. 在 IPsec 连接页面，在操作列单击 “更多” ，选择 “下载对端配置” ，查看配置信息，本地网关设备需要照此进行配置，如果配置不一致，会导致协商失败。
7. 在下载对端配置对话框，单击 “确定” 关闭对话框。

3.3.3.5 删除 IPsec 连接

注意：当路由条目的下一跳指向了某 IPsec 连接时，该 IPsec 连接不允许被删除。

操作步骤

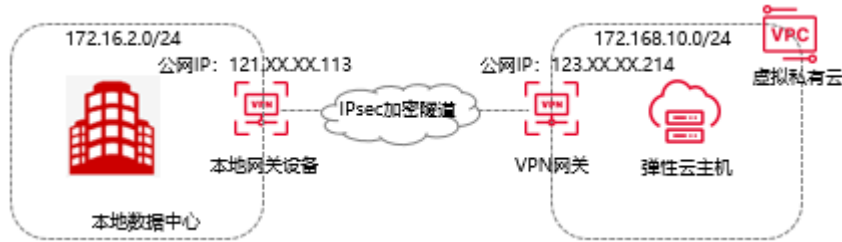
1. 登录控制中心。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择 “VPN 连接” ，进入 VPN 连接页面。
4. 在左侧网络控制台，选择 “IPsec VPN” ，进入 IPsec VPN 页面。
5. 单击 “IPsec 连接” ，进入 “IPsec 连接” 页签。
6. 在 IPsec 连接页面，在操作列单击 “更多” ，选择 “删除” 。
7. 在删除对话框，单击 “确定” ，删除 IPsec 连接。

3.3.4 本地网关配置

3.3.4.1 strongSwan 配置

使用 IPsec VPN 建立站点到站点的连接时，在配置完 VPN 网关后，您还需在本地数据中心的网关设备中添加 VPN 配置。

场景示例



本文以上图场景为例。某公司在天翼云拥有一个 VPC，VPC 网段为 192.168.10.0/24，VPC 中使用弹性云主机部署了应用服务。同时该公司在本地拥有一个数据中心 IDC，本地 IDC 网段为 172.16.2.0/24。公司因业务发展，需要本地 IDC 与云上 VPC 互通，实现资源互访。该公司计划使用 IPsec VPN 产品，在本地 IDC 与云上 VPC 之间建立 IPsec 连接，实现云上和云下的互通。

本文涉及的网络配置请参见下表。

配置项	示例值
VPC	待和本地 IDC 互通的私网网段。
VPN 网关	天翼云 VPN 网关的公网 IP 地址。
本地 IDC	待和天翼云 VPC 互通的私网网段。
	本地网关设备的公网 IP 地址。

前提条件

- 已下载 IPsec 连接的配置。

- 已在天翼云侧完成创建 VPN 网关、创建用户网关、创建 IPsec 连接、配置 VPN 网关路由的操作。

本文 IPsec 连接的配置如下表所示。

配置项		示例值
预共享密钥		aa123bb****
IKE 配置	IKE 版本	IKEv1
	协商模式	main
	加密算法	AES-128
	认证算法	SHA1
	DH 分组	Group2
	SA 生存周期 (秒)	86400
IPsec 配置	加密算法	AES-128
	认证算法	SHA1
	PFS	DH group2
	SA 生存周期 (秒)	3600

步骤一：安装 strongSwan 软件

步骤涉及的命令仅供参考，实际配置命令请以您本地网关设备的操作手册为准。

1. 登录本地网关设备的命令行界面。
2. 执行以下命令安装 strongSwan 软件。

```
yum install strongswan
```

3. 可选：执行以下命令查看系统自动安装的 strongSwan 软件版本。

```
strongswan version
```

步骤二：配置 strongSwan

1. 执行以下命令打开 ipsec.conf 配置文件。

```
vi /etc/strongswan/ipsec.conf
```

2. 请参见以下配置，更改 ipsec.conf 配置文件。

```
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup

    uniqueids=never

conn %default

    authby=psk                #使用预共享密钥认证方式

    type=tunnel

conn tomyidc

    keyexchange=ikev1        #IPsec 连接使用的 IKE 协议的版本

    left=121.XX.XX.113       #本地网关设备的公网 IP 地址。如果您使用本地网关设备的私网 IP 地址建立 IPsec VPN 连接，则本项需配置为本地网关设备的私网 IP 地址。

    leftsubnet=172.16.2.0/24 #本地 IDC 待和 VPC 互通的私网网段

    leftid=121.XX.XX.113     #本地网关设备的标识。如果您使用本地网关设备的私网 IP 地址建立 IPsec VPN 连接，建议您使用本地网关设备的私网 IP 地址作为标识。

    right=123.XX.XX.214      #VPN 网关的公网 IP 地址
```

```
rightsubnet=192.168.10.0/24 #VPC 待和本地 IDC 互通的私网网段

rightid=123.XX.XX.214      #VPN 网关的标识

auto=route

ike=aes-sha1-modp1024      #IPsec 连接中 IKE 协议的加密算法-认证算法
-DH 分组

ikelifetime=86400s        #IKE 协议的 SA 生命周期

esp=aes-sha1-modp1024      #IPsec 连接中 IPsec 协议的加密算法-认证
算法-DH 分组

lifetime=3600s            #IPsec 协议的 SA 生命周期

type=tunnel
```

3. 配置 ipsec.secrets 文件。

A. 执行以下命令打开 ipsec.secrets 文件。

```
vi /etc/strongswan/ipsec.secrets
```

B. 添加以下配置。以下两种配置方式，任选一种即可。

方式一：

```
121.XX.XX.113 123.XX.XX.214 : PSK aa123bb**** #aa123bb****为预共享
密钥，本地 IDC 和 VPN 网关的预共享密钥需保持一致。
```

方式二：

```
123.XX.XX.214 : PSK aa123bb**** #aa123bb****为 IPsec 连接的预共享密
钥，本地 IDC 侧和 VPN 网关侧的预共享密钥需保持一致。
```

4. 打开系统转发配置。

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

5. 执行以下命令启动 strongSwan 服务。

```
systemctl enable strongswan  
systemctl start strongswan
```

6. 在您本地 IDC 侧，设置本地 IDC 客户端到 strongSwan 本地网关设备及 strongSwan 本地网关设备到本地 IDC 客户端的路由。
7. 如果您使用 strongSwan 建立了 3 条（不包含 3 条）以上的 IPsec 连接，您需要修改/etc/strongswan/strongswan.d/charon.conf 中的配置。

删除 max_ikev1_exchanges = 3 命令前的注释符号，启用此命令，并修改命令中参数的值大于您建立的 IPsec 连接数。

例如：您使用 strongSwan 建立了 4 条 IPsec 连接，您可以修改该命令为

max_ikev1_exchanges = 5。

3.3.4.2 Juniper 防火墙配置

使用 IPsec VPN 建立站点到站点的连接时，在配置完天翼云 VPN 网关后，您还需在本地站点的网关设备中进行 VPN 配置。

前提条件

- 已经在天翼云 VPC 内创建了 IPsec 连接。
- 已经下载了 IPsec 连接的配置。

IPsec 协议信息

配置		示例值
IKE	认证算法	SHA256
	加密算法	3DES

	DH 分组	Group2
	IKE 版本	IKEv1
	生命周期	86400
	协商模式	main
	PSK	aa123bb****
IPsec	认证算法	SHA256
	加密算法	3DES
	PFS	DH group2
	生命周期	3600

网络配置信息

配置项	
VPC	待和本地 IDC 互通的私网网段。
VPN 网关	天翼云 VPN 网关的公网 IP 地址。
本地 IDC	待和天翼云 VPC 互通的私网网段。
	本地网关设备的公网 IP 地址。

操作步骤

按照以下操作，在 Juniper 防火墙中加载用户网关的配置。

1. 登录防火墙设备的命令行配置界面。
2. 配置基本网络、安全域和地址簿信息。

```
Set security zones security-zone trust address-book address net-cfgr_192-
```

```
168-18-0--24 192.168.18.0/24
```

```
set security zones security-zone vpn address-book address net-cfgr_192-
```

```
168-1-0--24 192.168.1.0/24
```

3. 配置 IKE 策略。

```
set security ike policy ike-policy-cfgr mode main
```

```
set security ike policy ike-policy-cfgr pre-shared-key ascii-text
```

```
"aa123bb****"
```

4. 配置 IKE 网关、出接口和协议版本。

```
set security ike gateway ike-gate-cfgr ike-policy ike-policy-cfgr
```

```
set security ike gateway ike-gate-cfgr address 121.xxx.xxx.113
```

```
set security ike gateway ike-gate-cfgr external-interface ge-0/0/3
```

```
set security ike gateway ike-gate-cfgr version v1-only
```

5. 配置 IPsec 策略。

```
set security ipsec policy ipsec-policy-cfgr proposal-set standard
```

6. 应用 IPsec 策略。

```
set security ipsec vpn ipsec-vpn-cfgr ike gateway ike-gate-cfgr
```

```
set security ipsec vpn ipsec-vpn-cfgr ike ipsec-policy ipsec-policy-cfgr
```

```
set security ipsec vpn ipsec-vpn-cfgr bind-interface st0.0
```

```
set security ipsec vpn ipsec-vpn-cfgr establish-tunnels immediately
```



```
set security ipsec policy ipsec-policy-cfgr perfect-forward-secrecy keys  
group2
```

7. 配置出站策略。

```
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr  
match source-address net-cfgr_192-168-18-0--24  
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr  
match destination-address net-cfgr_192-168-1-0--24  
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr  
match application any  
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr  
then permit
```

8. 配置入站策略。

```
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr  
match source-address net-cfgr_192-168-1-0--24  
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr  
match destination-address net-cfgr_192-168-18-0--24  
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr  
match application any  
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr  
then permit
```

3.3.4.3 思科防火墙配置

使用 IPsec VPN 建立站点到站点的连接时，在配置完天翼云 VPN 网关后，您还需在本地站点的网关设备中进行 VPN 配置。

背景信息

VPC 和本地 IDC 的网络配置如下：

配置项	
VPC	待和本地 IDC 互通的私网网段。
VPN 网关	天翼云 VPN 网关的公网 IP 地址。
本地 IDC	待和天翼云 VPC 互通的私网网段。
	本地网关设备的公网 IP 地址。

前提条件

- 您已经在天翼云 VPC 内创建了 IPsec 连接。
- 已经下载了 IPsec 连接的配置。

配置 IKEv1 VPN

协议	配置	示例值
IKE	认证算法	SHA1
	加密算法	AES-128
	DH 分组	Group2
	IKE 版本	IKEv1
	生命周期	86400
	协商模式	main
	PSK	aa123bb****

IPsec	认证算法	SHA1
	加密算法	AES-128
	PFS	DH group2
	生命周期	3600
	传输协议	ESP

操作步骤

1. 登录防火墙设备的命令行配置界面。
2. 配置 isakmp 策略。

```
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. 配置预共享密钥。

```
crypto isakmp key aa123bb**** address 121.XX.XX.113
```

4. 配置 IPsec 安全协议。

```
crypto ipsec transform-set ipsecpro64 esp-aes esp-sha-hmac
mode tunnel
```

5. 配置 ACL (访问控制列表), 定义需要保护的数据流。

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.11.0 0.0.0.255
```

如果本地网关设备配置了多网段，则需要分别针对多个网段添加 ACL 策略。

6. 配置 IPsec 策略。

```
crypto map ipsecpro64 10 ipsec-isakmp  
  
set peer 121.XX.XX.113  
  
set transform-set ipsecpro64  
  
set pfs group2  
  
match address 100
```

7. 应用 IPsec 策略。

```
interface g0/0  
  
crypto map ipsecpro64
```

8. 配置静态路由。

```
ip route 192.168.10.0 255.255.255.0 121.XX.XX.113  
  
ip route 192.168.11.0 255.255.255.0 121.XX.XX.113
```

9. 测试连通性。

您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。

3.3.4.4 山石防火墙配置

使用 IPsec VPN 建立站点到站点的连接时，在配置完天翼云 VPN 网关后，您还需在本地站点的网关设备中进行 VPN 配置。

前提条件

- 已经在天翼云 VPC 内创建了 IPsec 连接。
- 已经下载了 IPsec 连接的配置。

IPsec 协议信息

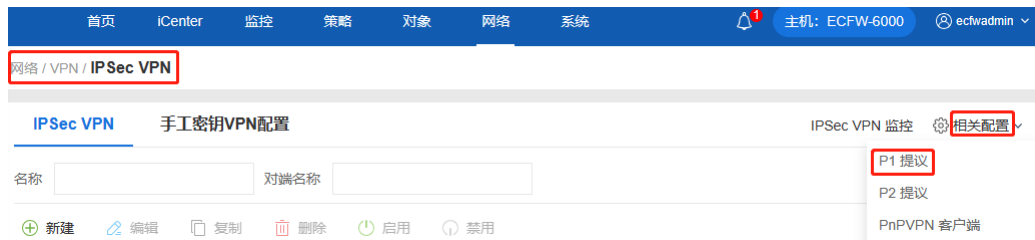
配置		示例值
IKE	认证算法	SHA256
	加密算法	3DES
	DH 分组	Group14
	IKE 版本	IKEv1
	生命周期	86400
	协商模式	main
	PSK	aa123bb****
IPsec	认证算法	SHA256
	加密算法	3DES
	PFS	DH group5
	生命周期	3600

网络配置信息

配置项	
VPC	待和本地 IDC 互通的私网网段。
VPN 网关	天翼云 VPN 网关的公网 IP 地址。
本地 IDC	待和天翼云 VPC 互通的私网网段。
	本地网关设备的公网 IP 地址。

操作步骤

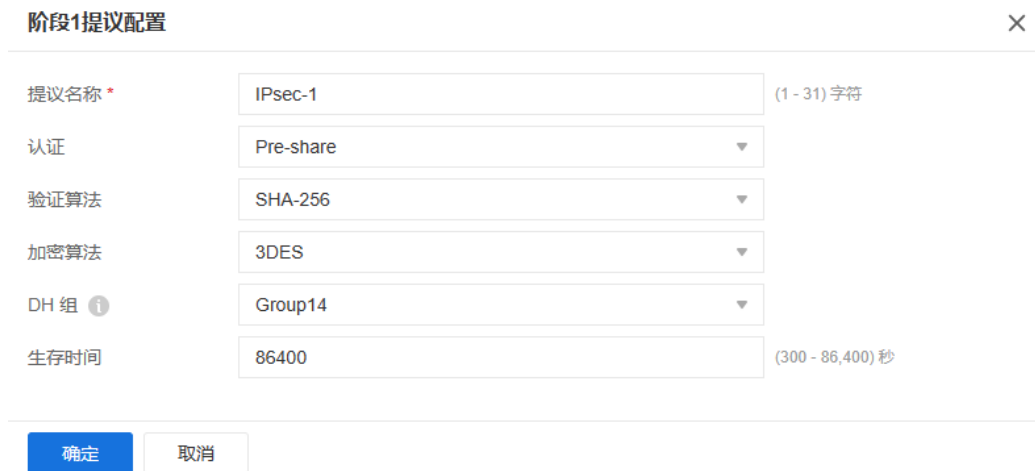
1. 登录防火墙 Web 页面，在网络>VPN>IPsec VPN 页面，在右上角的相关配置中选择 P1 提议，进入 P1 提议页面。



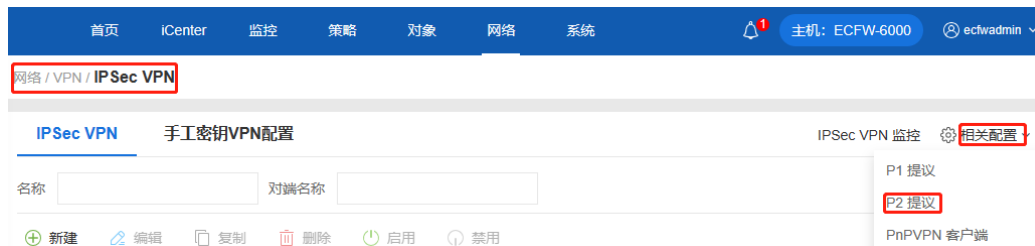
2. 在 P1 提议页面，单击“新建”，进入阶段 1 提议配置页面。



3. 在阶段 1 提议配置页面，根据天翼云 IPsec 连接中的配置信息进行配置，单击“确定”，完成配置。



4. 在右上角的相关配置中选择 P2 提议，进入阶段 2 提议页面。



5. 在 P2 提议页面，单击“新建”，进入阶段 2 提议配置页面。

P2 提议 ×

+ 新建 编辑 删除

<input type="checkbox"/>	名称	协议	验证算法	加密算法	压缩	PFS 组	生存时间	生存大小
<input type="checkbox"/>	esp-sha256-...	esp	sha-256	aes		2	28,800 秒	
<input type="checkbox"/>	esp-sha256-...	esp	sha-256	aes		no pfs	28,800 秒	

6. 在阶段 2 提议配置页面，根据天翼云 IPsec 连接中的配置信息进行配置，单击“确定”，完成配置。

阶段2提议配置 ×

提议名称 * (1 - 31) 字符

协议 ESP AH

验证算法 ⓘ MD5 SHA-256 SHA-512 NULL
 SHA SHA-384 SM3

加密算法 ⓘ 3DES AES-256 AES-GCM-192 NULL
 AES DES AES-GCM-256
 AES-192 AES-GCM-128 SM4

压缩 None Deflate

PFS 组 ⓘ ▼

生存时间 (180 - 86,400) 秒

启用生存大小

确定 取消

7. 在 IPsec VPN 页面，单击“新建”，进入 IPsec VPN 配置页面。

网络 / VPN / IPsec VPN

IPsec VPN 手工密钥VPN配置 IPsec VPN 监控 ⚙️ 相关配置 ▼

名称 对端名称

+ 新建 编辑 复制 删除 启用 禁用

8. 在 IPsec VPN 配置页面，展开“对端选择”下拉框，单击 +，进入 VPN 对端配置页面。



云下一代防火墙 ECFW

网络 / VPN / IPsec VPN

IPSec VPN 配置

对端名称

对端选项 *

隧道

名称 * ctyun_ipsec (1 - 31) 字符

模式 **隧道模式** 传输模式

P2提议 *

代理 ID **自动** 手工

高级配置 ▶

确定 取消

9. 在 VPN 对端配置页面 根据天翼云 IPsec 连接中的配置信息进行配置 ,单击 “确定” , 完成配置。

VPN 对端配置

接口 *	ethernet0/0
协议标准	<input checked="" type="checkbox"/> IKEV1 <input type="checkbox"/> GUOMI
认证模式	<input checked="" type="checkbox"/> 主模式 <input type="checkbox"/> 野蛮模式
类型	<input checked="" type="checkbox"/> 静态 IP <input type="checkbox"/> 动态 IP <input type="checkbox"/> 用户组
对端地址 *	121.**.**.80
本地 ID类型	
对端 ID类型	
提议 1 *	IPsec-1
提议 2	
提议 3	
提议 4	
预共享密钥 * (5 - 127) 字符
高级配置 ▶	

10. 在 IPsec VPN 配置页面，选择创建好的对端体，并根据天翼云 IPsec 连接中的配置信息完成隧道配置，单击“确定”。

网络 / VPN / IPsec VPN

IPsec VPN 配置

对端名称

对端选项 *

隧道

名称 * (1 - 31) 字符

模式 隧道模式 传输模式

P2提议 *

代理 ID 自动 手工

高级配置 ▶

11. 配置完成后，可以在 IPsec VPN 页面查看相关配置信息。

网络 / VPN / IPsec VPN

IPsec VPN 手工密钥VPN配置 IPsec VPN 监控 相关配置

名称 对端名称

<input type="checkbox"/>	名称	启用状态	对端名称	对端地址	接口	P1 提议	P2 提议	认证模式	协议标准
<input type="checkbox"/>	IPsec-1	<input checked="" type="checkbox"/>	ctyun_ipsec	121.229.11...	ethernet0/0	ctyun-ipsec...	IPsec-1	主模式	IKEV1

12. 在网络>安全域页面，单击“新建”按钮新建安全域。在安全域名称页面，输入安全域的名称，并在类型中选择三层安全域。



13. 在网络>接口页面，单击“新建”隧道接口，在隧道接口配置页面，根据提示输入配置接口名称、安全域、IP配置、绑定隧道配置（选择IPSec VPN及VPN名称）等，单击“确定”，完成配置。

隧道接口

接口名称 * tunnel 11 (1 - 64)

描述 (0 - 63) 字符

绑定安全域 二层安全域 三层安全域 TAP 无绑定

安全域 * ctyun

HA同步

IP配置

类型 静态IP 自动获取 PPPoE

IP地址 12.**.**.2

子网掩码 24

配置为Local IP

高级选项 DHCP v

确定 取消

隧道接口

接口名称 * tunnel 11 (1 - 64)

描述 (0 - 63) 字符

绑定安全域 二层安全域 三层安全域 TAP 无绑定

安全域 * ctyun

HA同步

IP配置

类型 静态IP 自动获取 PPPoE

IP地址

子网掩码

配置为Local IP

确定 取消

14. 在策略>安全策略页面，单击“新建”，进入安全策略页面。根据提示输入配置，单击“确定”，配置完成。

策略 / 安全策略 / 策略

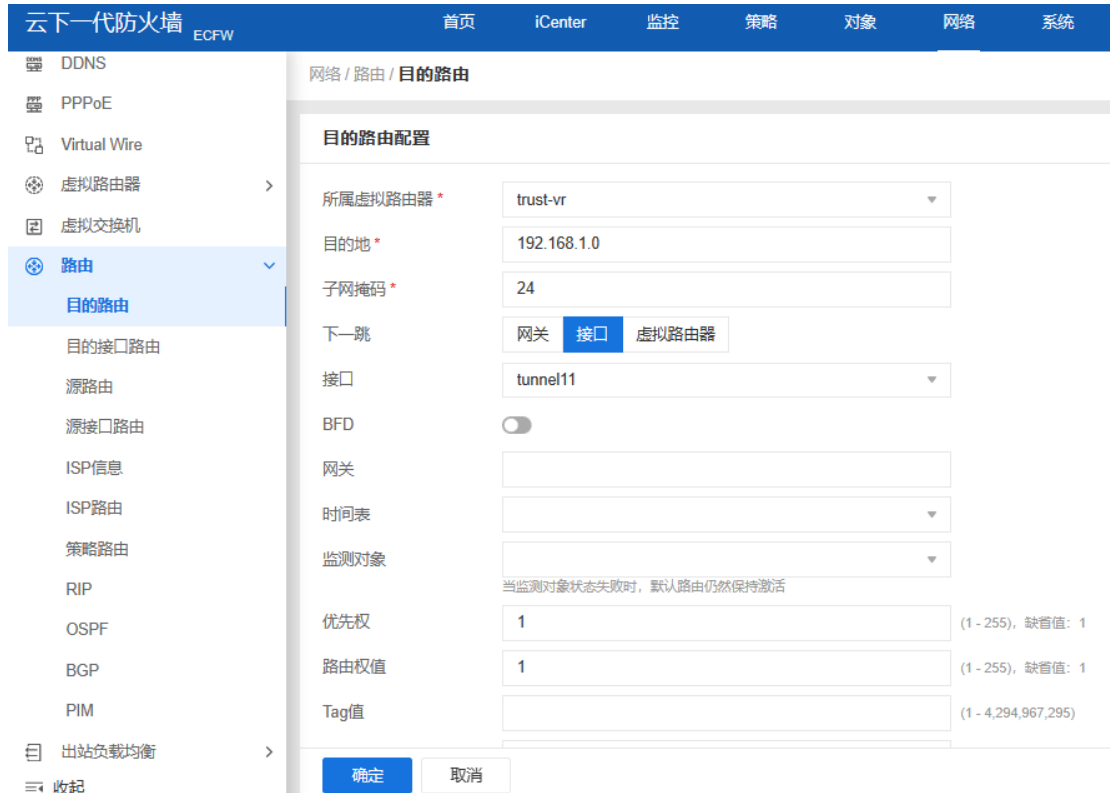
策略配置

名称	<input type="text"/>	(0 - 95) 字符
源安全域	Any	最大选中数为1
源地址	<input type="text" value="Any"/>	最大选中数为1,024
	<input type="button" value="+"/>	
源用户	<input type="text"/>	用户, 用户组, 角色最大选中数分别为8
目的安全域	Any	最大选中数为1
目的地址	<input type="text" value="Any"/>	最大选中数为1,024
	<input type="button" value="+"/>	
服务	Any	最大选中数为1,024
	<input type="button" value="+"/>	
应用	<input type="text"/>	最大选中数为1,024
VLAN ID	<input type="text"/>	最多配置32条

(每个VLAN ID, 请至少配置一个)

15. 在网络>路由页面，单击“新建”分别添加上行和下行路由。

上行路由：目的地址为天翼云 VPC 的网段，下一跳为新建的隧道接口。



下行路由：如果目的网段非本地直连路由，请按需添加下行路由。

16. 测试连通性。

可以利用您的云主机和您的数据中心主机进行连通性测试。

3.3.4.5 H3C 路由器配置

使用 IPsec VPN 建立站点到站点的连接时，在配置完天翼云 VPN 网关后，您还需在本地站点的网关设备中进行 VPN 配置。

前提条件

- 已经在天翼云 VPC 内创建了 IPsec 连接。
- 已经下载了 IPsec 连接的配置。

IPsec 协议信息

配置		示例值
IKE	认证算法	SHA1

	加密算法	AES-128
	DH 分组	Group5
	IKE 版本	IKEv1
	生命周期	86400
	协商模式	main
	PSK	ct***h3c
IPsec	认证算法	SHA1
	加密算法	AES-128
	PFS	DH group5
	生命周期	3600

网络配置信息

配置项		示例值
VPC	待和本地 IDC 互通的私网网段。	192.168.3.0/24
VPN 网关	天翼云 VPN 网关的公网 IP 地址。	121.xxx.xxx.152
本地 IDC	待和天翼云 VPC 互通的私网网段。	192.16.0.0/24
	本地网关设备的公网 IP 地址。	49.xxx.xxx.89

操作步骤

1. 以命令行方式登录 H3C 路由器命。
2. 配置 IKE 预共享密钥。

```
ike keychain ctyun
```



```
pre-shared-key address 121.229.145.152 255.255.255.255 key simple  
ctyun_h3c
```

3. 配置 IKE 提议。

```
ike proposal 10000  
sa duration 86400  
authentication-algorithm sha  
encryption-algorithm aes-cbc-128  
dh group5
```

4. 配置 IKE 安全框架。

```
ike profile ctyun  
exchange-mode main  
keychain ctyun  
local-identity address 49.7.205.89  
proposal 10000  
match remote address 121.229.145.152
```

5. 配置 ACL，定义要保护的数据流。

```
acl advanced 3402  
rule 0 permit ip source 192.16.0.0 0.0.0.255 destination 192.168.3.0 0.0.0.255  
rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.16.0.0 0.0.0.255
```

6. 配置 IPsec 安全提议。

```
ipsec transform-set ctyun  
protocol esp
```

```
esp encryption-algorithm aes-cbc-128  
esp authentication-algorithm sha1  
pfs dh-group5
```

7. 配置 IPsec 安全策略。

```
ipsec policy ctyun 10 isakmp  
sa duration time-based 3600  
transform-set ctyun  
security acl 3402  
remote-address 121.229.145.152  
ike-profile ctyun
```

8. 在 GigabitEthernet1/0 接口上应用 IPsec 安全策略 ctyun。

```
interface GigabitEthernet1/0  
ipsec apply policy ctyun
```

9. 配置静态路由。

```
ip route 192.168.3.0 255.255.255.0 121.XX.XX.152
```

10. 测试连通性。

您可以利用您的云主机和数据中心的主机进行连通性测试。

3.4 配置 SSL VPN

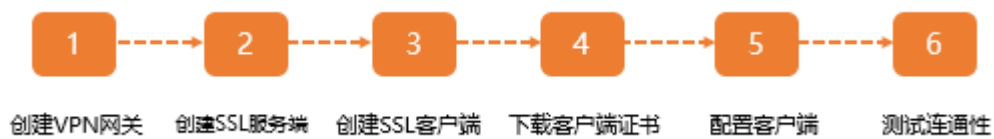
3.4.1 SSL VPN 配置概览

前提条件

- 客户端可以访问互联网。

- 客户端的私网网段和 VPC 的私网网段没有重合，否则无法访问 VPC 内的网络资源。
- 您已了解 VPC 中所应用的安全组规则，并确保安全组规则允许客户端访问云上资源。

使用流程



7. 创建 VPN 网关。

创建 VPN 网关并开启 SSL VPN 功能。

8. 创建 SSL 服务端。

创建相应的 SSL 服务端，用于接入用户侧连接 SSL VPN 服务。

9. 创建 SSL 客户端。

在控制台创建 SSL 客户端，用于生成客户端连接 SSL VPN 服务端的配置。

10. 下载客户端证书。

在控制台下载客户端证书，一共三个证书。

11. 配置客户端。

下载客户端软件，安装并配置客户端。详情请参见 [SSL VPN \(Windows 客户端双因子认证\)](#)、[SSL VPN \(Android 客户端双因子认证\)](#)、[SSL VPN \(macOS 客户端双因子认证\)](#) 步骤五操作。

12. 测试连通性。

登录客户端，访问 VPC，测试网络连通性。

3.4.2 管理 SSL 服务端

3.4.2.1 创建 SSL 服务端

创建 VPN 网关后，需要创建相应的 SSL 服务端，用于用户侧连接 SSL VPN 服务。服务端配置时需要注意，SSL 客户侧地址池与 VPC 的子网网段没有重合，否则无法通信。

前提条件

您已经创建了 VPN 网关并开启了 SSL VPN，请参见[创建和管理 IPsec 连接](#)。

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 进入 SSL VPN 列表页面中，单击“创建 SSL 服务端”。
6. 按照提示配置用户网关参数。

参数	说明	取值样例
名称	SSL 服务端的名称。	SSL-server1
区域	VPN 网关所在的资源池。	华东 1

参数	说明	取值样例
VPN 网关	选择需要使用的 VPN 网关。	vpn-gateway-a5f1-ssl
虚拟私有云	选择要使用的 VPC 作为本端资源。	vpc-a7f3
本端子网	选择本端需要连接的子网网段信息（可以复选，最多 5 个网段）。	subnet-yl(192.168.0.0/24)
客户端地址池	配置客户端地址池范围。	10.0.0.0/24
协议	SSL VPN 使用的协议。 默认：TCP	TCP
端口	SSL VPN 使用的端口，端口可配置范围： 1024 ~ 49151。 默认：1194	1194
加密算法	SSL VPN 使用的加密算法。 默认：AES-256-GCM	AES-256-GCM
是否压缩	是否对传输数据进行压缩处理。 默认：否	否

参数	说明	取值样例
自定义 DNS	SSL VPN 需要配置的自定义 DNS 地址。	10.10.1.1
启用双因子认证	<ul style="list-style-type: none">启用双因子认证，客户端登录不仅需要证书，同时需要输入密码。取消双因子认证，登录端登录只需要证书，无需密码。	开启

7. 单击“确定”，创建成功。修改 SSL 服务端

3.4.2.2 修改 SSL 服务端

创建 SSL 服务端后，您可以修改 SSL 服务端的名称、本端子网、客户端地址池和高级配置。


注意

- 如果您修改了 SSL 服务端高级配置中协议、是否压缩或双因子认证的配置会使 SSL 服务端关联的 SSL 客户端证书失效，您需要重新创建 SSL 客户端证书，然后在客户端中安装新的证书并重新发起 SSL VPN 连接。
- 如果您在 SSL 服务端下创建了 SSL 客户端，无法修改 SSL 服务端下的的本端子网及客户端地址池等配置。

前提条件

您已经创建了 VPN 网关并开启了 SSL VPN，请参见[创建和管理 IPsec 连接](#)。

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 在 SSL 服务端页面，找到目标 SSL 服务端，在操作列单击“修改”。
6. 在编辑 SSL 服务端页面，修改 SSL 服务端的名称、本端子网、客户端地址池或高级配置，然后单击“确定”。

3.4.2.3 删除 SSL 服务端

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 在 SSL 服务端页面，找到目标 SSL 服务端，在操作列单击“删除”。

注意：当 SSL 服务端下配置了 SSL 客户端时，该 SSL 服务端不允许被删除。

6. 在删除 SSL 服务端对话框中，单击“确定”。

3.4.3 管理 SSL 客户端


3.4.3.1 创建 SSL 客户端

创建 SSL 客户端时，需要选择绑定的 SSL 服务端，并指定账号名称。创建完成后，可以在该页面下载 SSL 证书，如果启用双因子认证，还需要查看并在客户端配置密码，用于服务端和客户端进行双向认证。

前提条件

您已经创建了 VPN 网关并开启了 SSL VPN，请参见[创建和管理 IPsec 连接](#)。

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 进入 SSL VPN 页面中，单击“SSL 客户端”，进入 SSL 客户端页面，单击“创建客户端”。
6. 按照提示配置用户网关参数，单击“确定”，创建成功。

参数	说明	取值样例
SSL 服务端	与当前创建客户端互联的 SSL 服务端。	SSL-server1
账号名称	用于客户端登陆的账号信息。	sslclient1
隧道限速	限速开关，选择是否对当前客户端的隧道进行限速。	关


9. 在操作列单击“查看账号密码”，记录该密码，客户端登录的时候使用。

3.4.3.2 删除 SSL 客户端

前提条件


您已经创建了 SSL 客户端。

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 进入 SSL VPN 页面中，单击“SSL 客户端”，进入 SSL 客户端页面。

6. 在 SSL 客户端列表，找到目标 SSL 客户端，在操作列单击“更多”，选择“删除”。
7. 在删除 SSL 客户端对话框中，单击“确定”，删除 SSL 客户端。

3.4.3.3 下载 SSL 客户端证书

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 页面。
5. 进入 SSL VPN 页面中，单击“SSL 客户端”，进入 SSL 客户端页面。
6. 在 SSL 客户端列表，找到目标 SSL 客户端，在操作列单击“更多”，选择“证书下载”。

3.4.4 修改 SSL 并发连接数

您可以根据业务需要修改 VPN 网关实例的 SSL 连接数规格。

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。

4. 在 VPN 连接页面，单击“VPN 网关”。
5. 在 VPN 网关页面，找到目标 VPN 网关实例，功能配置为“SSL”，在操作列单击“扩容”。
6. 在变配页面，选择新的 SSL 连接数，单击“确定”。
7. 单击“立即支付”并完成支付。

3.4.5 查看 SSL 客户端的连接信息

客户端建立 SSL VPN 连接后，您可以在 SSL 客户端页面查看已连接的客户端信息。

操作步骤

1. 登录控制中心。
2. 单击控制中心左上角的 ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“SSL VPN”，进入 SSL VPN 列表页面。
5. 在 SSL VPN 页面，单击“SSL 客户端”。
6. 在 SSL 客户端页面，找到目标 SSL 客户端，可以查看 SSL 客户端的连接信息。

3.5 证书管理

3.5.1 证书类型概览

VPN 网关	IPse 连接：	IPsec 连接：	是否需要证书	应用场景
--------	----------	-----------	--------	------

类型	认证类型	认证选择		
国密	证书认证	上传的证书	需要上传国密证书,参见 上传证书 。	仅适用于支持国密算法的企业本地数据中心、企业办公网络与天翼云云 VPC 之间建立网络连接。
普通	密钥认证	—	—	适用于在企业本地数据中心、企业办公网络、互联网客户端与天翼云 VPC 之间建立网络连接。
	证书认证	自签(默认)	不需要上传证书,系统自动创建一套证书。	
		上传的证书	需要上传证书,参见 上传证书 。	


3.5.2 上传证书

操作场景

- 国密型 VPN 网关,需要上传国密证书,用于和对端网关建立 IPsec 连接。
- 普通型 VPN 网关,IPsec 连接选择“证书认证”且用户自备证书场景,需要上传证书。

操作步骤

1. 登录[控制中心](#)。

2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择 “VPN 连接” ，进入 VPN 连接页面。
4. 在左侧网络控制台，选择 “证书管理” ，进入 VPN 证书管理页面。
5. 在 VPN 证书管理页面，单击 “上传证书” ，进入上传证书页面，按照证书类型和提示上传证书。

普通型证书上传页面如下：

VPN上传证书 ×

证书类型: 普通 国密

* CA证书

* VPN网关证书

* VPN网关密钥

* 证书名称

证书名称: cert-67e2

国密型证书上传页面如下：

VPN上传证书×

证书类型: 普通 国密

* CA证书 ↑

* VPN网关证书 ↑

* VPN网关密钥 ↑

* 签名证书 ↑

* 签名密钥 ↑

* 证书名称
证书名称: cert-67e2

确定取消

6. 上传完成，单击“确定”。

3.5.3 删除证书

操作场景

当证书失效后，需要更换新的证书，此时可以删除相关证书。

操作步骤

1. 登录[控制中心](#)。
2. 单击控制中心左上角的  ，选择 VPN 网关实例所在地域。
3. 在网络产品中选择“VPN 连接”，进入 VPN 连接页面。
4. 在左侧网络控制台，选择“证书管理”，进入上传 VPN 证书管理页面。

5. 在 VPN 证书管理页面，找到目标证书，在操作列单击“删除”。注意：当证书被 VPN 连接绑定时，不支持删除。

6. 在删除证书对话框，单击“确定”，删除证书。

3.6 配额管理

服务配额是指一个天翼云账号可以使用的云资源的最大值或操作次数的最大值。

配额简介

天翼云服务配额一般基于账号或地域限定，按照限制的维度可分为以下几种类型：

- 通用配额：指一个天翼云账号可使用的云资源的最大值。
- 权益配额：指一个天翼云账号通过天翼云授权后获得的权益，如使用特定功能的权益。

通用配额

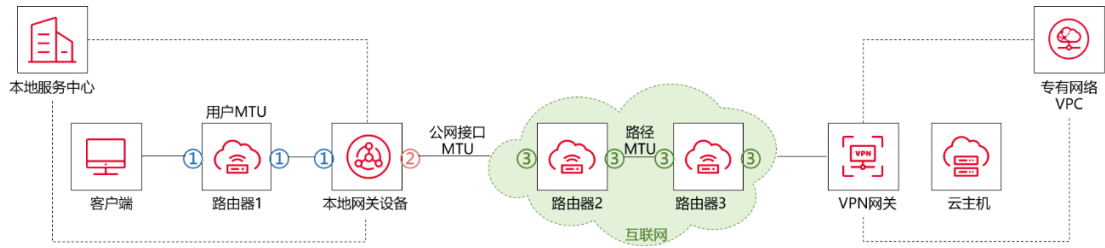
配额名称	描述	默认值	是否支持调整
IPsec VPN 网关	一个天翼云账号在一个资源池下支持创建的 IPsec VPN 网关实例的数量	20	是
SSL VPN 网关	一个天翼云账号在一个资源池下支持创建的 SSL VPN 网关实例的数量	20	是
VPN 网关绑定 VPC 的数量	一个 VPN 网关支持绑定的 VPC 的数量	1	否
VPN 用户网关个数上限	一个天翼云账号在一个资源池下支持创建的 IPsec 用户网关实例的数量	100	是

VPN 连接个数上限	一个天翼云账号在一个资源池下支持创建的 VPN 连接的数量	100	是
VPN 连接对端网络数量	一个 IPsec 连接支持添加的远端网段的数量	5	是
VPN 连接本端子网数量	一个 IPsec 连接支持添加的本端子网的数量	5	否
策略路由条目上限	一个 VPN 网关实例支持创建的策略路由条目的数量	20	否
目的路由条目上限	一个 VPN 网关实例支持创建的目的路由条目的数量	20	否
VPN 证书个数上限	一个天翼云账号支持创建的 SSL 客户端证书的数量	10	否
SSL 服务端个数上限	一个天翼云账号在一个资源池下支持创建的 SSL 服务端的数量	20	否

3.7 MTU 配置说明

VPN 网关只支持传输已经分片的数据包，不支持对数据包分片及数据包分片重组。在您使用 IPsec VPN 时，IPsec 协议会对数据包进行加密，加密过程会扩大数据包长度，扩大后的数据包长度可能会超过网络中设置的最大数据传输单元 MTU，影响数据包的正常传输。

MTU 配置原则



本文以图中场景为例说明 MTU 配置原则。本地数据中心已与天翼云 VPC 建立了 IPsec VPN 连接。在客户端访问 VPC 资源时，数据包将被本地网关设备加密并被传输至互联网，经过互联网中的网络设备（如图中路由器 2 和路由器 3）传输至天翼云 VPN 网关。

数据包从客户端传输至 VPN 网关的过程中，数据包的大小将会受到以下三种 MTU 的限制：

- 用户 MTU

用户 MTU 即客户端和本地网关设备之间所有网络设备接口 MTU 的最小值。该 MTU 会限制客户端发送的数据包的大小。

如图中用户 MTU 取标记为 1 的接口中 MTU 的最小值。

- 公网接口 MTU

公网接口 MTU 即本地网关设备连接 VPN 网关的公网接口上的 MTU。该 MTU 会限制被加密后的数据包的大小。

如图中公网接口 MTU 取标记为 2 的接口的 MTU。

- 路径 MTU

路径 MTU 即互联网中所有网络设备接口 MTU 的最小值。该 MTU 会限制被加密后的数据包的大小。

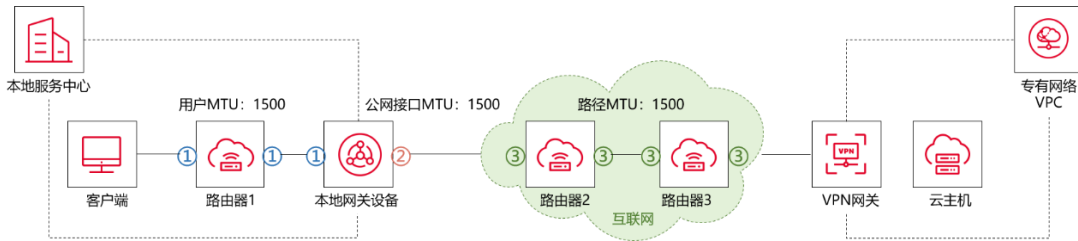
您可以向互联网厂商咨询路径 MTU。通常以太网的路径 MTU 默认为 1500 字节。

如图中路径 MTU 取标记为 3 的接口中 MTU 的最小值。

为确保数据包被正常传输，您需要在本地数据中心配置用户 MTU 和公网接口 MTU，使上述三种 MTU 满足以下关系：

用户 MTU 的最大值 = $\min\{\text{公网接口 MTU}, \text{路径 MTU}\} - 101$ # 101 是 IPsec 协议为数据包加密后占用的最大字节数。

MTU 配置示例



假设路径 MTU 为 1500 字节，您设置的本地网关设备公网接口的 MTU 也为 1500 字节，则：

用户 MTU 的最大值 = $\min\{1500, 1500\} - 101 = 1500 - 101 = 1399$ 字节

即客户端发送数据包时，数据包的大小建议不超过 1399 字节，否则可能会导致数据包无法正常传输。

MSS 配置建议

在通过 IPsec VPN 连接传输 TCP 流量的场景下 如果需要确保数据包不被分段传输，则最大分段大小 MSS 和用户 MTU 需保证以下关系：

$MSS = \text{用户 MTU} - \text{IP 数据包头部占用字节数} (20 \text{ 字节}) - \text{TCP 数据包头部占用字节数} (20 \text{ 字节})$

例如，在公网接口 MTU 和路径 MTU 均为 1500 字节的情况下，用户 MTU 最大为 1399 字节，为确保数据包不被分段传输，MSS 的最大值为 1359 字节。

4 VPN 连接常见问题

4.1 IPsec VPN 连接常见问题

创建 IPsec VPN 连接需要帐户名和密码吗？

天翼云的 IPsec VPN 在协商时使用预共享密钥方式或证书方式进行认证。当使用预共享密钥方式进行认证时，密钥是配置在 IPsec 连接上的，在协商完成后即建立隧道进行通信。VPN 隧道所保护的主机在通信时无需输入帐户名和密码。

IPsec 连接状态为“第一阶段协商失败”怎么办？

常见的 IPsec 连接对端网关设备导致“第一阶段协商失败”的原因如下表所示。

原因	解决方案
IPsec 连接对端网关设备工作异常。	请排查对端网关设备。 具体操作，请咨询设备所属厂商。
IPsec 连接对端网关设备尚未添加 IPsec VPN 配置。	请为对端网关设备添加 IPsec VPN 配置，需确保对端网关设备的配置与 IPsec 连接的配置一致。 具体操作，请参见用户指南>本地网关配置。
IPsec 连接对端网关设备所应用的访问控制策略未放行 UDP 协议 500 及 4500 端口。	请排查对端网关设备应用的访问控制策略，确保其满足以下条件： <ul style="list-style-type: none">● 出方向和入方向均放开 UDP 协议 500 及 4500 端口。● 出方向和入方向均放行 VPN 网关实例的 IP 地址和用户网关的 IP 地址。

<p>IPsec 连接对端厂商限制，需要有数据流量时才能触发 IPsec 协议协商。</p>	<p>请确认 IPsec 连接对端 VPN 网关是否存在此使用限制。</p> <p>如果存在此限制，请向对端厂商咨询如何触发 IPsec 协议协商。</p>
--	--

IPsec 连接状态为“第二阶段协商成功”，但 IPsec 连接协商状态间歇性变为失败怎么办？

办？

产生当前问题的可能原因及解决方案如下表所示。

分类	可能原因	解决方案
IPsec VPN 配置	<p>IPsec 连接及其对端网关设备在 IPsec 配置阶段 DH 算法参数的配置不一致。</p>	<p>请排查 IPsec 连接或者对端网关设备在 IPsec 配置阶段的 DH 算法参数的配置，使两端的 DH 算法参数的值配置相同。</p>
	<p>对端网关设备的 IPsec VPN 配置中，某个参数被指定了多个值。</p> <p>如配置对端网关设备时，指定 IKE 配置阶段加密算法的值为 AES128、AES192。</p>	<p>在天翼云侧配置 IPsec 连接时，每个参数仅支持指定一个值。请排查对端网关设备的 IPsec VPN 配置，确保每个参数也仅指定了一个值，且与云侧 VPN 网关配置的 IPsec 连接的值相同。</p>
<p>网络质量不佳</p>	<p>由于 IPsec 连接和对端网关设备之间的网络质量不佳，造成</p>	<p>排查底层互联网网络质量。</p>

	DPD 协议报文、IPsec 协议报文丢失后超时，导致 IPsec VPN 连接中断。	
IPsec 连接对端限制	IPsec 连接对端厂商限制，需要有数据流量时才能触发 IPsec 协议协商。	<p>请确认 IPsec 连接对端 VPN 网关是否存在此限制。</p> <p>如果存在此限制，请向对端厂商咨询如何触发 IPsec 协议协商。</p>

为什么 IPsec 连接状态为“第二阶段协商成功”，但 VPC 内的云主机实例无法访问本地数据中心内的服务器？

VPC 的路由配置、安全组规则或本地数据中心的路由配置、访问控制策略未允许 VPC 内的云主机实例访问本地数据中心内的服务器。

分类	解决方案
VPC	<ul style="list-style-type: none"> ● 排查 VPC 路由表中的路由配置。确保 VPC 路由表内已存在相关路由使云主机实例可以通过 IPsec VPN 连接访问本地数据中心的服务器。 ● 排查 VPC 应用的安全组规则。确保安全组规则允许云主机实例和服务器之间互相访问。
本地数据中心	<ul style="list-style-type: none"> ● 排查本地数据中心的路由配置。确保本地数据中心已配置了相关路由使服务器可以对云主机实例做出应答。

	<ul style="list-style-type: none"> ● 排查本地数据中心的访问控制策略。确保本地数据中心允许云主机实例和服务器互相访问。
--	--

为什么 IPsec 连接状态为“第二阶段协商成功”，但本地数据中心内的服务器无法访问 VPC 内的云主机实例？

VPC 的路由配置、安全组规则或本地数据中心的路由配置、访问控制策略未允许本地数据中心内的服务器访问 VPC 内的云主机实例。

分类	解决方案
VPC	<ul style="list-style-type: none"> ● 排查 VPC 路由表中的路由配置。确保 VPC 路由表内已存在相关路由使云主机实例可以对服务器的访问做出应答。 ● 排查 VPC 应用的安全组规则。确保安全组规则允许云主机实例和服务器之间互相访问。
本地数据中心	<ul style="list-style-type: none"> ● 排查本地数据中心的路由配置。确保本地数据中心已配置了相关路由使服务器可以通过 IPsec VPN 连接访问云主机实例。 ● 排查本地数据中心的访问控制策略。确保本地数据中心允许云主机实例和服务器互相访问。

为什么 IPsec 连接状态为“第二阶段协商成功”，但 IPsec VPN 连接单向不通？

原因：

在 IPsec 连接的对端网关设备使用的是华为防火墙的情况下，如果对端网关设备的出接口配置了 nat enable，将会导致从该接口发出的所有数据包的源 IP 地址都被转换为该

接口的 IP 地址，导致 IPsec VPN 连接单向不通。

解决方案：

1. 运行 nat disable 命令，关闭出接口的 NAT 功能。
2. 设置 NAT 策略。

```
nat-policy interzone trust untrust outbound  
  
policy 0  
  
action no-nat  
  
policy source 192.168.0.0 mask 24  
  
policy destination 192.168.1.0 mask 24  
  
policy 1  
  
action source-nat  
  
policy source 192.168.0.0 mask 24  
  
easy-ip Dialer0
```

其中：

192.168.0.0：网关设备的私网网段。

192.168.1.0：VPC 的私网网段。

Dialer0：网关设备的出接口。

为什么 IPsec 连接状态为“第二阶段协商成功”，能 ping 通但业务访问不通或部分端口访问不通？

原因：

VPC 应用的安全组规则或本地数据中心应用的访问控制策略未放行对应的 IP 地址、协议类型和端口号。

解决方案：

请按照以下操作排查相关配置：

- 排查 VPC 应用的安全组规则。确保安全组规则已放行本地数据中心和 VPC 之间需要互通的 IP 地址、协议类型和端口号。
- 排查本地数据中心应用的访问控制策略。确保访问控制策略已放行本地数据中心和 VPC 之间需要互通的 IP 地址、协议类型和端口号。

如果本地数据中心侧有业务策略、域名解析等配置建议一并排查。确保本地数据中心和 VPC 之间需要互通的 IP 地址、协议类型和端口号已放行。

如何解决 VPN 连接无法建立连接的问题？

1. 检查云上 VPN 连接中的 IKE 策略和 IPsec 策略是否与远端配置一致。
 - 如果第一阶段 IKE 策略未建立，常见原因为云上 IKE 策略与数据中心远端的配置不一致。
 - 如果第一阶段 IKE 策略已经建立，第二阶段的 IPsec 策略未开启，常见原因为云上 IPsec 策略与数据中心远端的配置不一致。
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配置的 ACL，应匹配数据中心子网和 VPC 内子网——对应的通信规则，如下所示：

```
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 IPsec VPN 是否可以连接，ping 测试两端内网是否正常通信。

如何理解 IPsec VPN 连接中的远端网关和远端子网？

远端网关和远端子网是个相对的概念。在建立 IPsec VPN 连接时，从天翼云的角度出发，天翼云中的 VPC 网络就是本地子网，创建的 VPN 网关就是本地网关；与之对接的用户侧网络就是远端子网，用户侧的网关就是远端网关。远端网关 IP 就是用户侧网关的公网 IP，远端子网指需要和天翼云 VPC 子网互联的用户侧子网。

IPsec VPN 连接远端子网是否可以包含本端子网？

不可以。在建立 IPsec VPN 连接时，做好两端的网段地址规划是至关重要的。在 IPsec VPN 中，通常是通过路由的方式来实现子网之间的通信。如果网段地址存在重叠，将会导致网络通信的混乱和安全问题的产生。因此，当您在建立 IPsec VPN 连接时，您需要确保连接的远端子网和本端子网不能互相包含，请在创建 IPsec VPN 前做好两端的网段地址规划，避免地址重叠。

4.2 SSL VPN 连接常见问题

如何理解 SSL VPN 连接中的本端子网和客户端地址池？

在建立 SSL VPN 服务端时，从天翼云的角度出发，天翼云中的 VPC 网络就是本端子网，客户端地址池就是分配给客户端虚拟网卡的 IP 地址集合。

客户端连接失败怎么办？

产生当前问题的可能原因及解决方案如下表。

分类	原因	解决方案
配置错误	SSL 客户端配置错误。	请排查客户端 VPN 软件的配置是否与服务端配置一致。
SSL 客户端证书到期	SSL 客户端证书过期或无效。	<ol style="list-style-type: none"> 1. 请排查 SSL 客户端证书的有效性。 SSL 客户端证书默认有效期为 10 年。 2. 请删除现有的 SSL 客户端证书及所有配置，然后重新创建、下载、安装 SSL 客户端证书。 开启和关闭双因子认证功能、修改 SSL 服务端的配置，均需要重新下载、安装 SSL 客户端证书。
客户端连接数超限	当前 SSL 服务端下的客户端连接数超限。	在 VPN 网关实例下查看已连接的客户端数量，确认在线客户端数量是否超限。
IP 地址问题	VPC 下的 IP 地址与客户端的 IP 地址冲突。	请根据实际情况，修改 SSL 服务端的本端网段（VPC 或云间高速的网段）或者客

		户端网段以确保两侧 IP 地址不冲突。
	SSL 服务端的客户端网段配置的太小，导致客户端无法被分配 IP 地址。	请确保您指定的客户端网段所包含的 IP 地址数量大于 SSL VPN 客户端数量。
VPN 软件问题	客户端 VPN 软件冲突。	如果您的客户端上安装了多个 VPN 客户端软件，建议仅使用一个 VPN 客户端软件建立 SSL VPN 连接。

客户端之前连接成功，但间歇性中断下线怎么办？

产生当前问题的可能原因及解决方案如下表。

分类	原因	解决方案
公网链路质量不佳	由于客户端和 VPN 网关之间的公网链路质量不佳导致客户端间歇性中断下线。	公网链路质量不佳（延时高或丢包率高等），可联系运营商协助进行故障排查。
SSL 服务端配置变更	SSL 服务端配置变更导致客户端中断下线。	SSL 服务端修改配置后，请在客户端调整配置，重新发起连接。

客户端连接成功，但无法 ping 通 VPC 内的网络资源怎么办？

原因：

1. VPC 应用的访问控制策略禁止 ping 命令探测。
2. 未配置对应的 VPC 子网资源。

3. VPC 应用的安全组规则未放通客户端地址池。

解决方案：

1. 请排查 VPC 内的网络资源是否禁止 ping 命令探测 ,如果是 ,请修改访问控制策略。
默认情况下 Windows 操作系统的客户端的防火墙是禁止 ping 命令探测的 ,您需要修改 Windows 防火墙的入站规则允许 ICMPv4-In。
2. 排查 VPC 本端子网的配置 ,确保本端子网中包含了需要访问的网络资源。
3. 排查 VPC 应用的安全组规则。确保安全组规则允许云主机实例和客户端之间互相访问。

4.3 VPN 网关常见问题

如何选择 VPN 连接的数量？

IPsec VPN 连接的数量通常与用户本地数据中心的数量有关 ,每条 IPsec VPN 连接可以打通当前云上资源与企业的一个数据中心网络。请用户在购买包周期 VPN 网关时 ,根据规划连通的数据中心数量选择合适的 IPsec VPN 连接数。

SSL VPN 连接数量与配置的客户端数量有关 ,每个 SSL VPN 连接数可以允许一个客户端接入访问云上资源。考虑到同时在线的客户端数量小于已配置的客户端数量 ,SSL VPN 连接数可以小于配置的客户端数量。请用户在购买时候根据规划选择合适的 SSL VPN 连接数。

VPN 网关是否可以自动建立连接？

触发 IPsec 连接建立的方式有两种 ,一种是 “立即协商” ,即通过建立 IPsec VPN 连接的网关设备之间自动触发协商 ;另一种是 “流量触发” ,即通过云上云下主机间的交互流量触发。

VPN 网关在完成两侧配置后，如果协商生效选择了“立即协商”，则会自动触发建立连接；如果协商生效选择了“流量触发”，则不会自行建立连接，需要由两侧主机间的数据流来触发协商。如果云上与用户侧数据中心没有交互数据流，IPsec VPN 的连接状态会一直处于“第一阶段协商未成功”状态。所谓的数据流，可以是真实的业务访问数据，也可以是主机间 ping 测数据。

推荐您在首次建立连接时，分别验证两侧的交互数据流均可触发建立连接。即用用户侧数据中心主机 ping 云上主机可触发连接建立，然后断开连接，确认云上主机 ping 用户侧数据中心主机亦可触发连接建立。ping 包的源地址、目的地址需要处于 IPsec VPN 保护的范围内。在创建 IPsec 连接之后，用户侧 VPN 网关才能 ping 通云上 VPN 网关，但是 ping 网关 IP 并不能触发 VPN 连接的建立。

VPN 网关删除后公网 IP 是否可以保留？

VPN 网关删除后不保留网关 IP 地址。通过控制台界面删除 VPN 网关后，VPN 网关相关联的资源，如公网 IP、配置信息即被释放，不会保留。

因为 VPN 网关和公网 IP 是相关联的资源，一旦 VPN 网关被删除，其相关联的公网 IP 也会被释放。这个过程是自动进行的，以确保资源的有效利用和管理。在某些情况下，如果 VPN 网关删除后仍然保留了公网 IP，可能会导致潜在的安全风险和配置问题。

因此，一般来说，当删除 VPN 网关时，相关联的公网 IP 也会被一并释放。

自己创建的弹性公网 IP 能作为 VPN 网关的 IP 地址吗？

不可以。弹性公网 IP 是一种独立的公网 IP 地址，可以与云服务器进行绑定和解绑，实现 IP 地址的动态管理。但是，弹性公网 IP 不具备对接 VPN 网关服务的功能，不能直接用作 VPN 网关的 IP 地址。

VPN 网关是一种用于建立加密通道的设备，用于连接内网和外网。在创建 VPN 网关时，系统会分配一个特定的 IP 地址作为 VPN 网关的地址。这个 IP 地址是专门用于连接 VPN 网关的，不能随意更改。

通过 VPN 互访的云主机需要购买弹性公网 IP 吗？

一般是不需要购买弹性公网 IP 的，因为 VPN 连接是在网络层上进行的，它可以在云主机和本地主机之间建立安全的加密通道，使得它们可以相互通信。如果您的云主机仅需要通过 VPN 连接与其他 VPC 的云主机或本地主机进行互访，那么您不需要购买弹性公网 IP。

然而，如果您的云主机需要向公网用户提供服务，比如通过互联网访问您的网站或应用程序，那么您需要购买弹性公网 IP。弹性公网 IP 可以让您的云主机具有一个独立的公网 IP 地址，使得用户可以通过这个 IP 地址访问您的服务。这样可以让您的服务更具有可访问性和可用性。

本地站点通过 IPsec VPN 接入 VPC 的前提条件是什么？

- 本地站点的网关设备必须至少支持 IKEv1 和 IKEv2 协议中的一种。
- 本地站点的网关设备必须配置静态公网 IP 地址。
- 本地站点和 VPC 之间需要互通的网段没有重叠。

跨地域 VPC 是否可以通过 VPN 网关互通？

主备模式资源池：同地域不同 VPC 可以通过 VPN 网关互通。

集群模式资源池：同地域不同 VPC 不可以通过 VPN 网关互通。

VPN 网关之间的互通流量是否经过互联网？

在使用 VPN 网关实现 VPC 与 VPC 互通的场景下：

- 如果两个 VPC 位于不同的地域，则流量会经过互联网。
- 如果两个 VPC 位于相同的地域，则流量不会经过互联网。

是否可以升级或降低 VPN 网关的配置？

- 目前仅支持升级 VPN 网关的配置，暂不支持降级。
- 如果您需要立即升级 VPN 网关的带宽规格，请参见[创建和管理 VPN 网关实例](#)。
- 如果您需要立即升级 VPN 网关的 SSL 连接数规格，请参见[修改 SSL 并发连接数](#)。
- 如果您需要开启 VPN 网关的 IPsec VPN 功能或 SSL VPN 功能，请参见[开启 IPsec VPN 和 SSL VPN](#)。

VPN 网关支持查看 SSL VPN 连接下客户端的连接信息吗？

支持。

具体操作，请参见[查看 SSL 客户端的连接信息](#)。

配置 IPsec VPN 连接时，如何选择 IKE 版本？

在配置 IPsec VPN 连接时，您需要根据 IPsec 连接对端网关设备的支持情况来选择 IKE 的版本，选择两端都支持的 IKE 版本。

在 VPN 网关实例下添加路由时系统提示路由重复等报错时怎么办？

在 VPN 网关实例下添加路由时系统报错，可能原因如下：

- 您添加的路由与 VPN 网关实例下的路由冲突，请排查 VPN 网关实例策略路由表、目的路由表下的路由配置，解决路由冲突问题。

- 如果您添加的是目的路由，且目的路由的目标网段和下一跳与 VPN 网关实例下已有的目的路由的目标网段和下一跳相同，则会产生路由冲突。
- 如果您添加的是策略路由，且策略路由的源网段、目标网段、下一跳与 VPN 网关实例下已有的策略路由的源网段、目标网段、下一跳相同，则会产生路由冲突。

4.4 如何配置本地网关设备

使用 VPN 网关 IPsec VPN 功能过程中，您需要在本地网关设备添加 VPN 配置才能与天翼云成功建立 IPsec VPN 连接。

- 请参见用户指南 > [strongSwan 配置](#)
- 请参见用户指南 > [Juniper 防火墙配置](#)
- 请参见用户指南 > [思科防火墙配置](#)

4.5 多网段互通配置建议及常见问题

多网段配置建议

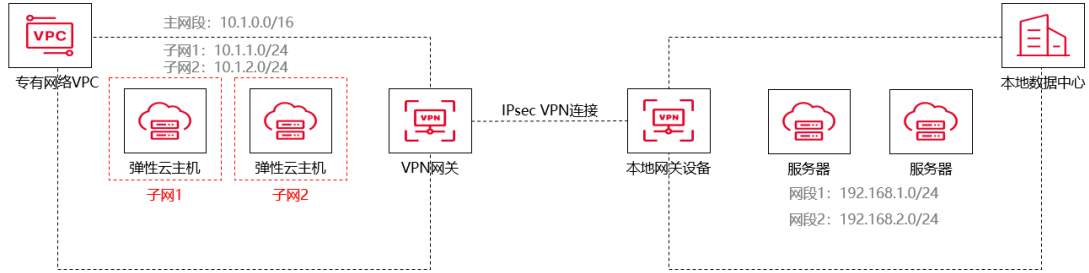
- 由于天翼云侧 IPsec 连接 IKE 配置阶段以及 IPsec 配置阶段的加密算法、认证算法、DH 算法均仅支持指定一个值，因此您在对端网关设备上添加 VPN 配置时，IKE 配置阶段以及 IPsec 配置阶段的加密算法、认证算法、DH 算法 (PFS) 也都只能指定一个值，且需和天翼云侧相同。
- 如果天翼云侧 IPsec 连接开启了 DPD 功能，则对端网关设备需支持标准的 DPD 功能。

天翼云侧 IPsec 连接和对端网关设备配置的生存周期需相同。

多网段配置方案推荐

某公司希望将本地数据中心和天翼云 VPC 通过 IPsec VPN 连接实现多网段互通：天翼

云 VPC 下的多个网段为 10.1.1.0/24 和 10.1.2.0/24，本地数据中心下的多个网段为 192.168.1.0/24 和 192.168.2.0/24，拓扑图如下：



推荐配置方案如下：

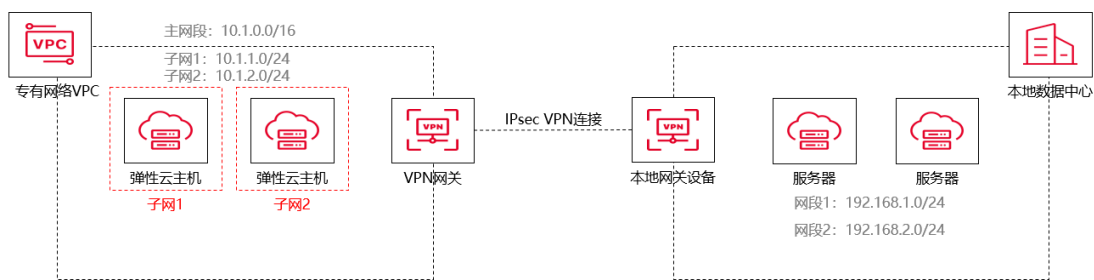
方案	适用的 IKE 版本	方案说明	方案优势或限制	配置示例
方案一(推荐)	IKEv1/IKEv2	本地数据中心和 VPC 之间建议使用一个 IPsec VPN 连接进行通信，天翼云侧 IPsec 连接使用“目的路由”的路由模式，用户侧的网关设备配置	<p>方案优势：</p> <p>后续如果新增或删除待互通的网段，仅需调整路由的配置，无须修改 IPsec VPN 连接的配置。</p> <p>在您新增或删除待互通的网段时，IPsec VPN 连接不会中断，对其余路由的流量也不会产生影响。</p>	方案一配置实例

		<p>源网段为 0.0.0.0/0、目的网段为 0.0.0.0/0 的感兴趣流，然后通过在本 VPN 网关和本地数据中心配置静态路由控制流量转发。</p>		
<p>方案二(次选)</p>	<p>1/ IKEv2</p>	<p>本地数据中心和 VPC 之间建议使用一个 IPsec VPN 连接进行通信，将本地数据中心侧和 VPC 侧待互通的网</p>	<p>方案限制： 后续如果新增或删除网段，您可能需要重新指定聚合网段，然后重新对天翼云侧及其用户侧网关设备进行配置，此操作会导致 IPsec VPN 连接重新协商，造成短暂的流量中断。</p>	<p>方案二配置实例</p>

		<p>段分别聚合为 1 个网段，然后为 IPsec 连接和对端网关设备配置聚合网段。</p>		
<p>方案三</p>	<p>IKEv1/ IKEv2</p>	<p>本地数据中心和 VPC 之间建议使用一个 IPsec VPN 连接进行通信,IPsec 连接及其对端网关设备下配置多个本端网段或对端网段实现多网段互通。</p>	<p>方案限制： 后续如果有新增或删除的网段，您需要重新为 IPsec 连接及其对端网关设备配置感兴趣流网段，此操作会导致 IPsec VPN 连接重新协商，造成短暂的流量中断。 一个 IPsec 连接支持添加的本端网段的数量最多为 5 个、支持添加的对端网段的数量最多也是 5 个。</p>	<p>方案三 配置实例</p>

方案一配置示例

- 在天翼云侧配置 IPsec 连接时，IPsec 连接的路由模式使用“目的路由”模式。具体操作，请参见[用户指南>创建 IPsec 连接](#)。
- 在 VPN 网关实例下添加路由配置时，推荐使用“目的路由”，并添加相关路由配置。具体操作，请参见[用户指南>使用目的路由](#)。
- 在本地网关设备上添加源网段为 0.0.0.0/0、目的网段为 0.0.0.0/0 的感兴趣流。具体命令，请咨询本地网关设备所属厂商。



IPsec连接网关配置	
路由模式	目的路由

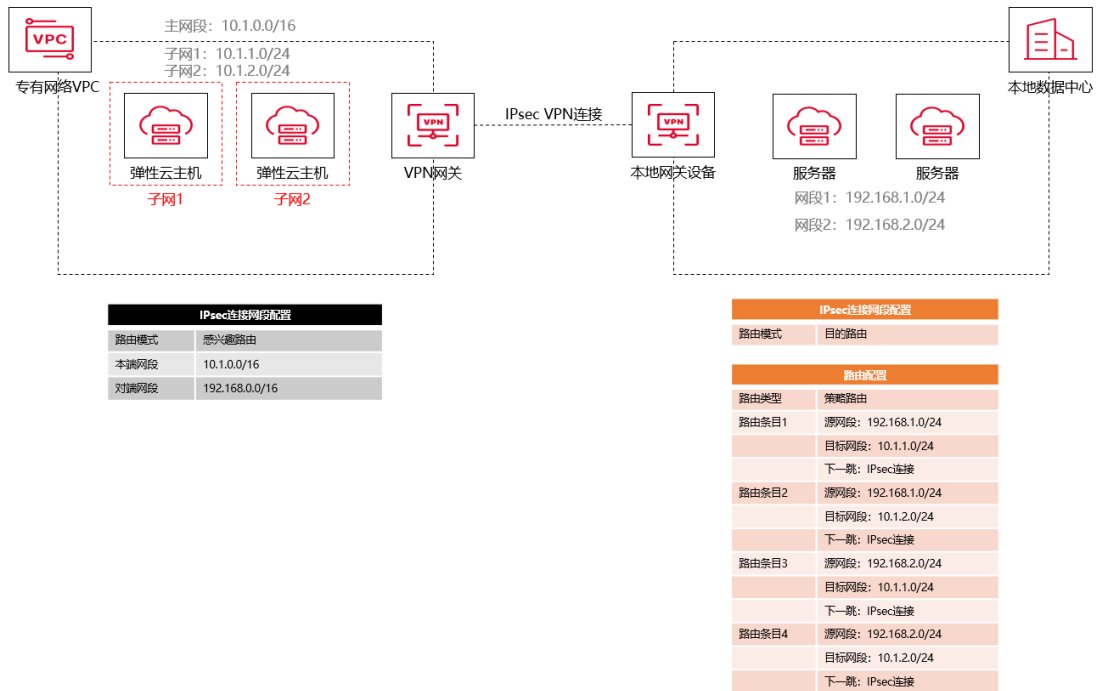
路由配置	
路由类型	目的路由
路由条目1	目标网段: 192.168.1.0/24
	下一跳: IPsec连接
路由条目2	目标网段: 192.168.2.0/24
	下一跳: IPsec连接

IPsec连接网关配置	
路由模式	目的路由

路由配置	
路由类型	策略路由
路由条目1	源网段: 192.168.1.0/24
	目标网段: 10.1.1.0/24
	下一跳: IPsec连接
路由条目2	源网段: 192.168.1.0/24
	目标网段: 10.1.2.0/24
	下一跳: IPsec连接
路由条目3	源网段: 192.168.2.0/24
	目标网段: 10.1.1.0/24
	下一跳: IPsec连接
路由条目4	源网段: 192.168.2.0/24
	目标网段: 10.1.2.0/24
	下一跳: IPsec连接

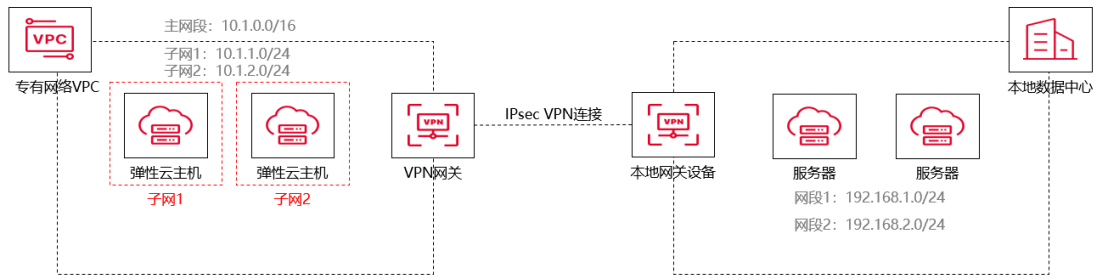
方案二配置示例

- 在天翼云侧配置 IPsec 连接时，IPsec 连接的路由模式使用感兴趣流模式，IPsec 连接本端网段配置为 VPC 下的聚合网段 10.1.0.0/16，对端网段配置为本地数据中心下的聚合网段 192.168.0.0/16。具体操作，请参见[用户指南>创建 IPsec 连接](#)。
- IPsec 连接的路由模式为感兴趣流模式时，系统会自动创建相关的转发策略，并将其发布给 VPC 默认路由表。该转发策略对用户不可见，用户不需要额外去创建目的路由或者是策略路由。



方案三配置示例

- 在天翼云侧配置 IPsec 连接时，IPsec 连接的路由模式使用感兴趣流模式，IPsec 连接本端网段配置为 VPC 下的 2 个网段 10.1.1.0/24 和 10.1.2.0/24，对端网段配置为本地数据中心下的 2 个网段 192.168.1.0/24 和 192.168.2.0/24。具体操作，请参见[用户指南>创建 IPsec 连接](#)。
- IPsec 连接的路由模式为感兴趣流模式时，系统会自动创建相关的转发策略，并将其发布给 VPC 默认路由表。该转发策略对用户不可见，用户不需要额外去创建目的路由或者是策略路由。



IPsec连接网段配置	
路由模式	静态路由
本端网段	10.1.0.0/16
	10.1.2.0/24
对端网段	192.168.0.0/16
	192.168.2.0/24

IPsec连接网段配置	
路由模式	目的路由
路由配置	
路由类型	策略路由
路由条目1	源网段: 192.168.1.0/24 目标网段: 10.1.1.0/24 下一跳: IPsec连接
路由条目2	源网段: 192.168.1.0/24 目标网段: 10.1.2.0/24 下一跳: IPsec连接
路由条目3	源网段: 192.168.2.0/24 目标网段: 10.1.1.0/24 下一跳: IPsec连接
路由条目4	源网段: 192.168.2.0/24 目标网段: 10.1.2.0/24 下一跳: IPsec连接

4.6 其他问题

VPN 连接的计费方式？

VPN 连接产品支持按连接数规格、带宽大小的包年包月计费。

VPN 网关、用户网关、IPsec 连接之间有什么关系？

VPN 网关：VPN 网关是 VPN 连接的接入点。一个 VPN 网关仅能绑定一个 VPC，每个 VPN 网关可以创建多个 VPN 连接。每个 VPN 网关默认分配了一个公网 IP 地址，可以满足用户本地数据中心侧 VPN 设备或移动终端接入 VPC 的业务需求。

用户网关：用户企业侧的 VPN 网关，与 VPC 侧 VPN 网关互为本端、远端。用户侧数据中心 VPN 网关需具备固定公网 IP，动态拨号公网 IP 无法进行 IPsec VPN 对接。如果用户侧公网 IP 进行了变更，则需要尽快在天翼云上进行同步修改。否则，会导致 IPsec VPN 协商失败，流量转发不通。

IPsec 连接是一种基于 IP 协议的加密技术，用于构建 VPN 网关和用户本地数据中心远端网关之间的安全、可靠的加密通道。VPN 连接使用 IKE（Internet Key Exchange，网络密钥交换协议）和 IPsec 协议对传输数据进行加密，保证数据安全可靠，并且 IPsec VPN 连接基于互联网进行传输，更加节约成本。

本地数据中心的什么设备可以建立 IPsec VPN 连接？

设备型号多为路由器、防火墙等，天翼云的 VPN 支持标准 IPsec 协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与天翼云进行对接：

- 设备是否具备 IPsec 功能和授权：请查询设备的特性列表获取是否支持 IPsec VPN。
- 关于组网结构，要求用户侧数据中心有固定的公网 IP 或者经过 NAT 映射后的固定公网 IP（即 NAT 穿越，VPN 设备在 NAT 网关后部署）也可以。

IPsec VPN 连接支持将两个 VPC 互连吗？

支持将两个 VPC 互连。不仅可以实现天翼云不同区域资源池中 VPC 互通，也可以连通其他云服务商的 VPC 网络（前提是对方也具备相同的 VPN 接入能力）。

为这两个 VPC 分别创建 VPN 网关，并为两个 VPN 网关创建用户网关和 IPsec 连接。将两个 IPsec 连接的用户网关设置为对方 VPN 网关的网关 IP，将两个 VPN 连接的对端网段设置为对方 VPC 的网段，两个 VPN 连接的预共享密钥和算法参数需保持一致。

是否可以通过 IPsec 连接实现跨境访问国外网站？

不可以。IPsec 连接仅支持在中国境内实现将云上的 VPC 子网和用户侧数据中心的数据中心网络打通的场景。

如果您有跨境访问国外网站的需求，建议使用天翼云 SD-WAN 产品的跨境能力。SD-WAN 是一种基于软件定义的广域网（WAN）技术，它可以提供更加灵活、智能和安全的网络连接服务。通过天翼云 SD-WAN 的跨境能力，您可以在中国和国外之间建立一个安全的网络连接，实现跨境访问和数据传输。

是否可以通过 SSL VPN 实现跨境访问国外网站？

不可以。SSL VPN 是一种基于 SSL 协议的虚拟专用网络（VPN）服务，它仅支持在中国境内实现用户终端接入天翼云 VPC 的场景，即在用户终端和天翼云 VPC 之间建立一个安全的加密通道，使得用户可以通过 VPN 访问天翼云内的资源。

但是，SSL VPN 并不支持跨境访问国外网站，使用 SSL VPN 访问国外网站可能会被中国政府视为违反相关法规，从而被禁止或限制。

如果您有跨境访问国外网站的需求，建议使用天翼云 SD-WAN 产品的跨境能力。SD-WAN 是一种基于软件定义的广域网（WAN）技术，它可以提供更加灵活、智能和安全的网络连接服务。通过天翼云 SD-WAN 的跨境能力，您可以在中国和国外之间建立一个安全的网络连接，实现跨境访问和数据传输。

如果数据中心有多个子网，应该如何配置 IPsec 连接数？

一个 IPsec 连接中可以配置多个本端子网（VPC 中的子网）和对端子网（用户侧子网），无需配置多个连接。

