虚拟专用网络

最佳实践

文档版本	01
发布日期	2025-11-13

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

1 站点入云 VPN 企业版

1.1 通过 VPN 实现云上云下网络互通（双活模式）

1.1.1 方案概述

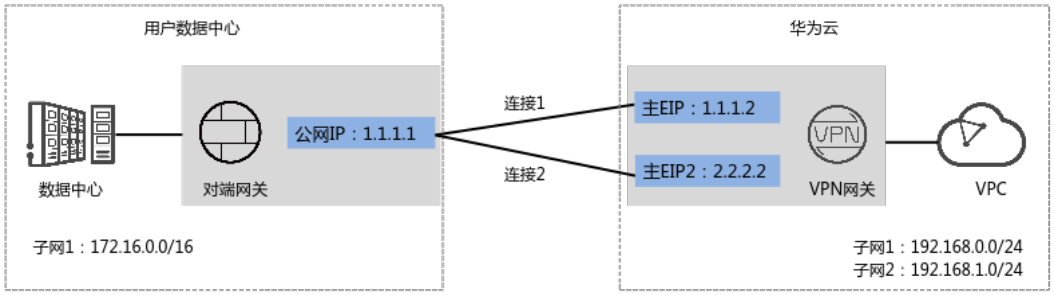
应用场景

当用户数据中心需要和VPC下的ECS资源进行相互访问时，可以通过VPN快速实现云上云下网络互通。

方案架构

本示例中，用户数据中心和VPC之间采用一组VPN连接保证网络可靠性。当其中一条VPN连接故障时，系统可以自动切换到另一条VPN连接，保证网络不中断。

图 1-1 方案架构



方案优势

- 双连接：VPN网关提供两个接入地址，支持一个对端网关创建两条相互独立的VPN连接，一条连接中断后流量可快速切换到另一条连接。
- 双活网关：VPN双活网关部署在不同的AZ区域，实现AZ级高可用保障。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

1.1.2 组网和资源规划

数据规划

表 1-1 规划数据

类别	规划项	规划值
VPC	待互通子网	• 192.168.0.0/24 • 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： • 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
VPN连接	“连接1配置”中的Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30
用户数据中心	待互通子网	172.16.0.0/16
对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 1.1.1.1
IKE/IPsec策略	预共享密钥	Test@123

类别	规划项	规划值
	IKE策略	• 版本：v2 • 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 15 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group15 • 传输协议：ESP • 生命周期（秒）：3600

1.1.3 操作步骤

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 数据中心侧
  - 用户数据中心的VPN设备已经完成IPsec连接相关配置。相关操作步骤请参见**管理员指南**。

操作步骤

华为云VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 登录管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如**表1-2**所示。

表 1-2 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。 关联ER场景时，请选择“企业路由器”。	虚拟私有云
企业路由器	仅关联场景为“企业路由器”时需要选择。	er-001
虚拟私有云	选择用于分配互联子网的VPC。 关联场景为“企业路由器”时，该VPC可以对接ER，也可以不对接ER。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	仅关联场景为“虚拟私有云”时需要配置。 – 输入网段 输入需要和用户数据中心通信的子网，该子网可以在关联VPC内，也可以不在关联VPC内。 – 选择子网 选择关联VPC内的子网信息，用于和用户数据中心通信。	192.168.0.0/24，192.168.1.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“双活”。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。
   对端网关参数说明如**表1-3**所示。

表 1-3 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw
标识	对端网关和华为云VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	1.1.1.1

步骤5 配置VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**表 VPN连接参数说明**所示。

表 1-4 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关已绑定的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关已绑定的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1/30

参数	说明	取值参数
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.71.1/30
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.70.2/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

步骤6 配置对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。详细配置方法，请参见**管理员指南**。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
  选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

1.2 通过 VPN 实现云上云下网络互通（主备模式）

1.2.1 方案概述

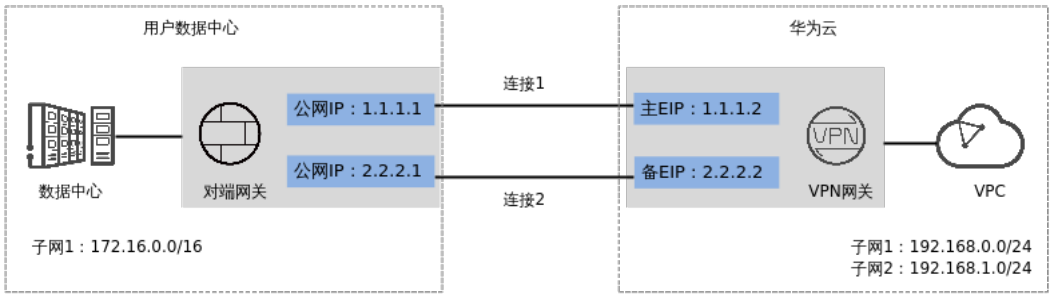
应用场景

当用户数据中心需要和VPC下的ECS资源进行相互访问时，可以通过VPN快速实现云上云下网络互通。

方案架构

本示例中，用户数据中心和VPC之间采用一组VPN连接保证网络可靠性，连接1和连接2互为主备。当其中一条VPN连接故障时，系统可以自动切换到另一条VPN连接，保证网络不中断。

图 1-2 方案架构



方案优势

- 双连接：VPN网关提供两个接入地址，支持一个对端网关创建两条相互独立的VPN连接，一条连接中断后流量可快速切换到另一条连接。
- 主备网关：VPN网关和对端网关通过主连接进行通信；当主连接发生故障时，VPN连接会自动切换到备连接；故障恢复后，VPN连接会自动切回到主连接。方便用户确定VPN连接的流量路径，出云流量优先走主EIP。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

1.2.2 组网和资源规划

数据规划

表 1-5 规划数据

类别	规划项	规划值
VPC	待互通子网	• 192.168.0.0/24 • 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	主备

类别	规划项	规划值
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： ● 主EIP：1.1.1.2 ● 备EIP：2.2.2.2
VPN连接	“连接1配置”中的Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 ● 本端隧道接口地址：169.254.70.1/30 ● 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	● 本端隧道接口地址：169.254.71.1/30 ● 对端隧道接口地址：169.254.71.2/30
用户数据中心	待互通子网	172.16.0.0/16
对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： ● 1.1.1.1 ● 2.2.2.1
IKE/IPsec策略	预共享密钥	Test@123
	IKE策略	● 版本：v2 ● 认证算法：SHA2-256 ● 加密算法：AES-128 ● DH算法：Group 15 ● 生命周期（秒）：86400 ● 本端标识：IP Address ● 对端标识：IP Address
	IPsec策略	● 认证算法：SHA2-256 ● 加密算法：AES-128 ● PFS：DH Group15 ● 传输协议：ESP ● 生命周期（秒）：3600

1.2.3 操作步骤

前提条件

- 云侧

  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 数据中心侧
  - 用户数据中心的VPN设备已经完成IPsec连接相关配置。相关操作步骤请参见**管理员指南**。

操作步骤

华为云VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 登录管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如**表1-6**所示。

表 1-6 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。 关联ER场景时，请选择“企业路由器”。	虚拟私有云
企业路由器	仅关联场景为“企业路由器”时需要选择。	er-001
虚拟私有云	选择用于分配互联子网的VPC。 关联场景为“企业路由器”时，该VPC可以对接ER，也可以不对接ER。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24

参数	说明	取值参数
本端子网	仅关联场景为“虚拟私有云”时需要配置。 – 输入网段 输入需要和用户数据中心通信的子网，该子网可以在关联VPC内，也可以不在关联VPC内。 – 选择子网 选择关联VPC内的子网信息，用于和用户数据中心通信。	192.168.0.0/24，192.168.1.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“主备”。	主备
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
备EIP	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。
   对端网关参数说明如**表1-7**所示。

表 1-7 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw
标识	对端网关和华为云VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	1.1.1.1

步骤5 配置VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**表1-8**所示。

表 1-8 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2

参数	说明	取值参数
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的备EIP。	2.2.2.2
连接2对端网关	选择连接2对端网关。	2.2.2.1
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1/30
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2/30
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认

参数	说明	取值参数
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

步骤6 配置对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。详细配置方法，请参见**管理员指南**。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
  选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

1.3 通过 VPN 实现云上云下网络互通（非固定 IP 接入）

1.3.1 方案概述

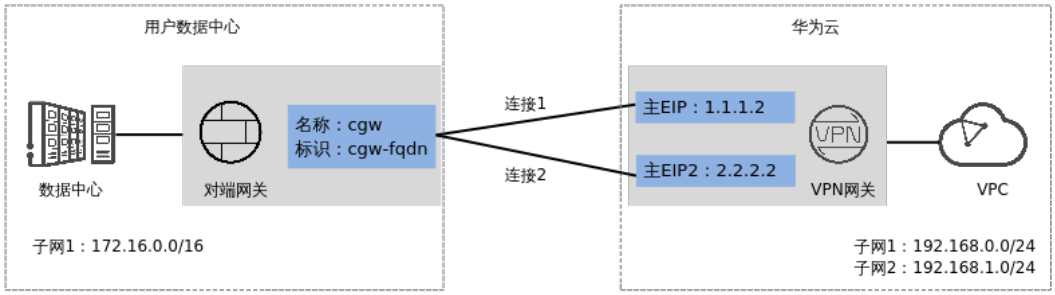
应用场景

当用户数据中心需要和VPC下的ECS资源进行相互访问时，支持用户侧网络使用非固定IP接入，实现云上云下网络互通。

方案架构

本示例中，用户数据中心和VPC之间采用一组VPN连接保证网络可靠性。当其中一条VPN连接故障时，系统可以自动切换到另一条VPN连接，保证网络不中断。

图 1-3 方案架构



方案优势

本地数据中心可以使用不固定的公网IP接入，组网更灵活，宽带费用更低。

约束与限制

- 本地数据中心的VPN连接只支持策略模式。
- 必须由本地数据中心主动发起协商。
- 非固定IP接入模式下仅支持IKEv2，不支持IKEv1。

1.3.2 组网和资源规划

数据规划

表 1-9 规划数据

类别	规划项	规划值
VPC	待互通子网	• 192.168.0.0/24 • 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： • 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
用户数据中心	待互通子网	172.16.0.0/16
对端网关	标识	选择FQDN类型，命名为“cgw-fqdn”。
策略模板	IKE策略	• 版本：v2 • 认证算法：SHA2-256 • 加密算法：AES-128-GCM-16 • DH算法：Group 15 • 生命周期（秒）：86400 • 本端标识：IP Address
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128-GCM-16 • PFS：DH Group15 • 传输协议：ESP • 生命周期（秒）：3600

1.3.3 操作步骤

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 数据中心侧
  - 用户数据中心的VPN设备已经完成IPsec连接相关配置。相关操作步骤请参见**管理员指南**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如**表1-10**所示。

表 1-10 VPN 网关参数说明

参数	说明	取值参数
计费模式	选择“包年/包月”。	包年/包月
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。 关联ER场景时，请选择“企业路由器”。	虚拟私有云
企业路由器	仅“关联模式”为“企业路由器”时需要选择。	er-001
虚拟私有云	选择用于分配互联子网的VPC。 “关联模式”为“企业路由器”时，该VPC可以对接ER，也可以不对接ER。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24

参数	说明	取值参数
本端子网	仅“关联模式”为“虚拟私有云”时需要配置。 – 输入网段 输入需要和用户数据中心通信的子网，该子网可以在关联VPC内，也可以不在关联VPC内。 – 选择子网 选择关联VPC内的子网信息，用于和用户数据中心通信。	192.168.0.0/24，192.168.1.0/24
规格	选择“专业型1”，并勾选“非固定IP接入”。	专业型1-非固定IP。
HA模式	选择“双活”。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。
   对端网关参数说明如**表1-11**所示。

表 1-11 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw
标识	选择FQDN，并输入对端网关标识。	FQDN cgw-fqdn

步骤5 配置VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**VPN连接参数说明**所示。

表 1-12 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2

参数	说明	取值参数
连接1对端网关	选择连接1对端网关。	cgw-fqdn
连接2网关IP	选择VPN网关的备EIP。	2.2.2.2
连接2对端网关	选择连接2对端网关。	cgw-fqdn
连接模式	选择“策略模板模式”。	策略模板模式
对端子网	指需要通过VPN连接访问云上VPC的用户侧子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的预共享密钥、确认密钥、和策略模板配置。	*请根据实际设置*
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略模板配置	和对端网关的策略配置需要保持一致。	保持默认
连接2配置	选择是否“与连接1保持一致”。 **说明** 建议连接2配置和连接1配置保持一致。	开启

步骤6 配置对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。详细配置方法，请参见**管理员指南**。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
  选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

1.4 通过 VPN Hub 实现云下多分支网络互通

1.4.1 方案概述

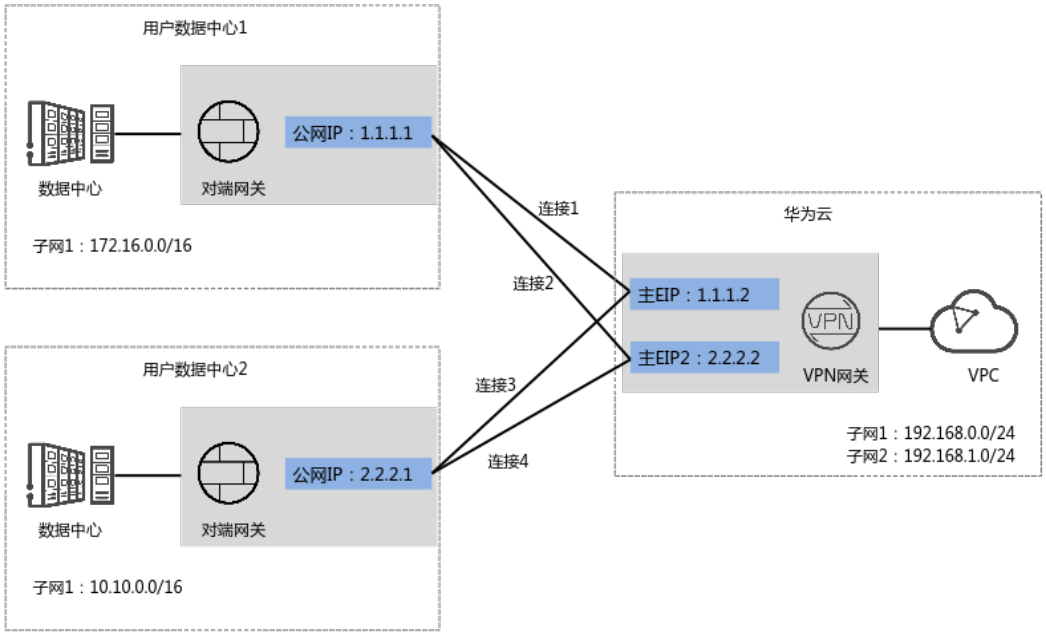
场景描述

由于业务需要，A企业的数据中心1和2需要实现网络互通。

组网方案

VPN服务提供的组网方案如图 组网方案所示。

图 1-4 组网方案



方案优势

- 支持分支互访：支持云上VPN网关作为VPN Hub，云下站点通过VPN Hub实现分支互访，无需两两站点之间配置VPN连接。
- 双连接：VPN网关提供两个接入地址，支持一个对端网关创建两条相互独立的VPN连接，一条连接中断后流量可快速切换到另一条连接，保证连接可靠性。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

1.4.2 组网和资源规划

数据规划

表 1-13 规划数据

类别	规划项	规划值
VPC	待互通子网	• 192.168.0.0/24 • 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： • 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
用户数据中心1	待互通子网	172.16.0.0/16
用户数据中心1对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 1.1.1.1
用户数据中心1VPN连接	“连接1配置”中的Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30
用户数据中心2	待互通子网	10.10.0.0/16
用户数据中心2对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 2.2.2.1
用户数据中心2VPN连接	“连接1配置”中的Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.72.1/30 • 对端隧道接口地址：169.254.72.2/30

类别	规划项	规划值
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.73.1/30 • 对端隧道接口地址：169.254.73.2/30
IKE/IPsec策略	预共享密钥	Test@123
	IKE策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 15 • 版本：v2 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group15 • 传输协议：ESP • 生命周期（秒）：3600

1.4.3 操作步骤

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 数据中心侧
  - 用户数据中心1和2的VPN设备已经完成IPsec连接相关配置。相关操作步骤请参见**管理员指南**。
  - 用户数据中心1的VPN设备对端网络中需要包含华为云VPC的本端子网和用户数据中心2的待互通子网；用户数据中心2的VPN设备对端网络中需要包含华为云VPC的本端子网和用户数据中心1的待互通子网。

操作步骤

华为云VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。
   VPN网关参数说明如**表1-14**所示。

表 1-14 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。 关联ER场景时，请先选择ER信息。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
本端子网	华为云VPC需要与用户数据中心互通的子网。	192.168.0.0/24，192.168.1.0/24
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“双活”。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤2 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。
   对端网关参数说明如**表1-15**所示。

表 1-15 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw1
标识	数据中心1下对端网关和华为云VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	1.1.1.1

3. 参见上述步骤，配置数据中心2的对端网关信息（2.2.2.1）。

步骤3 配置云侧和数据中心1的VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**表1-16**所示。

表 1-16 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心1中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1/30
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2/30

参数	说明	取值参数
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

步骤4 配置云侧和数据中心2的VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 根据界面提示配置VPN连接参数，单击“立即购买”。
   VPN连接参数说明如表1-17所示。

表 1-17 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	2.2.2.1
连接2网关IP	选择VPN网关的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	2.2.2.1
连接模式	选择“静态路由模式”。	静态路由模式

参数	说明	取值参数
对端子网	用户数据中心2中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	10.10.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.72.1/30
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.72.2/30
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和用户数据中心2对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和用户数据中心2对端网关的策略配置需要保持一致。	保持默认
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.73.1/30

参数	说明	取值参数
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.73.2/30

步骤5 配置数据中心1/2的对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。详细配置方法，请参见**管理员指南**。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
  选择“虚拟专用网络 > 企业版-VPN连接”，四条VPN连接状态显示为正常。
- 用户数据中心1内的服务器和用户数据中心2内的服务器可以相互Ping通。

1.5 通过企业路由器构建 DC/VPN 双链路主备混合云组网

1.5.1 方案概述

应用场景

云专线（Direct Connect，DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud，VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线构建满足企业通信的大规模混合云组网。

虚拟专用网络（Virtual Private Network，VPN）用于在线下IDC和华为云VPC之间建立一条安全加密的公网通信隧道。相比通过DC构建混合云，使用VPN更加快速，成本更低。

为了助力企业客户实现混合云组网的高可靠性，并且控制成本费用，我们推荐您在企业路由器中同时接入DC和VPN两条网络链路，构建主备双链路的混合云组网。当主链路故障后，可自动切换至备链路，降低了单链路故障导致的业务中断风险。

说明

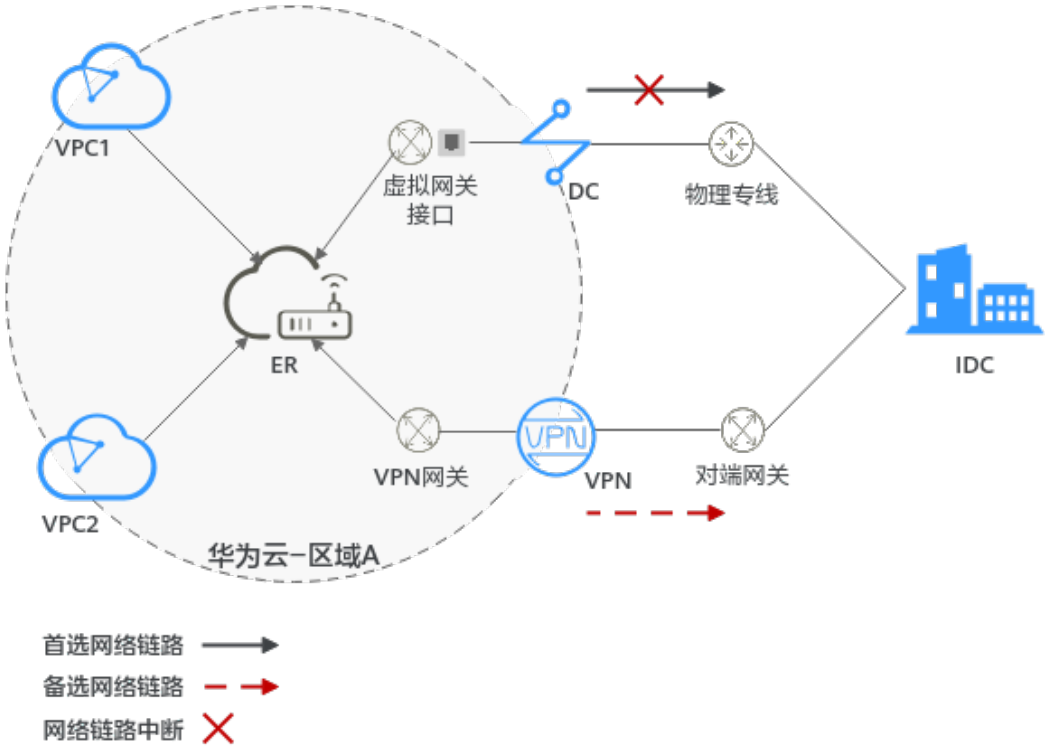
关于企业路由器更详细的介绍，请参见**企业路由器产品介绍**。

方案架构

为了提升混合云组网的可靠性，XX企业同时部署了DC和VPN两条网络链路，均可以连通云上VPC和线下IDC的网络。DC和VPN两条网络链路互为主备，主链路为DC，备链路为VPN，当DC链路故障时，可自动切换到VPN链路，降低网络中断对业务造成的影响。

- 将VPC1、VPC2以及DC接入企业路由器中，VPC1和VPC2网络互通，并且均可以通过DC和线下IDC通信。
- 将VPN接入企业路由器中，当主链路DC故障时，VPC1和VPC2可以通过备链路VPN和线下IDC通信。

图 1-5 DC/VPN 双链路主备混合云组网



方案优势

通过企业路由器，可以实现DC和VPN主备链路的自动切换，不需要手动切换双链路，不仅避免业务受损，同时降低维护成本。

约束与限制

云上VPC子网网段与客户IDC侧子网网段不能重复。

1.5.2 组网和资源规划

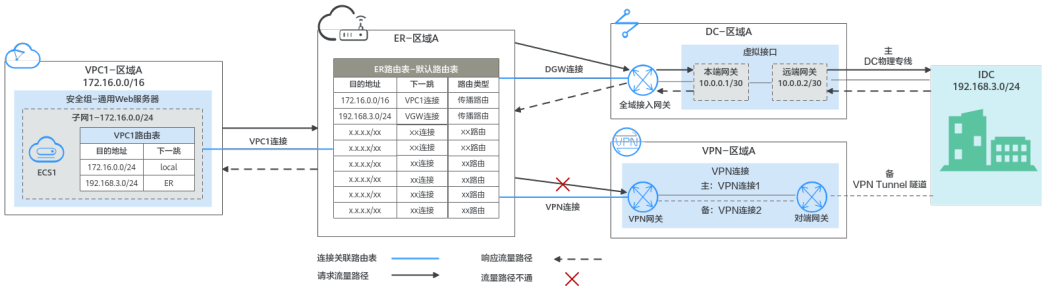
通过企业路由器构建DC/VPN双链路主备混合云组网，您需要规划资源和组网，本示例中为您详细介绍资源和组网情况。

- **网络规划说明**：规划VPC及其子网、DC、VPN和ER的网段、路由等。
- **资源规划说明**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC、VPN以及ER等。

网络规划说明

DC/VPN双链路主备混合云组网规划如**图1-6**所示，将VPC、DC和VPN分别接入ER中，组网规划说明如**表1-19**所示。

图 1-6 DC/VPN 双链路主备混合云组网规划



DC和VPN互为主备网络链路，在DC网络链路正常的情况下，流量优选云专线DC。

- 在ER路由表中只显示优选路由，由于DGW连接(DC)路由的优先级高于VPN连接，因此ER路由表中不显示VPN连接的路由。
- 云上VPC和线下IDC通信时，默认使用DC这条网络链路，本示例的网络流量路径说明请参见**表1-18**

表 1-18 网络流量路径说明

路径	说明
请求路径：VPC1→线下IDC	1. 在VPC1路由表中，通过下一跳为ER的路由将流量转送到ER。 2. 在ER路由表中，通过下一跳为DGW连接的路由将流量转送到全域接入网关。 3. 全域接入网关连接虚拟接口，通过虚拟接口将流量从远端网关转送到物理专线。 4. 通过物理专线将流量送达线下IDC。
响应路径：线下IDC→VPC1	1. 通过物理专线将流量转送到虚拟接口。 2. 虚拟接口连接全域接入网关，通过虚拟接口将流量从本端网关转送到全域接入网关。 3. 通过全域接入网关将流量转送到ER。 4. 在ER路由表中，通过下一跳为VPC1连接的路由将流量送达VPC1。

表 1-19 DC/VPN 双链路互备混合云组网规划说明

资源	说明
VPC	业务VPC，实际运行客户业务的VPC，本示例中为VPC1，具体说明如下： ● VPC网段与客户IDC侧网段不能重复。 ● VPC有一个默认路由表。 ● VPC默认路由表中的路由说明如下： – local：表示VPC本地IPV4的默认路由条目，用于VPC内子网通信，系统自动配置。 – ER：表示将VPC子网流量转发至ER，此处目的地址配置为IDC的子网网段，路由信息如**表1-20**所示。
	VPN网关使用的子网，建议您创建一个新的VPC，并从中分配子网。 您在创建VPN网关时，需要填写该子网网段，VPN网关使用的子网不能与VPC内已有的子网网段重叠。
DC	● 1个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。 ● 1个全域接入网关：将全域接入网关接入ER中，即表示将“全域接入网关（DGW）”连接添加到ER。 ● 1个虚拟接口：连接全域接入网关和物理连接。
VPN	● 1个VPN网关：将VPN接入ER中，即表示将“VPN网关（VPN）”连接添加到ER。 ● 1个对端网关：用户IDC侧的对端网关。 ● 1组VPN连接：连接VPN网关和对端网关，2条VPN连接互为主备链路。
ER	开启“默认路由表关联”和“默认路由表传播”功能，添加完连接后，系统会自动执行以下配置： ● VPC： – 将1个“虚拟私有云（VPC）”连接关联至ER默认路由表。 – 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如**表1-21**所示。 ● DC： – 将1个“全域接入网关（DGW）”连接关联至ER默认路由表。 – 在默认路由表中创建“全域接入网关（DGW）”连接的传播，路由自动学习DC侧的所有路由信息，路由信息如**表1-21**所示。 ● VPN： – 将1个“VPN网关（VPN）”连接关联至ER默认路由表。 – 在默认路由表中创建“VPN网关（VPN）”连接的传播，路由自动学习VPN侧的所有路由信息，路由信息如**表1-21**所示。

资源	说明
ECS	1个ECS位于业务VPC内，本示例用该ECS来验证云上和线下IDC的网络通信情况。 如果您有多台ECS，并且这些ECS位于不同的安全组，需要在安全组中添加规则放通网络。

表 1-20 VPC 路由表

目的地址	下一跳	路由类型
192.168.3.0/24	企业路由器	静态路由：自定义

说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由。

表 1-21 ER 路由表

目的地址	下一跳	路由类型
VPC1网段：172.16.0.0/16	VPC1连接：er-attach-01	传播路由
IDC侧网段：192.168.3.0/24	DGW连接：dgw-demo	传播路由
IDC侧网段：192.168.3.0/24	VPN连接：vpngw-demo	传播路由

须知

- 当两条路由功能一样时，ER路由表中只会显示优选路由。当DC和VPN网络链路均正常时，由于DGW连接和VPN连接的传播路由均指向线下IDC，因此只能在ER路由表中看到优先级较高的DGW连接的路由，暂时不支持查看ER路由中VPN连接的所有路由（包括未优选的路由）。
- 当DC出现故障，网络链路切换到VPN时，此时通过管理控制台，可以在ER路由表中看到VPN连接的传播路由。

资源规划说明

企业路由器ER、云专线DC、虚拟专用网络VPN、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 1-22 DC/VPN 双链路互备混合云组网资源规划总体说明

资源类型	资源数量	说明
VPC	2	业务VPC，实际运行客户业务的VPC，需要接入ER中。 ● VPC名称：请根据实际情况填写，本示例为vpc-for-er。 ● IPv4网段：VPC网段与客户IDC侧网段不能重复，请根据实际情况填写，本示例为172.16.0.0/16。 ● 子网名称：请根据实际情况填写，本示例为subnet-for-er。 ● 子网IPv4网段：VPC子网网段与客户IDC侧子网网段不能重复，请根据实际情况填写，本示例为172.16.0.0/24。
		VPN网关使用的VPC，需要从中分配一个子网提供给VPN网关使用。 ● VPC名称：请根据实际情况填写，本示例为vpc-for-vpn。 ● IPv4网段：请根据实际情况填写，本示例为10.0.0.0/16。 ● 子网名称：您创建VPC时，必须创建一个默认子网，请根据实际情况填写，本示例为subnet-01。 ● 子网IPv4网段：默认子网在本示例中不使用，请根据实际情况填写，本示例为10.0.0.0/24。 **须知** 您在创建VPN网关时，“虚拟私有云”需要选择该VPC，“互联子网”填写该VPC下的网段，请确保选择的互联子网存在4个及以上可分配的IP地址。
ER	1	● 名称：请根据实际情况填写，本示例为er-test-01。 ● ASN：此处AS号不能和线下IDC的AS号一样，本示例中保持默认值64512。 ● 默认路由表关联：开启 ● 默认路由表传播：开启 ● 自动接受共享连接：请根据实际情况选择，本示例选择“开启”。 ● 连接，本示例需要在企业路由器中添加3个连接： – VPC连接：er-attach-VPC – DGW连接：er-attach-DGW – VPN连接：er-attach-VPN
DC	1	物理连接：请根据实际需求创建。

资源类型	资源数量	说明
		全域接入网关 ● 名称：请根据实际情况填写，本示例为dgw-demo。 ● 关联模式：请选择“企业路由器”。 ● 企业路由器：选择您的企业路由器，本示例为er-test-01。 ● BGP ASN：此处AS号和企业路由器的AS号一样或者不一样均可，本示例中和ER的AS号一致，保持默认值64512。
		虚拟接口 ● 名称：请根据实际情况填写，本示例vif-demo。 ● 全域接入网关：选择您的全域接入网关，本示例为dgw-demo。 ● 本端网关：请根据实际情况填写，本示例为10.0.0.1/30。 ● 远端网关：请根据实际情况填写，本示例为10.0.0.2/30。 ● 远端子网：请根据实际情况填写，本示例为192.168.3.0/24。 ● 路由模式：请选择“BGP”。 ● BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上全域接入网关的AS号一样，本示例为65525。
VPN	1	VPN网关 ● 名称：请根据实际情况填写，本示例为vpngw-demo。 ● 关联模式：请选择“企业路由器”。 ● 企业路由器：选择您的企业路由器，本示例为er-test-01。 ● BGP ASN：由于DC和VPN为双链路互备，此处AS号和DC全域接入网关的AS号必须一样，本示例为64512。 ● 虚拟私有云：选择您的虚拟私有云，本示例为vpc-for-vpn。 ● 互联子网：用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。请根据实际情况填写，本示例为10.0.5.0/24。
		对端网关 ● 名称：请根据实际情况填写，本示例为cgw-demo。 ● 路由模式：请选择“动态BGP”。 ● BGP ASN：此处为线下IDC侧的AS号，由于DC和VPN为双链路互备，该AS号和DC虚拟接口处设置的AS号必须一样，本示例为65525。

资源类型	资源数量	说明
		2条VPN连接，互为主备： • 名称：请根据实际情况填写，本示例中，主VPN连接为vpn-demo-01，备VPN连接为vpn-demo-02。 • VPN网关：选择您的VPN网关，本示例为vpngw-demo。 • 公网IP：请根据实际情况选择，主VPN连接选择主EIP，备VPN连接选择备EIP。 • 连接模式：请选择“路由模式”。 • 对端网关：选择您的对端网关，本示例为cgw-demo。 • 接口地址分配方式：本示例选择“自动分配”。 • 路由模式：请选择“BGP”。
ECS	1	• 名称：根据实际情况填写，本示例为ecs-demo。 • 镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。 • 网络： – 虚拟私有云：选择您的虚拟私有云，本示例为vpc-for-er。 – 子网：选择子网，本示例为subnet-for-er。 • 安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。 • 私有IP地址：172.16.1.137

须知

- 由于DC和VPN是主备链路，为了防止网络环路，DC全域接入网关和VPN网关的AS号必须保持一致，本示例为64512。
- ER的AS号和DC、VPN的一样或者不一样均可，本示例为64512。
- 线下IDC侧的AS号，不能和云上服务的AS号一样，请根据客户的实际情况填写，本示例为65525。

1.5.3 DC/VPN 双链路互备混合云组网构建流程

本章节介绍通过企业路由器构建DC/VPN双链路主备混合云组网总体流程，流程说明如**表1-23**所示。

表 1-23 构建 DC/VPN 双链路主备混合云组网流程说明

步骤	说明
步骤一：创建云服务资源	1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。 2. 创建业务VPC和子网，本示例中创建1个VPC和子网。 3. 在业务VPC子网内，创建ECS，本示例中创建1个ECS。
步骤二：在企业路由器中添加并配置DGW连接	1. 创建物理连接，物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。 2. 创建全域接入网关：创建1个关联企业路由器的全域接入网关，企业路由器中会自动添加“全域接入网关（DGW）”连接。 3. 创建虚拟接口：创建关联全域接入网关的虚拟接口，连接全域接入网关和物理连接。 4. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。
步骤三：在企业路由器中添加并配置VPC连接	1. 在企业路由器中添加“虚拟私有云（VPC）”连接：将1个业务VPC接入企业路由器中。 2. 在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息，目的地址为IDC侧网段。
步骤四：验证DC链路的通信情况	登录ECS，执行**ping**命令，验证DC链路的网络互通情况。
步骤五：在企业路由器中添加并配置VPN连接	1. 创建VPN网关：创建1个关联企业路由器的VPN网关，企业路由器中会自动添加“VPN网关（VPN）”连接。 2. 创建对端网关：创建1个用户IDC侧的对端网关。 3. 创建1组VPN连接：VPN连接用来连通VPN网关和对端网关，两条VPN连接互为主备链路。 4. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。
步骤六：验证VPN链路的通信情况	登录ECS，执行**ping**命令，验证VPN链路的网络互通情况。 由于VPN链路为备选，如果您需要验证VPN链路通信情况，需要先构造DC主链路故障，然后验证备VPN链路的通信情况。

1.5.4 DC/VPN 双链路互备混合云组网构建步骤

步骤一：创建云服务资源（业务 VPC、ECS、ER）

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见**表1-22**。

步骤1 创建企业路由器。

创建企业路由器，具体方法请参见**创建企业路由器**。

步骤2 创建业务VPC。

创建VPC及子网，具体方法请参见**创建虚拟私有云和子网**。

步骤3 创建业务ECS。

本示例中1个业务ECS主要用于验证云上VPC和线下IDC通信使用，数量和配置仅供参考，请您根据实际需要创建业务ECS。

创建ECS，具体方法请参见**购买方式概述**。

----结束

步骤二：在企业路由器中添加并配置 DGW 连接

本示例中，云专线DC资源的总体规划说明，请参见**表1-22**。

步骤1 创建物理连接。

创建方法，具体请参见**物理连接接入**。

步骤2 创建全域接入网关，即在企业路由器中添加“全域接入网关（DGW）”连接。

1. 在云专线管理控制台，创建全域接入网关。
   具体方法请参见**步骤2：创建全域接入网关**。
2. 在企业路由器控制台，查看“全域接入网关（DGW）”连接的添加情况。
   具体方法请参见**查看连接**。
   “全域接入网关（DGW）”连接的状态“正常”，表示已成功接入企业路由器中。
   由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“全域接入网关（DGW）”连接后，以下均为系统自动配置：
   - 在ER默认路由表中创建关联。
   - 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。
     需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

步骤3 创建虚拟接口。

创建虚拟接口用来连接全域接入网关和线下IDC，具体方法请参见**步骤3：创建虚拟接口**。

步骤4 在IDC侧的网络设备上，配置网络参数。

由于组网为DC和VPN的双链路互备，因此配置路由时，需要注意以下方面：

- DC和VPN的路由类型保持一致，构造双链路互备需要配置为BGP路由。
- 配置DC和VPN路由的主备优先级，确保DC的优先级高于VPN。
- DC和VPN网络链路的断连感知时间建议和云上网络保持一致。

----结束

步骤三：在企业路由器中添加并配置 VPC 连接

步骤1 将业务VPC接入企业路由器中。

添加连接时，不开启“配置连接侧路由”功能。

须知

开启该功能后，会自动VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。本示例中，需要在VPC路由表中手动配置指向ER的路由，目的地址为IDC侧的网段。

添加“虚拟私有云（VPC）”连接，具体方法请参见**在企业路由器中添加VPC连接**。

步骤2 检查ER路由表中指向VPC的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见**表1-19**和**表1-21**。

查看ER路由，具体方法请参见**查看路由**。

步骤3 在业务VPC的路由表中，添加指向ER的路由。

VPC路由规划详情，请参见**表1-20**。

配置路由信息，具体方法请参见**在VPC路由表中配置路由**。

----结束

步骤四：验证 DC 链路的通信情况

步骤1 登录弹性云服务器ecs-demo。

弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

本示例是通过管理控制台远程登录（VNC方式）。

步骤2 执行以下命令，验证业务VPC与IDC是否可以通过ER通信。

ping *IDC侧任意一个IP地址*

命令示例：

ping 192.168.3.10

回显类似如下信息，表示vpc-for-er与IDC可以通过ER通信。

```
[root@ecs-A02 ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.102) 56(84) bytes of data.
64 bytes from 192.168.3.102: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.102: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.102: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.102: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.102 ping statistics ---
```

----结束

步骤五：在企业路由器中添加并配置 VPN 连接

本示例中，虚拟专用网络VPN、VPN网关使用的VPC资源的总体规划说明，请参见**表1-22**。

步骤1 创建1个VPN网关使用的VPC。

创建VPC及子网，具体方法请参见**创建虚拟私有云和子网**。

须知

您在创建VPN网关时，“虚拟私有云”需要选择该VPC，“互联子网”填写该VPC下的网段，请确保选择的互联子网存在4个及以上可分配的IP地址。

步骤2 创建VPN网关，即在企业路由器中添加“VPN网关（VPN）”连接。

1. 在虚拟专用网络管理控制台，创建VPN网关。
   具体方法请参见**创建VPN网关**。
2. 在企业路由器控制台，查看“VPN网关（VPN）”连接的添加情况。
   具体方法请参见**查看连接**。
   “VPN网关（VPN）”连接的状态“正常”，表示已成功接入企业路由器中。
   由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“VPN网关（VPN）”连接后，以下均为系统自动配置：
   - 在ER默认路由表中创建关联。
   - 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。
     需要执行以下步骤连通VPN后，才可以在ER路由表中查看到IDC侧的路由信息。

步骤3 创建对端网关。

具体方法请参见**创建对端网关**。

步骤4 创建主备VPN连接。请参见**创建VPN连接**。

步骤5 在IDC侧的网络设备上，配置网络参数。

由于组网为DC和VPN的双链路互备，因此配置路由时，需要注意以下方面：

- DC和VPN的路由类型保持一致，构造双链路互备需要配置为BGP路由。
- 配置DC和VPN路由的主备优先级，确保DC的优先级高于VPN。
- DC和VPN网络链路的断连感知时间建议和云上网络保持一致。

----结束

步骤六：验证 VPN 链路的通信情况

由于VPN链路为备选，如果您需要验证VPN链路通信情况，需要先构造DC主链路故障，然后验证备VPN链路的通信情况。

步骤1 构造DC主链路的故障，确保业务VPC已无法通过该链路和IDC通信。

须知

请您务必在没有业务的情况下，构造DC链路故障，以免对业务造成影响。

步骤2 登录弹性云服务器ecs-demo。

弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

本示例是通过管理控制台远程登录（VNC方式）。

步骤3 执行以下命令，验证业务VPC与IDC是否可以通过ER通信。

ping *IDC侧任意一个IP地址*

命令示例：

ping 192.168.3.10

回显类似如下信息，表示vpc-for-er与IDC可以通过ER通信。

```
[root@ecs-A02 ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.102) 56(84) bytes of data.
64 bytes from 192.168.3.102: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.102: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.102: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.102: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.102 ping statistics ---
```

----结束

1.6 通过 VPN 实现双 Internet 线路上云

1.6.1 方案概述

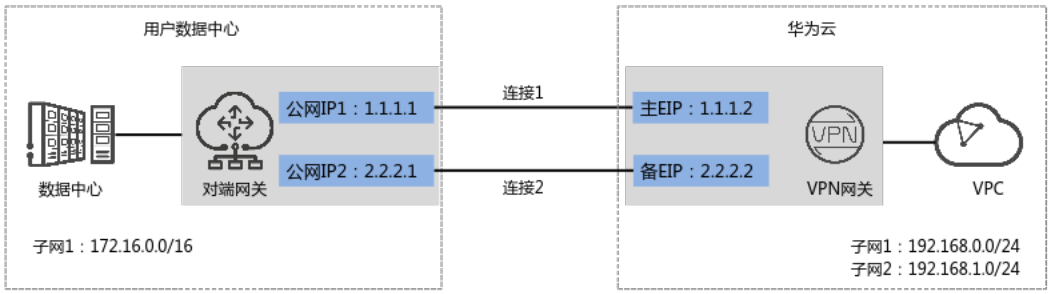
应用场景

由于业务需要，A企业的数据中心需要和云上的VPC实现网络互通，同时希望用户数据中心通过2个公网IP地址和VPN网关相连，以提升连接可靠性。

方案架构

VPN服务提供的组网方案如图 组网方案所示。

图 1-7 组网方案



方案优势

- 双连接：VPN网关提供两个接入地址，支持一个对端网关创建两条相互独立的VPN连接，一条连接中断后流量可快速切换到另一条连接，保证连接可靠性。
- 双活网关：VPN双活网关部署在不同的AZ区域，实现AZ级高可用保障。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

1.6.2 组网和资源规划

数据规划

表 1-24 规划数据

类别	规划项	规划值
VPC	待互通子网	• 192.168.0.0/24 • 192.168.1.0/24
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	主备
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： • 主EIP：1.1.1.2 • 备EIP：2.2.2.2
VPN连接	“连接1配置”中的Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30
用户数据中心	待互通子网	172.16.0.0/16
对端网关	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： • 公网IP1：1.1.1.1 • 公网IP2：2.2.2.1
IKE/IPsec策略	预共享密钥	Test@123

类别	规划项	规划值
	IKE策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 15 • 版本：v2 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group15 • 传输协议：ESP • 生命周期（秒）：3600

1.6.3 操作步骤

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 数据中心侧
  - 用户数据中心的VPN设备已经完成IPsec连接相关配置。相关操作步骤请参见**管理员指南**。

操作步骤

华为云VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如**表1-25**所示。

表 1-25 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“虚拟私有云”。 关联ER场景时，请先选择ER信息。	虚拟私有云
虚拟私有云	选择华为云需要和用户数据中心通信的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	仅关联场景为“虚拟私有云”时需要配置。 – 输入网段 输入需要和用户数据中心通信的子网，该子网可以在关联VPC内，也可以不再关联VPC内。 – 选择子网 选择关联VPC内的子网信息，用于和用户数据中心通信。	192.168.0.0/24，192.168.1.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“主备”。	主备
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
备EIP	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示，配置第一个对端网关参数。
   对端网关参数说明如**表1-26**所示。

表 1-26 第一个对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ar01
标识	对端网关和华为云VPN网关通信的IP地址。 请确认数据中心中的对端网关已经放通UDP端口4500。	1.1.1.1

3. 根据界面提示，配置第二个对端网关参数。
   对端网关参数说明如**表1-27**所示。

表 1-27 第二个对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-ar02
标识	对端网关和华为云VPN网关通信的IP地址。 请确认数据中心中的对端网关已经放通UDP端口4500。	2.2.2.1

步骤5 配置VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**表1-28**所示。

表 1-28 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关的备EIP。	2.2.2.2
连接2对端网关	选择连接2对端网关。	2.2.2.1
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16

参数	说明	取值参数
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	- 手动分配 本示例以“手动分配”为例。 - 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1/30
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2/30
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

步骤6 配置对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。详细配置方法，请参见**管理员指南**。

----结束

结果验证

- 大约5分钟后，查看VPN连接状态。
  选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

1.7 通过 VPN 实现专线加密

1.7.1 方案概述

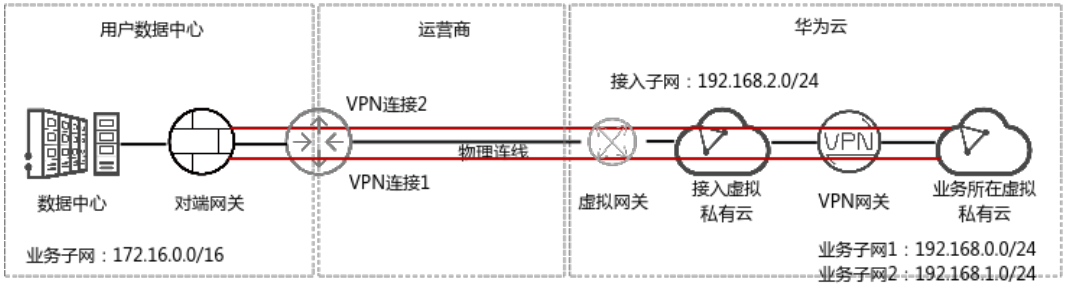
应用场景

某金融企业的数据中心通过专线入云，出于数据传输安全的考虑，希望VPN对其出入云的数据进行加密。

方案架构

VPN服务提供的组网方案如图 组网方案所示。

图 1-8 组网方案



方案优势

- 双连接：VPN网关提供两个接入地址，支持一个对端网关创建两条相互独立的VPN连接，一条连接中断后流量可快速切换到另一条连接。
- 更安全：专线提供独立的线路，保证数据传输质量；VPN提供数据加密，保证数据传输安全。

约束与限制

- VPN网关的本端子网与对端子网不能相同，即VPC和用户数据中心待互通的子网不能相同。
- VPN网关和对端网关的IKE策略、IPsec策略、预共享密钥需要相同。
- VPN网关和对端网关上配置的本端接口地址和对端接口地址需要互为镜像。
- VPC内弹性云服务器安全组允许访问对端和被对端访问。

1.7.2 组网和资源规划

数据规划

表 1-29 规划数据

类别	规划项	规划值
用户数据中心	待互通业务子网	VPN对端网关IP所在子网。 172.16.0.0/16
	接入子网	专线对端网关IP所在子网。接入子网可以和业务子网相同。本示例以接入子网和业务子网相同为例。 172.16.0.0/16
业务子网所在虚拟私有云	虚拟私有云名称	tenant_vpc
专线虚拟网关	虚拟私有云	需要和VPN网关的接入虚拟私有云保持一致。 tenant_vpc
	本端子网	需要和VPN网关的接入子网保持一致。 192.168.2.0/24
专线虚拟接口	本端网关IP地址	用于专线虚拟网关和远端网关建立通信，配置时两边需要互为镜像。 1.1.1.1/30
	远端网关IP地址	2.2.2.2/30
	远端子网	专线对端网关所在的接入子网信息。 172.16.0.0/16
VPN网关	虚拟私有云	即业务子网所在虚拟私有云。 tenant_vpc
	互联子网	用于VPN网关和虚拟私有云通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	本端子网	虚拟私有云用于和用户数据中心通信的子网。 ● 192.168.0.0/24 ● 192.168.1.0/24
	HA模式	双活
	接入虚拟私有云	可以和虚拟私有云相同，也可以和虚拟私有云不同。 本示例中以接入虚拟私有云和虚拟私有云相同为例。 tenant_vpc

类别	规划项	规划值
	接入子网	• 如果接入虚拟私有云和虚拟私有云相同，且接入子网和互联子网相同，请确保选择的互联子网存在4个及以上可分配的IP地址。本示例以该场景为例。 192.168.2.0/24 • 如果接入虚拟私有云和虚拟私有云相同，且接入子网和互联子网不同，请确保选择的接入子网存在2个及以上可分配的IP地址。 • 如果接入虚拟私有云和虚拟私有云不同，请确保选择的接入子网存在2个及以上可分配的IP地址。
	接入IP	手动指定网关IP地址。 • 私网IP地址1：192.168.2.100 • 私网IP地址2：192.168.2.101
VPN连接	“连接1配置”中的Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30
	“连接2配置”中的Tunnel接口地址	• 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30
VPN对端网关	网关IP	IP地址由用户数据中心管理员规划配置。 172.16.0.111
IKE/IPsec策略	预共享密钥	Test@123
	IKE策略	• 版本：v2 • 认证算法：SHA2-256 • 加密算法：AES-128 • DH算法：Group 15 • 生命周期（秒）：86400 • 本端标识：IP Address • 对端标识：IP Address
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group15 • 传输协议：ESP • 生命周期（秒）：3600

1.7.3 配置 DC

操作步骤

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 云专线”。

步骤3 配置物理连接。

物理连接接入提供自建专线接入和一站式接入两种创建方式，用户可根据具体业务场景选择合适的创建方式。

详细操作步骤，请参见**物理连接接入**。

表 1-30 物理连接参数说明

参数	说明	取值参数
物理连接名称	物理连接的名称。	phlk_01

步骤4 配置虚拟网关。

虚拟网关参数说明如**表1-31**所示。详细全量参数解释请参见**创建虚拟网关**。

表 1-31 虚拟网关参数说明

参数	说明	取值参数
名称	虚拟网关的名称。	dcgw_01
虚拟私有云	虚拟网关所关联的虚拟私有云信息。 本场景中选择接入虚拟私有云。	tenant_vpc
本端子网	云专线允许访问的虚拟私有云子网。 本场景中选择接入虚拟私有云对应的接入子网。	192.168.2.0/24

步骤5 配置虚拟接口。

虚拟接口参数说明如**表1-32**所示。详细全量参数解释请参见**创建虚拟接口**。

表 1-32 虚拟接口参数说明

参数	说明	取值参数
名称	虚拟接口名称。	dcif_01
物理连接	选择可用的物理连接。	phlk_01
虚拟网关	选择可用的虚拟网关。	dcgw_01

参数	说明	取值参数
本端网关（华为云侧）	华为云侧网络接口互联的IP地址。	1.1.1.1/30
远端网关（用户侧）	用户数据中心侧网络接口互联的IP地址。 远端网关与本端网关需要设置为同一网段的IP地址，一般使用30位掩码。	2.2.2.2/30
远端子网	用户数据中心接入子网和子网掩码。	172.16.0.0/16
路由模式	支持静态路由和BGP两种路由模式。	静态路由

----结束

1.7.4 配置 VPN

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
  - 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 数据中心侧
  - 用户数据中心的VPN设备已经完成IPsec连接相关配置。相关操作步骤请参见**管理员指南**。

操作步骤

华为云VPN服务支持静态路由模式、BGP路由模式和策略模式三种连接模式。本示例以静态路由模式进行配置讲解。

步骤1 登录华为云管理控制台。

步骤2 选择“网络 > 虚拟专用网络”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关参数说明如**表1-33**所示。

表 1-33 VPN 网关参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001

参数	说明	取值参数
网络类型	选择“私网”。	私网
关联模式	选择“虚拟私有云”。 关联ER场景时，请选择“企业路由器”。	虚拟私有云
企业路由器	仅关联场景为“企业路由器”时需要选择。	er-001
虚拟私有云	选择待和用户数据中心通信子网所在的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	仅关联场景为“虚拟私有云”时需要配置。 – 输入网段 输入需要和用户数据中心通信的子网，该子网可以在关联虚拟私有云内，也可以不在关联虚拟私有云内。 – 选择子网 选择关联虚拟私有云内的子网信息，用于和用户数据中心通信。	192.168.0.0/24，192.168.1.0/24
HA模式	选择“双活”。	双活
高级配置	仅关联场景为“虚拟私有云”且网络类型为“私网”时需要配置。	-
接入虚拟私有云	– 与网关关联的虚拟私有云一致 使用已关联虚拟私有云作为接入虚拟私有云。 – 选择其他虚拟私有云 选择其他虚拟私有云作为接入虚拟私有云。	与网关关联的虚拟私有云一致
接入子网	– 接入虚拟私有云选择“与网关关联的虚拟私有云一致” ■ 与互联子网一致 VPN网关私网IP地址从互联子网分配。由于接入子网和互联子网各需要分配2个IP地址，请确保选择的接入子网存在4个及以上可分配的IP地址。 ■ 选择其他子网 请确保选择的接入子网存在2个及以上可用IP地址。 – 接入虚拟私有云选择其他虚拟私有云 请确保选择的接入子网存在2个及以上可分配的IP地址。	与互联子网一致

参数	说明	取值参数
网关接入IP	选择“手动指定IP地址”，并指定网关IP。	– 私网IP地址1：192.168.2.100 – 私网IP地址2：192.168.2.101

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。
   对端网关参数说明如**表1-34**所示。

表 1-34 对端网关参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw
标识	对端网关和华为云VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	172.16.0.111

步骤5 配置VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置VPN连接参数，单击“立即购买”。
   VPN连接参数说明如**表1-35**所示。

表 1-35 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关。	vpngw-001
连接1网关IP	选择VPN网关已绑定的私网IP。	192.168.2.100
连接1对端网关	选择连接1对端网关。	172.16.0.111
连接2网关IP	选择VPN网关已绑定的另一个私网IP地址。	192.168.2.101
连接2对端网关	选择连接2对端网关。	172.16.0.111
连接模式	选择“静态路由模式”。	静态路由模式

参数	说明	取值参数
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1/30
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2/30
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.71.2/30

步骤6 配置对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。详细配置方法，请参见**管理员指南**。

----结束

1.7.5 结果验证

- 大约5分钟后，查看VPN连接状态。
  选择“虚拟专用网络 > 企业版-VPN连接”，两条VPN连接状态显示为正常。
- 用户数据中心内服务器和华为云VPC子网内服务器可以相互Ping通。

1.8 通过 VPN 负载分担实现云上云下大带宽流量互通

1.8.1 方案概述

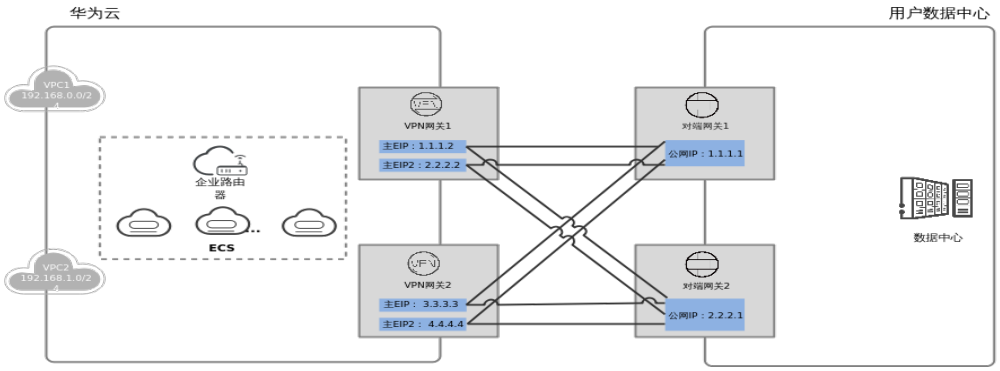
应用场景

当ER的网关和对端网关建立多条BGP连接时，需要多个网关通过ER做负载分担，来实现大带宽的使用场景。

组网方案

VPN服务提供的组网方案如**图 组网方案**所示。

图 1-9 组网方案



方案优势

支持多个VPN网关与对端多个网关组成full-mesh组网，达到负载分担，提供大带宽能力。

约束与限制

- 每个ER网关最多可关联10个VPN网关。
- 最大规格为专业型2的单个VPN网关转发能力为2G，10个VPN网关的最大转发能力为20G。

1.8.2 组网和资源规划

数据规划

表 1-36 规划数据

类别	规划项	规划值
VPC	待互通子网	• VPC1：192.168.0.0/24 • VPC2：192.168.1.0/24
	ER	关联VPC1和VPC2的企业路由器。
	ECS	3个ECS分别位于不同的VPC内，VPC中的ECS如果位于不同的安全组，需要在安全组中添加规则放通对端安全组的网络。
VPN网关1	接入子网	用于VPN网关和VPC通信，请确保选择的接入子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关1默认使用2个EIP。本示例假设EIP地址生成如下： • 主EIP：1.1.1.2 • 主EIP2：2.2.2.2
	“连接1配置”中的Tunnel接口地址	用于VPN网关1和对端网关1建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.70.1/30 • 对端隧道接口地址：169.254.70.2/30 用于VPN网关1和对端网关2建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.71.1/30 • 对端隧道接口地址：169.254.71.2/30
	“连接2配置”中的Tunnel接口地址	用于VPN网关1和对端网关1建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.72.1/30 • 对端隧道接口地址：169.254.72.2/30 用于VPN网关1和对端网关2建立IPsec隧道，配置时两边需要互为镜像。 • 本端隧道接口地址：169.254.73.1/30 • 对端隧道接口地址：169.254.73.2/30
VPN网关2	接入子网	用于VPN网关和VPC通信，请确保选择的接入子网存在4个及以上可分配的IP地址。 192.168.3.0/24

类别	规划项	规划值
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关2默认使用2个EIP。本示例假设EIP地址生成如下： ● 主EIP：3.3.3.3 ● 主EIP2：4.4.4.4
	“连接1配置”中的Tunnel接口地址	用于VPN网关2和对端网关1建立IPsec隧道，配置时两边需要互为镜像。 ● 本端隧道接口地址：169.254.74.1/30 ● 对端隧道接口地址：169.254.74.2/30 用于VPN网关2和对端网关2建立IPsec隧道，配置时两边需要互为镜像。 ● 本端隧道接口地址：169.254.75.1/30 ● 对端隧道接口地址：169.254.75.2/30
	“连接2配置”中的Tunnel接口地址	用于VPN网关2和对端网关1建立IPsec隧道，配置时两边需要互为镜像。 ● 本端隧道接口地址：169.254.76.1/30 ● 对端隧道接口地址：169.254.76.2/30 用于VPN网关2和对端网关2建立IPsec隧道，配置时两边需要互为镜像。 ● 本端隧道接口地址：169.254.77.1/30 ● 对端隧道接口地址：169.254.77.2/30
用户数据中心	待互通子网	172.16.0.0/16
对端网关1	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 1.1.1.1
对端网关2	公网IP地址	公网IP地址由运营商统一分配。本示例假设公网IP地址如下： 2.2.2.1
IKE/IPsec策略	预共享密钥	Test@123
	IKE策略	● 版本：v2 ● 认证算法：SHA2-256 ● 加密算法：AES-128 ● DH算法：Group 15 ● 生命周期（秒）：86400 ● 本端标识：IP Address ● 对端标识：IP Address

类别	规划项	规划值
	IPsec策略	• 认证算法：SHA2-256 • 加密算法：AES-128 • PFS：DH Group15 • 传输协议：ESP • 生命周期（秒）：3600

1.8.3 操作步骤

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
  - 请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。
- 数据中心侧
  - 用户数据中心的VPN设备已经完成IPsec连接相关配置。相关操作步骤请参见**管理员指南**。

操作步骤

本示例以BGP路由模式进行配置讲解，需要在云侧和数据中心之间共创建4条VPN连接。

步骤1 登录管理控制台。

步骤2 选择“网络 > 虚拟专用网络VPN”。

步骤3 配置VPN网关。

1. 选择“虚拟专用网络 > 企业版-VPN网关”，单击“创建站点入云VPN网关”。
2. 根据界面提示配置参数。

   VPN网关1参数说明如**表 VPN网关1参数说明**所示。

表 1-37 VPN 网关 1 参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-001
网络类型	选择“公网”。	公网
关联模式	选择“企业路由器”。	企业路由器

参数	说明	取值参数
企业路由器	选择待接入企业路由器。	er-001
接入虚拟私有云	仅选择“企业路由器”时需要配置。	vpc-001(192.168.0.0/24)
接入子网	用于VPN网关1和VPC通信，请确保选择的接入子网存在4个及以上可分配的IP地址。	192.168.2.0/24
BGP ASN	BGP自治系统编号。	64512
HA模式	选择“双活”。	双活
主EIP	VPN网关和用户数据中心通信的公网IP1。	1.1.1.2
主EIP2	VPN网关和用户数据中心通信的公网IP2。	2.2.2.2

3. 参见上述步骤，配置VPN网关2的参数（192.168.3.0/24）。

   说明

   此处仅名称、接入子网、主EIP和主EIP2的配置参数与VPN网关1不同，未提及参数建议和VPN网关1的配置保持一致。

表 1-38 VPN 网关 2 参数说明

参数	说明	取值参数
名称	VPN网关的名称。	vpngw-002
接入子网	用于VPN网关2和VPC通信，请确保选择的接入子网存在4个及以上可分配的IP地址。	192.168.3.0/24
主EIP	VPN网关和用户数据中心通信的公网IP1。	3.3.3.3
主EIP2	VPN网关和用户数据中心通信的公网IP2。	4.4.4.4

步骤4 配置对端网关。

1. 选择“虚拟专用网络 > 企业版-对端网关”，单击“创建对端网关”。
2. 根据界面提示配置参数。

   对端网关参数1说明如**对端网关1参数说明**所示。

表 1-39 对端网关 1 参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw1

参数	说明	取值参数
标识	对端网关1和华为云VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	1.1.1.1
BGP ASN	BGP自治系统编号。	65000

3. 参见上述步骤，配置对端网关2的参数（2.2.2.1）。

   说明

   此处仅名称和网关IP的配置参数与对端网关1不同，未提及参数建议和对端网关1的配置保持一致。

表 1-40 对端网关 2 参数说明

参数	说明	取值参数
名称	对端网关的名称。	cgw-fw2
标识	对端网关2和华为云VPN网关通信的IP地址。 请确认数据中心的对端网关已经放通UDP端口4500。	2.2.2.1

步骤5 配置云侧VPN网关1和数据中心的VPN连接。

1. 选择“虚拟专用网络 > 企业版-VPN连接”，单击“创建VPN连接”。
2. 配置第一组VPN连接参数，单击“立即购买”。

   VPN连接参数说明如表1-41所示。

表 1-41 第一组 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-001
VPN网关	选择VPN网关1。	vpngw-001
连接1网关IP	选择VPN网关1的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	1.1.1.1
连接2网关IP	选择VPN网关1的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	1.1.1.1
连接模式	选择“BGP路由模式”。	BGP路由模式

参数	说明	取值参数
对端子网	用户数据中心中需要和华为云VPC通信的子网。 – 对端子网与本端子网可以重叠，不能重合；对端子网不能被本网关关联的VPC内已有子网所包含。 – 部分网段是VPC预留网段，不能作为对端子网，例如：100.64.0.0/10、100.64.0.0/12，214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。	172.16.0.0/16
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
接口地址分配方式	– 手动分配 本示例以“手动分配”为例。 – 自动分配	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	169.254.70.1/30
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	169.254.70.2/30
检测机制	用于多链路场景下路由可靠性检测，通过ICMP报文检测实现；使能NQA，您的对端设备需要允许ICMP响应请求。	勾选“使能NQA”
预共享密钥、确认密钥	和对端网关的预共享密钥需要保持一致。	Test@123
策略配置	和对端网关的策略配置需要保持一致。	保持默认
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.72.1/30

参数	说明	取值参数
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.72.2/30

3. 配置第二组VPN连接参数。

说明

此处仅名称、对端网关、本端隧道接口地址和对端隧道接口地址的配置参数与第一组VPN连接不同，未提及参数建议和第一组VPN连接配置保持一致。

表 1-42 第二组 VPN 连接参数说明

参数	说明	取值参数
名称	VPN连接的名称。	vpn-002
连接1网关IP	选择VPN网关1的主EIP。	1.1.1.2
连接1对端网关	选择连接1对端网关。	2.2.2.1
连接2网关IP	选择VPN网关1的主EIP2。	2.2.2.2
连接2对端网关	选择连接2对端网关。	2.2.2.1
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥和策略配置。	*请根据实际设置*
本端隧道接口地址	VPN网关的Tunnel隧道接口IP地址。	169.254.71.1/30
对端隧道接口地址	对端网关的Tunnel隧道接口IP地址。	169.254.71.2/30
连接2配置	选择是否“与连接1保持一致”。 **说明** 当选择关闭时，连接2配置仅本端隧道接口地址和对端隧道接口地址与连接1配置不同，其他参数建议和连接1配置保持一致。	关闭
本端隧道接口地址	VPN网关的Tunnel隧道IP地址。	169.254.73.1/30
对端隧道接口地址	对端网关的Tunnel隧道IP地址。	169.254.73.2/30

步骤6 配置云侧VPN网关2和数据中心的VPN连接。

配置步骤与VPN网关1的步骤相同。

步骤7 配置数据中心的对端网关信息。

根据对端网关类型不同，配置操作可能存在差异。详细配置方法，请参见**管理员指南**。

----结束

1.8.4 结果验证

- 大约5分钟后，查看VPN连接状态。
  选择“虚拟专用网络 > 企业版-VPN连接”，8条VPN连接状态显示为正常。
- 用户数据中心内的服务器和华为云VPC子网内服务器可以相互Ping通。
- 通过对端网关的监控来查看入网流量，可以负载分担到各个网关上。

2 站点入云 VPN 经典版

2.1 通过 VPN 连接云下数据中心与云上 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子网的连通性，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

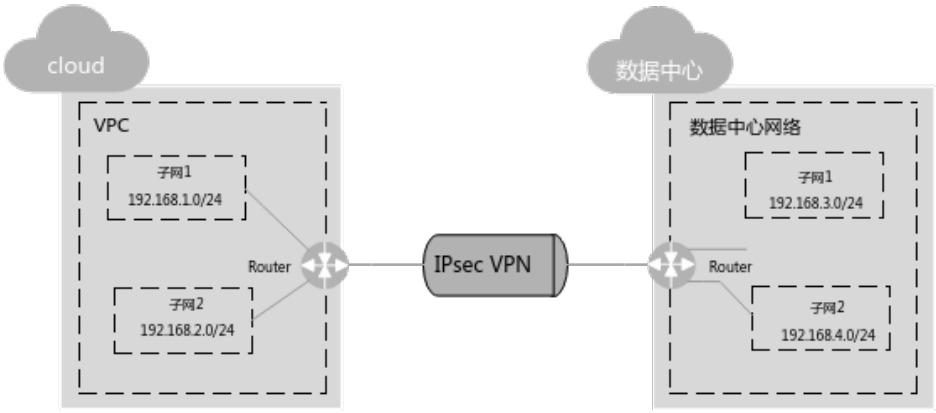
已创建VPN所需的虚拟私有云和子网。

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2-1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 2-1 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. 为弹性云服务器配置安全组规则，允许通过VPN进出用户数据中心的报文。
4. 检查VPC安全组。

   从用户数据中心ping云服务器，验证安全组是否允许通过VPN进出用户数据中心的报文。
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。

2.2 通过 VPN 和云连接构建跨境网络连接

2.2.1 方案概述

应用场景

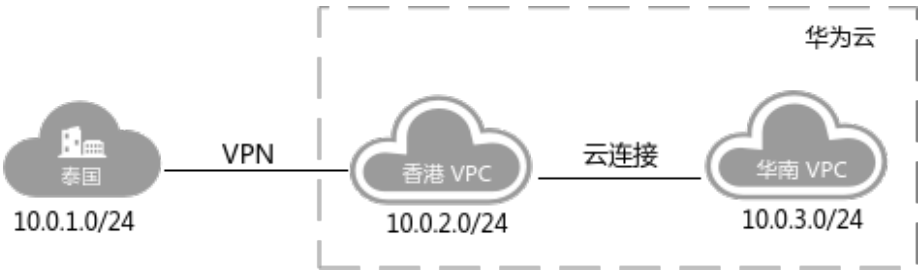
某大型跨国公司数据中心部署在泰国，云上业务部署在华为云华南区，存在云上云下业务访问诉求。该场景下如果直接将泰国数据中心通过虚拟专用网络VPN连接到华南区的私有虚拟云VPC，则会出现网络不稳定的问题。

本方案采用云连接CC配合虚拟专用网络，实现跨境网络稳定连通。

方案架构

将用户的数据中心就近连接到华为云区域，例如泰国区域的用户可以使用VPN，将数据中心连接到香港区域。再通过云连接连通各个区域，例如将香港区域与华南区域的VPC连接起来，如图2-2所示。

图 2-2 方案架构



方案优势

- 可靠连接，网络稳定。
- 按需计费，多种付费模式。

2.2.2 资源和成本规划

该解决方案主要部署如下资源，每月花费如**表2-1**所示，具体请参见华为云官网**价格详情**，实际收费以账单为准：

表 2-1 资源和成本规划

产品	配置示例	成本预估/月
虚拟专用网络	按需计费：VPN网关带宽费用2.8美元/小时+VPN连接费用0.05美元/小时，更多计费详情请参见**价格详情**。 ● 区域：中国-香港 ● 计费模式：按需计费 ● 计费方式：按带宽计费 ● 带宽大小：100 Mbit/s	2052.46美元
云连接	按月计费：11996.85美元/月，更多计费详情请参见**价格详情**。 ● 计费模式：包年/包月 ● 计费方式：按带宽计费 ● 互通类型：跨大区互通 ● 互通大区：中国大陆 - 亚太 ● 带宽：100 Mbit/s	11996.85美元
合计	—	14049.31美元

2.2.3 实施步骤（手动）

2.2.3.1 配置 VPN

步骤1 在华为云香港区域购买VPN，配置云上VPN服务。

1. 在管理控制台左上角单击 图标，选择“中国-香港”区域。
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 > 经典版”。
4. 在VPN网关页面，单击“创建VPN网关”
5. 根据界面提示，如表2-2所示填写对应参数后，单击“立即购买”。

表 2-2 VPN 网关参数说明

参数	说明	取值样例
计费模式	当前区域的VPN网关支持按需计费。	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。 本案例中请选择“中国-香港”。	中国-香港
名称	VPN网关的名称。	vpcgw-001
虚拟私有云	VPN接入的VPC名称。 选择香港区域对应的VPC。	vpc-001
类型	VPN类型。默认为选择“IPsec”。	IPsec
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。 – 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。 可以在云监控服务中配置告警规则对带宽进行监控。	100

表 2-3 VPN 连接参数说明

参数	说明	取值样例
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。 这里选择网段，来指定本端子网，此处需要将香港和华南两个子网都填写进去，以保证华南发出的流量也能进入VPN隧道。 这里填写10.0.2.0/24，10.0.3.0/24。	10.0.2.0/24， 10.0.3.0/24
远端网关	用户数据中心侧的VPN网关地址。 这里填写泰国区域数据中心的VPN网关地址。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。 这里填写10.0.1.0/24。	10.0.1.0/24
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： – 取值长度：6~128位。 – 只能包括以下几种字符： ■ 数字 ■ 大小写字母 ■ 特殊符号：包括“~”、“`”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“[”、“]”、“{”、“}”、“|”、"\"、";"、":"、"/"、“:”和“;”	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	– 默认配置。 – 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见表2-4和表2-5。	自定义配置

表 2-4 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：SHA2-256。	SHA2-256
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 1、Group 2、Group 5、Group 14、Group 15、Group 16、Group 19、Group 20、Group 21。 默认配置为：Group 14。 协商双方的dh算法必须一致，否则会导致协商失败。	Group 14
版本	IKE密钥交换协议版本，支持的版本：v1（有安全风险不推荐）、v2。 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Association）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 2-5 IPsec 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：SHA2-256。	SHA2-256
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

参数	说明	取值样例
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 1、DH group 2、DH group 5、DH group 14、DH group 15、DH group 16、DH group 19、DH group 20、DH group 21。 默认配置为：DH group 14。	DH group 14
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 Association）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

注意

以下算法安全性较低，请慎用：

- **认证算法：**SHA1、MD5。
- **加密算法：**3DES。
- **DH算法：**Group 1、Group 2、Group 5。

步骤2 配置用户侧数据中心的VPN网关（即泰国的用户VPN网关）。

根据用户使用的VPN网关设备型号，进行相应的配置。

说明

在IPsec策略中引用的ACL，应配置如下：

- 源网段：10.0.1.0/24。
- 目的网段：10.0.2.0/24，10.0.3.0/24。

----结束

2.2.3.2 配置 CC

步骤1 在云连接服务中购买云连接实例。

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 云连接 CC”。
3. 进入云连接服务信息页面，单击“创建云连接”，开始创建云连接实例。
4. 在创建云连接服务页面中，根据表2-6填写对应参数。

表 2-6 创建云连接参数

参数	说明
名称	云连接的名称。 长度为1~64个字符，中、英文字母，数字，下划线，中划线，点。
标签	云连接服务的标识，包括键和值。可以为云连接服务创建10个标签。
描述	云连接的描述。 长度为0~255个字符。

表 2-7 云连接服务标签命名规则

参数	规则
键	- 不能为空。 - 对于同一资源键值唯一。 - 长度不超过36个字符。 - 取值只能包含大写字母、小写字母、数字、中划线、下划线以及从\u4e00到\u9fff的Unicode字符。
值	- 可以为空。 - 长度不超过43个字符。 - 取值只能包含大写字母、小写字母、数字、点、中划线、下划线以及从\u4e00到\u9fff的Unicode字符。

5. 单击“确定”，完成云连接实例的创建。

步骤2 加载网络实例。

将香港区域的VPC和华南区域的VPC加入到云连接中。

说明

- 加载香港VPC时，配置的参数请参见**表 加载同账号网络实例参数**。
- 加入华南VPC时，只需要指定VPC子网10.0.3.0/24即可，不需要重复指定泰国的网段10.0.1.0/24 。

表 2-8 加载同账号网络实例参数

参数	说明	取值样例
账号	加载的网络实例的账号类型。	同账号加载
区域	需要连接的VPC所在区域。	中国-香港

参数	说明	取值样例
实例类型	需要加载到云连接实例中实现网络互通的实例类型。	虚拟私有云（VPC）
VPC	需要加载到云连接实例中实现网络互通的VPC名称。 这里选择在步骤**步骤1.5**时选择的VPC。	vpc-001
VPC CIDRs	需要加载到云连接实例中实现网络互通的网段路由。 当类型参数选择虚拟私有云时，需配置以下两个参数： • 子网：选择VPC管理的子网，这里选10.0.2.0/24。 • 其他网段：为了使云连接能够转发到达泰国数据中心的流量，此处需要增加自定义网段10.0.1.0/24。	子网：10.0.2.0/24 其他网段：10.0.1.0/24

步骤3 配置域间带宽。

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 云连接 CC”。
3. 进入云连接服务信息页面，在云连接列表中，单击已创建的云连接实例名称，进入云连接实例详情页面。
4. 在云连接实例详情页面中，单击“域间带宽”页签。
5. 在域间带宽页签中，单击“配置域间带宽”，按照**表2-9**填写对应参数。

表 2-9 配置域间带宽参数

参数	说明
互通区域	需要实现互通的区域名称。 请选择两个需要互通的区域。
带宽包	云连接绑定的带宽包。
带宽	两个区域实现互通的带宽。 所有基于该带宽包配置的域间带宽总和不超过带宽包的带宽，请预先做好规划。

6. 单击“确定”，完成配置。

   配置完域间带宽后，配置了带宽的区域间就可以进行正常通信。

   说明

   系统默认安全组规则是入方向访问受限，请确认区域内互访资源的安全组出方向、入方向规则配置正确，保证跨区域通信正常。

步骤4 检查路由信息。

在香港VPC实例中，应该包括目的网段为10.0.1.0/24和10.0.2.0/24两条路由信息。

在华南VPC实例中，应该包括10.0.3.0/24一条路由信息。

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 云连接”。
3. 在云连接列表中，单击需要查看的云连接名称，在云连接页面中单击“路由信息”页签。
4. 在下拉框中选择需要查询的路由所在区域。
5. 在路由信息列表中查看路由信息。

----结束

2.2.3.3 验证操作是否成功

步骤1 在华南区域创建虚拟机部署用户业务。

步骤2 从华南区域虚拟机ping包到泰国数据中心机器。

正常情况下，ping包会通，同时在用户侧数据中心VPN网关上可以查看到IPsec VPN隧道信息（不同型号的网关查看方式略有不同）。

----结束

2.3 VPN 与云连接配合使用实现云下数据中心与云上多 VPC 互通

操作场景

本任务中用户通过VPN接入华为云，在华为云端有多个区域，每个区域中都创建了VPC。通过配置云连接实现用户数据中心网络和云端多个区域的VPC子网互联互通。

说明

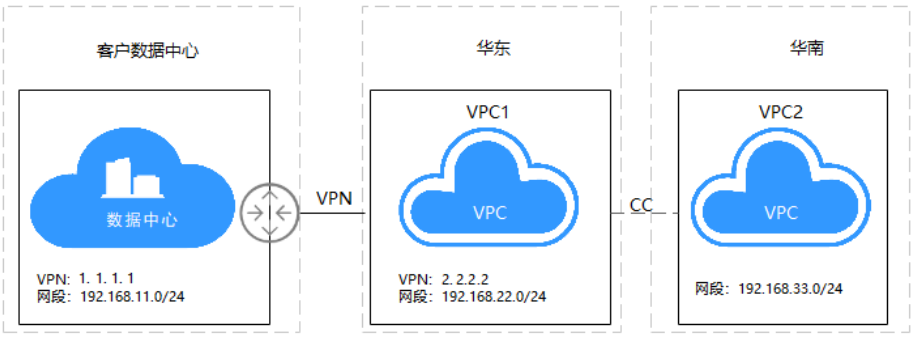
相同区域的多个VPC也可通过云连接互联。

前提条件

1. 前置资源。
   - 用户已购买了VPN连接，完成了用户端数据中心网络和云端VPC的VPN连接。
   - 用户购买了多个Region的VPC，且每个VPC下的子网不冲突，云端多个VPC下的ECS服务正常。

2. 连接拓扑。

图 2-3 VPN 与云连接配合使用



说明

- 用户数据中心本地子网：192.168.11.0/24，VPN网关IP：49.4.113.226
- VPC1子网：192.168.22.0/24，VPN网关122.112.222.135
- VPC2子网：192.168.33.0/24

3. 配置概述。

表 2-10 配置说明

用户数据中心	VPC1（华东节点）	VPC2（华南节点）
VPN连接子网配置 本端网关：49.4.113.226 本地子网：192.168.11.0/24 远端子网：192.168.22.0/24 192.168.33.0/24 远端网关：122.112.222.135 网关IP与VPC1互为镜像 VPN资源与VPC1相同	**VPN连接子网配置** 本端网关： 122.112.222.135 本端子网： 192.168.22.0/24 192.168.33.0/24 远端网关：49.4.113.226 远端子网： 192.168.11.0/24 **云连接网络实例配置** 网络实例： 192.168.22.0/24 192.168.11.0/24	**云连接网络实例配置** 网络实例： 192.168.33.0/24

说明

云连接网络实例可在任一Region配置，通过查看路由信息验证网络实例配置。

4. 配置思路。
   - 通过CC将华东VPC1和华南VPC2进行连接。

- 用户数据中心VPN连接的本地子网不变，远端子网变为192.168.22.0/24和192.168.33.0/24。
- VPC1的VPN连接的本地子网变更为192.168.22.0/24和192.168.33.0/24，远端子网不变。
- VPC1的CC更新VPC CIDRs的网段信息，将192.168.11.0/24添加至VPC子网中。
- VPC2的网络信息无变化。
- 配置域间带宽。
- 验证云连接路由信息。

配置步骤

步骤1 创建云连接。

1. 登录控制台，在服务列表中选择“云连接”，在页面左侧页签中选择“云连接”，单击页面右上方“创建云连接”。
2. 根据界面提示配置相关参数，单击“确定”。

图 2-4 创建云连接

云连接的创建可在VPC的所在的任意一个区域发起，创建阶段填写云连接的名称、企业项目和描述等信息。如果客户在同一个Region中有两个VPC，可选择对等连接（时延相对小）或云连接互联VPC，如果VPC数量多于两个，请选择云连接进行互联。

3. 云连接创建完成后，单击云连接名称。
4. 选择“网络实例”页签，单击“加载网络实例”。

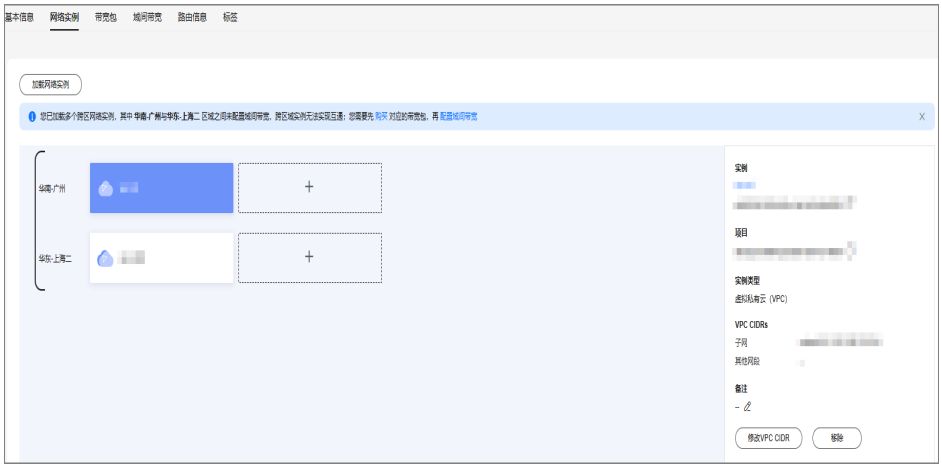
   根据界面提示配置相关参数，单击“确定”。

图 2-5 加载网络实例 1

5. 添加华南区域的VPC2，选择VPC名称和VPC CIDRs，VPC CIDRs可选择全部子网或部分子网，也可通过自定义网段进行添加VPC的子网。

   同理，添加华东区域的VPC1及网络配置，添加完成信息配置如图2-6所示。

图 2-6 加载网络实例 2



说明

- 云连接提供同账号或跨账号的连接，跨账号连接需要先获取授权。
- 自定义添加的子网系统不会做校验。

6. 选择“域间带宽”页签，单击“配置域间带宽”，如果存在多个Region，需要按照链路使用情况将云连接建立时的总带宽进行划分，本实例将所有带宽用于两个Region互联，配置信息如图。

图 2-7 配置域间带宽

7. 验证路由信息，选择“路由信息”。

   系统可展示区域互联的路由信息，路由中存在的子网即为通过云连接互通的子网，此时VPC1和VPC2的子网可以互相访问。

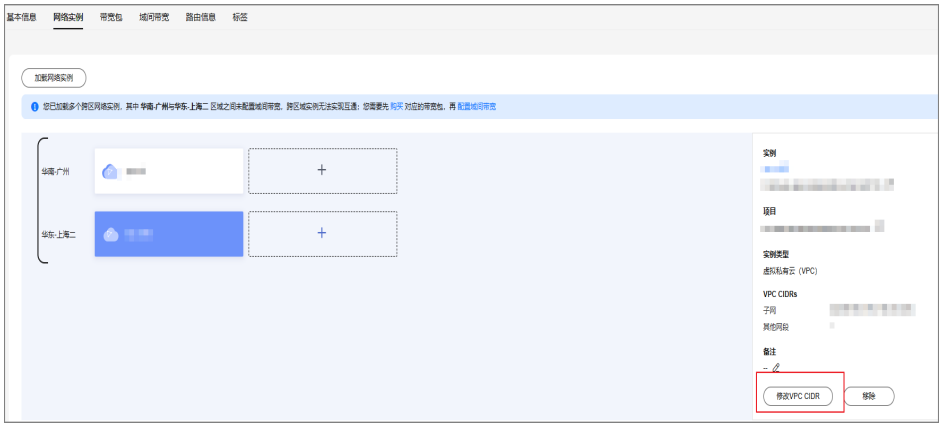
图 2-8 验证路由信息

步骤2 更新VPC CIDRs。

VPC1与VPC2之间建立的云连接，在配置网络实例时，VPC1除自身的子网外，连接VPN的子网也被视同为连接在VPC1下，VPC2的子网只包含自身子网。因此，需要对VPC1的网络实例进行修改。

1. 单击云连接名称进入云连接实例。
2. 在“网络实例”页签中，选择华东-上海二的实例。
3. 单击页面右侧“修改VPC CIDRs”。

图 2-9 修改 VPC CIDRs



4. 根据界面提示，在“高级配置”的“其他网段”中输入VPC1通过VPN连接的客户侧子网，单击“添加”。

图 2-10 修改 VPC CIDRs

5. 验证配置更新信息，请单击页面“路由信息”进行查验。

图 2-11 验证信息

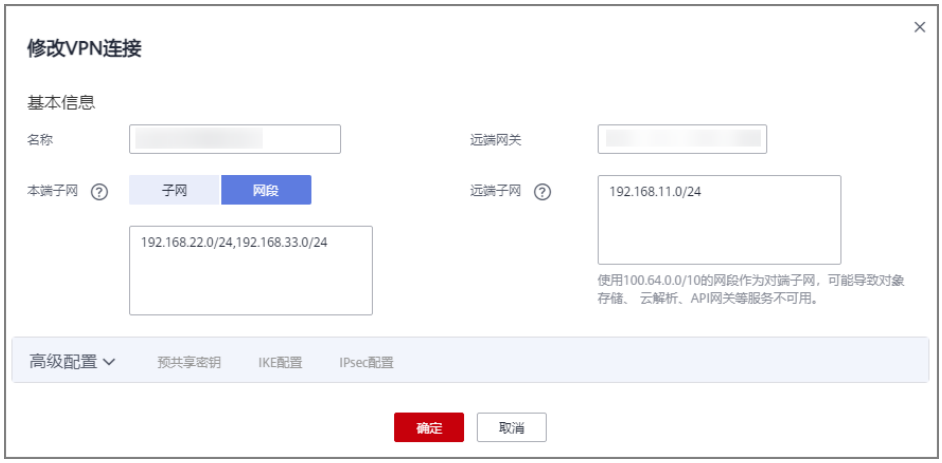
步骤3 更新VPN配置。

VPC1和VPC2通过CC连接后，用户数据中心网络和VPC1之间的VPN子网也随即发生了变化，从VPN连接的角度看，VPC1的本地子网应该包含自身的子网和通过CC连接的VPC2的子网，同理，客户端VPN的远端子网也需要做相应的调整。

- 客户侧：本端子网不变，远端子网添加VPC2的子网，本实例为192.168.33.0/24。
- VPC1侧：本端子网添加VPC2的子网，本实例为192.168.33.0/24，远端子网不变。

1. 选择“虚拟专用网络 > 经典版 ”，在“VPN连接”界面找到VPC1创建的VPN连接，在“更多”列单击“修改”。
2. 在修改VPN连接页面将本端子网变更为“网段”，并输入VPC1的子网和VPC2的子网，两个网段之间使用英文逗号隔开，远端子网和其它信息保持不变。

图 2-12 修改 VPN 连接



3. 用户侧的VPN配置需要修改远端子网。

   请将华为云端的VPC1子网、VPC2子网添加至VPN连接的远端子网配置中，其它配置保持不变。

----结束

配置验证

本环境中在用户数据中心、VPC1、VPC2中分别存三台ECS，IP地址分别为192.168.11.11、192.168.22.170和192.168.33.33的三台主机，初始情况下ECS1（192.168.11.11）可以和ECS2（192.168.22.170）互联互通（通过VPN访问），ECS3（192.168.33.33）无法和其它主机互通，在建立云连接CC后，ECS3可以和ECS2互通，但无法和ECS1互通。

经过更新VPC CIDRs和更新VPN配置的配置调整后，已实现ECS1、ECS2和ECS3之间互联互通，结果验证如下。

- 用户数据中心。

  ECS1访问VPN连接VPC1子网下的ECS2：结果OK。

```
[root@ecs--11 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.11  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::f816:3eff:fefc:eef5  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:fc:ee:f5  txqueuelen 1000  (Ethernet)
        RX packets 5325  bytes 503031 (491.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12328  bytes 1165686 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs--11 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=30.8 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=30.0 ms
64 bytes from 192.168.22.170: icmp_seq=3 ttl=61 time=29.3 ms
```

  ECS1访问VPC2子网下的ECS3：结果OK。

```
[root@ecs--11 ~]# ping 192.168.33.33
PING 192.168.33.33 (192.168.33.33) 56(84) bytes of data.
64 bytes from 192.168.33.33: icmp_seq=1 ttl=59 time=64.2 ms
64 bytes from 192.168.33.33: icmp_seq=2 ttl=59 time=63.5 ms
64 bytes from 192.168.33.33: icmp_seq=3 ttl=59 time=63.2 ms
64 bytes from 192.168.33.33: icmp_seq=4 ttl=59 time=63.2 ms
```

- 华为云云端VPC1。

  VPC1子网下的ECS2访问用户数据中心子网下的ECS1：结果OK。

```
[root@ecs-vpc2-22 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.22.170  netmask 255.255.255.0  broadcast 192.168.22.255
        inet6 fe80::f816:3eff:fe4d:4bbd  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:4d:4b:bd  txqueuelen 1000  (Ethernet)
        RX packets 1693564  bytes 600255226 (572.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1903616  bytes 3023942348 (2.8 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc2-22 ~]# ping 192.168.11.11
PING 192.168.11.11 (192.168.11.11) 56(84) bytes of data.
64 bytes from 192.168.11.11: icmp_seq=1 ttl=62 time=31.4 ms
64 bytes from 192.168.11.11: icmp_seq=2 ttl=62 time=29.4 ms
```

  VPC1子网下的ECS2访问VPC2子网下的ECS3：结果OK。

```
[root@ecs-vpc2-22 ~]# ping 192.168.33.33
PING 192.168.33.33 (192.168.33.33) 56(84) bytes of data.
64 bytes from 192.168.33.33: icmp_seq=1 ttl=61 time=42.2 ms
64 bytes from 192.168.33.33: icmp_seq=2 ttl=61 time=36.7 ms
64 bytes from 192.168.33.33: icmp_seq=3 ttl=61 time=37.4 ms
```

- 华为云云端VPC2。

  VPC2子网下的ECS3访问VPC1子网下的ECS2：结果OK。

```
[root@ecs-vpc2-33 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.33.33  netmask 255.255.255.0  broadcast 192.168.33.255
        inet6 fe80::f816:3eff:fe23:c69e  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:23:c6:9e  txqueuelen 1000  (Ethernet)
        RX packets 10127  bytes 1005602 (982.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13258  bytes 1258814 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc2-33 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=37.7 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=36.7 ms
64 bytes from 192.168.22.170: icmp_seq=3 ttl=61 time=36.5 ms
```

  VPC2子网下的ECS3访问用户数据中心子网下的ECS1：结果OK。

```
[root@ecs-vpc2-33 ~]# ping 192.168.11.11
PING 192.168.11.11 (192.168.11.11) 56(84) bytes of data.
64 bytes from 192.168.11.11: icmp_seq=1 ttl=60 time=64.9 ms
64 bytes from 192.168.11.11: icmp_seq=2 ttl=60 time=63.7 ms
64 bytes from 192.168.11.11: icmp_seq=3 ttl=60 time=64.0 ms
```

2.4 VPN 与 VPC peering 配合使用实现云下数据中心与云上同区域 VPC 互通

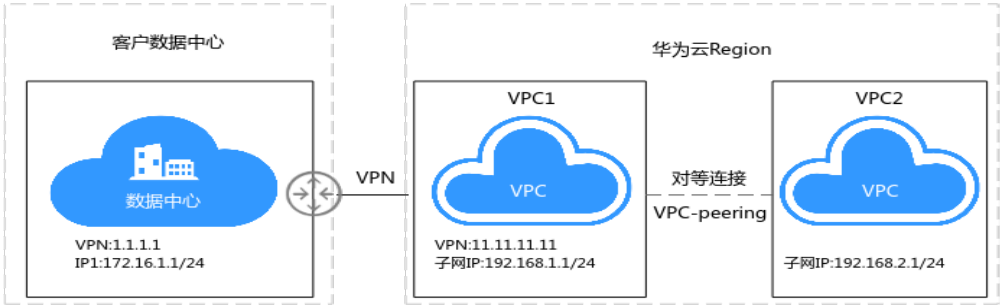
操作场景

用户在华为云的同区域中创建了两个VPC，用户数据中心通过VPN连接至其中一个VPC。本任务指导书通过在两个VPC之间建立VPC-peering使得用户数据中心的网络和华为云端两个VPC之间的网络数据互联互通。

前提条件

1. 前置资源。
   - 用户已购买了VPN连接，完成了用户端数据中心网络和云端VPC的VPN连接；
   - 用户购买了多个VPC，且每个VPC下的子网不冲突，云端多个VPC下的ECS服务正常；
2. 连接拓扑。

图 2-13 VPN 与 VPC peering 配合使用



说明

- 用户数据中心本地子网：172.16.1.0/24，VPN网关IP：1.1.1.1
- VPC1子网：192.168.1.0/24，VPN网关IP：11.11.11.11
- VPC2子网：192.168.2.0/24

3. 配置概述。

表 2-11 局点配置说明

配置说明	用户数据中心	VPC1	VPC2
VPN连接子网配置	本端网关：1.1.1.1 本地子网：172.16.1.0/24 远端子网：192.168.1.0/24 192.168.2.0/24 远端网关：11.11.11.11 **说明** • 网关IP与VPC1互为镜像。 • VPN资源与VPC1相同。	本端网关：11.11.11.11 本端子网：192.168.1.0/24； 192.168.2.0/24 远端网关：1.1.1.1 远端子网：172.16.1.0/24	-
VPC对等连接路由配置	-	VPC1目的地址：192.168.2.0/24	VPC2目的地址： 172.16.1.0/24； 192.168.1.0/24

配置说明	用户数据中心	VPC1	VPC2
备注	• 本示例在创建VPC-peering时指定VPC1为本端，VPC2为远端。 • 云连接网络实例可在任一局点配置，通过查看路由信息验证网络实例配置。		

4. 配置思路。
   - 通过VPC-peering将VPC1和VPC2进行连接。
   - 用户数据中心VPN连接的本地子网不变，远端子网变为192.168.1.0/24和192.168.2.0/24。
   - VPC1的VPN连接的本地子网变更为192.168.1.0/24和192.168.2.0/24，远端子网不变。
   - VPC1的VPC-peering本端路由仅包含目标网段为VPC2子网192.168.2.0/24的路由。
   - VPC2的VPC-peering远端路由包含目标网段为VPC1子网192.168.1.0/24和客户子网172.16.1.0/24。

配置步骤

步骤1 创建VPC-peering。

1. 登录管理控制台，选择VPC所在的区域，然后在服务列表中选择“虚拟私有云 VPC”，在页面左侧页签中选择“对等连接”，单击页面右上方“创建对等连接”，在弹出页面中选择本端的VPC和对端VPC信息，单击“确定”进行创建。

   本端VPC和对端VPC是在创建VPC对等连接时选择的，请按照VPC子网网段确认是否匹配，VPC-peering创建后无法变更VPC信息，只能修改VPC-peering的名称和VPC的路由。
2. VPC-peering创建完成后可查询对等连接的相关信息，同时VPC的对等连接会提示本端连接的VPC网络和对端连接的VPC网络，两端网络互通需要添加路由信息。

   本示例中选择VPN连接侧的VPC1为本端，VPC2为远端。

步骤2 添加VPC-peering路由。

1. 普通的VPC-peering连接只需要添加两侧VPC的子网网络路由，本示例中本端VPC分别通过VPN连接了用户数据中心网络，因此在添加网络路由时需要将客户的网络也进行添加。在对等连接页面单击要编辑的VPC对等连接的名称，进入添加路由页面。
2. 在关联路由页面，单击“添加路由”。

   在弹出页面填写目的地址网络信息，多条路由可逐条添加。

   说明

   VPC1通过VPN连接的用户数据中心网络，对于VPC2来讲，是通过VPC-peering连接的，所以对端路由除去往本端子网的路由外，还需要包含去往用户数据中心子网的路由。

   添加路由的下一跳地址由VPN对端连接自动生成，配置页面无需修改。

步骤3 修改VPN配置。

1. VPC1和VPC2通过VPC-peering连接后，用户数据中心网络和VPC1之间的VPN子网也随即发生了变化，从VPN连接的角度看，VPC1的本地子网应该包含自身的子网和通过VPC-peering连接的VPC2的子网，同理，客户端VPN的远端子网也需要做相应的调整。

说明

客户侧：本端子网不变，远端子网添加VPC2的子网，本示例为192.168.2.0/24。

VPC1侧：本端子网添加VPC2的子网，本示例为192.168.2.0/24，远端子网不变。

2. 选择“虚拟专用网络 > 经典版 ”，在“VPN连接”界面找到VPC1创建的VPN连接，选择“更多 > 修改”。
3. 在修改VPN连接页面将本端子网变更为“网段”，并输入VPC1的子网和VPC2的子网，两个网段之间使用英文逗号隔开，远端子网和其它信息保持不变。

   用户侧的VPN配置需要修改远端子网，请将华为云端的VPC1子网、VPC2子网添加至VPN连接的远端子网配置中。

----结束

配置验证

本环境中在用户数据中心、VPC1、VPC2中分别存三台ECS，IP地址分别为172.16.1.1、192.168.1.1和192.168.2.1的三台主机，初始情况下ECS1（172.16.1.1）可以和ECS2（192.168.1.1）互联互通（通过VPN访问），ECS3（192.168.2.1）无法和其它主机互通，在建立VPC-peering后，ECS3可以和ECS2互通，但无法和ECS1互通。

经过步骤3的配置调整后，可以实现ECS1、ECS2和ECS3之间互联互通，结果验证如下。

- 用户数据中心。

  ECS1访问VPN连接VPC1子网下的ECS2：结果OK。

```
[root@ecs-1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.1    netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::f816:3eff:fe8c:1ec9  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:8c:1e:c9  txqueuelen 1000  (Ethernet)
        RX packets 1190  bytes 155372 (151.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1223  bytes 113478 (110.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-1 ~]# ping 192.168.1.1
PING 192.168.1.1  (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=61 time=38.4 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=61 time=31.4 ms
```

  ECS1访问VPC2子网下的ECS3：结果OK。

```
[root@ecs-1 ~]# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=61 time=31.7 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=61 time=31.6 ms
```

- 华为云端VPC1。

  VPC1子网下的ECS2访问用户数据中心子网下的ECS1：结果OK。

```
[root@ecs-vpc1-11x ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1    netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe43:2462  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:43:24:62  txqueuelen 1000  (Ethernet)
        RX packets 190954  bytes 61952364 (59.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 215881  bytes 253528145 (241.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc1-11x ~]# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=61 time=33.8 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=61 time=31.6 ms
```

  VPC1子网下的ECS2访问VPC2子网下的ECS3：结果OK。


```
[root@ecs-vpc1-11x ~]# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=7.18 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=3.05 ms
```

- 华为云端VPC2。

  VPC2子网下的ECS3访问VPC1子网下的ECS2：结果OK。

```
[root@ecs-vpc2-22 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.1  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::f816:3eff:fe4d:4bbd  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:4d:4b:bd  txqueuelen 1000  (Ethernet)
        RX packets 138865  bytes 56965509 (54.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 160536  bytes 250433082 (238.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc2-22 ~]# ping 192.168.11.84
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=9.78 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=4.29 ms
```

  VPC2子网下的ECS3访问用户数据中心子网下的ECS1：结果OK。

```
[root@ecs-vpc2-22 ~]# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=61 time=34.0 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=61 time=31.7 ms
```

2.5 基于 VPN 和云连接使用 VPN hub 功能实现云下多个数据中心互通

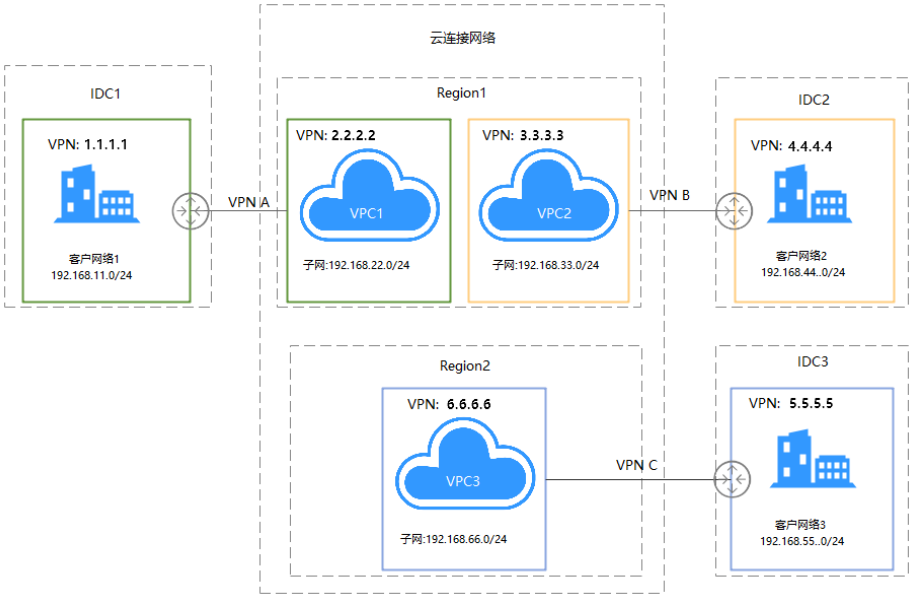
操作场景

用户在华为云的多个区域购买了VPC，同时用户存在多地数据中心，每个数据中心都通过VPN连接了云上的VPC网络。本任务指导用户通过同区域和跨区域的云连接，将多个数据中心网络连接起来，打通用户数据中心网络，使得云上云下各个数据中心的网络可以相互访问。

前提条件

1. **前置资源**
   - 用户在华为云上多个区域内购买了VPC，且某个区域中存在多个VPC。
   - 每个区域都通过VPN和不同的用户数据中心连接。
   - 云上VPC和用户的数据中心的子网不冲突，ECS服务正常。
2. **连接拓扑**

图 2-14 VPN hub 连接拓扑



3. **配置思路：**
   a. 通过云连接将VPC1、VPC2和VPC3进行连接，并配置云连接路由，实际网络配置需要购买带宽包。
   b. 分别创建IDC1-VPC1、IDC2-VPC2、IDC3-VPC3的VPN网络。
   c. 更新每一段VPN的本地子网和远端子网。
4. **局点配置说明**

表 2-12 配置说明

节点	标识	VPN本端网关	VPN本地子网	VPN远端网关	VPN远端子网	CC网络实例
IDC1	VPN A	49.4.113.226	192.168.11.0/24	122.112.222.135	192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.55.0/24 192.168.66.0/24	-

节点	标识	VPN本端网关	VPN本地子网	VPN远端网关	VPN远端子网	CC网络实例
VPC 1		122.112.222.135	192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.55.0/24 192.168.66.0/24	49.4.113.226	192.168.11.0/24	192.168.22.0/24 192.168.11.0/24
IDC 2	VPN B	139.159.222.28	192.168.44.0/24	122.112.222.112	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.55.0/24 192.168.66.0/24	-
VPC 2		122.112.222.112	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.55.0/24 192.168.66.0/24	139.159.222.28	192.168.44.0/24	192.168.33.0/24 192.168.44.0/24
IDC 3	VPN C	139.9.226.244	192.168.55.0/24	122.112.222.112	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.66.0/24	-

节点	标识	VPN本端网关	VPN本地子网	VPN远端网关	VPN远端子网	CC网络实例
VPC3		117.78.30.55	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.66.0/24	139.9.226.244	192.168.55.0/24	192.168.55.0/24 192.168.66.0/24

说明

- 云连接网络实例可在任一局点配置，通过查看路由信息验证网络实例配置。
- 用户侧VPN网关IP与VPC互为镜像，VPN连接创建的资源信息与华为云一致。

配置步骤

步骤1 创建云连接

1. 登录控制台，选择VPC1所在的区域，然后在服务列表中选择网络下的“云连接”，根据图2-15输入相关创建信息后，单击“确定”创建云连接。

图 2-15 创建云连接

2. 选择已创建的云连接，单击名称添加网络实例。

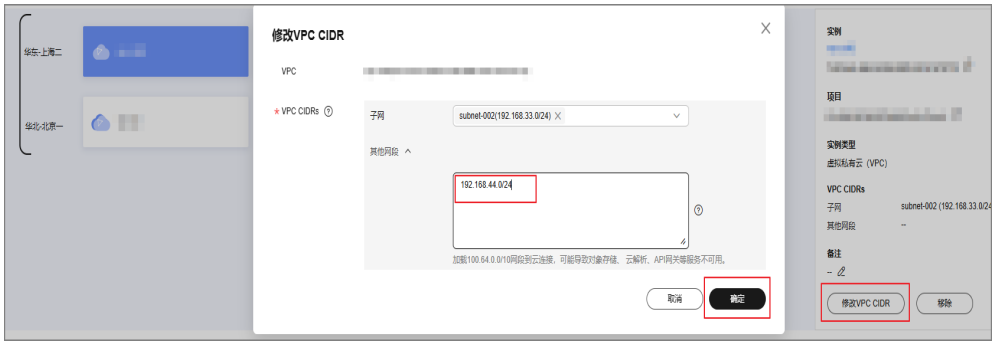
图 2-16 已创建的云连接

在新页签中选择“加载网络实例”，添加云连接所连接的VPC网络，VPC子网可直接进行选择，通过VPN连接的客户网络需要手动添加在自定义网段中，然后单击“确定”。

图 2-17 加载网络实例

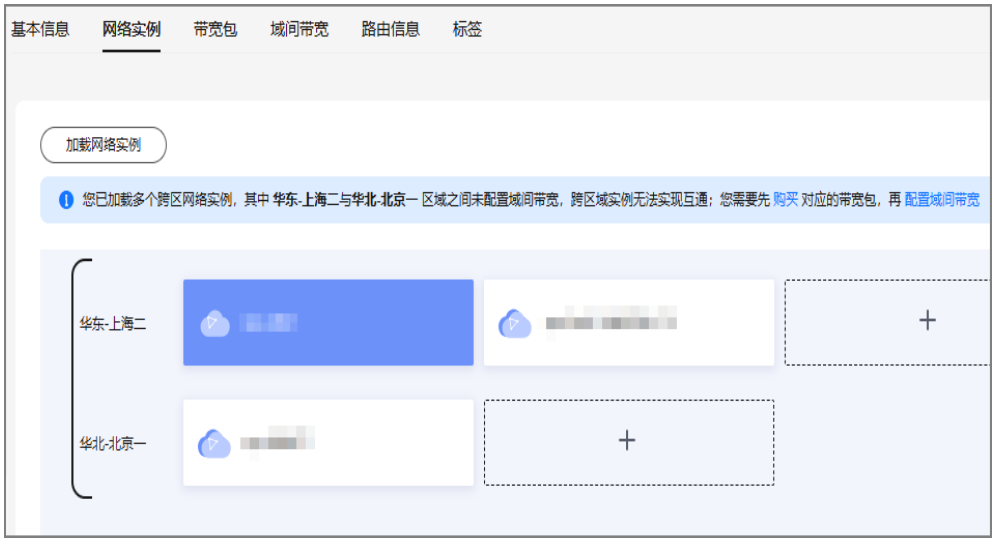
另一侧VPC2配置信息和VPC1的相同，请不要忘记添加VPN连接的客户网络，如果忘记添加可通过选择云连接中的VPC，然后单击右侧“修改VPC CIDRs”进行添加。

图 2-18 修改 VPC CIDRs



云连接配置完成后， 网络实例连接示意图如下所示。

图 2-19 网络实例连接



通过查看路由信息验证路由配置。

图 2-20 验证路由配置

步骤2 更新VPN网络配置

修改思路：

用户侧：本端子网不变，远端子网添加VPC2的子网。

VPC侧：本端子网添加VPC2的子网，远端子网不变。

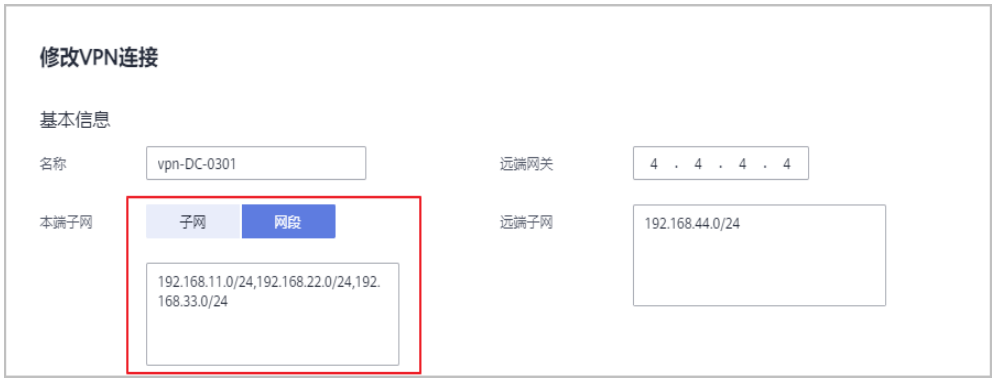
1. 选择华为云端的虚拟专用网络配置，在已创建的VPN连接中修改本端子网配置。
2. 更改本端子网类型为网段，添加云连接所连接的VPC1的网络实例和本端VPC子网，远端网络信息不变

   VPC1的VPN连接信息配置如下图所示。

图 2-21 修改 VPN 连接

VPC2的VPN连接信息配置如下图所示。

图 2-22 修改 VPN 连接



----结束

配置验证

本环境中在用户数据中心、VPC1、VPC2中分别存在三台ECS，IP地址分别为192.168.1.151、192.168.11.84和192.168.22.170的三台主机，初始情况下ECS1（192.168.1.151）可以和ECS2（192.168.11.84）互联互通（通过VPN访问），ECS3（192.168.22.170）无法和其它主机互通，在建立VPC-peering后，ECS3可以和ECS2互通，但无法和ECS1互通。

经过步骤**步骤2**的配置调整后，可以实现ECS1、ECS2和ECS3之间互联互通，结果验证如下。

- IDC1

  ECS1访问VPN连接VPC1子网下的ECS2：结果OK。

```
[root@ecs-1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.151  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe8c:1ec9  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:8c:1e:c9  txqueuelen 1000  (Ethernet)
        RX packets 1190  bytes 155372 (151.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1223  bytes 113478 (110.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-1 ~]# ping 192.168.11.84
PING 192.168.11.84 (192.168.11.84) 56(84) bytes of data.
64 bytes from 192.168.11.84: icmp_seq=1 ttl=61 time=38.4 ms
64 bytes from 192.168.11.84: icmp_seq=2 ttl=61 time=31.4 ms
```

ECS1访问VPC2子网下的ECS3：结果OK。

```
[root@ecs-1 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=31.7 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=31.6 ms
```

- IDC2

  ECS1访问VPN连接VPC1子网下的ECS2：结果OK。

```
[root@ecs-1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.151  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe8c:1ec9  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:8c:1e:c9  txqueuelen 1000  (Ethernet)
        RX packets 1190  bytes 155372 (151.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1223  bytes 113478 (110.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-1 ~]# ping 192.168.11.84
PING 192.168.11.84 (192.168.11.84) 56(84) bytes of data.
64 bytes from 192.168.11.84: icmp_seq=1 ttl=61 time=38.4 ms
64 bytes from 192.168.11.84: icmp_seq=2 ttl=61 time=31.4 ms
```

  ECS1访问VPC2子网下的ECS3：结果OK。

```
[root@ecs-1 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=31.7 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=31.6 ms
```

- 华为云端VPC1

  VPC1子网下的ECS2访问用户数据中心子网下的ECS1：结果OK

```
[root@ecs-vpc1-11x ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.84  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::f816:3eff:fe43:2462  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:43:24:62  txqueuelen 1000  (Ethernet)
        RX packets 190954  bytes 61952364 (59.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 215881  bytes 253528145 (241.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc1-11x ~]# ping 192.168.1.151
PING 192.168.1.151 (192.168.1.151) 56(84) bytes of data.
64 bytes from 192.168.1.151: icmp_seq=1 ttl=61 time=33.8 ms
64 bytes from 192.168.1.151: icmp_seq=2 ttl=61 time=31.6 ms
```

  VPC1子网下的ECS2访问VPC2子网下的ECS3：结果OK

```
[root@ecs-vpc1-11x ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=63 time=7.18 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=63 time=3.05 ms
```

- 华为云端VPC2

  VPC2子网下的ECS3访问VPC1子网下的ECS2：结果OK。

```
[root@ecs-vpc2-22 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.22.170  netmask 255.255.255.0  broadcast 192.168.22.255
        inet6 fe80::f816:3eff:fe4d:4bbd  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:4d:4b:bd  txqueuelen 1000  (Ethernet)
        RX packets 138865  bytes 56965509 (54.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 160536  bytes 250433082 (238.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc2-22 ~]# ping 192.168.11.84
PING 192.168.11.84 (192.168.11.84) 56(84) bytes of data.
64 bytes from 192.168.11.84: icmp_seq=1 ttl=63 time=9.78 ms
64 bytes from 192.168.11.84: icmp_seq=2 ttl=63 time=4.29 ms
```

VPC2子网下的ECS3访问用户数据中心子网下的ECS1：结果OK。

```
[root@ecs-vpc2-22 ~]# ping 192.168.1.151
PING 192.168.1.151 (192.168.1.151) 56(84) bytes of data.
64 bytes from 192.168.1.151: icmp_seq=1 ttl=61 time=34.0 ms
64 bytes from 192.168.1.151: icmp_seq=2 ttl=61 time=31.7 ms
```

3 终端入云 VPN

3.1 通过企业版终端入云 VPN 实现移动端和 VPC 互通（证书认证方式）

3.1.1 方案概述

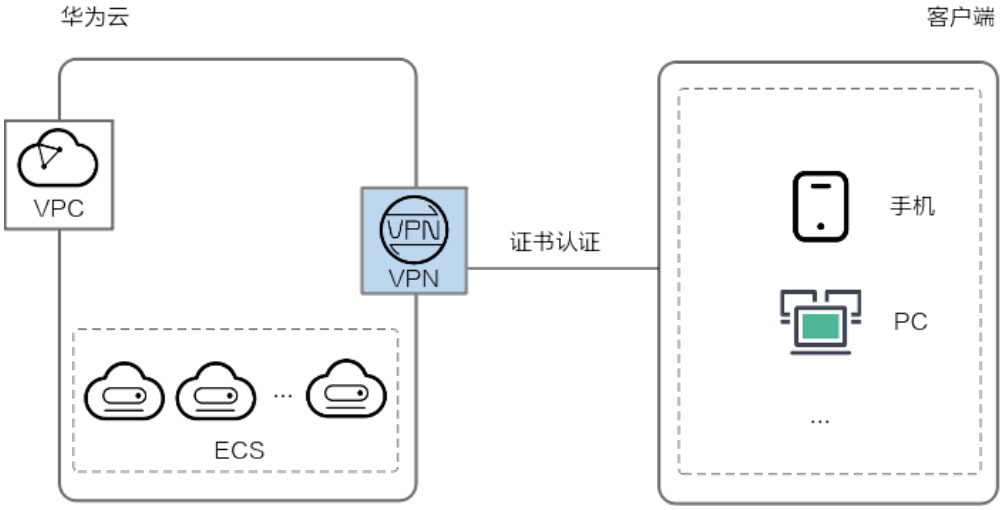
应用场景

终端入云VPN支持证书认证，服务端使用客户端CA证书验证客户端身份。

方案架构

支持多个客户端使用CA颁发的证书，登录连接VPN网关访问到云上VPC的场景。

图 3-1 方案架构



方案优势

用户通过客户端证书认证方式连接到VPN网关，用户数据传输更安全。

约束与限制

最多支持添加10个客户端CA证书。

3.1.2 组网和资源规划

数据规划

表 3-1 规划数据

类别	规划项	规划值
VPC	待互通子网	192.168.0.0/16
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在3个及以上可分配的IP地址。 192.168.2.0/24
	已创建/剩余连接数	0/10
	EIP地址	EIP地址在购买EIP时由系统自动生成。 本示例假设EIP地址生成如下：11.xx.xx.11
服务端	本端网段	192.168.0.0/24
	服务端证书	选择已有证书：cert-server（使用云证书与管理服务托管的服务端证书名称）
客户端	SSL参数	• 协议：TCP • 端口：443 • 加密算法：AES-128-GCM • 认证算法：SHA256 • 是否压缩：否
	客户端网段	172.16.0.0/16
	客户端认证类型	选择“证书认证”，单击上传CA证书。 • 名称：ca-cert-client • 内容： -----BEGIN CERTIFICATE----- od2VC7zXq7vmsVS5ZuyzeZA9CG +kzHsznZnmMjK+L9ddtRrLolRKIlE7VgWSVvn NCnGre6nQErWV688fsKJFIJ7xEBpt +S10zNuuk42OA36RsSauJWtLtebvhTav5df -----END CERTIFICATE-----

3.1.3 操作步骤

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
- 数据中心侧
  - 用户终端设备已经完成VPN客户端软件相关配置。相关操作步骤请参见**管理员指南**。

约束与限制

最多支持添加10个客户端CA证书。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”页签，进入终端入云VPN网关页面。

步骤6 配置VPN网关。

1. 在“终端入云VPN网关”页面，单击“创建终端入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”并完成支付。
   VPN网关参数请参见**表 VPN网关参数说明**。

表 3-2 VPN 网关参数说明

参数	说明	取值样例
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	*请根据实际需要进行选择*
名称	输入VPN网关的名称。	p2c-vpngw-001
虚拟私有云	选择虚拟私有云VPC信息。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在3个及以上可分配的IP地址。	192.168.66.0/24

参数	说明	取值样例
规格	支持专业型1和专业型2两种类型。 详细规格差异请参见**规格介绍**。	专业型1
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 – 当存在两个及以上可用区时，必须选择两个可用区。 部署在两个可用区的VPN网关具备更高的可用性。建议您根据VPC内资源所在的可用区选择网关的可用区。 – 当仅存在一个可用区时，可选择此可用区创建VPN网关。	可用区1、可用区2
连接数	VPN网关最多支持10个免费的VPN连接，提供可选连接数规格，支持用户自定义。	10
EIP	用于VPN网关和客户端进行网络连接。 – 现在创建：购买新EIP，新购买EIP的计费模式为按需。 – 使用已有：使用已有EIP，仅支持使用独享带宽的EIP。 **说明** 使用已有EIP时，已有EIP的计费模式可以为按需，也可以为包年/包月。	现在创建
弹性公网IP类型	仅“EIP”选择“现在创建”时需要配置。 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保持客户使用的网络持续稳定、高效。 弹性公网IP类型的详细介绍请参见**什么是弹性公网IP**。	全动态BGP

参数	说明	取值样例
带宽大小	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽大小，单位：Mbit/s。 – 所有使用该EIP创建的VPN连接均会分摊占用该EIP的带宽大小，所有VPN连接的带宽总和不能超过该EIP的带宽大小。 当网络流量超过EIP的带宽大小时，有可能造成网络拥塞导致VPN连接中断，请提前做好带宽规划。 – 支持在云监控中配置告警规则对带宽进行监控。 – 支持用户在允许的带宽范围内自定义带宽大小。 – 部分区域默认仅支持300M带宽。如果需要更大带宽，您可以先申请300M带宽，然后**提交工单**进行带宽扩容。	20 Mbit/s
带宽名称	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽对象的名称。	p2c-vpngw-bandwidth1

步骤7 配置服务端。

1. 在“终端入云VPN网关”页面，可以单击目标VPN网关操作列的“配置服务端”，也可以单击目标VPN网关名称进入详情页配置服务端。
2. 根据界面提示配置参数，单击“确定”。

   服务端配置参数请参见**表3-3**。

表 3-3 服务端参数说明

区域	参数	说明	取值样例
基本信息	本端网段	本端网段是客户端通过终端入云VPN网关访问的目标网络的地址段。本端网段可以是华为云VPC的网段，或与华为云VPC互联网络的网段。 最多可指定20个本端网段。本端网段的全0配置，暂不开放支持。本端网段的限制网段为0.0.0.0/8，224.0.0.0/4，240.0.0.0/4，127.0.0.0/8，不能与这些特殊网段重叠或冲突。 – 选择子网： 选择本VPC子网信息。 – 输入网段： 可以输入本VPC下的子网信息；也可以输入与本VPC建立了对等网络的VPC子网信息。 **说明** 本端网段修改后，客户端需要重新连接。	192.168.0.0/24

区域	参数	说明	取值样例
	客户端网段	客户端网段是分配给客户端虚拟网卡地址的网段，不能与本端网段重叠，不能与网关所在VPC的路由表内路由重叠。当客户端连接网关时，会从中分配一个IP地址给客户端使用。 客户端网段需要满足点分十进制/掩码格式，掩码位数在16~26之间。系统在为每个客户端分配IP地址时，需要划分出一个子网掩码为30的子网段，用以保证网络通信正常。因此，请确保您指定的客户端网段所包含的IP地址个数是VPN网关连接数的4倍及以上。 不同VPN连接数建议的客户端网段请参见**表 建议的客户端网段**。 **说明** 客户端网段修改后，客户端需要重新连接。	172.16.0.0/16
	隧道类型	SSL协议是一种传输层安全协议，用于构建客户端和服务端之间的安全通道。 OpenVPN（SSL），不支持修改。	OpenVPN（SSL）
认证信息	服务端证书	服务端证书是服务端使用的SSL证书，客户端会基于此证书验证服务端的身份。 选择已有证书：查看并选择已上传证书。 – 上传证书：单击下拉框最下方的“上传证书”，跳转至云证书与管理服务。按照界面提示上传服务端证书，详细步骤请参见**上传已有SSL证书**。 – 推荐使用强密码算法的证书，如RSA3072/4096。 **说明** 用户在完成服务端配置后，在云证书与管理服务中删除了引用的服务端证书，并不影响服务端证书的可用性。	选择已有证书

区域	参数	说明	取值样例
	客户端认证类型	选择“客户端认证类型 > 证书认证”。 – 单击“上传CA证书”，以文本格式打开CA证书PEM格式的文件，将证书内容复制到“上传CA证书”的“内容”文本框内。最多支持添加10个客户端CA证书。 推荐使用强密码算法的证书，如RSA3072/4096。RSA2048加密算法的证书存在风险，请慎用。 – 证书验证通过后，您可以在列表中查看CA证书基本信息，包含名称、序列号、签名算法、颁发者、使用者、过期时间。 **说明** 删除该CA证书后，相关的客户端无法再正常连接。	证书认证
高级配置	协议	终端入云VPN连接使用的协议。 – TCP（默认）	TCP
	端口	终端入云VPN连接使用的端口。 – 443（默认） – 1194	443
	加密算法	终端入云VPN连接使用的加密算法。 – AES-128-GCM（默认） – AES-256-GCM	AES-128-GCM
	认证算法	终端入云VPN连接使用的认证算法。 – 加密算法为AES-128-GCM时，对应认证算法为SHA256。 – 加密算法为AES-256-GCM时，对应认证算法为SHA384。	SHA256
	是否压缩	是否对传输数据进行压缩处理。 默认不压缩，不支持修改。	否

表 3-4 建议的客户端网段

VPN连接数	建议的客户端网段
10	子网掩码位数小于或等于26的网段。 例如：10.0.0.0/26、10.0.0.0/25。
20	子网掩码位数小于或等于25的网段。 例如：10.0.0.0/25、10.0.0.0/24。

VPN连接数	建议的客户端网段
50	子网掩码位数小于或等于24的网段。 例如：10.0.0.0/24、10.0.0.0/23。
100	子网掩码位数小于或等于23的网段。 例如：10.0.0.0/23、10.0.0.0/22。
200	子网掩码位数小于或等于22的网段。 例如：10.0.0.0/22、10.0.0.0/21。
500	子网掩码位数小于或等于21的网段。 例如：10.0.0.0/21、10.0.0.0/20。

3. 上传服务端证书。
   a. 在“服务端”界面，选择“服务端证书”，在下拉选项中单击“上传证书”进入“云证书与管理服务”页面。
   b. 在“SSL证书管理”页面，选择“上传证书 > 上传证书”，根据界面提示填写相关信息。
      上传证书参数请参见**表 上传国际标准证书参数说明**。

      表 3-5 上传国际标准证书参数说明

参数	说明
证书标准	选择国际标准证书。
证书名称	用户自定义。
企业项目	将上传的SSL证书分配至对应的企业项目中。
证书文件	以文本编辑器（如Notepad++）打开待上传证书里的PEM格式的文件，将证书内容复制到此处。 按照“服务端证书--CA证书”的顺序依次排列上传。 上传证书文件格式如**图 证书上传格式**。
证书私钥	以文本编辑器（如Notepad++）打开待上传证书里的KEY格式的文件，将私钥内容复制到此处。 仅上传服务端证书私钥。 上传证书私钥格式如**图 证书上传格式**。

图 3-2 证书上传格式

说明

服务端证书的CN必须是域名格式。

c. 单击“确定”，完成上传证书。

d. 查看证书列表，确认证书状态为“托管中”。

4. 上传客户端CA证书。

a. 在“服务端”界面，在“客户端认证类型”下拉选项中选择“证书认证 ”，单击“上传CA证书”。

b. 根据界面提示填写相关信息。

表 3-6 上传 CA 证书参数说明

参数	说明	取值样例
名称	支持修改。	ca-cert-xxxx
内容	以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。 **说明** ■ 推荐使用强密码算法的证书，如RSA3072/4096。 ■ RSA2048加密算法的证书存在风险，请慎用。	-----BEGIN CERTIFICATE----- 证书内容 -----END CERTIFICATE-----

c. 单击“确定”。

说明

最多支持添加10个客户端CA证书。

步骤8 下载客户端配置。

1. 在“终端入云VPN网关”页面，单击目标VPN网关所在行操作列的“下载客户端配置”。
2. 解压缩得到“client_config.conf”、“client_config.ovpn”、“README.md”三个文件。
   - “client_config.conf”适用于Linux。
   - “client_config.ovpn”适用于Windows、Mac或Android。

步骤9 补充证书信息。

1. 以文本编辑器（如Notepad++）打开“client_config.ovpn”文件。
2. 在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
客户端证书
</cert>
<key>
客户端证书私钥
</key>
```

3. 保存修改并退出。

步骤10 配置客户端。

说明

本示例为您介绍如何配置Windows客户端，不同类型VPN客户端软件及版本可能存在差异，配置时请以实际为准。

- 操作系统：Windows 10
- 客户端软件：OpenVPN Connect 3.4.2（3160）

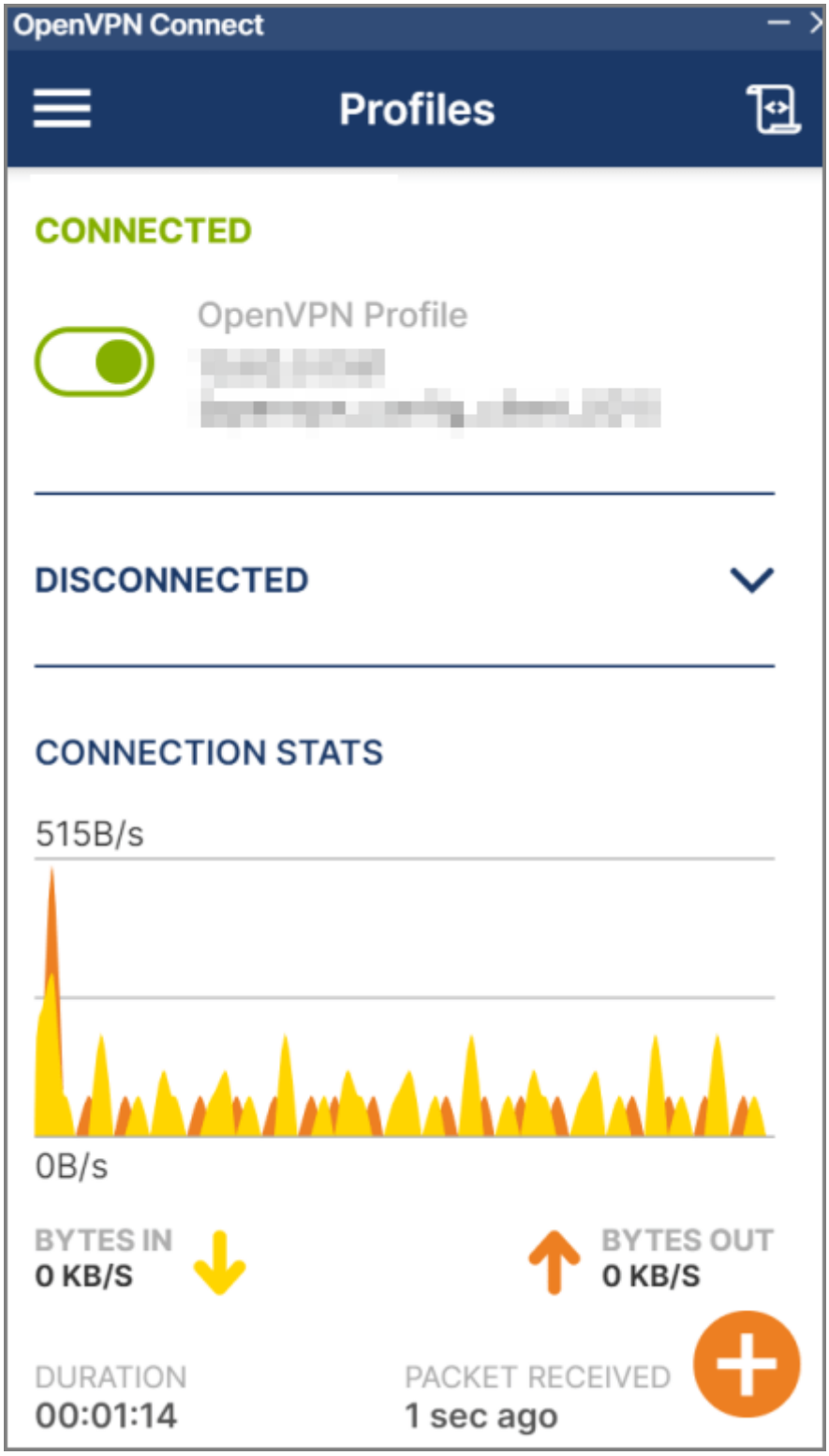
更多客户端配置案例，请参见**配置客户端**。

1. 在OpenVPN官方网站**下载OpenVPN Connect**，根据界面提示进行安装。
2. 启动OpenVPN Connect客户端，在“FILE”页签下单击“BROWSE”，上传客户端配置文件。

图 3-3 上传配置文件

3. 单击“CONNECT”尝试建立VPN连接，若出现类似下图所示界面，代表连接成功。

图 3-4 连接成功



----结束

结果验证

1. 打开客户端设备的命令行窗口。
2. 执行以下命令，验证连通性。

   ping 192.168.1.10

   其中，192.168.1.10为客户端需要访问的弹性云服务器的IP地址，请根据实际替换。
3. 回显如下信息，表示网络已通。

```
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=27ms TTL=245
```

3.2 通过终端入云 VPN 实现移动端和 VPC 互通（IAM 认证方式）

3.2.1 方案概述

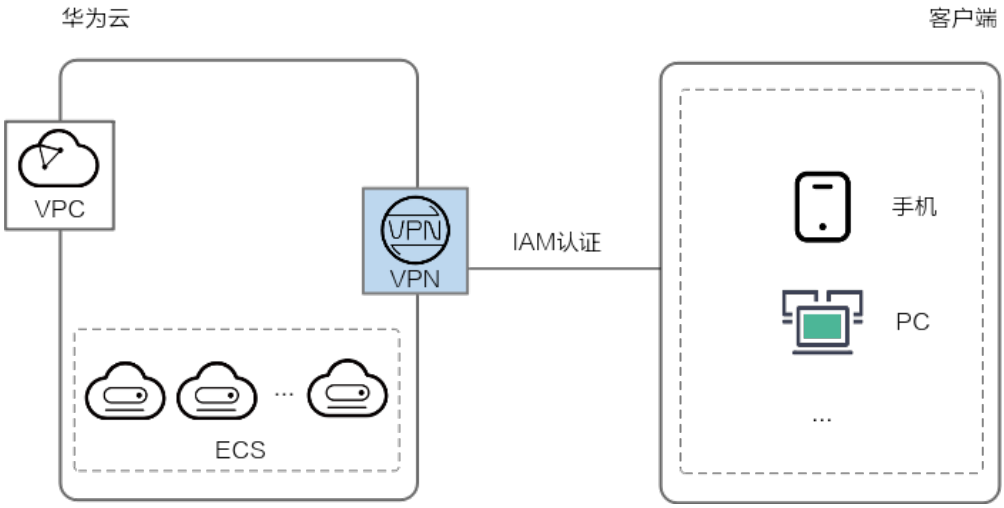
应用场景

终端入云VPN支持三方用户认证，服务端使用客户端IAM认证来验证客户端身份。

方案架构

支持多个客户端使用IAM认证，登录连接VPN网关访问到云上VPC的场景。

图 3-5 方案架构



方案优势

用户可以通过客户端IAM认证方式进行统一账户管理。

约束与限制

当客户端认证类型为“IAM认证”时，不支持使用区域子项目中的网关资源。关于子项目的详细介绍，请参考**项目管理**。

3.2.2 组网和资源规划

数据规划

表 3-7 规划数据

类别	规划项	规划值
VPC	待互通子网	192.168.0.0/16
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在3个及以上可分配的IP地址。 192.168.2.0/24
	已创建/剩余连接数	0/10
	EIP地址	EIP地址在购买EIP时由系统自动生成。 本示例假设EIP地址生成如下：11.xx.xx.11
服务端	本端网段	192.168.0.0/24
	服务端证书	服务自签名证书
客户端	SSL参数	• 协议：TCP • 端口：443 • 加密算法：AES-128-GCM • 认证算法：SHA256 • 是否压缩：否
	客户端网段	172.16.0.0/16
	客户端认证类型	选择“IAM认证”。

3.2.3 操作步骤

前提条件

- 云侧
  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。

- 数据中心侧
  用户终端设备已经完成VPN客户端软件相关配置。相关操作步骤请参见**管理员指南**。

操作须知

更换客户端认证类型会导致已有VPN连接中断，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“管理与监管 > 统一身份认证服务 IAM”。

步骤4 创建IAM用户、用户组并授权。

1. 创建用户组。
   a. 在左侧导航栏，单击“用户组”。
   b. 在“用户组”页签中，单击“创建用户组”。
   c. 根据界面提示，输入“用户组名称”。
   d. 单击“确定”，用户组创建完成。
      在用户组列表中，可以查看新创建的用户组。
2. 用户组授权。
   a. 选择目标用户组，单击操作列的“授权”。
   b. 在右上方搜索“VPN SSOAccessPolicy”，勾选该权限。
   c. 单击“下一步”，根据实际情况选择授权范围方案。
   d. 单击“确定”，用户组授权完成。
3. 创建IAM用户。
   a. 在左侧导航栏，单击“用户”。
   b. 在“用户”页签中，单击“创建用户”。
   c. 根据界面提示，配置用户基本信息。
      如何配置用户基本信息，请参见**创建IAM用户**。
   d. 单击“下一步”。
   e. （可选）勾选要加入的用户组，将用户加入到用户组。
      加入用户组后，用户将具备用户组的权限。

步骤5 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤6 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤7 单击“终端入云VPN网关”页签，进入终端入云VPN网关页面。

步骤8 配置VPN网关。

1. 在“终端入云VPN网关”页面，单击“创建终端入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”并完成支付。

VPN网关参数请参见**表 VPN网关参数说明**。

表 3-8 VPN 网关参数说明

参数	说明	取值样例
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	*请根据实际需要进行选择*
名称	输入VPN网关的名称。	p2c-vpngw-001
虚拟私有云	选择虚拟私有云VPC信息。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在3个及以上可分配的IP地址。	192.168.66.0/24
规格	支持专业型1和专业型2两种类型。 详细规格差异请参见**规格介绍**。	专业型1
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 – 当存在两个及以上可用区时，必须选择两个可用区。 部署在两个可用区的VPN网关具备更高的可用性。建议您根据VPC内资源所在的可用区选择网关的可用区。 – 当仅存在一个可用区时，可选择此可用区创建VPN网关。	可用区1、可用区2
连接数	VPN网关最多支持10个免费的VPN连接，提供可选连接数规格，支持用户自定义。	10
EIP	用于VPN网关和客户端进行网络连接。 – 现在创建：购买新EIP，新购买EIP的计费模式为按需。 – 使用已有：使用已有EIP，仅支持使用独享带宽的EIP。 **说明** 使用已有EIP时，已有EIP的计费模式可以为按需，也可以为包年/包月。	现在创建
弹性公网IP类型	仅“EIP”选择“现在创建”时需要配置。 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保持客户使用的网络持续稳定、高效。 弹性公网IP类型的详细介绍请参见**什么是弹性公网IP**。	全动态BGP

参数	说明	取值样例
带宽大小	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽大小，单位：Mbit/s。 – 所有使用该EIP创建的VPN连接均会分摊占用该EIP的带宽大小，所有VPN连接的带宽总和不能超过该EIP的带宽大小。 当网络流量超过EIP的带宽大小时，有可能造成网络拥塞导致VPN连接中断，请提前做好带宽规划。 – 支持在云监控中配置告警规则对带宽进行监控。 – 支持用户在允许的带宽范围内自定义带宽大小。 – 部分区域默认仅支持300M带宽。如果需要更大带宽，您可以先申请300M带宽，然后**提交工单**进行带宽扩容。	20 Mbit/s
带宽名称	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽对象的名称。	p2c-vpngw-bandwidth1

步骤9 配置服务端。

1. 在“终端入云VPN网关”页面，可以单击目标VPN网关操作列的“配置服务端”，也可以单击目标VPN网关名称进入详情页配置服务端。
2. 根据界面提示配置参数，单击“确定”。

   服务端配置参数请参见**表 服务端参数说明**。

表 3-9 服务端参数说明

区域	参数	说明	取值样例
基本信息	本端网段	本端网段是客户端通过终端入云VPN网关访问的目标网络的地址段。本端网段可以是华为云VPC的网段，或与华为云VPC互联网络的网段。 最多可指定20个本端网段。本端网段的全0配置，暂不开放支持。本端网段的限制网段为0.0.0.0/8，224.0.0.0/4，240.0.0.0/4，127.0.0.0/8，不能与这些特殊网段重叠或冲突。 – 选择子网： 选择本VPC子网信息。 – 输入网段： 可以输入本VPC下的子网信息；也可以输入与本VPC建立了对等网络的VPC子网信息。 **说明** 本端网段修改后，客户端需要重新连接。	192.168.0.0/24

区域	参数	说明	取值样例
	客户端网段	客户端网段是分配给客户端虚拟网卡地址的网段，不能与本端网段重叠，不能与网关所在VPC的路由表内路由重叠。当客户端连接网关时，会从中分配一个IP地址给客户端使用。 客户端网段需要满足点分十进制/掩码格式，掩码位数在16~26之间。系统在为每个客户端分配IP地址时，需要划分出一个子网掩码为30的子网段，用以保证网络通信正常。因此，请确保您指定的客户端网段所包含的IP地址个数是VPN网关连接数的4倍及以上。 不同VPN连接数建议的客户端网段请参见**表 建议的客户端网段**。 **说明** 客户端网段修改后，客户端需要重新连接。	172.16.0.0/16
	隧道类型	SSL协议是一种传输层安全协议，用于构建客户端和服务端之间的安全通道。 OpenVPN（SSL），不支持修改。	OpenVPN（SSL）
认证信息	服务端证书	选择“服务自签名证书”。	服务自签名证书
	客户端认证类型	选择“IAM认证”。	IAM认证
高级配置	协议	终端入云VPN连接使用的协议。 – TCP（默认）	TCP
	端口	终端入云VPN连接使用的端口。 – 443（默认） – 1194	443
	加密算法	终端入云VPN连接使用的加密算法。 – AES-128-GCM（默认） – AES-256-GCM	AES-128-GCM
	认证算法	终端入云VPN连接使用的认证算法。 – 加密算法为AES-128-GCM时，对应认证算法为SHA256。 – 加密算法为AES-256-GCM时，对应认证算法为SHA384。	SHA256
	是否压缩	是否对传输数据进行压缩处理。 默认不压缩，不支持修改。	否

表 3-10 建议的客户端网段

VPN连接数	建议的客户端网段
10	子网掩码位数小于或等于26的网段。 例如：10.0.0.0/26、10.0.0.0/25。
20	子网掩码位数小于或等于25的网段。 例如：10.0.0.0/25、10.0.0.0/24。
50	子网掩码位数小于或等于24的网段。 例如：10.0.0.0/24、10.0.0.0/23。
100	子网掩码位数小于或等于23的网段。 例如：10.0.0.0/23、10.0.0.0/22。
200	子网掩码位数小于或等于22的网段。 例如：10.0.0.0/22、10.0.0.0/21。
500	子网掩码位数小于或等于21的网段。 例如：10.0.0.0/21、10.0.0.0/20。

3. 单击“确定”。

步骤10 下载客户端配置。

1. 在“终端入云VPN网关”页面，单击目标VPN网关所在行操作列的“下载客户端配置”。
2. 解压缩得到“client_config.conf”、“client_config.ovpn”、“README.md”三个文件。
   - “client_config.conf”适用于Linux。
   - “client_config.ovpn”适用于Windows、Mac或Android。

步骤11 配置客户端。

说明

本示例为您介绍如何配置Windows客户端，不同类型VPN客户端软件及版本可能存在差异，配置时请以实际为准。

- 操作系统：Windows 10
- 客户端软件：OpenVPN Connect 3.4.2（3160）

  客户端仅3.4.0及以上版本支持IAM认证。

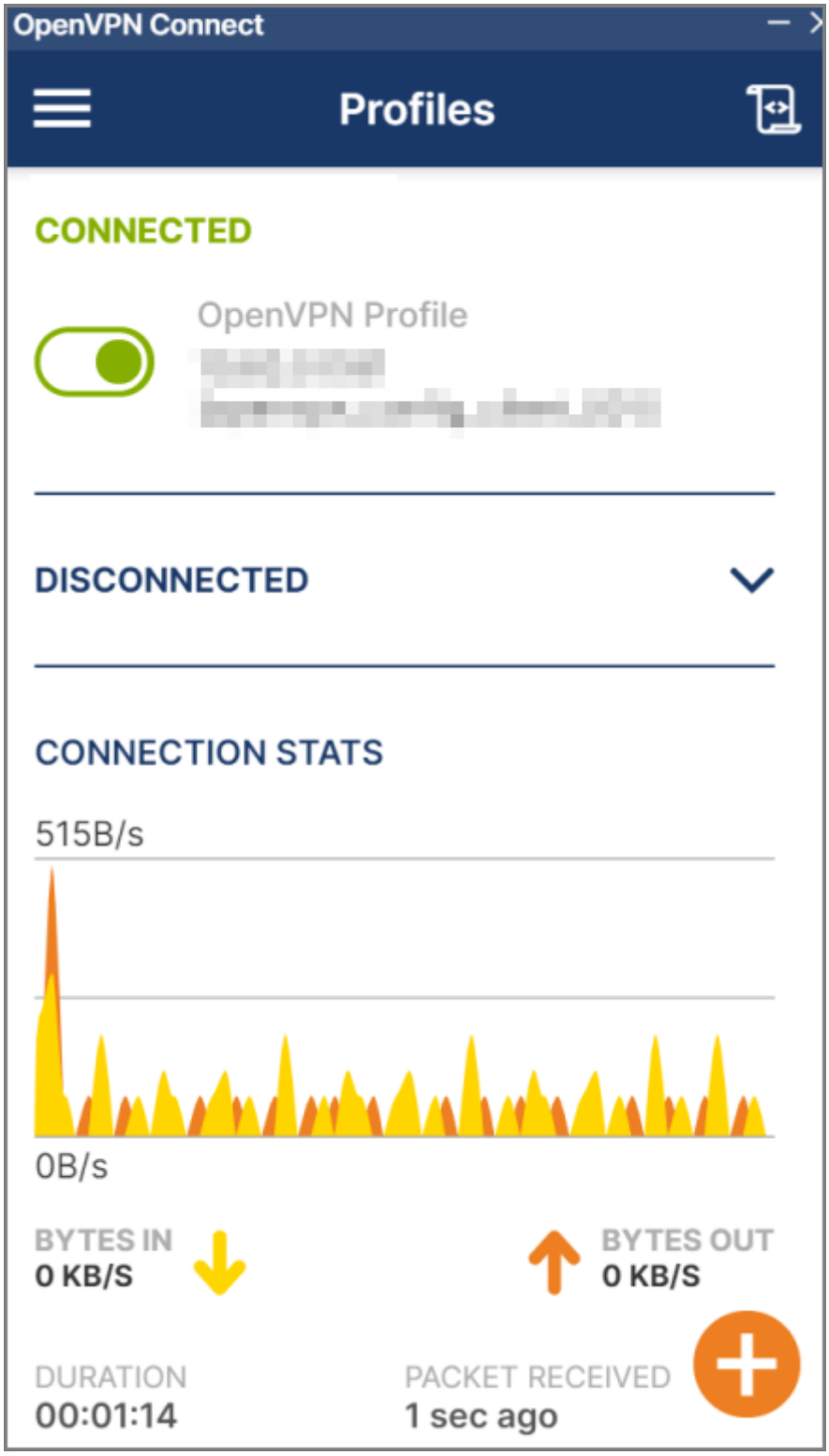
更多客户端配置案例，请参见**配置客户端**。

1. 在OpenVPN官方网站**下载OpenVPN Connect**，根据界面提示进行安装。
2. 启动OpenVPN Connect客户端，在“FILE”页签下单击“BROWSE”，上传客户端配置文件。

图 3-6 上传配置文件

3. 单击“CONNECT”尝试建立VPN连接，若出现类似下图所示界面，代表连接成功。

图 3-7 连接成功



4. 使用IAM用户名和密码登录web客户端。
   - 当登录页面显示认证成功时，表示成功建立VPN连接。

- 当登录页面显示认证失败时，可以根据错误信息修改对应配置。具体错误信息请参考《故障排除》。

----结束

结果验证

1. 按**win+R**键，输入**cmd**，打开客户端设备的命令行窗口。
2. 执行以下命令，验证连通性。

   ping 192.168.1.10

   其中，192.168.1.10为客户端需要访问的弹性云服务器的IP地址，请根据实际替换。
3. 回显如下信息，表示网络已通。

```
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=27ms TTL=245
```

3.3 通过终端入云 VPN 实现移动端和 VPC 互通（联邦认证方式）

3.3.1 方案概述

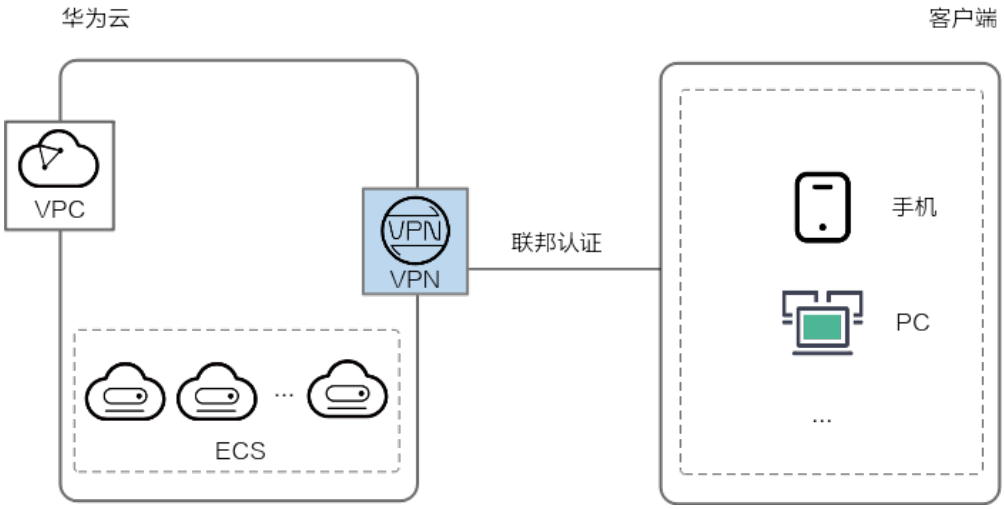
应用场景

终端入云VPN支持三方用户认证，服务端使用客户端联邦认证来验证客户端身份。

方案架构

支持多个客户端使用联邦认证，登录连接VPN网关访问到云上VPC的场景。

图 3-8 方案架构



方案优势

用户可以通过客户端联邦认证方式进行统一账户管理，用户数据传输更安全。

约束与限制

当客户端认证类型为“联邦认证”时，不支持使用区域子项目中的网关资源。关于子项目的详细介绍，请参考**项目管理**。

3.3.2 组网和资源规划

数据规划

表 3-11 规划数据

类别	规划项	规划值
VPC	待互通子网	192.168.0.0/16
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在3个及以上可分配的IP地址。 192.168.2.0/24
	已创建/剩余连接数	0/10
	EIP地址	EIP地址在购买EIP时由系统自动生成。 本示例假设EIP地址生成如下：11.xx.xx.11
服务端	本端网段	192.168.0.0/24
	服务端证书	服务自签名证书
客户端	SSL参数	• 协议：TCP • 端口：443 • 加密算法：AES-128-GCM • 认证算法：SHA256 • 是否压缩：否
	客户端网段	172.16.0.0/16
	客户端认证类型	选择“联邦认证”。
	身份提供商	p2c-vpngw-saml1

3.3.3 操作步骤

前提条件

- 云侧

  - 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
  - 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
- 数据中心侧
  - 用户终端设备已经完成VPN客户端软件相关配置。相关操作步骤请参见**管理员指南**。
  - 用户已配置身份提供商，当前仅支持基于SAML协议的虚拟用户SSO的身份提供商。如何配置虚拟用户SSO类型的身份提供商，请参见**基于SAML协议的虚拟用户SSO**。

    身份提供商必须配置身份转换规则。在配置身份转换规则时，选择拥有“VPN SSOAccessPolicy”权限的用户组。如何创建用户组，具体操作请参见**创建用户组并授权**。

    说明

    当用户通过编辑JSON文件来配置或修改身份转换规则时，用户名不能设置为全空格。

操作须知

更换客户端认证类型或身份提供商会导致已有VPN连接中断，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在页面左上角单击图标，选择“管理与监管 > 统一身份认证服务 IAM”。

步骤5 创建用户组并授权。

1. 创建用户组。
   a. 在左侧导航栏，单击“用户组”。
   b. 在“用户组”页签中，单击“创建用户组”。
   c. 根据界面提示，输入“用户组名称”。
   d. 单击“确定”，用户组创建完成。

      在用户组列表中，可以查看新创建的用户组。
2. 用户组授权。
   a. 选择目标用户组，单击操作列的“授权”。
   b. 在右上方搜索“VPN SSOAccessPolicy”，勾选该权限。
   c. 单击“下一步”，根据实际情况选择授权范围方案。
   d. 单击“确定”，用户组授权完成。

步骤6 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤7 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤8 单击“终端入云VPN网关”页签，进入终端入云VPN网关页面。

步骤9 配置VPN网关。

1. 在“终端入云VPN网关”页面，单击“创建终端入云VPN网关”。
2. 根据界面提示配置参数，单击“立即购买”并完成支付。
   VPN网关参数请参见**表 VPN网关参数说明**。

表 3-12 VPN 网关参数说明

参数	说明	取值样例
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	*请根据实际需要进行选择*
名称	输入VPN网关的名称。	p2c-vpngw-001
虚拟私有云	选择虚拟私有云VPC信息。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在3个及以上可分配的IP地址。	192.168.66.0/24
规格	支持专业型1和专业型2两种类型。 详细规格差异请参见**规格介绍**。	专业型1
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 – 当存在两个及以上可用区时，必须选择两个可用区。 部署在两个可用区的VPN网关具备更高的可用性。建议您根据VPC内资源所在的可用区选择网关的可用区。 – 当仅存在一个可用区时，可选择此可用区创建VPN网关。	可用区1、可用区2
连接数	VPN网关最多支持10个免费的VPN连接，提供可选连接数规格，支持用户自定义。	10
EIP	用于VPN网关和客户端进行网络连接。 – 现在创建：购买新EIP，新购买EIP的计费模式为按需。 – 使用已有：使用已有EIP，仅支持使用独享带宽的EIP。 **说明** 使用已有EIP时，已有EIP的计费模式可以为按需，也可以为包年/包月。	现在创建

参数	说明	取值样例
弹性公网IP类型	仅“EIP”选择“现在创建”时需要配置。 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保持客户使用的网络持续稳定、高效。 弹性公网IP类型的详细介绍请参见**什么是弹性公网IP**。	全动态BGP
带宽大小	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽大小，单位：Mbit/s。 – 所有使用该EIP创建的VPN连接均会分摊占用该EIP的带宽大小，所有VPN连接的带宽总和不能超过该EIP的带宽大小。 当网络流量超过EIP的带宽大小时，有可能造成网络拥塞导致VPN连接中断，请提前做好带宽规划。 – 支持在云监控中配置告警规则对带宽进行监控。 – 支持用户在允许的带宽范围内自定义带宽大小。 – 部分区域默认仅支持300M带宽。如果需要更大带宽，您可以先申请300M带宽，然后**提交工单**进行带宽扩容。	20 Mbit/s
带宽名称	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽对象的名称。	p2c-vpngw-bandwidth1

步骤10 配置服务端。

1. 在“终端入云VPN网关”页面，可以单击目标VPN网关操作列的“配置服务端”，也可以单击目标VPN网关名称进入详情页配置服务端。
2. 根据界面提示配置参数，单击“确定”。
   服务端配置参数请参见**表 服务端参数说明**。

表 3-13 服务端参数说明

区域	参数	说明	取值样例
基本信息	本端网段	本端网段是客户端通过终端入云VPN网关访问的目标网络的地址段。本端网段可以是华为云VPC的网段，或与华为云VPC互联网络的网段。 最多可指定20个本端网段。本端网段的全0配置，暂不开放支持。本端网段的限制网段为0.0.0.0/8，224.0.0.0/4，240.0.0.0/4，127.0.0.0/8，不能与这些特殊网段重叠或冲突。 – 选择子网：选择本VPC子网信息。 – 输入网段：可以输入本VPC下的子网信息；也可以输入与本VPC建立了对等网络的VPC子网信息。 **说明** 本端网段修改后，客户端需要重新连接。	192.168.0.0/24
	客户端网段	客户端网段是分配给客户端虚拟网卡地址的网段，不能与本端网段重叠，不能与网关所在VPC的路由表内路由重叠。当客户端连接网关时，会从中分配一个IP地址给客户端使用。 客户端网段需要满足点分十进制/掩码格式，掩码位数在16~26之间。系统在为每个客户端分配IP地址时，需要划分出一个子网掩码为30的子网段，用以保证网络通信正常。因此，请确保您指定的客户端网段所包含的IP地址个数是VPN网关连接数的4倍及以上。 不同VPN连接数建议的客户端网段请参见**表 建议的客户端网段**。 **说明** 客户端网段修改后，客户端需要重新连接。	172.16.0.0/16
	隧道类型	SSL协议是一种传输层安全协议，用于构建客户端和服务端之间的安全通道。 OpenVPN（SSL），不支持修改。	OpenVPN（SSL）
认证信息	服务端证书	选择“服务自签名证书”。	服务自签名证书
	客户端认证类型	选择“客户端认证类型 > 联邦认证”。	联邦认证

区域	参数	说明	取值样例
	身份提供商	选择已创建的身份提供商。 如果没有创建身份提供商，可以在下拉框中单击“新建身份提供商”，跳转至统一身份认证服务。如何创建身份提供商，请参见**创建身份提供商**。	*请根据实际需要进行选择*
高级配置	协议	终端入云VPN连接使用的协议。 – TCP（默认）	TCP
	端口	终端入云VPN连接使用的端口。 – 443（默认） – 1194	443
	加密算法	终端入云VPN连接使用的加密算法。 – AES-128-GCM（默认） – AES-256-GCM	AES-128-GCM
	认证算法	终端入云VPN连接使用的认证算法。 – 加密算法为AES-128-GCM时，对应认证算法为SHA256。 – 加密算法为AES-256-GCM时，对应认证算法为SHA384。	SHA256
	是否压缩	是否对传输数据进行压缩处理。 默认不压缩，不支持修改。	否

表 3-14 建议的客户端网段

VPN连接数	建议的客户端网段
10	子网掩码位数小于或等于26的网段。 例如：10.0.0.0/26、10.0.0.0/25。
20	子网掩码位数小于或等于25的网段。 例如：10.0.0.0/25、10.0.0.0/24。
50	子网掩码位数小于或等于24的网段。 例如：10.0.0.0/24、10.0.0.0/23。
100	子网掩码位数小于或等于23的网段。 例如：10.0.0.0/23、10.0.0.0/22。
200	子网掩码位数小于或等于22的网段。 例如：10.0.0.0/22、10.0.0.0/21。
500	子网掩码位数小于或等于21的网段。 例如：10.0.0.0/21、10.0.0.0/20。

3. 单击“确定”。

步骤11 下载客户端配置。

1. 在“终端入云VPN网关”页面，单击目标VPN网关所在行操作列的“下载客户端配置”。
2. 解压缩得到“client_config.conf”、“client_config.ovpn”、“README.md”三个文件。
   - “client_config.conf”适用于Linux。
   - “client_config.ovpn”适用于Windows、Mac或Android。

步骤12 配置客户端。

说明

本示例为您介绍如何配置Windows客户端，不同类型VPN客户端软件及版本可能存在差异，配置时请以实际为准。

- 操作系统：Windows 10
- 客户端软件：OpenVPN Connect 3.4.2（3160）

  客户端仅3.4.0及以上版本支持联邦认证。

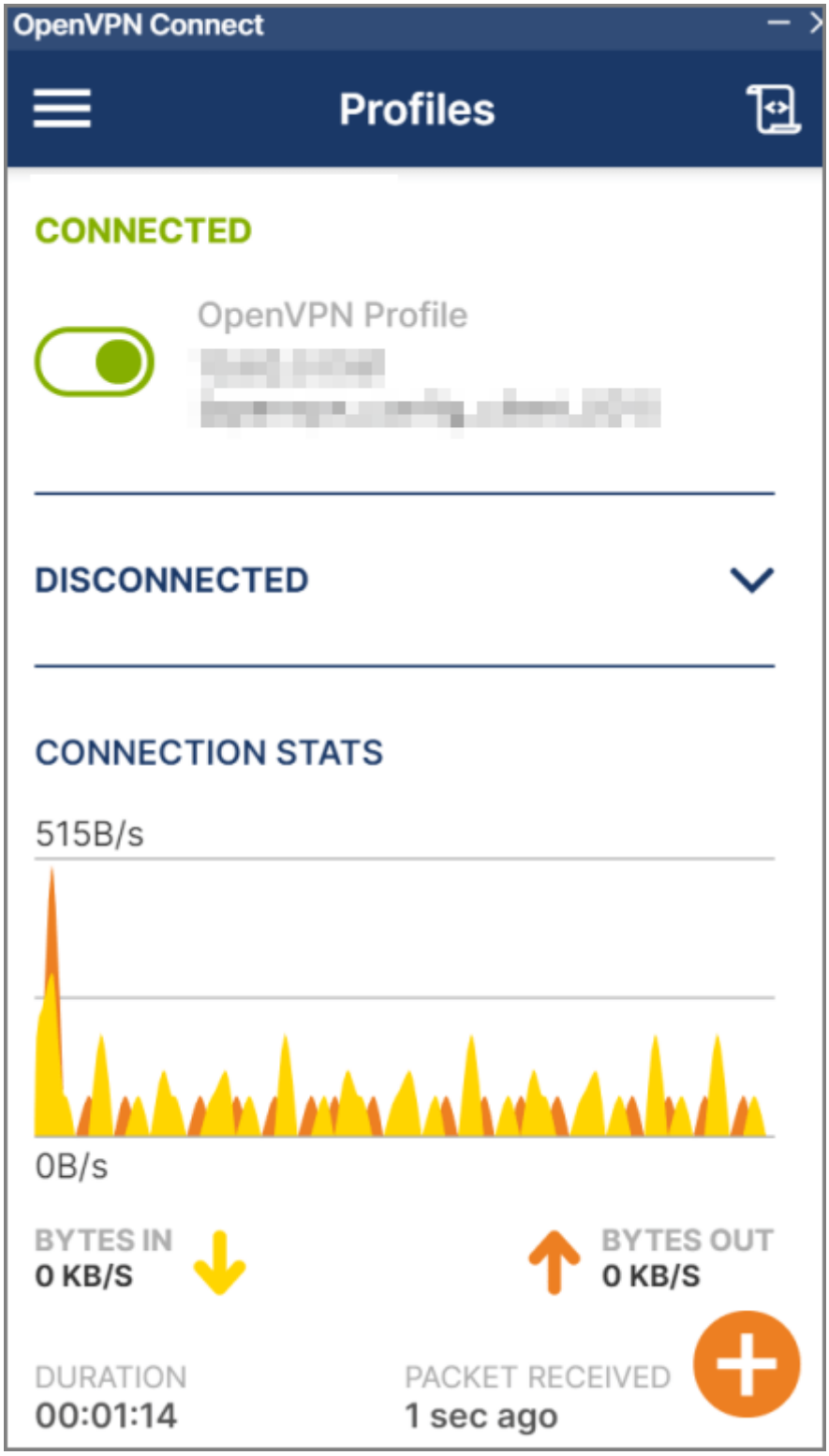
更多客户端配置案例，请参见**配置客户端**。

1. 在OpenVPN官方网站**下载OpenVPN Connect**，根据界面提示进行安装。
2. 启动OpenVPN Connect客户端，在“FILE”页签下单击“BROWSE”，上传客户端配置文件。

图 3-9 上传配置文件

3. 单击“CONNECT”尝试建立VPN连接，若出现类似下图所示界面，代表连接成功。

图 3-10 连接成功



步骤13 登录web客户端，使用联邦用户名和密码登录。

- 当登录页面显示认证成功时，表示成功建立VPN连接。

- 当登录页面显示认证失败时，可以根据错误信息修改对应配置。具体错误信息请参考《 故障排除 》。

----结束

结果验证

1. 打开客户端设备的命令行窗口。
2. 执行以下命令，验证连通性。

   ping 192.168.1.10

   其中，192.168.1.10为客户端需要访问的弹性云服务器的IP地址，请根据实际替换。
3. 回显如下信息，表示网络已通。

```
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=27ms TTL=245
```

