

解决方案实践

通过 VPN 构建跨境网络

文档版本 2.0
发布日期 2022-06-27



版权所有 © 华为技术有限公司 2022。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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。

目录

1 方案概述	1
2 资源和成本规划	2
3 实施步骤	3
3.1 配置 VPN.....	3
3.2 配置 CC.....	7
3.3 验证操作是否成功.....	10
4 修订记录	11

1 方案概述

应用场景

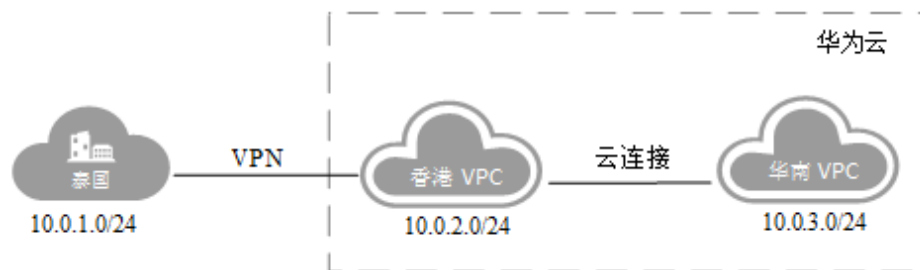
某大型跨国公司数据中心部署在泰国，云上业务部署在华为云华南区，存在云上云下业务访问诉求。该场景下如果直接将泰国本地数据中心通过虚拟专用网络VPN连接到华南区的私有虚拟云VPC，则会出现网络不稳定的问题。

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

将用户的本地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，将本地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1-1所示。

图 1-1 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

约束与限制

- 该方案只支持在华北-北京一、华北-北京四、华北-乌兰察布一、华东-上海一、华东-上海二、华南-广州、华南-深圳、西南-贵阳一、中国-香港、亚太-曼谷、非洲-约翰内斯堡、拉美-圣地亚哥部署。

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1所示，具体请参考华为云官网[价格详情](#)，实际收费以账单为准：

表 2-1 表 1 资源和成本规划

产品	配置示例	成本预估/月
虚拟私有网络	按需计费：VPN网关带宽费用20.075/小时+VPN连接费用0.36/小时，更多计费详情请参见 价格详情 。 <ul style="list-style-type: none">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	14713.2
云连接	按月计费：86000元/月，更多计费详情请参见 价格详情 。 <ul style="list-style-type: none">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	86000
合计	—	100713.2

3 实施步骤

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 > VPN网关”。
4. 在VPN网关页面，单击“创建VPN网关”。
5. 根据界面提示，如表3-1所示填写对应参数后，单击“立即购买”。

表 3-1 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

参数	说明	取值样例
计费方式	<p>按需计费支持两种计费方式：按带宽计费/按流量计费。</p> <ul style="list-style-type: none"> - 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 - 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。 	按流量计费
带宽大小	<p>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。</p> <p>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。</p> <p>可以在云监控服务中配置告警规则对带宽进行监控。</p>	100

表 3-2 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	<p>本端子网指需要通过VPN访问用户本地网络的VPC子网。</p> <p>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。</p> <p>这里填写10.0.2.0/24，10.0.3.0/24</p>	10.0.2.0/24, 10.0.3.0/24
远端网关	<p>用户本地数据中心侧的VPN网关地址</p> <p>这里填写泰国区域本地数据中心的VPN网关地址</p>	-
远端子网	<p>远端子网指需要通过VPN访问VPC的用户本地子网。</p> <p>这里填写10.0.1.0/24</p>	10.0.1.0/24

参数	说明	取值样例
预共享密钥	<p>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。</p> <p>取值范围：</p> <ul style="list-style-type: none"> - 取值长度：6~128位。 - 只能包括以下几种字符： <ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> - 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3-3和表3-4。 	自定义配置

表 3-3 IKE 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、SHA2-256、SHA2-384、SHA2-512、MD5。</p> <p>默认配置为：SHA2-256。</p>	SHA2-256
加密算法	<p>加密算法，支持的算法：AES-128、AES-192、AES-256、3DES（有安全风险不推荐）。</p> <p>默认配置为：AES-128。</p>	AES-128
DH算法	<p>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。</p> <p>默认配置为：Group 14。</p> <p>协商双方的dh算法必须一致，否则会导致协商失败。</p>	Group 14

参数	说明	取值样例
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 3-4 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
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

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”。
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3-5填写对应参数。

表 3-5 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。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
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 3-6 云连接服务标签命名规则

参数	规则
键	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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，配置参数请参见表3-7。
- 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 3-7 加载同帐号网络实例参数

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

参数	说明	取值样例
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： <ul style="list-style-type: none"> 子网：选择VPC管理的子网，这里选10.0.2.0/24 自定义网段：为了使云连接能够转发到达泰国本地数据中心的流量，此处需要增加自定义网段10.0.1.0/24 	子网：10.0.2.0/24 自定义网段：10.0.1.0/24
VGW	需要加载到云连接实例中实现网络互通的VGW名称。当类型选择虚拟网关时，需要配置此参数。	vgw-w2
VGW CIDRs	需要加载到云连接实例中，实现网络互通的VGW内的VPC和远端用户站点的网段路由。当类型参数选择虚拟网关时，需配置以下两个参数： <ul style="list-style-type: none"> VPC CIDRs 远端子网 	VPC CIDRs： 192.168.0.3/24

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”。
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3-8填写对应参数。

表 3-8 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。

参数	说明
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。

- 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。

- 登录管理控制台。
- 在系统首页，选择“网络 > 云连接”。
- 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。
- 在下拉框中选择需要查询的路由所在区域。
- 在路由信息列表中查看路由信息。

----结束

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

4 修订记录

发布日期	修改说明
2022-06-27	第二次正式发布。文档内容更新如下： <ul style="list-style-type: none">新增“资源和成本规划”章节。
2016-10-19	第一次正式发布。