



# 网络云服务 - 虚拟私有云



# 前言

- 面对日益增长的网上业务需求，企业网络面临系统上线时间长、运维成本高、安全风险大等诸多问题。越来越多的企业开始基于华为虚拟私有云（VPC）服务建设网上业务。
- 华为虚拟私有云（VPC）是华为云网络的基础，它基于安全的隧道网络技术，为您提供安全、隔离的网络环境。本章主要讲述华为VPC服务。



# 目标

- 学完本课程后，您将能够：
  - 了解华为云服务中虚拟私有云服务产品
  - 掌握虚拟私有云服务的概念、功能和场景
  - 掌握虚拟私有云的创建和管理



# 目录

- 1. VPC 简介**
2. VPC概念
3. VPC场景
4. VPC使用管理
5. VPC常见问题及故障
6. VPC和其他云服务配合使用

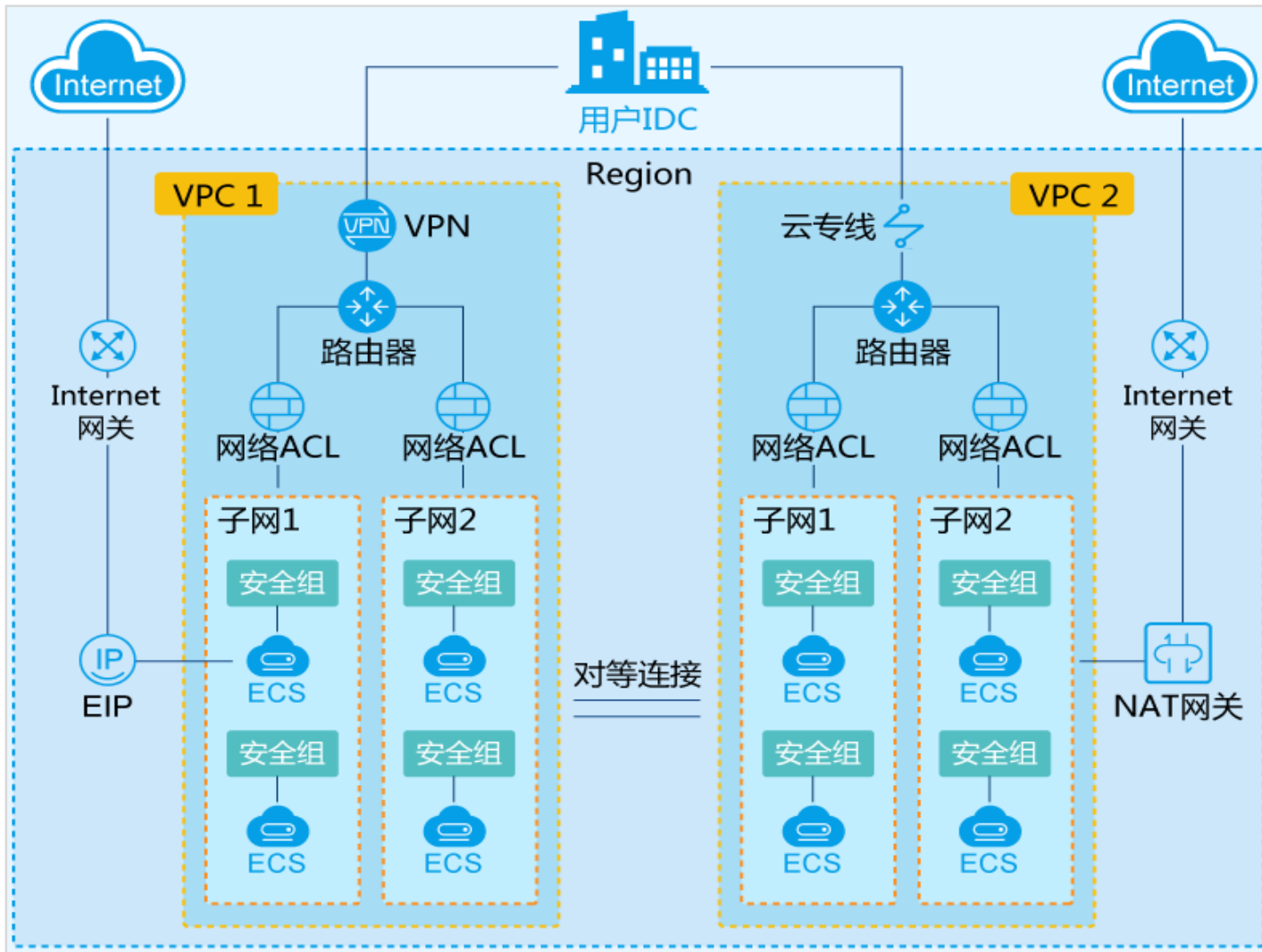


## VPC概念

- 虚拟私有云（Virtual Private Cloud）为用户在华为公有云上轻松构建隔离的虚拟网络环境。用户可以完全掌控自己的虚拟网络，包括申请弹性带宽/IP、创建子网、配置DHCP、设置安全组等。



# VPC产品架构





# VPC产品优势



## 安全可靠

云上私有网络，租户之间100%隔离，VPC能够支持跨AZ部署ECS实例



## 高速访问

全动态BGP高速接入华为云，云上业务访问更流畅



## 灵活配置

网络规划自主管理，操作简单，轻松自定义网络部署

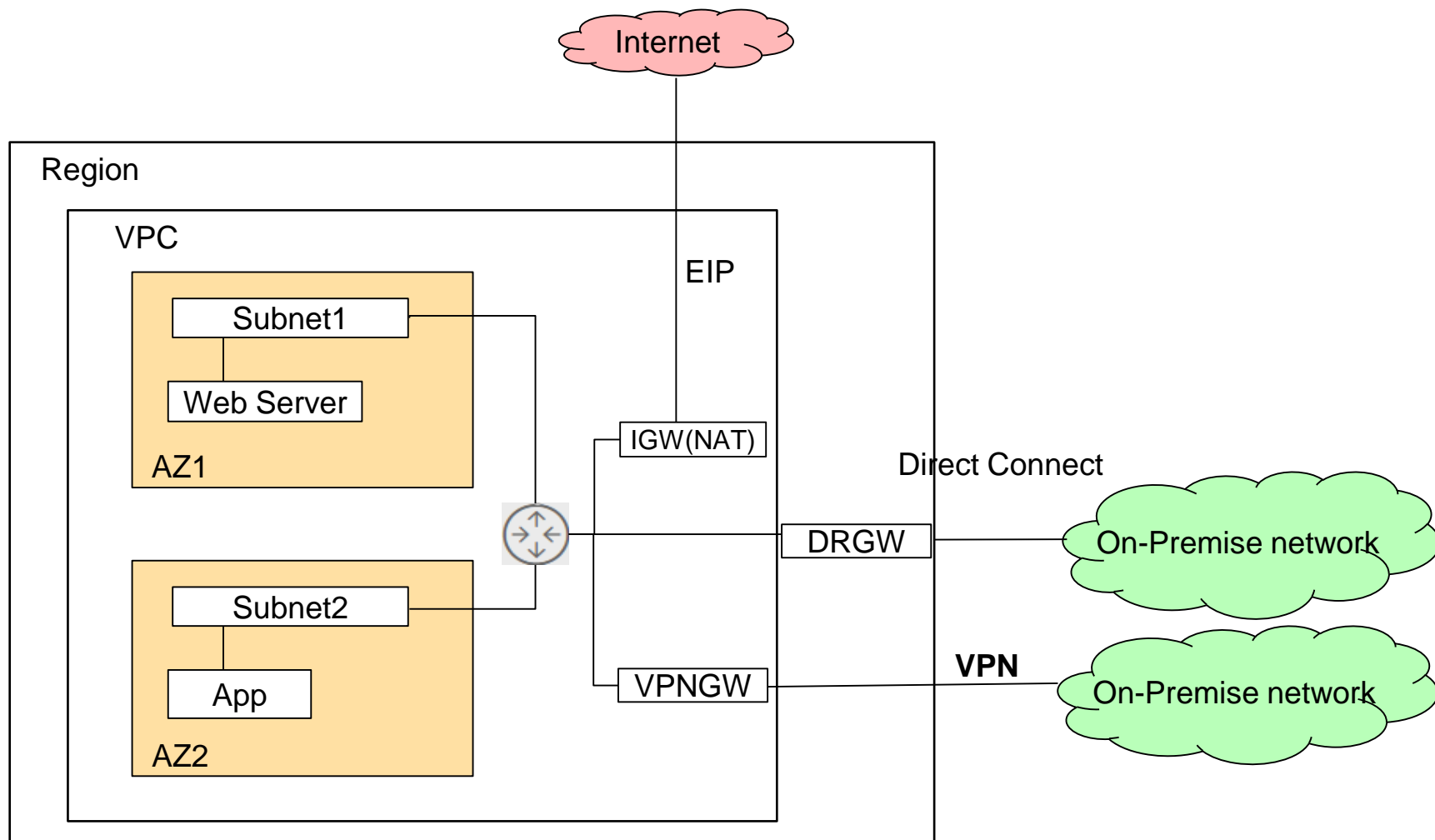


## 互联互通

华为云在安全隔离基础上，支持客户灵活配置VPC之间互联互通



# VPC应用场景 - 大型互联网应用







# VPC应用场景

- **通用性WEB应用**

- 适用场景：博客、简单的网站等。
- 场景特点：像使用普通网络一样，在VPC中托管Web应用或网站，也可以创建一个子网，在子网中启动云服务器，为云服务器申请弹性公网IP来联通Internet，对外提供Web服务。

- **企业混合云**

- 适用场景：电子商务类网站。
- 场景特点：通过VPN在传统数据中心与VPC之间建立通信隧道，可轻松实现企业的混合云架构，从而方便地使用云端的云服务器、块存储等资源，例如启动额外的Web服务器提升业务负载能力。

- **高安全业务系统**

- 适用场景：高安全业务系统。
- 场景特点：可通过安全组来控制多层Web应用之间的访问控制策略，例如：可以创建一个VPC，将WEB服务器和数据库服务器划分到不同的安全组中。WEB服务器所在的子网实现互联网访问，而数据库服务器只能通过内网访问，保护数据库服务器的安全，满足高安全场景。



# VPC功能描述

- **自由定义私有网络**

您可以在VPC内定义私有的子网， 根据需要将应用程序和其他服务部署在对应的子网下。

- **灵活配置安全策略**

使用安全组功能，将VPC中的弹性云服务器划分成不同的安全域，并为每个安全域定义不同的访问控制规则。使用网络ACL功能，对子网进行防护，控制进出子网的流量。

- **绑定弹性公网IP**

您可以申请独立的弹性公网IP地址。弹性公网IP可以按需绑定到弹性云服务器上，绑定和解绑操作都即时生效。

- **云专线/VPN接入**

在有需要的情况下，用户可通过VPN或者云专线方式，将VPC与传统数据中心互联互通，组建混合网络，助力应用的平滑迁移上云。



# 目录

1. VPC简介
- 2. VPC概念**
3. VPC场景
4. VPC使用管理
5. VPC常见问题及故障
6. VPC和其他云服务配合使用



# VPC相关概念

- 子网
- 弹性公网IP
- 带宽
- 安全组
- VPN
- 远端网关
- 远端子网



# 目录

1. VPC简介
2. VPC概念
- 3. VPC场景**
4. VPC使用管理
5. VPC常见问题及故障
6. VPC和其他云服务配合使用



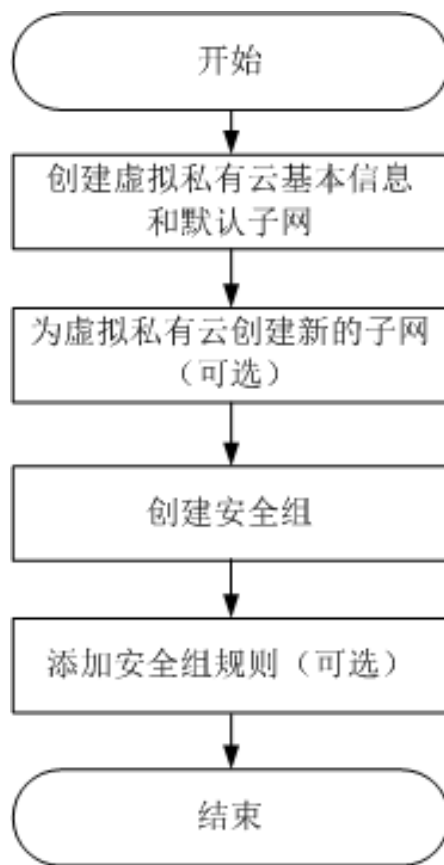
## VPC典型场景

- 配置无需访问公网的弹性云服务器的VPC
- 配置通过弹性公网IP访问公网的弹性云服务器的VPC
- 配置通过VPN访问公网的弹性云服务器的VPC



## VPC配置流程 (1/2)

当弹性云服务器无需访问公网时，例如用于搭建网站的数据库节点或服务器节点的弹性服务器无需连接公网，虚拟私有云的配置流程如下。





## VPC配置流程 (2/2)

任务	说明	可选/必选
01 创建VPC和默认子网	该任务是创建一个完整的虚拟私有云的第一步。 创建虚拟私有云的基本信息及默认子网后还需要根据您的实际网络需求，继续创建虚拟私有云中的其他网络资源。	必选任务
02 创建新的子网	当虚拟私有云除了创建的默认子网还需要添加其他子网时，可以通过创建新的子网来为VPC增加用户自己的私有网络。 此处创建的子网就是创建弹性云服务器时添加的网卡。	可选任务
03 创建安全组	您可以创建安全组，将虚拟私有云中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。 创建安全组成功后，具备默认的访问规则。默认规则是在出方向上的数据报文全部放行，安全组内的云服务器无需添加规则即可互相访问。当默认访问规则可以满足需求时，则无需单独再为该安全组添加安全组规则。	必选任务
04 添加安全组规则	安全组创建成功后，具备默认的访问规则。默认规则是在出方向上的数据报文全部放行，安全组内的云服务器无需添加规则即可互相访问。当默认访问规则可以满足需求时，则无需单独再为该安全组添加安全组规则。	可选任务





# 目录

1. VPC简介
2. VPC概念
3. VPC场景
- 4. VPC使用管理**
5. VPC常见问题及故障
6. VPC和其他云服务配合使用



# 常用操作

- VCP常用操作
- 安全组常用操作
- 弹性公网IP常用操作



# VPC常用操作

- 创建虚拟私有云基本信息及默认子网
- 修改虚拟私有云基本信息
- 为虚拟私有云创建新的子网
- 修改子网网络信息
- 删除虚拟私有云



# VPC创建操作

- **操作场景**

虚拟私有云可以为您的弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。要拥有一个完整的虚拟私有云，第一步先创建虚拟私有云的基本信息及默认子网；然后再根据实际网络需求，创建子网、申请弹性公网IP、安全组、VPN等网络资源。

- **操作步骤**

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



# VPC创建界面

创建虚拟私有云 ?

< 返回虚拟私有云列表

基本信息

区域

华北-北京一

不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

\* 名称

vpc-2644

\* 网段

192 · 168 · 0 · 0 / 16

建议使用网段：10.0.0.0/8~24，172.16.0.0/12~24，192.168.0.0/16~24

企业项目 ?

-请选择企业项目-

标签

如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。[查看预定义标签](#)

标签键

标签值

您还可以添加10个标签。

子网配置

默认子网

可用区 ?

可用区1

可用区2

可用区3

\* 名称

subnet-264b

\* 子网网段

192 · 168 · 0 · 0 / 24

立即创建



# VPC配置参数

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	华北-北京一
名称	VPC名称。	VPC-001
网段	VPC的地址范围，VPC内的子网地址必须在VPC的地址范围内。 目前支持网段范围：10.0.0.0/8~24、172.16.0.0/12~24、192.168.0.0/16~24	192.168.0.0/16
企业项目	VPC归属的企业项目，默认归属于Default项目。	Default
标签	虚拟私有云的标示，包括键和值。可以为虚拟私有云创建10个标签。	•键：vpc_key1 •值：vpc-01
子网名称	子网的名称。	Subnet
子网网段	子网的地址范围，需要在VPC的地址范围内。	192.168.0.0/24
网关	子网的网关。	192.168.0.1
DNS服务器地址	默认情况下使用网络外部DNS服务器地址，如果需要修改DNS服务器地址，请确保配置的DNS服务器地址可用。	192.168.1.0
子网标签	子网的标示，包括键和值。可以为子网创建10个标签。	•键：subnet_key1 •值：subnet-01



# VPC子网创建操作

## ● 操作场景

申请VPC时会创建一个子网，当该VPC还需要添加其他子网时，可以通过创建新的子网来为VPC增加用户自己的私有网络。

## ● 操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。
3. 在左侧导航树选择要创建子网的虚拟私有云。
4. 在“子网”界面，单击“创建子网”。
5. 在“创建子网”下拉区域，根据界面提示配置参数。
6. 单击“确定”。



# VPC子网创建界面

创建子网

★ 可用区 ?

可用区1

★ 名称

subnet-716f

★ 子网网段

192 · 168 · 0 · 0 / 24

可用网段: 192.168.0.0/16

可用IP数:250 子网创建完成后,子网网段无法修改

高级配置

默认配置

自定义配置

确定

取消





# VPC子网配置参数

参数	说明	取值样例
子网名称	子网的名称。	Subnet
子网网段	子网的地址范围，需要在VPC的地址范围内。	192.168.0.0/24
网关	子网的网关。	192.168.0.1
DNS服务器地址	默认情况下使用网络外部DNS服务器地址，如果需要修改DNS服务器地址，请确保配置的DNS服务器地址可用。	192.168.1.0
子网标签	子网的标示，包括键和值。可以为子网创建10个标签。	•键：subnet_key1 •值：subnet-01



# 安全组常用操作

- 创建安全组基本信息
- 为安全组添加安全组规则
- 删除安全组规则
- 删除安全组



# VPC创建安全组操作

## ● 操作场景

VPC内的安全组默认不允许任何源访问，因此如果需要使用VPN让云上云下设备互通，则需要在配置改VPC的安全组规则，允许对端VPN设备访问该VPC。

## ● 操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。
3. 在左侧导航树选择“安全组”。
4. 在“安全组”界面，单击“创建安全组”。
5. 在“创建安全组”下拉区域，根据界面提示配置参数。
6. 单击“确定”。

The screenshot shows a 'Create Security Group' (创建安全组) dialog box. It contains the following fields:

- 名称 (Name):** A text input field containing 'sg-d4e0'.
- 企业项目 (Enterprise Project):** A dropdown menu with a question mark icon and a refresh icon. The text inside is '-请选择企业项目-'.
- 描述 (Description):** A large text area for entering a description, currently empty.

At the bottom right of the description area, the character count '0/255' is displayed. At the bottom of the dialog, there are two buttons: '确定' (Confirm) in a red box and '取消' (Cancel) in a white box.



# VPC创建安全组规则 (1/2)

## • 操作场景

安全组创建成功后，即具备默认的安全组规则。您可以自定义添加新的出方向、入方向安全组规则。

入方向：指从外部访问安全组规则下的弹性云服务器。

出方向：指安全组规则下的弹性云服务器访问安全组外的实例。

## • 默认安全组规则

方向	协议	端口范围	目的地址/源地址	说明
出方向	All	All	目的地址：0.0.0.0/0	允许所有出站流量的数据报文通过。
入方向	All	All	源地址：当前安全组 ID (例如：sg-xxxxx)	仅允许安全组内的弹性云服务器彼此通信，丢弃其他入站流量的全部数据报文。
入方向	TCP	22	源地址：0.0.0.0/0	允许所有IP地址通过SSH远程连接到Linux弹性云服务器。
入方向	TCP	3389	源地址：0.0.0.0/0	允许所有IP地址通过RDP远程连接到Windows弹性云服务器。



## VPC创建安全组规则 (2/2)

- **操作步骤**

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



# VPC创建安全组规则界面

### 添加入方向规则 ②

安全组 **sg-cce7**

协议/应用	端口和源地址	描述	操作
<div>TCP</div>	<div>端口<div>例如：22或22-30</div></div> <div>源地址<div>IP地址<div>0 . 0 . 0 . 0 / 0</div></div></div>		<div></div> <div>复制 删除</div>

+

 增加1条规则 您还可以增加9条规则

确定

取消

### 添加出方向规则 ②

安全组 **sg-cce7**

协议/应用	端口和目的地址	描述	操作
<div>TCP</div>	<div>端口<div>例如：22或22-30</div></div> <div>目的地址<div>IP地址<div>0 . 0 . 0 . 0 / 0</div></div></div>		<div></div> <div>复制 删除</div>

+

 增加1条规则 您还可以增加9条规则

确定

取消



# VPC创建安全组规则参数

参数	说明	取值样例
协议	网络协议。	TCP
端口和源地址（入方向）	端口：安全组规则的端口范围，取值范围为：1 ~ 65535。	22或22-30
	源地址：可以是IP地址，也可以是安全组。例如： xxx.xxx.xxx.xxx/32（IPv4地址） xxx.xxx.xxx.0/24（子网） 0.0.0.0/0（任意地址）	0.0.0.0/0 default
端口和目的地址（出方向）	端口：安全组规则的端口范围，取值范围为：1 ~ 65535。	22或22-30
	源地址：可以是IP地址，也可以是安全组。例如： xxx.xxx.xxx.xxx/32（IPv4地址） xxx.xxx.xxx.0/24（子网） 0.0.0.0/0（任意地址）	0.0.0.0/0 default
描述	安全组的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-



# 弹性公网IP常用操作

- 为弹性云服务器申请和绑定弹性公网IP
- 查询和修改带宽





# 申请和绑定弹性公网IP (1/3)

- **操作场景**

可以通过申请弹性公网IP并将弹性公网IP绑定到弹性云服务器上，实现弹性云服务器访公网的目的。

- **操作步骤**

## 申请弹性IP

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。
3. 在左侧导航树，单击“弹性公网IP”。
4. 在“弹性公网IP”界面，单击“购买弹性公网IP”。
5. 根据界面提示配置参数。
6. 单击“立即购买”。



# 申请和绑定弹性公网IP (2/3)

购买弹性公网IP ?

< 返回弹性公网IP列表

计费模式

包年/包月

按需计费

区域

华北-北京一

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。

类型

全动态BGP

静态BGP

IPv6转换 ?

关闭

开启

公测期间IPv6转换功能免费。

带宽类型

独享带宽

计费方式

按带宽计费

带宽大小 (Mbit/s)

1

100

200

300

500

1,000

2,000

5

Anti-DDoS流量清洗服务可以为华为云内资源提供网络层和应用层的DDoS攻击防护和攻击实时告警通知。[了解更多 提升防护能力](#)

带宽名称

bandwidth-e42b

企业项目 ?

-请选择企业项目-

标签

如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。[查看预定义标签](#)

弹性公网IP费用 ¥0.00 + 带宽费用 ¥115.00

参考价格，具体扣费请以账单为准。[了解计费详情](#)

立即购买



# 申请和绑定弹性公网IP (3/3)

## 绑定弹性公网IP

1. 在“弹性公网IP”界面待绑定弹性公网IP地址所在行，单击“绑定”。
2. 选择实例。
3. 单击“确定”。

<input type="checkbox"/> 弹性公网IP/ID	状态 ▾	类型	带宽 ▾	带宽详情 ▾	已绑定实例 ▾	计费模式 ▾	企业项目	操作
<input type="checkbox"/> 10.154.121.111 8dea6d0f-4ebf-4521-bb04-51b76f11a8...	未绑定	全动态BGP	ecs-4disk-12nic-65eip-fileInject-Group...	按带宽计费 65 Mbit/s	-	按需 2018/11/27 18:26:04 创建	3333	<a href="#">绑定</a> <a href="#">解绑</a> <a href="#">更多 ▾</a>



# 查询和修改带宽 (1/2)

- **操作场景**

查看弹性公网IP的带宽，修改带宽的名称、大小等参数。

- **操作步骤**

1. 登录管理控制台。
2. 在系统首页，单击“网络 > 虚拟私有云”。
3. 在左侧导航树，单击“弹性公网IP”。
4. 在“操作”列，选择“修改带宽”。
5. 根据界面提示修改带宽参数。
6. 单击“确定”。



# 查询和修改带宽 (2/2)

修改带宽

[返回弹性公网IP列表](#)

当前配置

带宽名称	bandwidth-tj98	弹性公网IP	117.78.36.251
带宽大小 (Mbit/s)	1	计费方式	按带宽计费
带宽类型	独享		

变更规格

带宽名称

bandwidth-tj98

计费方式

按带宽计费

按流量计费

带宽大小 (Mbit/s)

1

100

200

300

500

1,000

2,000

1

变更后费用 **¥0.063**/小时

参考价格，具体扣费请以账单为准。[了解计费详情](#)

下一步



# 目录

1. VPC简介
2. VPC概念
3. VPC场景
4. VPC使用管理
- 5. VPC常见问题及故障**
6. VPC和其他云服务配合使用



# VPC使用常见问题

- **VPC是否收费？**

VPC本身不收取费用。但用户在使用带宽或VPN时需要按照收费标准购买。

- **VPC中可以使用哪些网段（CIDR）？**

当前VPC支持的网段有：10.0.0.0/8~24，172.16.0.0/12~24，192.168.0.0/16~24

- **子网间是否可以通信？**

子网属于VPC的资源，一个VPC内的子网可以通信，不同VPC的子网默认不能进行通信，可以通过创建对等连接使不同VPC的子网通信。

- **子网的网段是否可以修改？**

子网创建好后，网段不能进行修改。

- **子网的限额是多少？**

一个租户可以创建100个子网，如果无法满足实际需求，可以提工单申请扩容。

- **带宽的限速范围是多少？**

带宽的限速范围为1Mbit/s~2000Mbit/s。

- **带宽的类型有哪些？**

带宽支持独享和共享两种类型。独享带宽只能针对一个弹性IP进行限速，共享带宽可以针对多个弹性IP进行集中限速。



# 目录

1. VPC简介
2. VPC概念
3. VPC场景
4. VPC使用管理
5. VPC常见问题及故障
- 6. VPC和其他云服务配合使用**





# VPC和其他服务

- **弹性云服务器**

VPC为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。提供多种方式连接弹性云服务器与Internet。同时，用户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

- **弹性负载均衡**

弹性负载均衡需要使用虚拟私有云服务创建的弹性公网IP、带宽。

- **云监控**

当用户开通了虚拟私有云服务后，无需额外安装其他插件，即可在云监控查看对应服务的实例状态。

- **云审计**

通过云审计，您可以记录与虚拟私有云相关的操作事件，便于日后的查询、审计和回溯。



## 思考题

华为公有云VPC提供哪些网络功能（ ）？

- A. 自定义网段划分
- B. 自定义控制访问策略
- C. 支持EIP接入公网
- D. 支持VPN/云专线接入本地数据中心



## 本章总结

- 描述了华为云服务中VPC服务产品
- 讲解了VPC服务的概念、功能、场景
- 讲解了VPC服务的创建和管理



## 学习推荐

- **华为Learning网站**

<http://support.huawei.com/learning/Index!toTrainIndex>

- **华为公有云服务网站**

<https://www.huaweicloud.com> (中国站)



## 缩略语

缩写	全称	释义
AZ	Availability Zone	可用区
BGP	Border Gateway Protocol	边界网关协议
DNS	Domain Name Server	网域名称服务器
EIP	Elastic Internet Protocol	弹性公网IP
IPSec	Internet Protocol Security	互联网协议安全协议
VPN	Virtual Private Network	虚拟专用网络
IGW	Integration Gateway	集成网关
NAT	Network Address Translation	网络地址转换

The background of the slide features a blue-tinted image of several business professionals in a modern office setting. They are standing on a highly reflective floor, and their silhouettes are clearly visible. The individuals are engaged in various interactions, some holding documents or tablets, suggesting a collaborative work environment. The overall aesthetic is professional and corporate.

谢谢

[www.huawei.com](http://www.huawei.com)