AWS Academy Cloud Foundations

模块 5：联网和内容分发

aws academy

模块概览

主题

- 联网基础知识
- Amazon VPC
- VPC 联网
- VPC 安全

活动

- 标记网络图
- 设计基本的 VPC 架构

演示

- VPC 演示

实验

- 构建 VPC 并启动 Web 服务器

知识测验

模块目标

完成本模块后，您应能够：

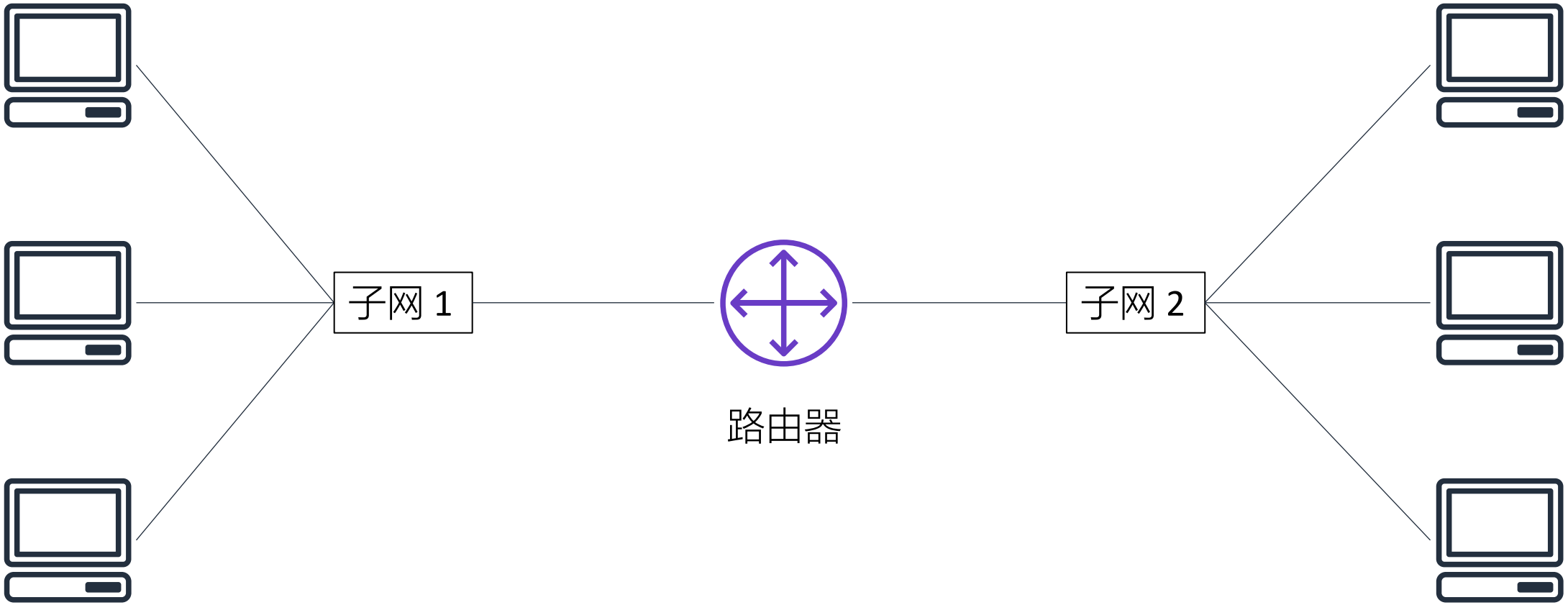
- 了解联网基础知识
- 描述如何在云中使用 Amazon VPC 建立虚拟网络
- 标记网络图
- 设计基本的 VPC 架构
- 指出构建 VPC 的步骤
- 识别安全组
- 创建您自己的 VPC 并向其添加其他组件，以生成自定义网络

模块 5：联网和内容分发

第 1 部分：联网基础知识

aws academy

网络



IP 地址

192 . 0 . 2 . 0

11000000 . 00000000 . 00000010 . 00000000

IPv4 和 IPv6 地址

IPv4（32 位）地址：192.0.2.0

IPv6（128 位）地址：2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

无类别域间路由 (CIDR)

网络标识符（路由前缀）

主机标识符

192 . 0 . 2 . 0 / 24

表明多少位是固定的

11000000 00000000 00000010 00000000 到 11111111

固定 固定 固定 灵活

开放系统互联 (OSI) 模型

层	数字	函数	协议/地址
应用层	7	应用程序访问计算机网络的方式	HTTP(S)、FTP、DHCP、LDAP
表示层	6	• 确保应用程序层可以读取数据 • 加密	ASCI、ICA
会话层	5	支持有序数据交换	NetBIOS、RPC
传输层	4	提供协议以支持主机到主机通信	TCP、UDP
网络层	3	路由和数据包转发（路由器）	IP
数据链路层	2	在同一 LAN 网络（集线器和交换机）中传输数据	MAC
物理层	1	通过物理介质传输和接收原始比特流	信号（1 和 0）

模块 5：联网和内容分发

第 2 部分：Amazon VPC

aws academy

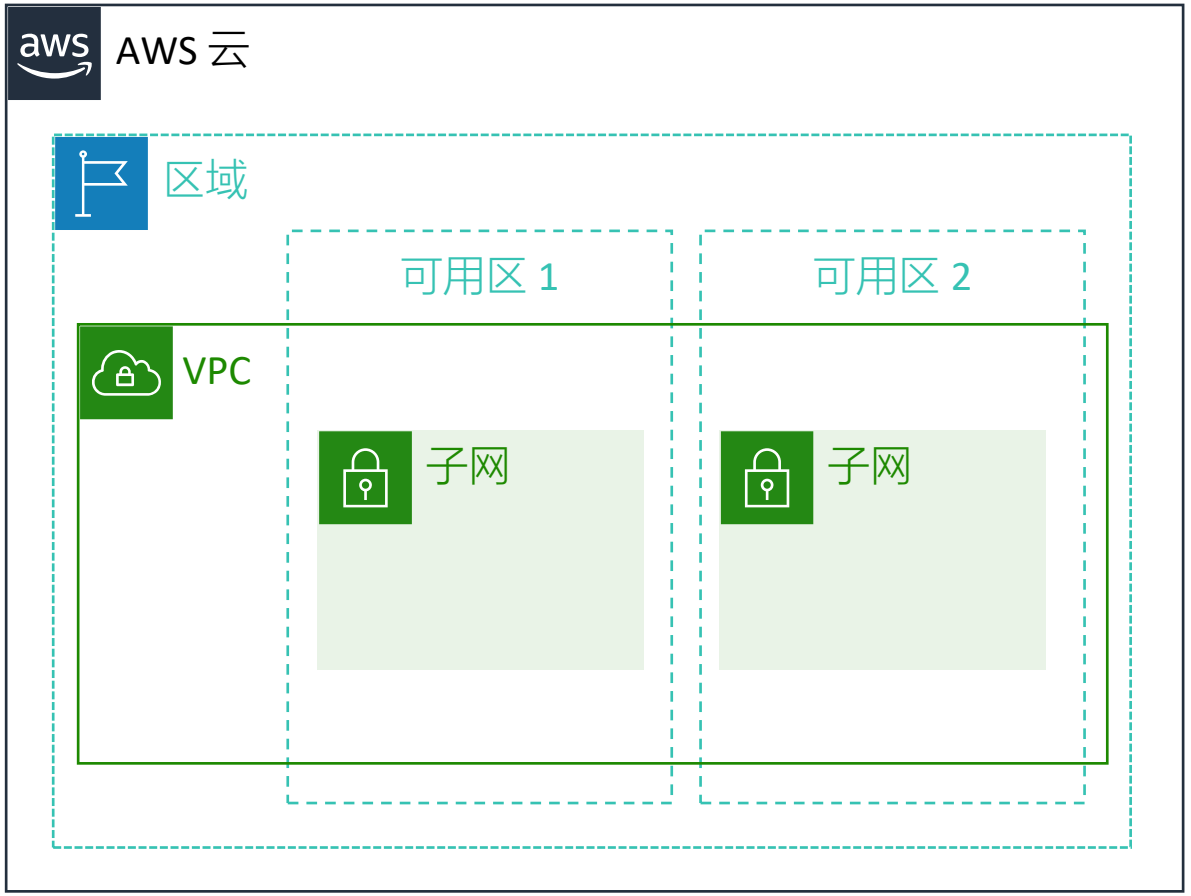
Amazon VPC

Amazon VPC

- 可让您在 AWS 云中预置一个**逻辑上隔离**的部分，从而在您自己定义的虚拟网络中启动 AWS 资源
- 您可以**控制您的虚拟联网资源**，包括：
  - IP 地址范围选择
  - 子网创建
  - 路由表和网络网关配置
- 可让您为自己的 VPC **自定义网络配置**
- 可让您使用**多个安全层**

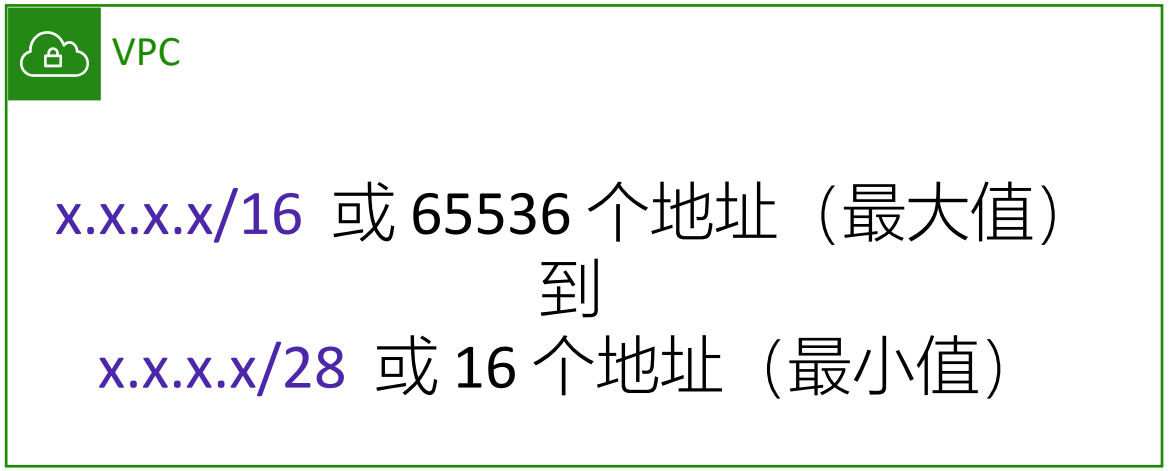
VPC 和子网 (Subnets)

- VPC：
  - 从逻辑上与其他 VPC 隔离
  - 专用于您的 AWS 账户
  - 属于单个 **AWS 区域**并可跨越多个可用区
- 子网：
  - 划分 **VPC 的** IP 地址范围
  - 属于单个可用区
  - 划分为公有 或 私有



IP 寻址 (Addressing)

- 创建 VPC 时，您应将其分配至一个 IPv4 **CIDR 块**（一系列**私有** IPv4 地址）。
- 创建 VPC 后，您**不能更改地址范围**。
- 最大的 **IPv4 CIDR 块大小为** /16。
- 最小的 **IPv4 CIDR 块大小为** /28。
- 也支持 IPv6（具有不同的块大小限制）。
- 子网的 CIDR 块**不能重叠**。



预留 IP 地址 (Reserved IP Addresses)

示例：IPv4 CIDR 块为 10.0.0.0/16 的 VPC 总共有 65536 个 IP 地址。VPC 有四个大小相同的子网。每个子网只能使用 251 个 IP 地址。

CIDR 块 10.0.0.0/24 的 IP地址	预留以用于
10.0.0.0	网络地址
10.0.0.1	内部通信
10.0.0.2	域名系统 (DNS) 解析
10.0.0.3	未来使用
10.0.0.255	网络广播地址

公有 IP 地址类型

公有 IPv4 地址

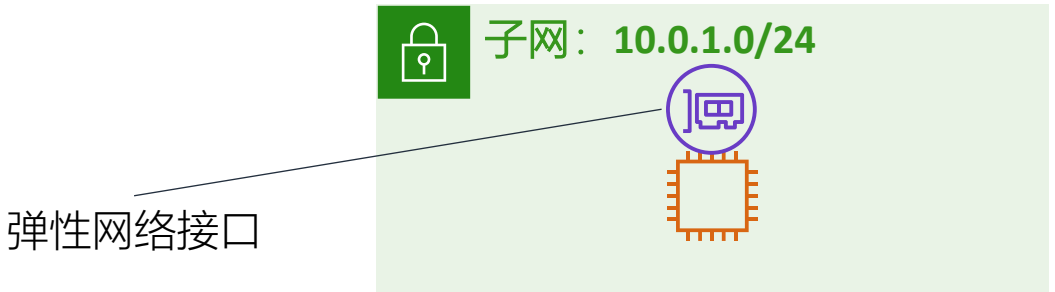
- 通过弹性 IP 地址手动分配
- 通过子网级别的自动分配公有 IP 地址设置自动分配

弹性 IP 地址

- 与 AWS 账户相关联
- 可以随时分配和重新映射
- 可能需要额外付费

弹性网络接口 (Elastic network interface)

- 弹性网络接口是一种**虚拟网络接口**，您可以将其：
  - 连接到实例。
  - 从实例中分离，然后连接到其他实例以重定向网络流量。
- 将其重新连接到新实例时，其**属性也随之附加到新实例**。
- 您的 VPC 中的每个实例都有一个**默认的网络接口**，该接口分配有一个在您的 VPC IPv4 地址范围内的私有 IPv4 地址。



路由表和路由 (Route tables and routes)

- 路由表包含一组规则（或路由），您可以将其配置为定向来自子网的网络流量。
- 每个路由都会指定一个目的地和一个目标。
- 默认情况下，每个路由表都包含用于在 VPC 内部进行通信的本地路由。
- 每个子网必须与一个路由表关联（最多一个）。

主（默认）路由表

目的地	目标
10.0.0.0/16	本地

VPC CIDR 块

第 2 部分要点

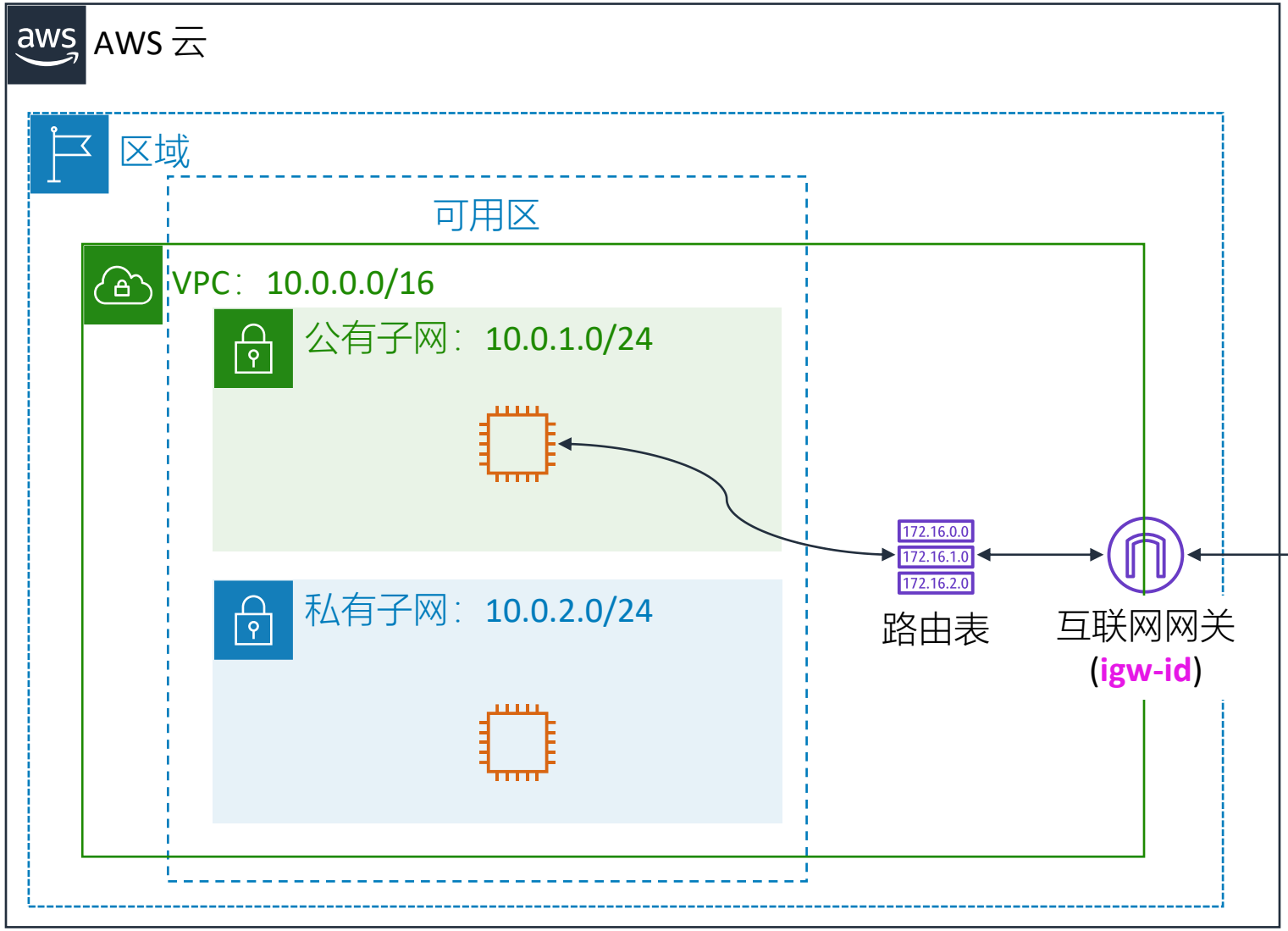
- VPC 是 AWS 云的逻辑隔离部分。
- VPC 属于一个区域，并且需要一个 CIDR 块。
- VPC 会划分为子网。
- 子网属于一个可用区，并且需要一个 CIDR 块。
- 路由表控制子网的流量。
- 路由表具有内置的本地路由。
- 您可向表中添加其他路由。
- 本地路由不能删除。

模块 5：联网和内容分发

第 3 部分：VPC 联网

aws academy

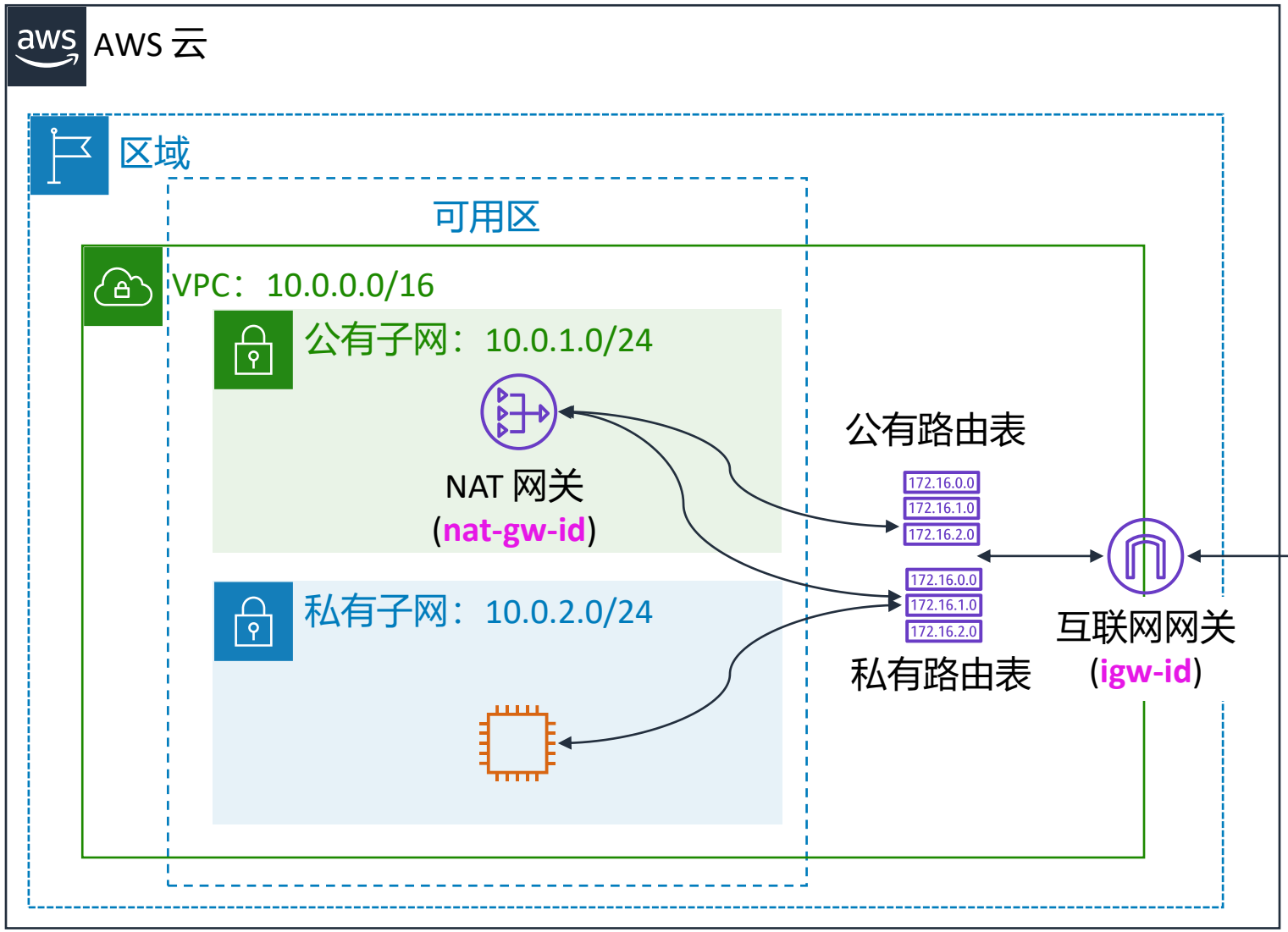
互联网网关 (Internet gateway)



公有子网路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	igw-id

网络地址转换 网关 (NAT gateway)



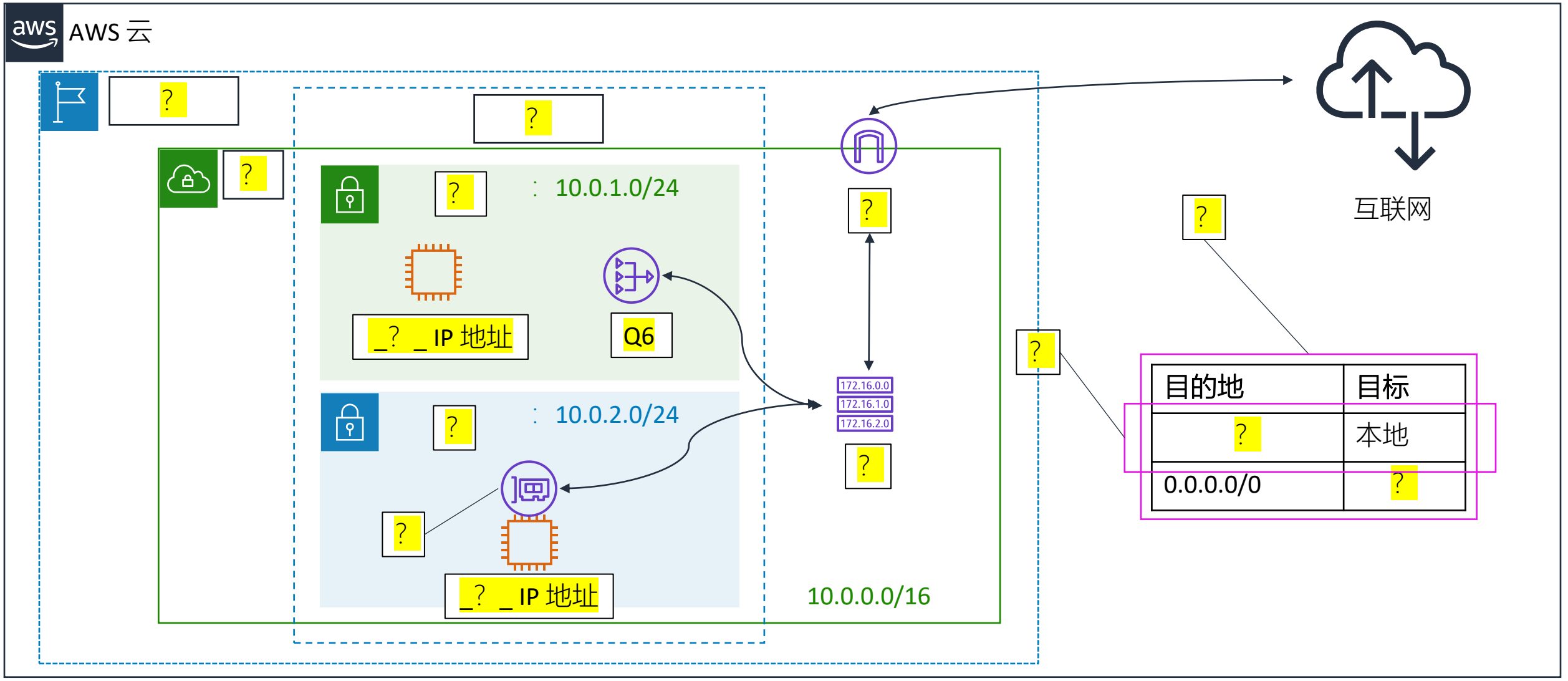
公有子网路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	igw-id

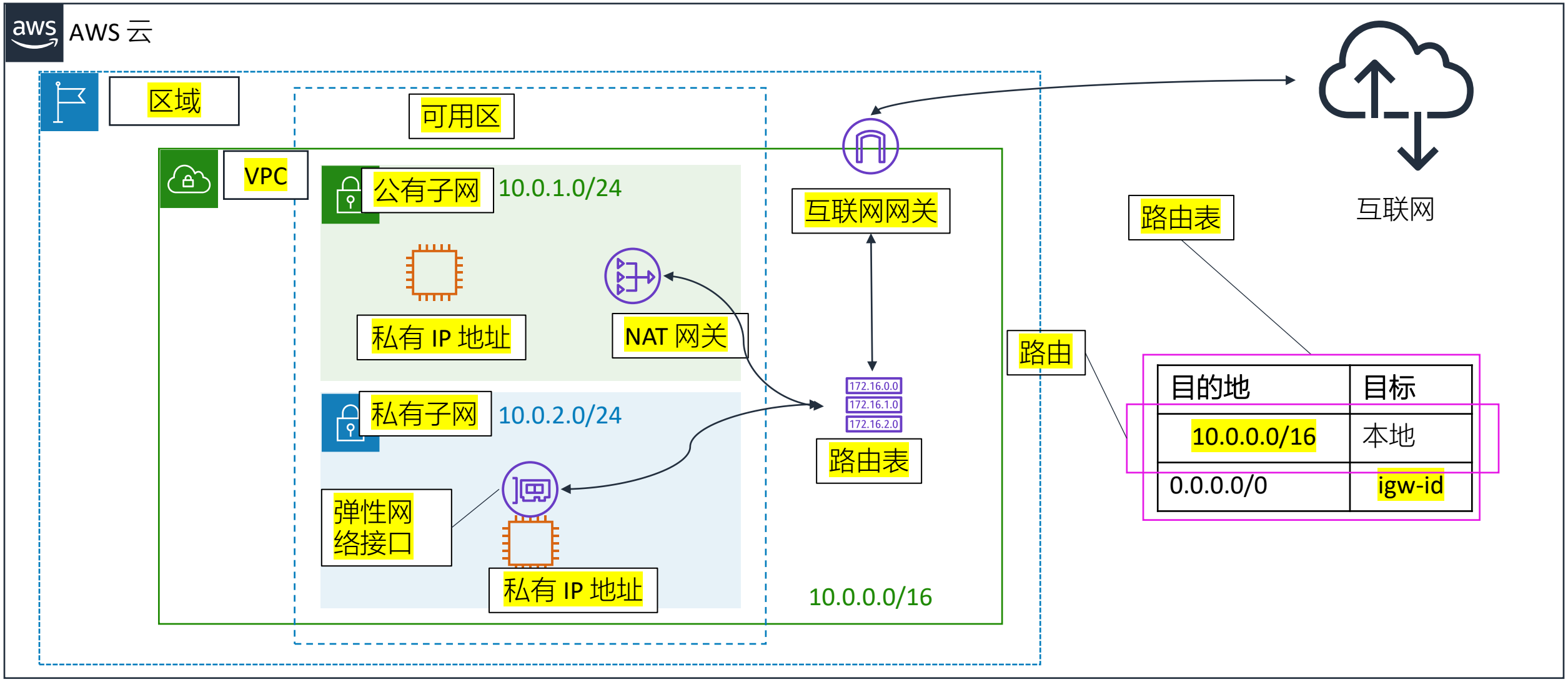
私有子网路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	nat-gw-id

活动：标记此网络图


AWS 云
?
?
?
?
: 10.0.1.0/24
?
_? _ IP 地址
Q6
: 10.0.2.0/24
?
?
_? _ IP 地址
10.0.0.0/16
?
?
172.16.0.0
172.16.1.0
172.16.2.0
?
?
互联网
?
目的地
目标
?
本地
0.0.0.0/0
?

活动：解决方案


AWS 云
区域
可用区
VPC
公有子网
10.0.1.0/24
私有 IP 地址
NAT 网关
私有子网
10.0.2.0/24
弹性网络接口
私有 IP 地址
10.0.0.0/16
互联网网关
路由表
172.16.0.0
172.16.1.0
172.16.2.0
路由
互联网
路由表
目的地
目标
10.0.0.0/16
本地
0.0.0.0/0
igw-id

第 3 部分要点

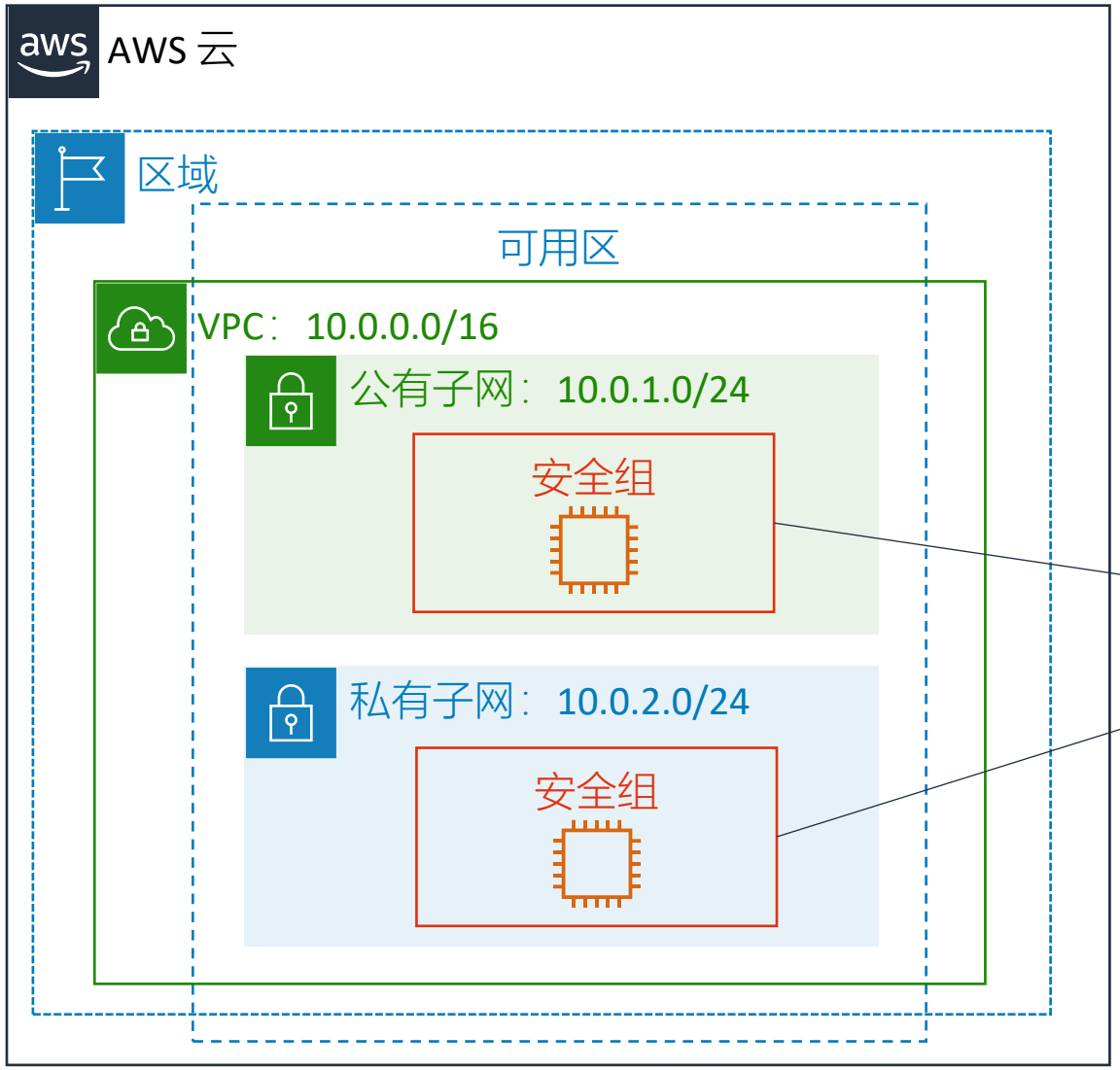
- VPC 联网选项包括：
  - 互联网网关
  - NAT 网关
  - VPC 终端节点

模块 5：联网和内容分发

第 4 部分：VPC 安全性

aws academy

安全组 (Security Group)



安全组在**实例级别**运行。

安全组

入站				
类型	协议	端口范围	源	描述
所有流量	全部	全部	sg-xxxxxxxx	
出站				
类型	协议	端口范围	源	描述
所有流量	全部	全部	sg-xxxxxxxx	

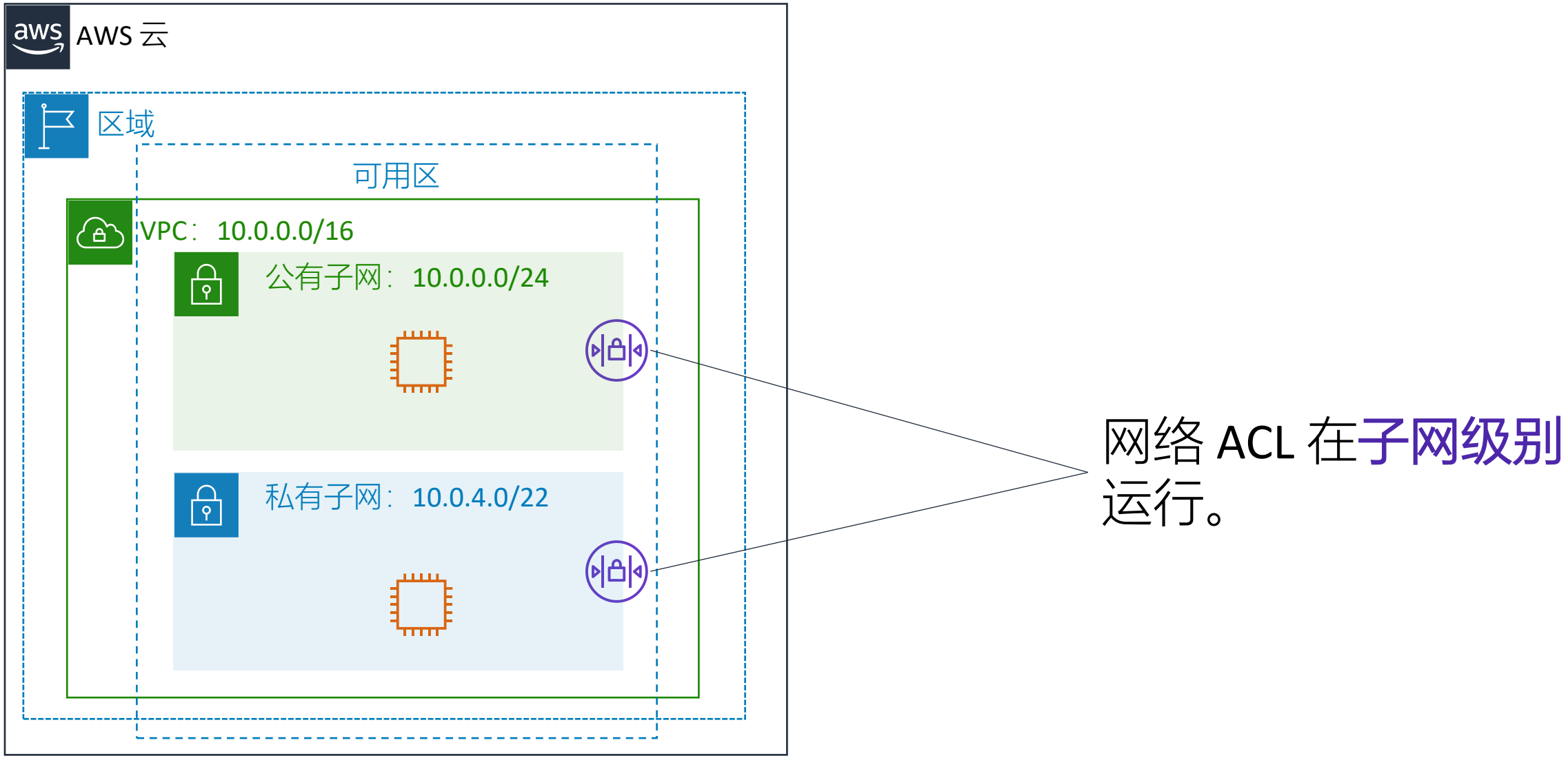
- 安全组具有控制实例入站和出站流量的 规则。
- 默认安全组拒绝所有入站流量，允许所有出站 流量。
- 安全组是有状态的 **(Stateful)**。

自定义安全组

入站				
类型	协议	端口范围	源	描述
HTTP	TCP	80	0.0.0.0/0	所有 Web 流量
HTTPS	TCP	443	0.0.0.0/0	所有 Web 流量
SSH	TCP	22	54.24.12.19/32	办公地址
出站				
类型	协议	端口范围	源	描述
所有流量	全部	全部	0.0.0.0/0	
所有流量	全部	全部	::/0	

- 您可以**指定“允许”**规则，但不可以指定“拒绝”规则。
- **在决定允许流量之前**评估所有规则。

网络访问控制列表（ACL: Access Control List）



网络 ACL 在子网级别运行。

网络 ACL

入站					
规则编号	类型	协议	端口范围	源	允许/拒绝
100	所有 IPv4 流量	全部	全部	0.0.0.0/0	允许
*	所有 IPv4 流量	全部	全部	0.0.0.0/0	拒绝
出站					
规则编号	类型	协议	端口范围	源	允许/拒绝
100	所有 IPv4 流量	全部	全部	0.0.0.0/0	允许
*	所有 IPv4 流量	全部	全部	0.0.0.0/0	拒绝

- 网络 ACL 有**单独的入站和出站规则**，每项规则都可以**允许或拒绝流量**。
- **默认**网络 ACL **允许**所有入站和出站 IPv4 流量。
- 网络 ACL **没有状态 (Stateless)**。

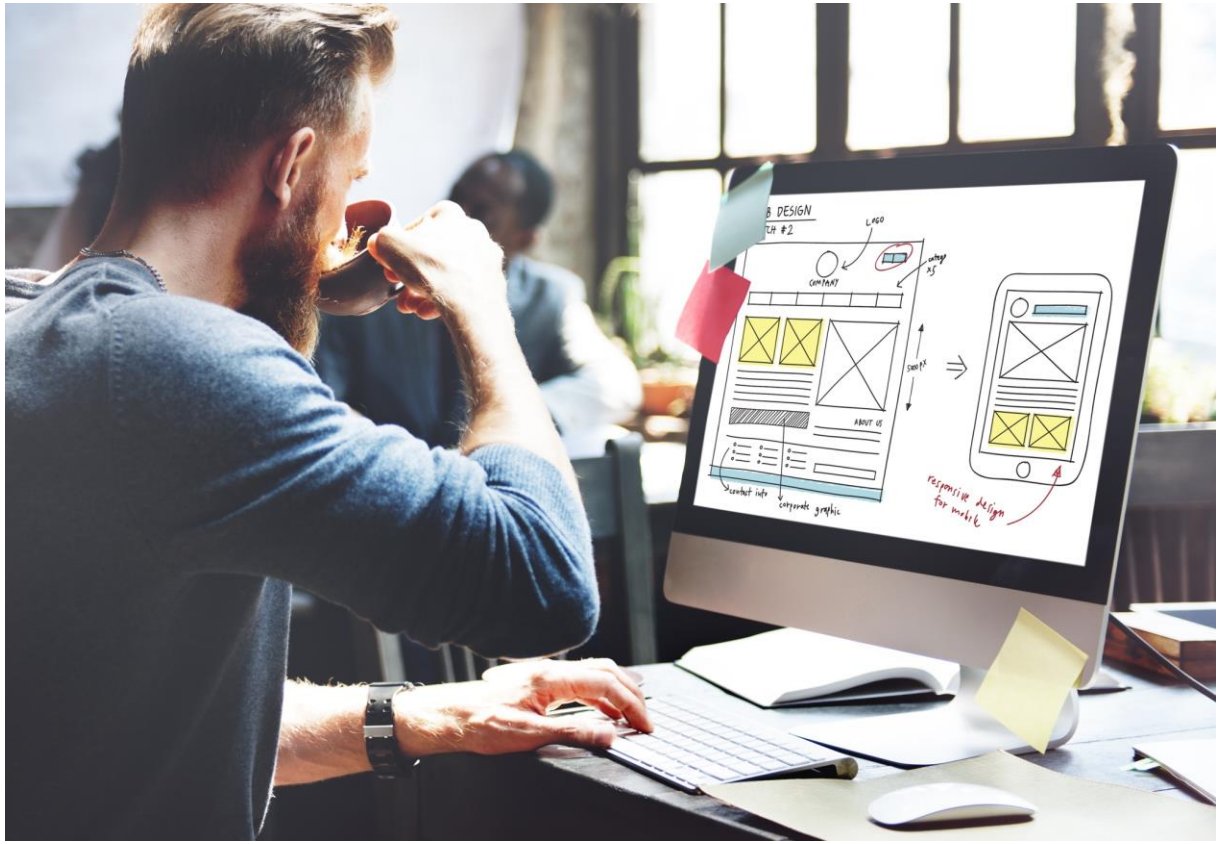
安全组与网络 ACL

属性	安全组	网络 ACL
范围	实例级别	子网级别
支持的规则	仅允许规则	允许和拒绝规则
状态	有状态（自动允许返回流量，不受规则影响）	无状态（返回流量必须由规则明确允许）
规则顺序	在决定允许流量之前评估所有规则	在决定允许流量之前，按数字顺序评估规则

第 4 部分要点

- 在您的 VPC 架构中构建安全功能：
  - 尽可能隔离子网。
  - 选择符合您需求的网关设备或 VPN 连接。
  - 使用防火墙。
- 安全组和网络 ACL 是可用来保护 VPC 的防火墙选项。

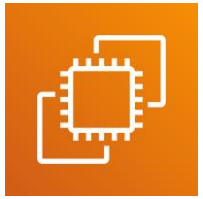
实验 2：构建 VPC 并启动 Web 服务器



实验 2：场景

在本实验中，您将使用 Amazon VPC 创建自己的 VPC 并添加一些组件，以生成自定义网络。您要为您的 VPC 创建安全组 。您还要创建 EC2 实例，然后将其配置为 Web 服务器并使用安全组。然后在 VPC 中启动 EC2 实例。

Amazon VPC



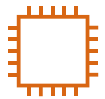
Amazon EC2

实验 2：任务

- 创建 VPC。

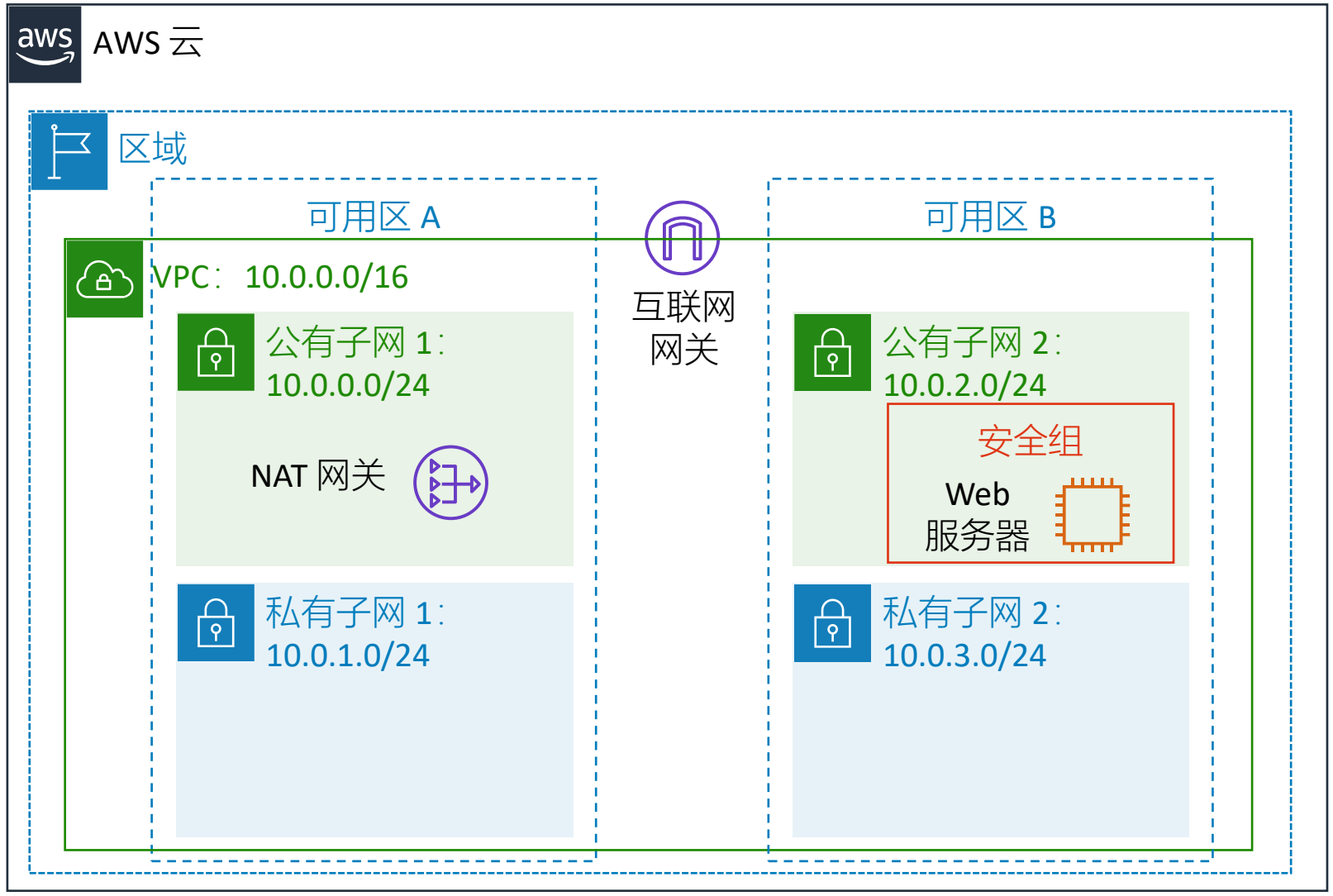
- 创建额外子网。

- 创建 VPC 安全组。



- 启动 Web 服务器实例。

实验 2：最终成果



公有路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	互联网网关

私有路由表

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	NAT 网关

大约 30 分钟

开始实验 2：构建 VPC 并启动 Web 服务器

模块 5：联网和内容分发

模块总结

aws academy

模块总结

总体来说，您在本模块中学习了如何：

- 了解联网基础知识
- 描述如何在云中使用 Amazon VPC 建立虚拟网络
- 标记网络图
- 设计基本的 VPC 架构
- 指出构建 VPC 的步骤
- 识别安全组
- 创建您自己的 VPC 并向其添加其他组件，以生成自定义网络

完成知识测验


CONTACT
SEARCH
NAVIGATION
GOODS
SOCIAL
FOOTER

<header id="topnav">
<nav>

<li class="active"><a class="scroll" href=
Home

Service

Products

Portfolio

Team

Contact

</nav>

<a href="./">
<img src="web/images/logo3.png" id="logo_1

样题

哪项 AWS 联网服务可帮助公司在 AWS 中创建虚拟网络?

A. AWS Config
B. Amazon Route 53
C. AWS Direct Connect
D. Amazon VPC

其他资源

- Amazon VPC 概览页面
- Amazon Virtual Private Cloud 连接选项白皮书
- One to Many: Evolving VPC Design AWS 架构博客文章
- Amazon VPC 用户指南
- Amazon CloudFront 概览页面

谢谢

aws academy