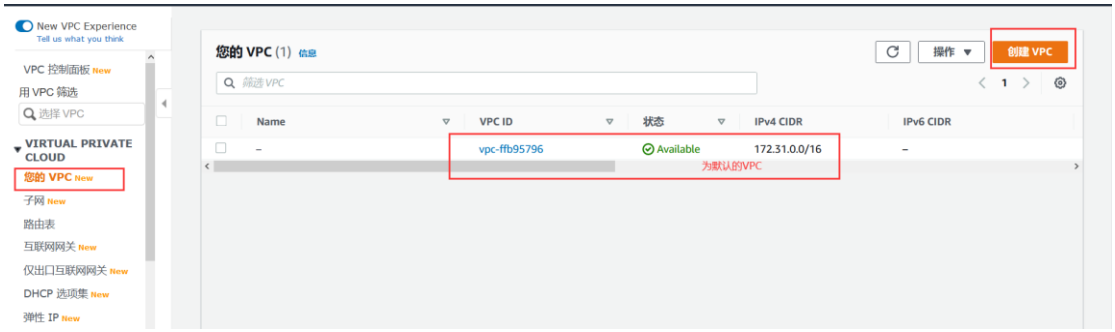
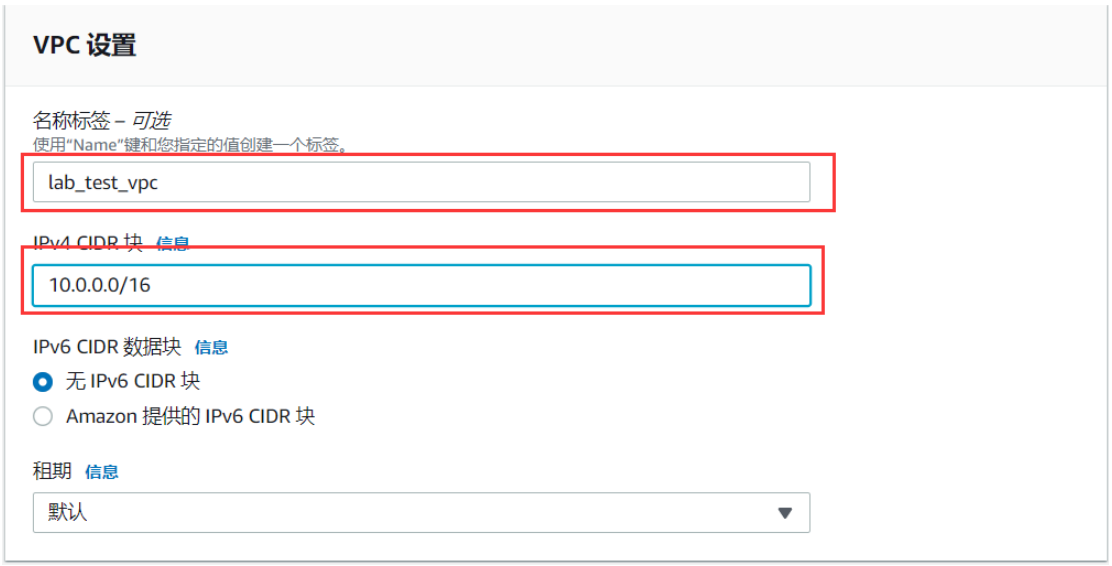
官方文档教程：

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html#VPC_Scenario2_Implementation

一、创建 VPC



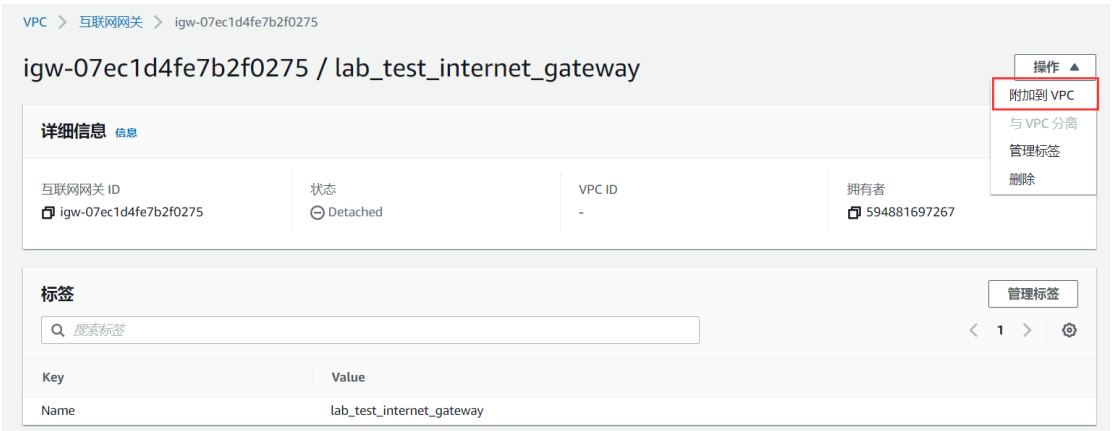


创建后的 VPC 信息（VPC ID: vpc-029133a194600425f）

创建 Internet 网关：

Internet 网关 ID：igw-07ec1d4fe7b2f0275

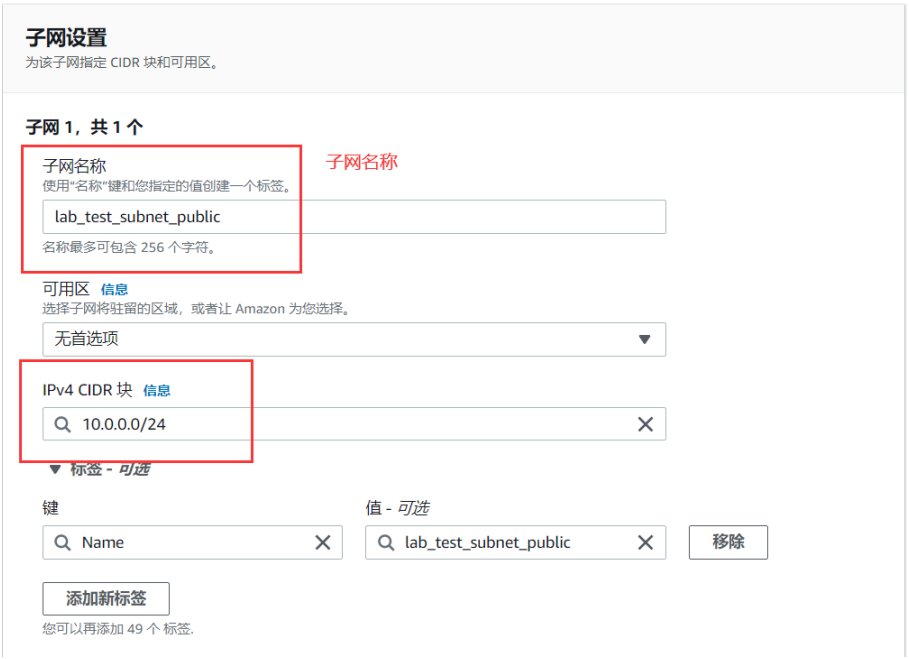
将网关附加到 VPC 上



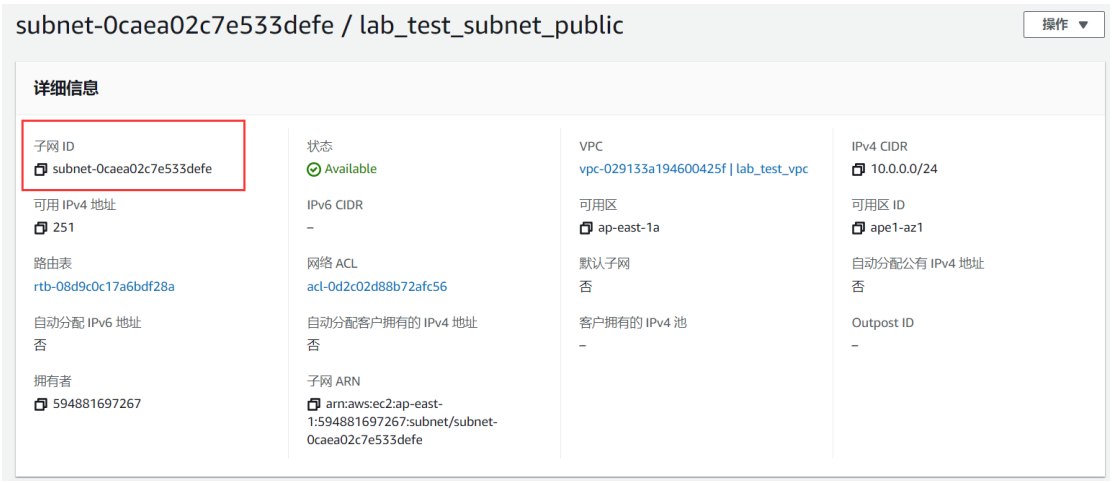

VPC > 互联网网关 > 附加到 VPC (igw-07ec1d4fe7b2f0275)
附加到 VPC (igw-07ec1d4fe7b2f0275) 信息
VPC
将互联网网关附加到 VPC 以实现 VPC 与互联网之间的通信。在下方指定您要附加的 VPC。
可用的 VPC
将互联网网关附加到该 VPC。
选择 VPC
vpc-029133a194600425f - lab_test_vpc
AWS 命令行界面命令
取消
连接互联网网关

二、创建公有子网


创建子网 信息
VPC
VPC ID
在此 VPC 中创建子网。
vpc-029133a194600425f (lab_test_vpc)
选择之前自定义的VPC
已关联的 VPC CIDR
IPv4 CIDR
10.0.0.0/16

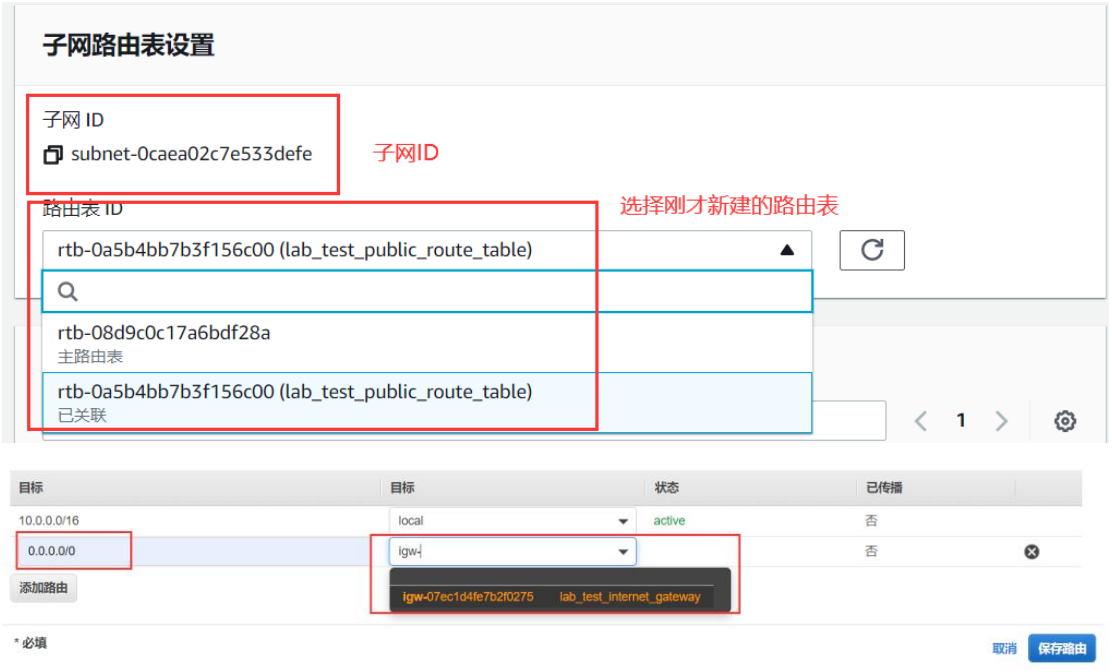

子网设置
为该子网指定 CIDR 块和可用区。
子网 1，共 1 个
子网名称
使用"名称"键和您指定的值创建一个标签。
lab_test_subnet_public
子网名称
名称最多可包含 256 个字符。
可用区 信息
选择子网将驻留的区域，或者让 Amazon 为您选择。
无首选项
IPv4 CIDR 块 信息
10.0.0.0/24
标签 - 可选
键
值 - 可选
Name
lab_test_subnet_public
移除
添加新标签
您可以再添加 49 个 标签。

子网 ID: subnet-0caea02c7e533defe



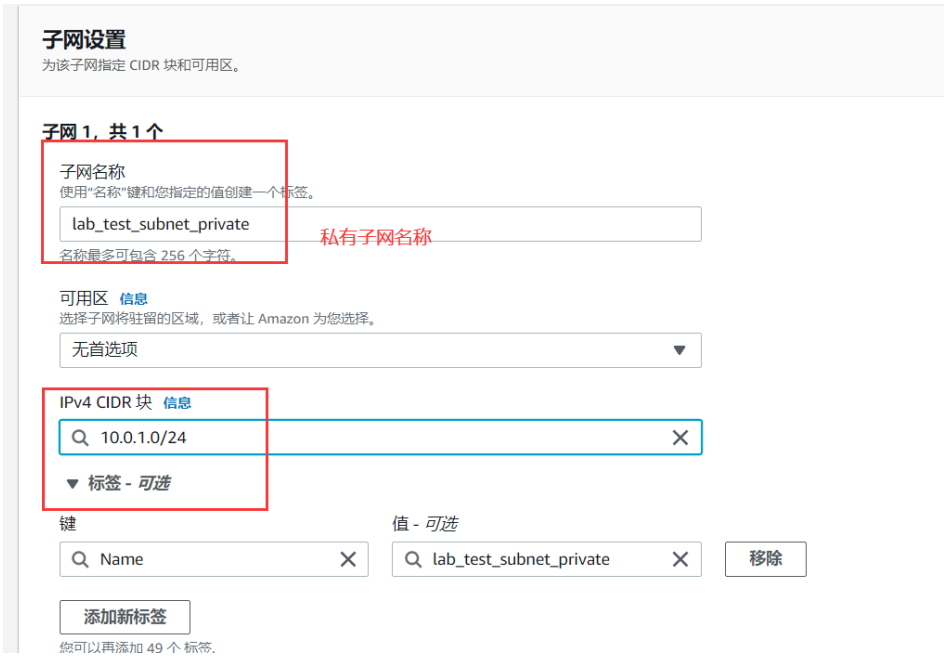
新建公有子网路由表（即图中的 Custom route table）：

公有子网与路由表关联，并设置路由：

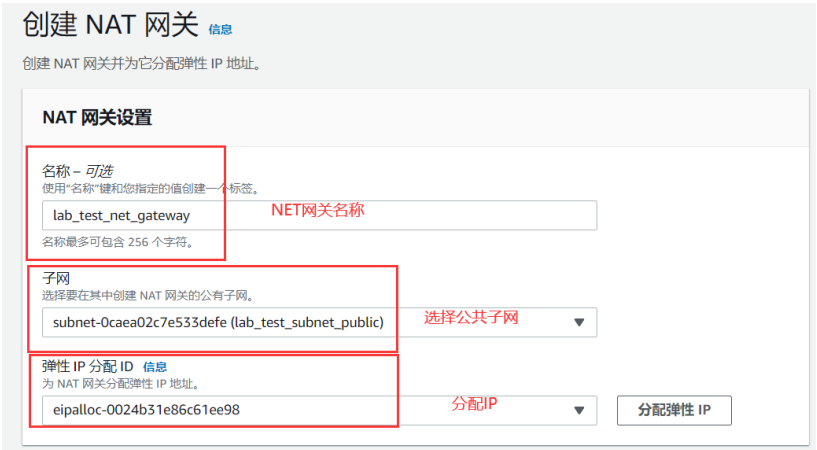


目前位置，此公有子网下的 EC2 经过附加公网 IP 后，都可以访问互联网或从互联网访问该实例。

三、创建私有子网（外部不能访问 ec2，但是 ec2 可以访问互联网）



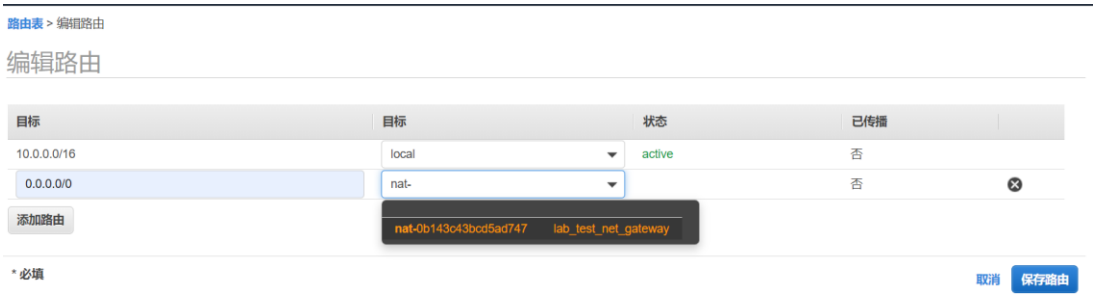
由于私有子网，需要通过 NAT 网关访问外部互联网，所有我们需要创建一个 NAT 网关：**（注意：NAT 网关必须附加在上面创建的公有子网中）**



net 网关 ID：nat-0b143c43bcd5ad747

新建私有子网路由表（即图中的 Main route table）：

私有子网与路由表关联，并设置路由：

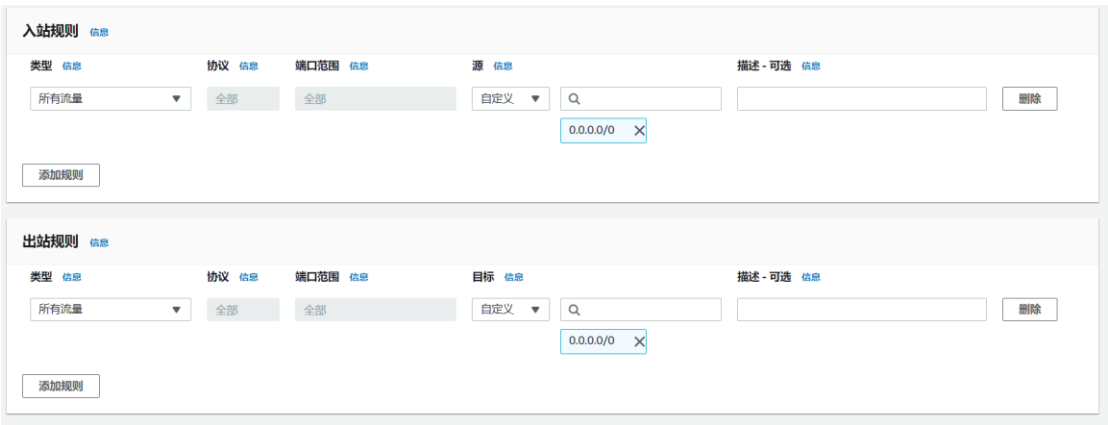


到目前位置，此私有子网下的 EC2 经过 NAT 网关访问互联网，但是从互联网不能访问该实例。

四、为 VPC 设置安全组

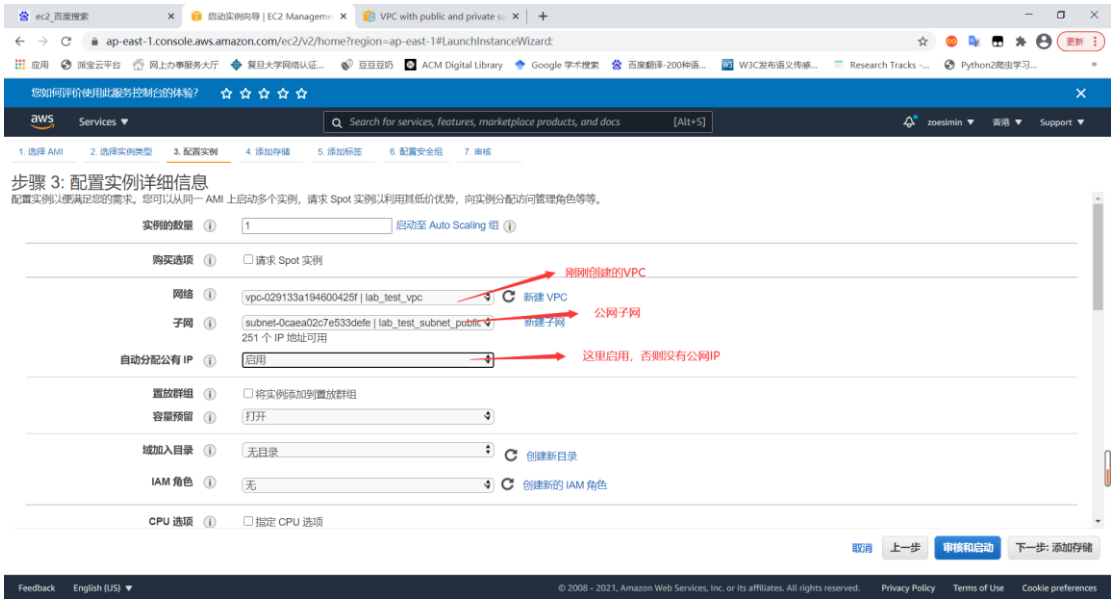
一般 EC2 实例会默认使用“default”安全组，并不符合要求，我们要自己创建并配置一个安全组。

创建完之后，选中安全组，创建如下规则。安全组可以控制流量出入，在本文中，为了方便和日后开发，统一采用粗粒度的设置方式，如果有同学想要更细粒度的管理，请自行配置。（此处可参考顶部连接内的设置）



四、基于自定义 VPC 创建 EC2 实例

分别再启动两个实例，系统选择 ubuntu18，分别加入到公网和私网中，公网中的实例要勾选自动分配 IP，如果在这里漏掉，可以在创建完实例之后为其分配弹性 IP。
如下图以公网的配置为例：



在创建的最后需要创建新的安全组并设置规则。这里给出推荐配置：

公网实例安全组`WebServerSG`

Inbound Rules

类型	协议	端口	来源
HTTP	TCP	80	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0

Outbound Rules

类型	协议	端口	目的地
所有流量	全部	全部	0.0.0.0/0

私网实例安全组`DBServerSG`

Inbound Rules

类型	协议	端口	来源
所有流量	全部	全部	10.0.0.0/24

Outbound Rules

类型	协议	端口	目的地
所有流量	全部	全部	0.0.0.0/0

五、与内网实例连接：

与公网实例的连接在 PART1 中“申请服务器”的实验中，同学们已经体验过了，现在要与内网实例连接。

选择通过公网实例连接到内网实例，如果有同学想要直接连接到内网实例，请自行尝试。

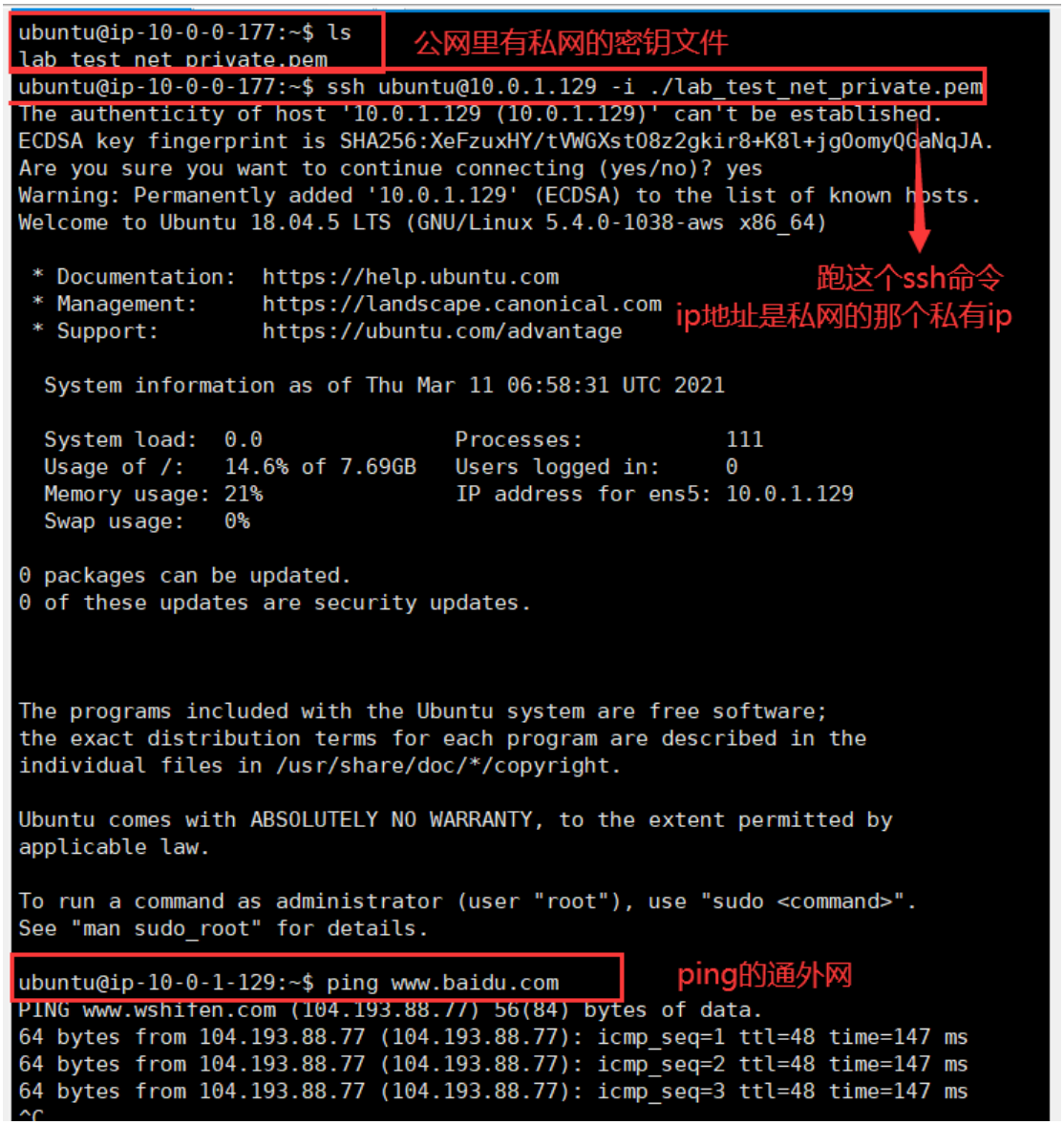
把密钥文件传输到公网实例中，先设置密钥权限，然后通过 ssh 命令连接到内网实例。

chmod 400 lab_test_net_private.pem

ssh ubuntu@10.0.1.129 -i ./ lab_test_net_private.pem

其中 10.0.1.129 是内网实例的私有 IP。

此时内网实例应该能与因特网连通，但是无法被外网访问到，只能通过 VPC 中的公有网段内的实例访问。（如下图所示）



至此我们完成了 VPC 的配置!