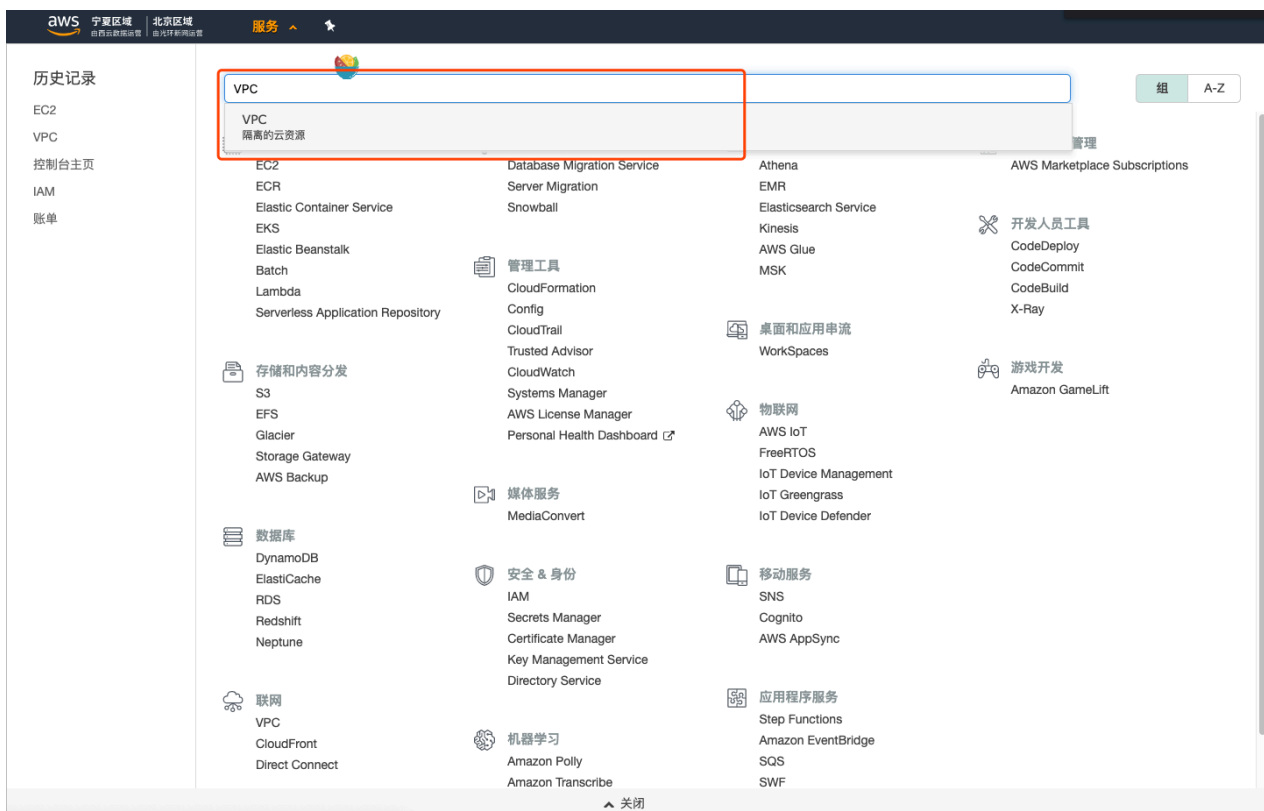


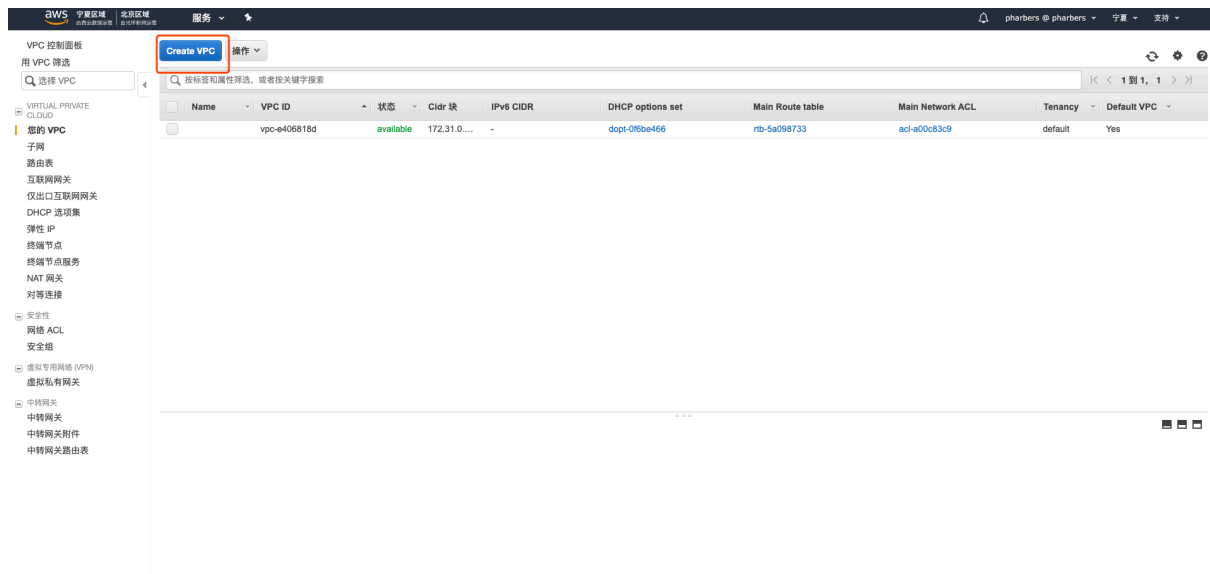
VPC 创建流程

Amazon Virtual Private Cloud (Amazon VPC) 允许您在已定义的虚拟网络内启动 AWS 资源。这个虚拟网络与您在数据中心中运行的传统网络极其相似，并会为您提供使用 AWS 的可扩展基础设施的优势。

1. 打开 Amazon VPC 控制台 <https://console.amazonaws.cn/vpc/>。



2. 在控制台选择创建一个新的 VPC



3. 输入 VPC 的名称和私有网段，然后点击创建

在创建 VPC 时，建议您指定来自私有 IPv4 地址范围 (如 /16 RFC 1918 所指定) 的 CIDR 块 (小于或等于)：

- 10.0.0.0 – 10.255.255.255 (10/8 前缀)
- 172.16.0.0 – 172.31.255.255 (172.16/12 前缀)
- 192.168.0.0 – 192.168.255.255 (192.168/16 前缀)



网关及路由表 创建流程（开放全部入网）

网关：

Internet 网关是一种横向扩展、支持冗余且高度可用的 VPC 组件，可实现 VPC 中的实例与 Internet 之间的通信。因此它不会对网络流量造成可用性风险或带宽限制。

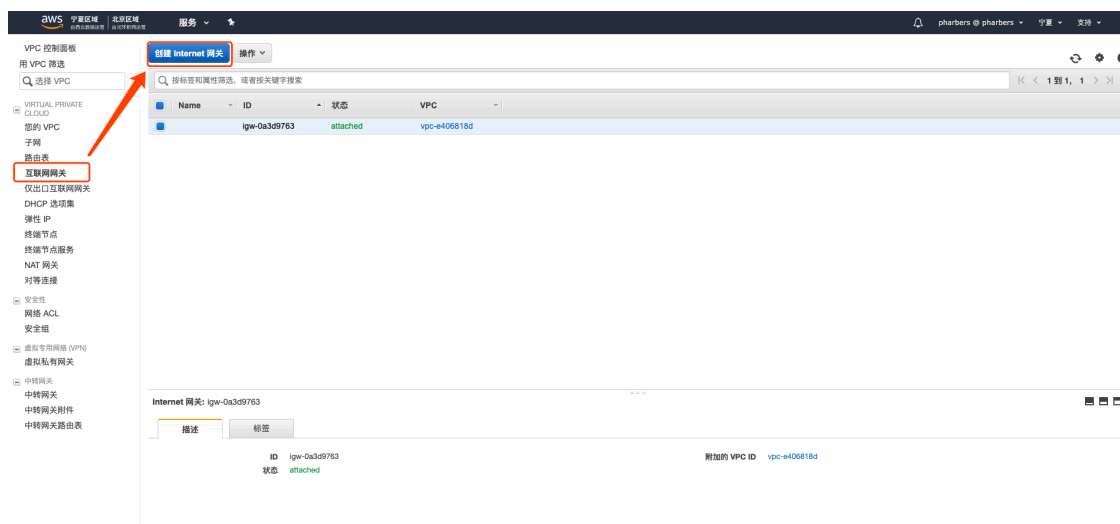
Internet 网关有两个用途，一个是在 VPC 路由表中为 Internet 可路由流量提供目标，另一个是为已经分配了公有 IPv4 地址的实例执行网络地址转换 (NAT)。

Internet 网关支持 IPv4 和 IPv6 流量。

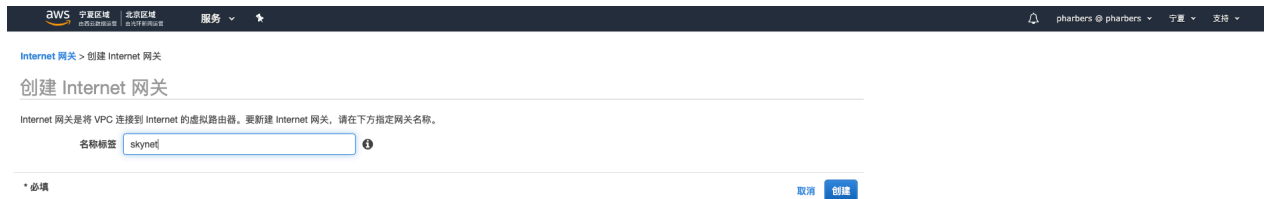
路由表：

路由表中包含一组被称为路由的规则，用于确定来自您的子网或网关的网络流量的导向何处。

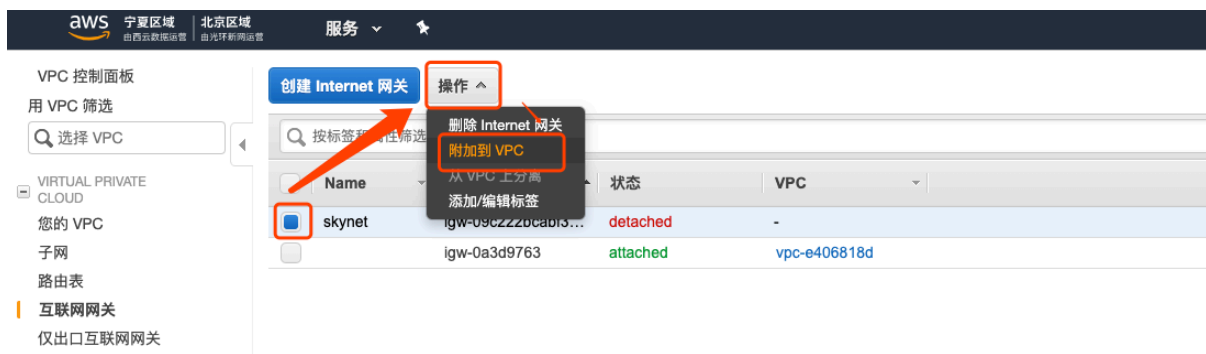
4. 在控制台选择创建一个新的 网关



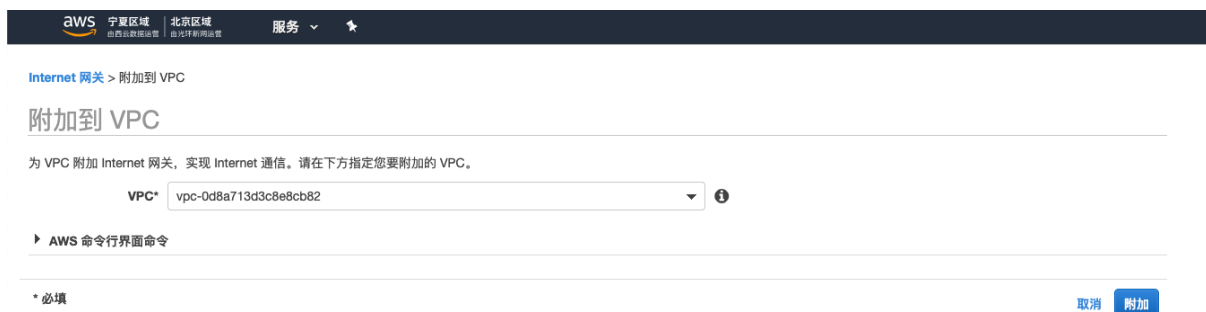
5. (可选) 为 Internet 网关命名，然后选择 Create (创建)



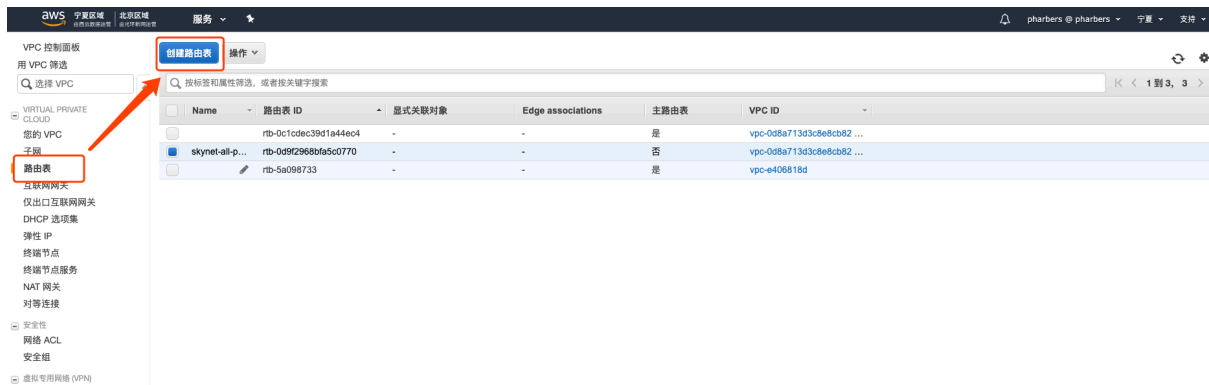
6. 选择刚刚创建的 Internet 网关，然后选择 操作, 附加到 VPC。



7. 从列表中选择目标 VPC，然后选择 附加。



8. 在控制台选择路由表，新建 路由表



9. 输入路由表名称和所属 VPC，创建

路由表 > 创建路由表

创建路由表

路由表指定在 VPC、Internet 和 VPN 连接内的子网之间转发数据包的方式。

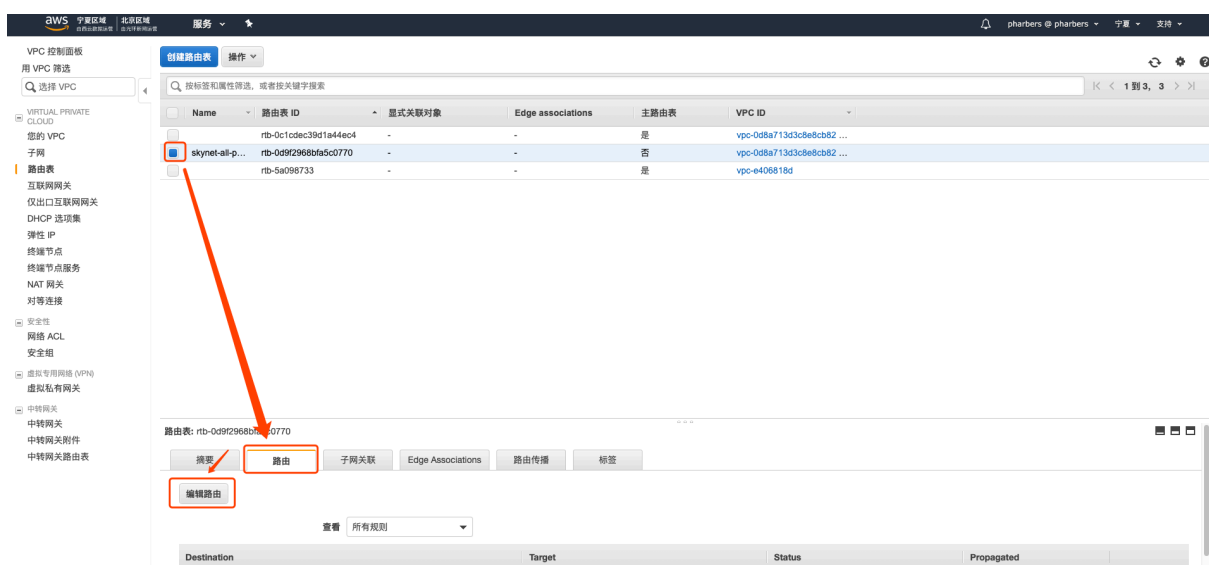
名称标签

VPC*

* 必填

[取消](#) [创建](#)

10. 为新建的路由表添加一条路由规则



11. 全部来源都走之前创建的网关

aws 宁夏区域 北京区域 服务

路由表 > 编辑路由

编辑路由

目标	目标	状态	已传播
192.168.0.0/16	local	active	否
0.0.0.0/0	lgw-		否

添加路由

lgw-09c222bcabf3c3b93 skynet

* 必填

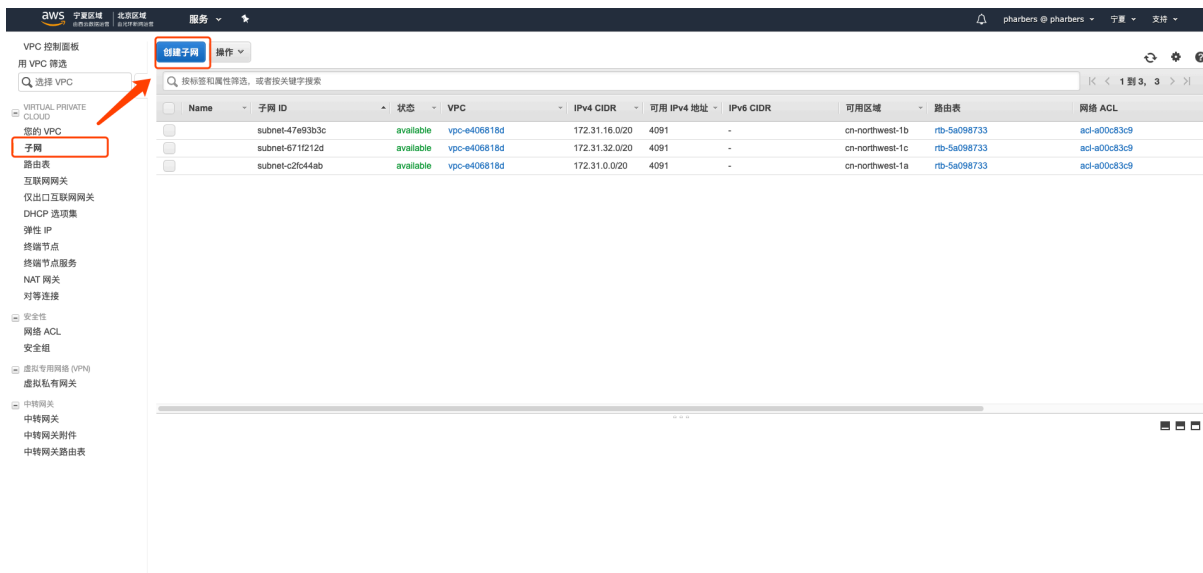
取消 保存路由

子网 创建流程

VPC 跨越区域中的所有可用区。所以在创建 VPC 之后，您可以在每个可用区中添加一个或多个子网。

在创建子网时，指定子网的 CIDR 块，它是 VPC CIDR 块的子集。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。

12. 在控制台选择创建一个新的 子网



The screenshot shows the AWS Management Console interface. In the left-hand navigation pane, the '子网' (Subnets) option is highlighted with a red box and a red arrow. In the top navigation bar, the '创建子网' (Create Subnet) button is also highlighted with a red box. The main content area displays a table of existing subnets.

Name	子网 ID	状态	VPC	IPv4 CIDR	可用 IPv4 地址	IPv6 CIDR	可用区域	路由表	网络 ACL
	subnet-47e93b3c	available	vpc-e406818d	172.31.16.0/20	4091	-	cn-northwest-1b	rtb-5a098733	acl-a00c83c9
	subnet-671f212d	available	vpc-e406818d	172.31.32.0/20	4091	-	cn-northwest-1c	rtb-5a098733	acl-a00c83c9
	subnet-c2f044ab	available	vpc-e406818d	172.31.0.0/20	4091	-	cn-northwest-1a	rtb-5a098733	acl-a00c83c9

13. 填写子网名称、所属 VPC、可用区和网段等信息

每个子网 CIDR 块中的前四个 IP 地址和最后一个 IP 地址无法供您使用，而且无法分配到一个实例。例如，在具有 CIDR 块 10.0.0.0/24 的子网中，以下五个 IP 地址是保留的：

- 10.0.0.0：网络地址。
- 10.0.0.1：由 AWS 保留，用于 VPC 路由器。
- 10.0.0.2：由 AWS 保留。DNS 服务器的 IP 地址是 VPC 网络范围的基址 + 2。对于包含多个 CIDR 块的 VPC，DNS 服务器的 IP 地址位于主要 CIDR 中。我们还为 VPC 中的所有 CIDR 块预留了每个子网范围加二的基址。有关更多信息，请参阅 Amazon DNS 服务器。
- 10.0.0.3：由 AWS 保留，供将来使用。
- 10.0.0.255：网络广播地址。我们在 VPC 中不支持广播，因此我们会保留此地址。

子网 > 创建子网

创建子网

以 CIDR 格式指定子网的 IP 地址块：例如，10.0.0.0/24。IPv4 块的大小必须介于 /16 网络掩码和 /28 网络掩码之间，可与您的 VPC 大小相同。IPv6 CIDR 块必须是 /64 CIDR 块。

名称标签

VPC

可用区域

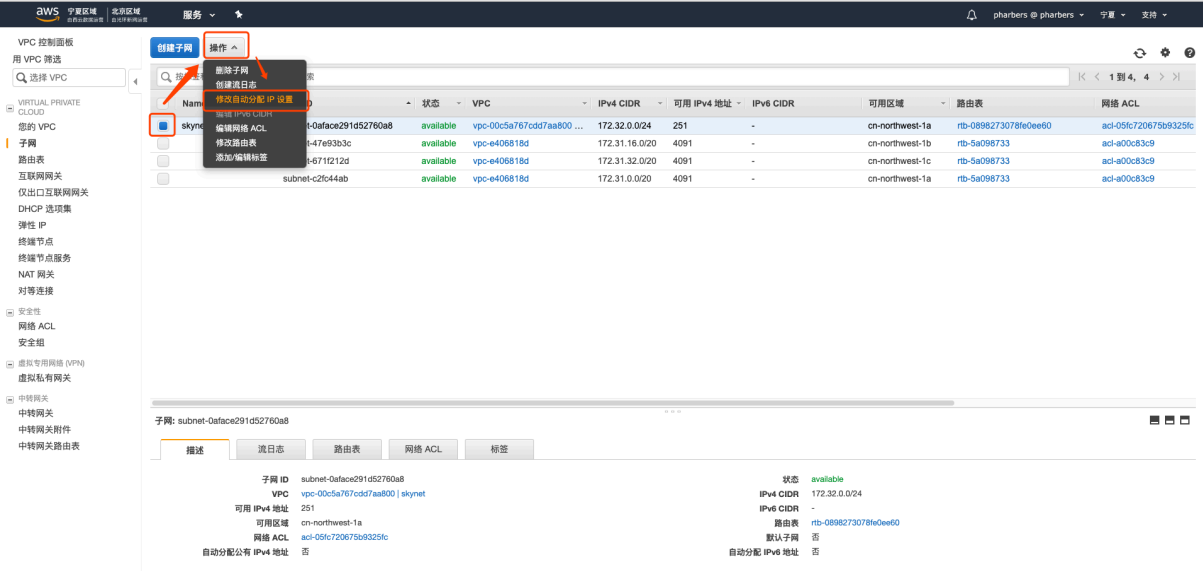
VPC CIDR	CIDR	Status	Status Reason
	192.168.0.0/16	associated	

IPv4 CIDR 块* 子网网段必须是 VPC 网段的子集

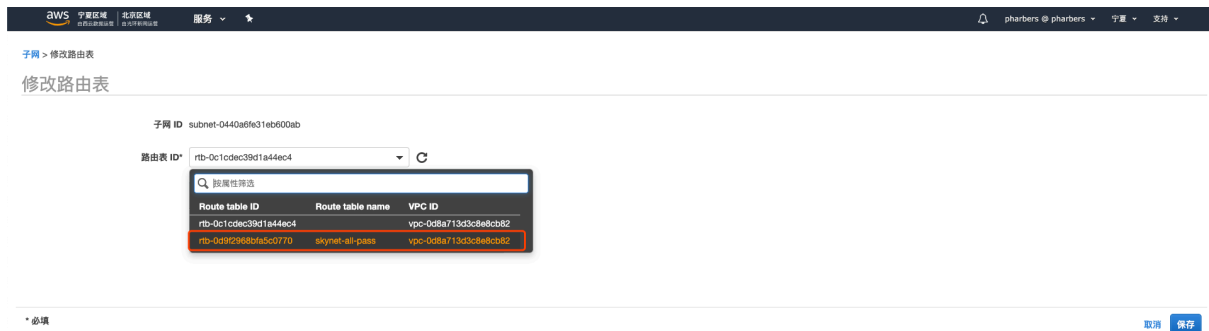
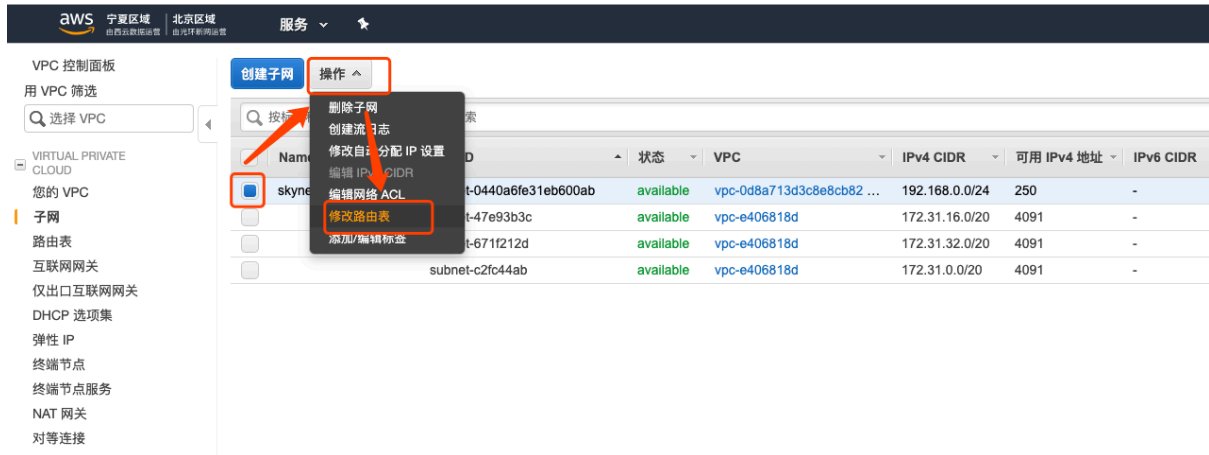
* 必填

取消 创建

14. 打开“自动分配公有 IPv4 地址”



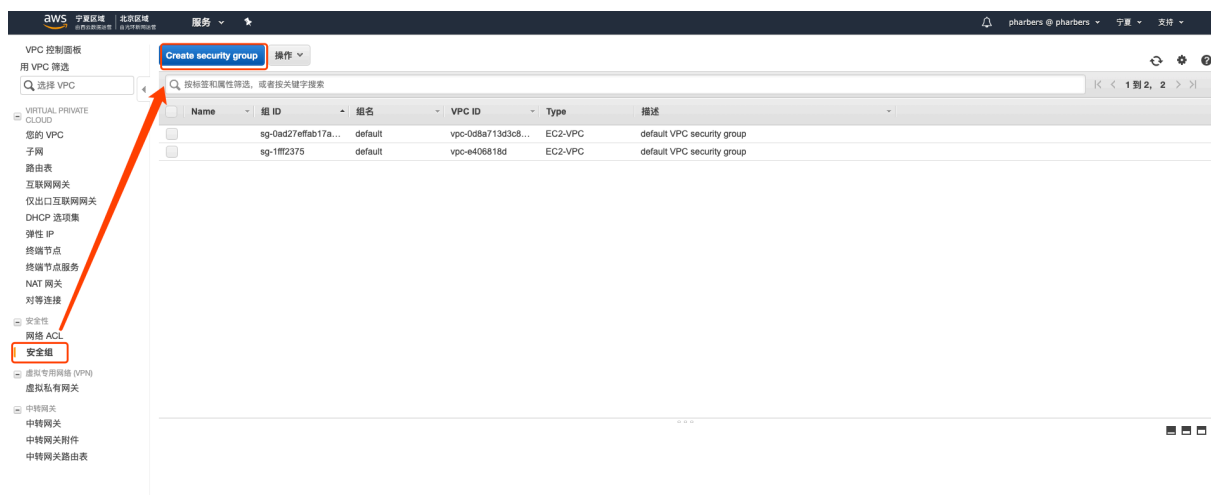
15. 修改路由表为之前创建的开放全部入网路由表



安全组 创建流程（SSH 举例）

安全组 起着虚拟防火墙的作用，可控制一个或多个实例的流量。

16. 在控制台选择创建一个新的 安全组



17. 填写安全组的名称、描述和所属 VPC

The screenshot shows the 'Create security group' form in the AWS Management Console. The form fields are filled with the following information:

- Security group name***: ssh
- Description***: SSH connection in the company
- VPC**: vpc-0d8a713d3c8e8cb82

At the bottom right, there are buttons for '取消' (Cancel) and 'Create'.

18. 新增入网规则

The screenshot shows the AWS Management Console interface for creating a security group. The left sidebar contains navigation links for VPC, Subnets, Route Tables, Internet Gateways, DHCP Options, Elastic IP, Endpoints, NAT Gateways, and Connections. The main content area displays a table of existing security groups:

Name	组 ID	组名	VPC ID	Type	描述
sg-0ad27efab17a...	default	default	vpc-0d8a713d3c8...	EC2-VPC	default VPC security group
sg-0c55bd938304...	ssh	ssh	vpc-0d8a713d3c8...	EC2-VPC	SSH connection in the company
sg-1ff2375	default	default	vpc-e406818d	EC2-VPC	default VPC security group

Below the table, the 'Inbound Rules' tab is selected, showing a table with columns: 类型 (Type), 协议 (Protocol), 端口范围 (Port Range), 来源 (Source), and 描述 (Description). The text '此安全组没有安全规则' (This security group has no security rules) is displayed below the table.

19. 加入公司外网IP

The screenshot shows the 'Edit inbound rules' page in the AWS Management Console. The page title is 'Edit inbound rules'. Below the title, it states: 'Inbound rules control the incoming traffic that's allowed to reach the instance.' The table below shows the existing rule:

类型 (Type)	协议 (Protocol)	端口范围 (Port Range)	来源 (Source)	描述 (Description)
SSH	TCP	22	自定义 (Custom)	221.219.246.98/32, 123.114.209.82/32

Below the table, there is a '添加规则' (Add rule) button. A note at the bottom states: 'NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.' At the bottom right, there are '取消' (Cancel) and 'Save rules' buttons.

2020年4月27日 星期一