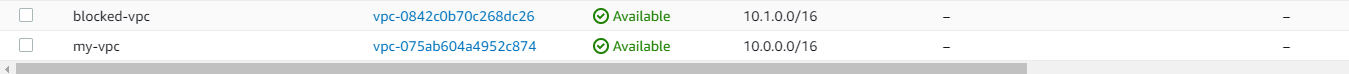
AWS Transit Gateway

官方文档：https://docs.aws.amazon.com/zh\_cn/vpc/latest/tgw/tgw-getting-started.html

实验一：连通两个VPC

前置条件：创建两个同区域的VPC，两个VPC使用不一样的cidr



步骤 1： 创建中转网关

在导航窗格中，选择 Transit Gateways (中转网关)。

选择 Create Transit Gateway (创建中转网关)。

对于 Amazon side ASN (Amazon 端 ASN)，键入中转网关的私有自治系统编号 (ASN)。这应该是边界网关协议 (BGP) 会话的 AWS 端的 ASN。

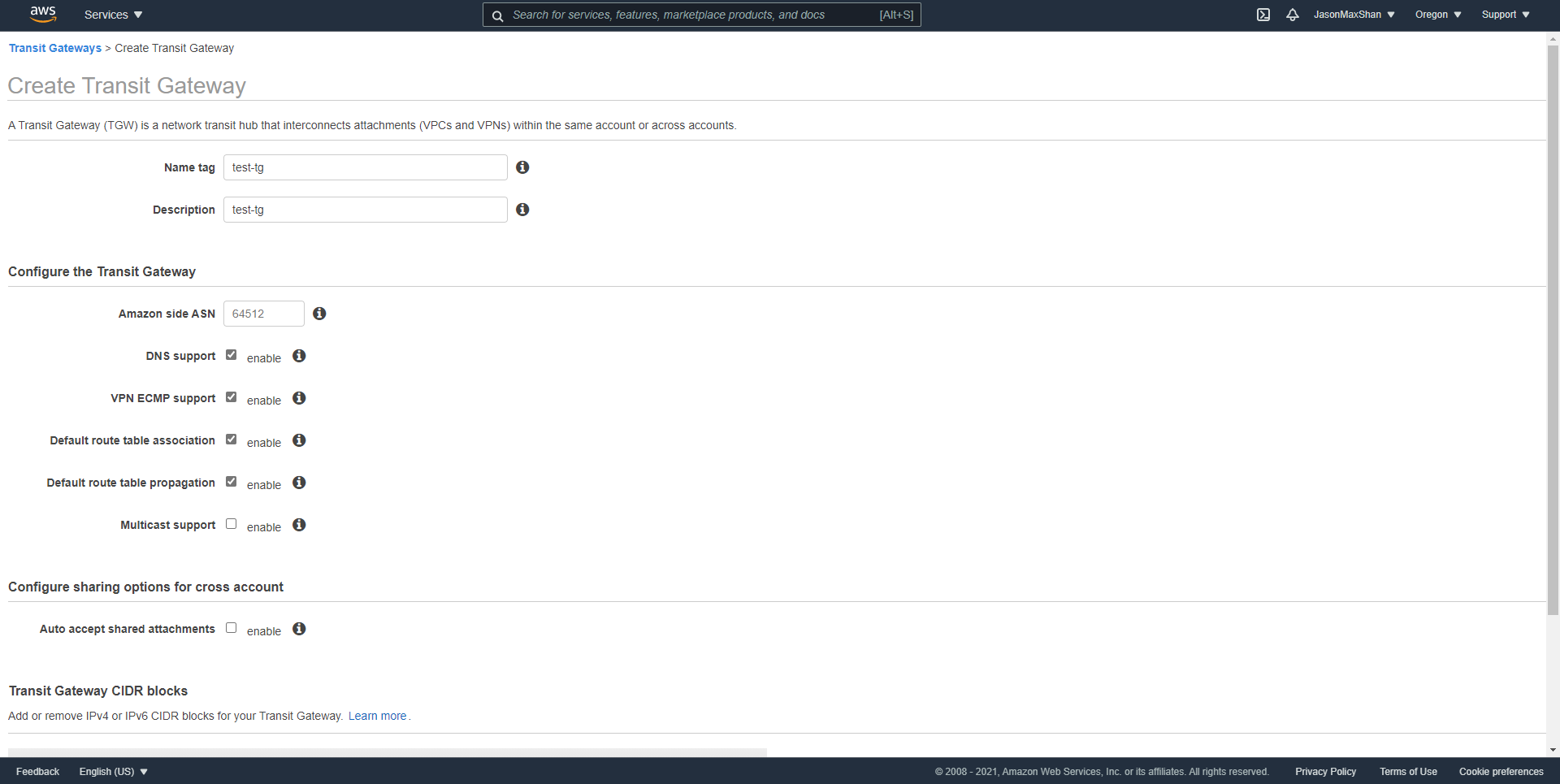
对于 16 位 ASN，范围为 64512 到 65534。

对于 32 位 ASN，范围为 4200000000 到 4294967294。

如果您有多区域部署，我们建议您为每个中转网关使用唯一的 ASN。

（可选）如果您需要禁用 DNS 支持，或者不想要默认的关联路由表或默认的传播路由表，则可以修改默认设置。

选择 Create Transit Gateway (创建中转网关)。

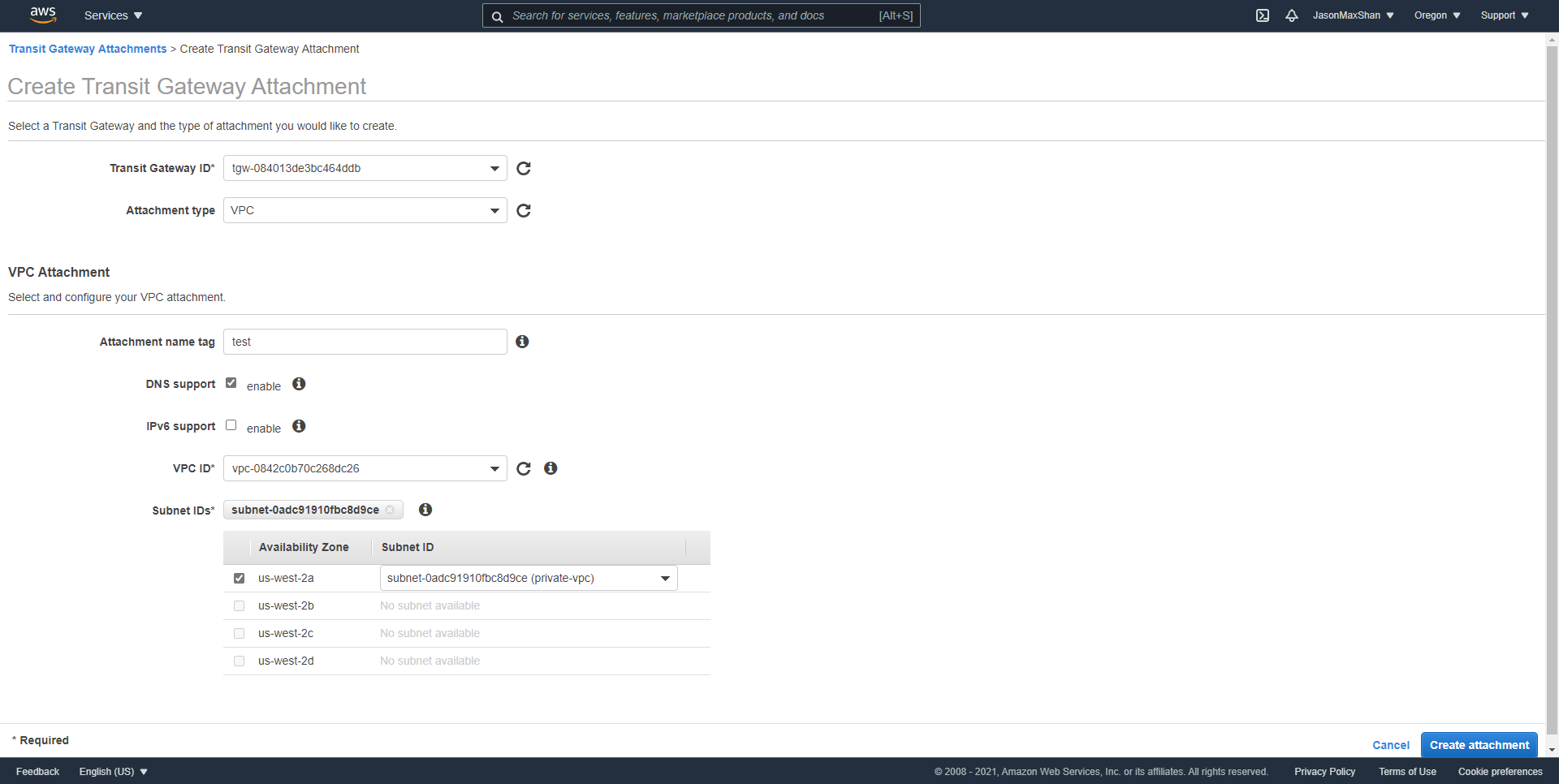


步骤 2： 创建 VPC 的中转网关连接

在导航窗格中，选择 Transit Gateway Attachments (中转网关挂载)。

对于 Attachment type (连接类型)，选择 VPC。

于 Subnet IDs (子网 ID)，为中转网关要用于路由流量的每个可用区域选择一个子网。您必须至少选择一个子网。只能为每个可用区域选择一个子网。



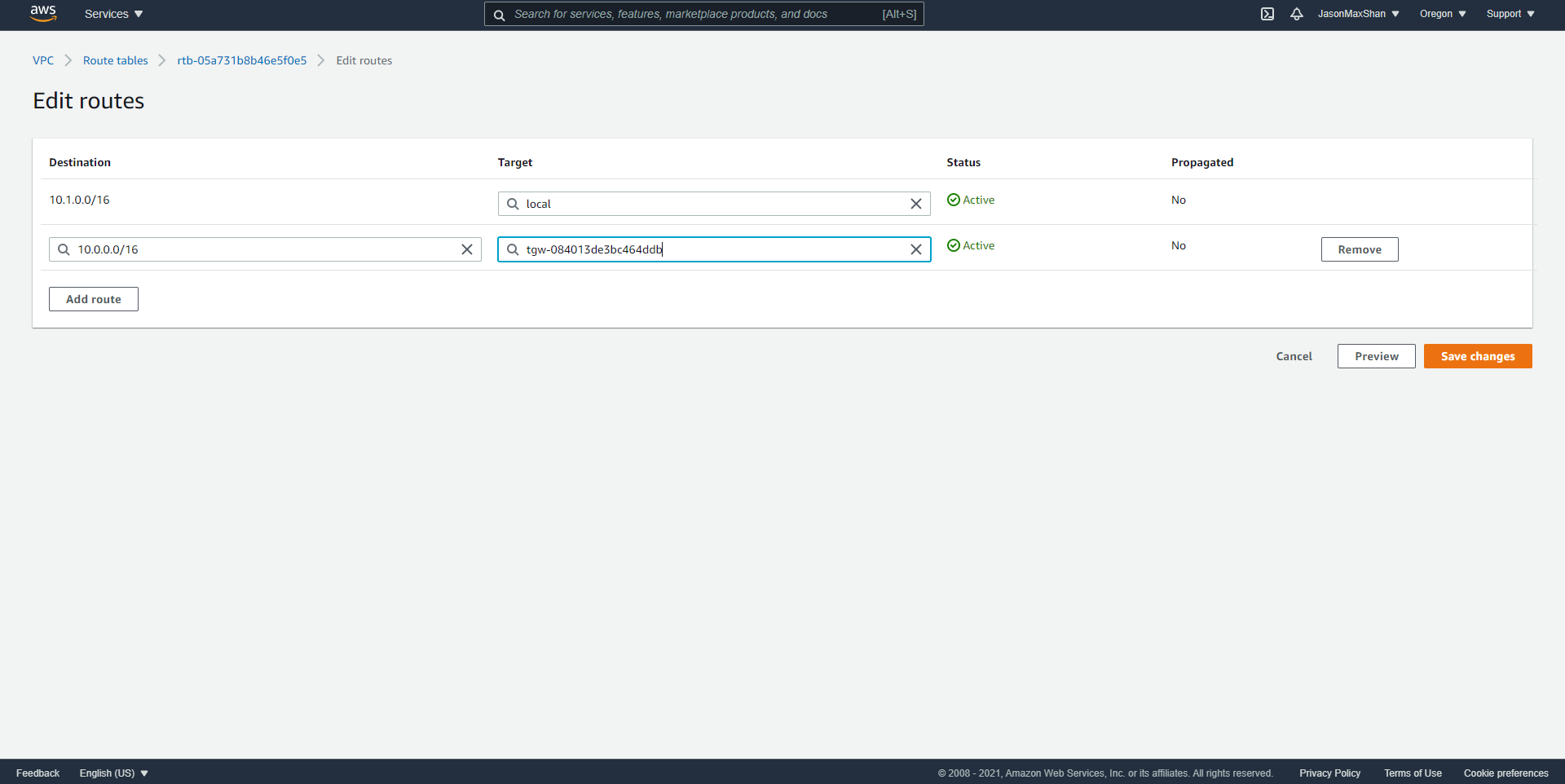
步骤 3：向 VPC 路由表中添加路由

在导航窗格中，选择路由表。

选择 Routes (路由) 选项卡，然后选择 Edit routes (编辑路由)。

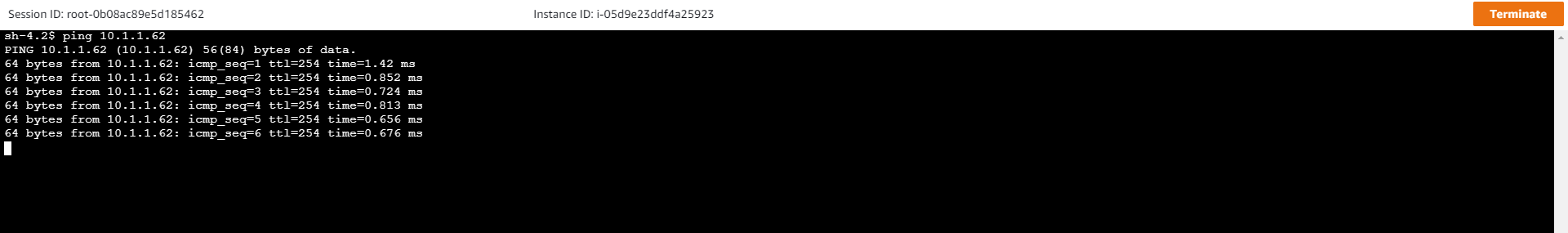
选择 Add route (添加路由)。

在 Destination (目的地) 列中，输入目的地VPC的cidr。对于 Target（目标），请选择中转网关挂载 ID。



步骤 4：测试中转网关

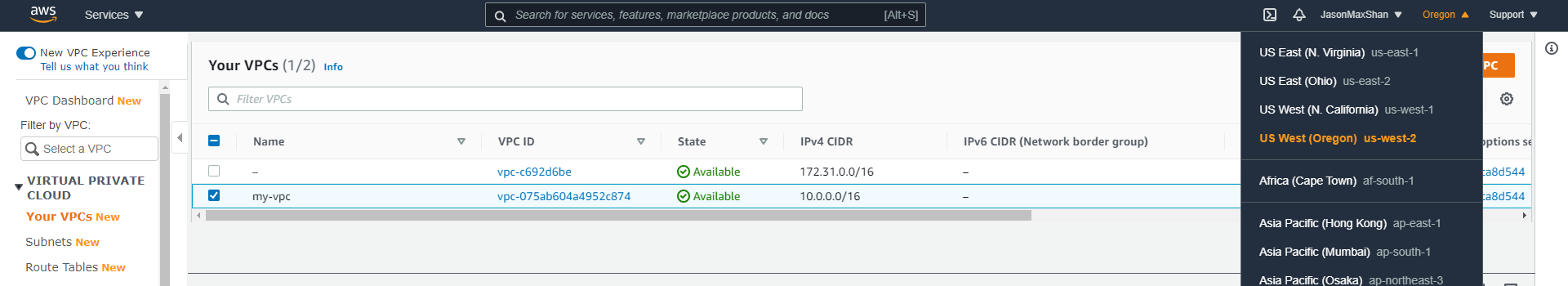
确认中转网关已成功创建，方法是：通过连接到每个 VPC 中的一个 EC2 实例，然后在它们之间发送数据，如 ping 命令。(使用私有IP发送ping)



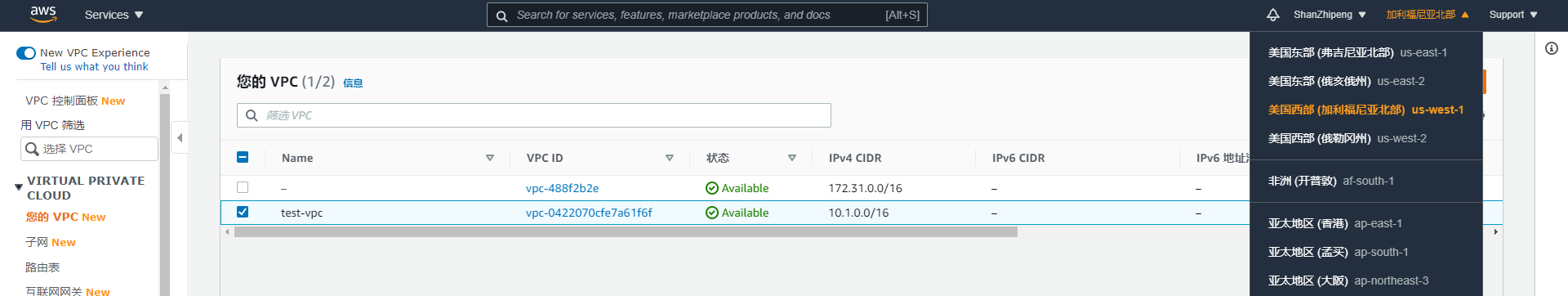
实验二：跨区域跨账号的VPC对等连接

前置条件：两个AWS账号，位于不同地区，各有一个VPC

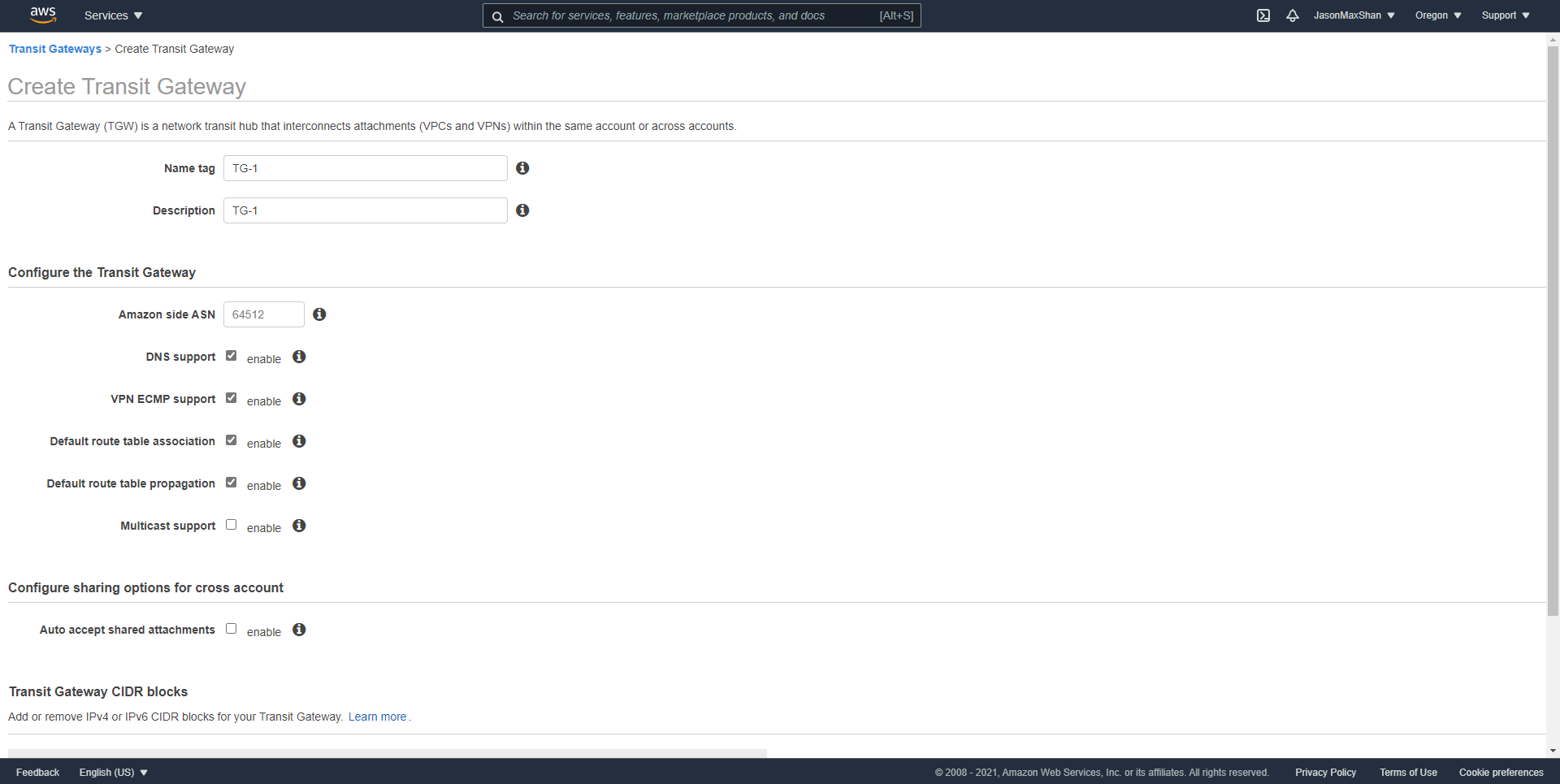
示例账号1位于US-west-2，使用的VPC的CIDR是10.0.0.0/16

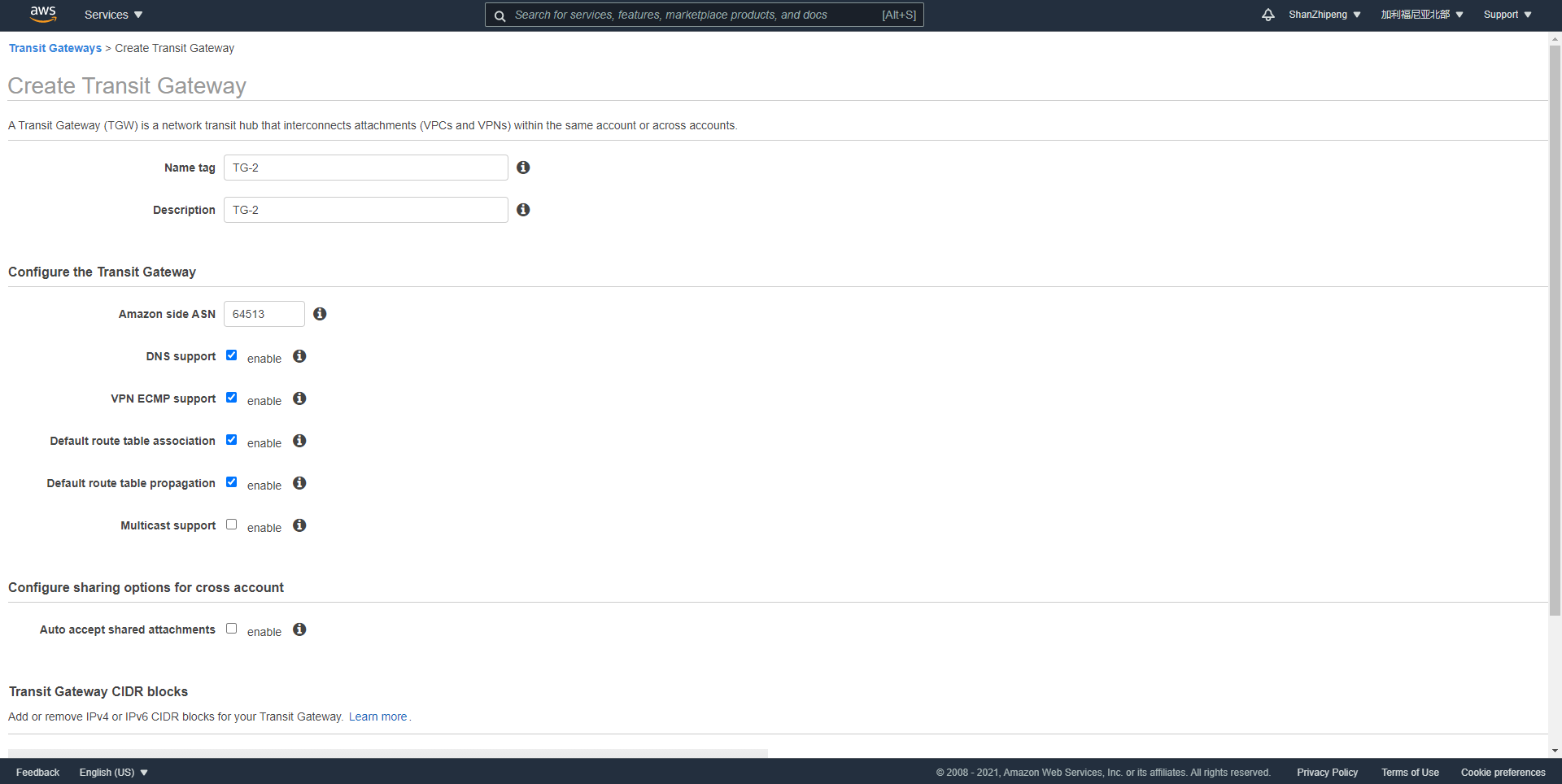


示例账号2位于US-west-1，使用的VPC的CIDR是10.1.0.0/16



步骤一：在两个账号都创建一个Transit Gateway，建议两个中转网关使用不同的ASN





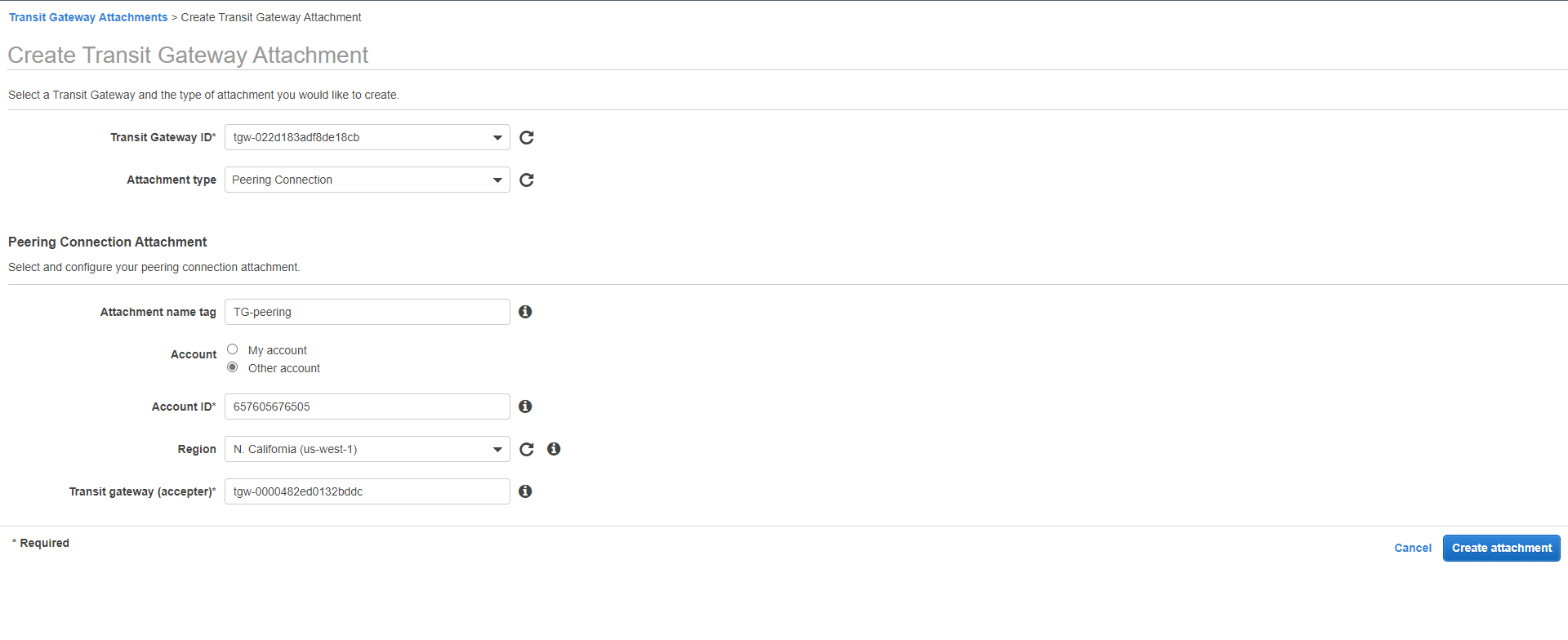
步骤二：两个中转网关创建对等连接

Attachment type选择Peering Connection

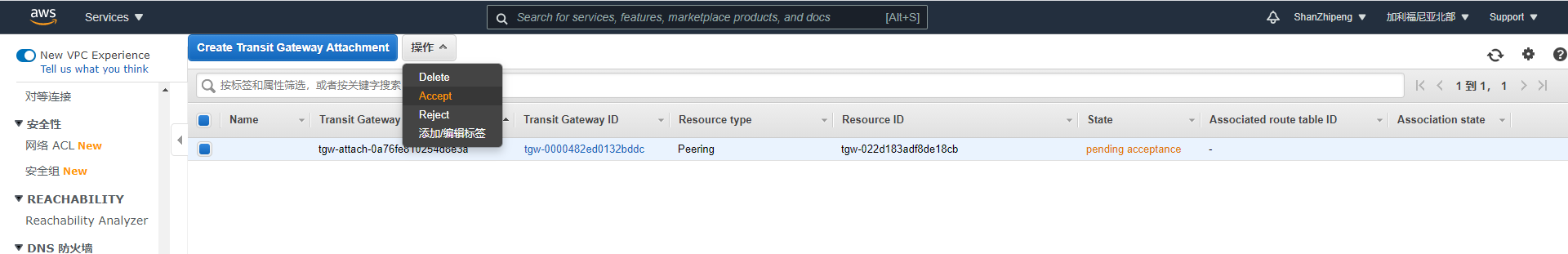
Account选择Other account

Account ID输入对方账号ID

Transit gateway (accepter)输入对方transit gateway的ID



Create attachment后去查看另一个账号，发现有一个连接请求，点击Actions，点击Accept



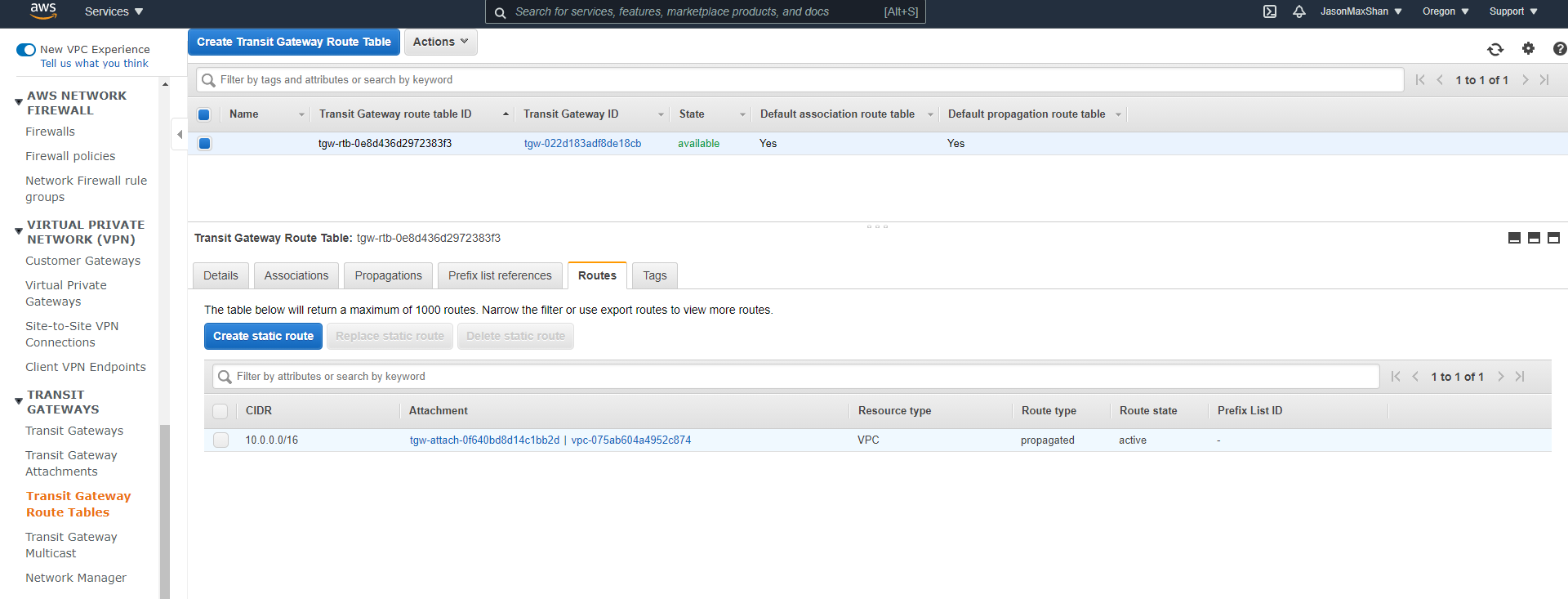
步骤三：将路由添加到中转网关路由表

要在对等中转网关之间路由流量，必须向中转网关路由表添加一个指向中转网关对等连接挂载的静态路由。接受方中转网关的拥有者还必须向其中转网关的路由表添加静态路由。

在导航窗格中，选择 Transit Gateway Route Tables (中转网关路由表)。

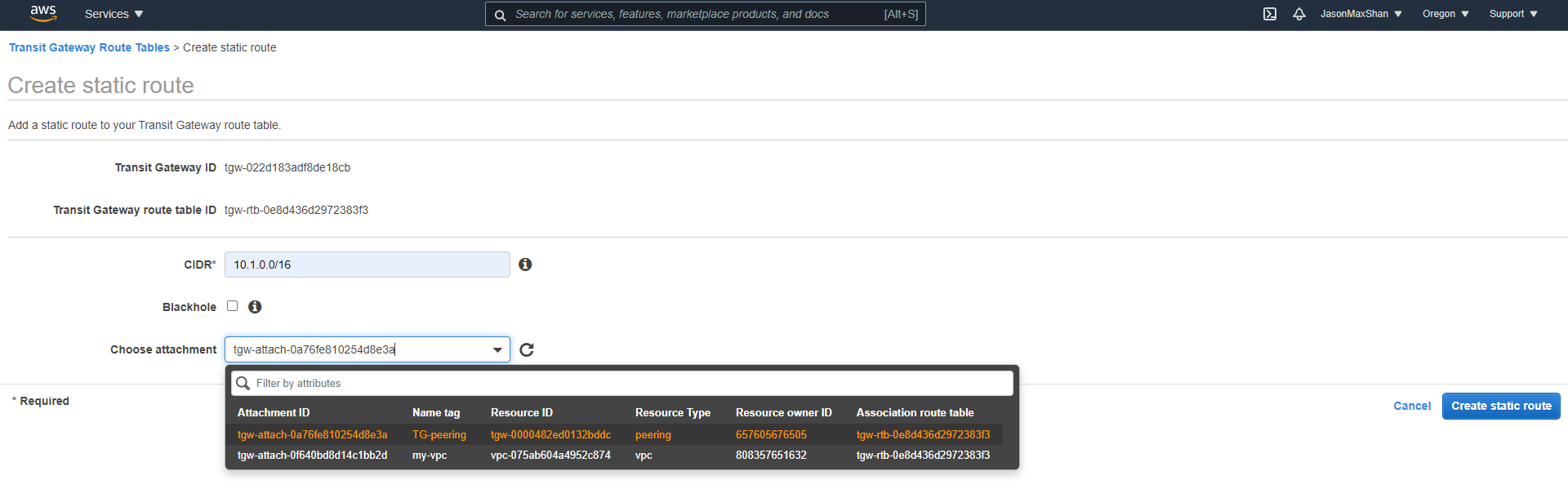
选择要为其创建路由的路由表。

选择 Actions (操作)、Create route (创建路由)。



在 Create route (创建路由) 页面上，输入为其创建路由的 CIDR 块。例如，指定连接到对等中转网关的 VPC 的 CIDR 块。

选择路由的对等连接挂载。



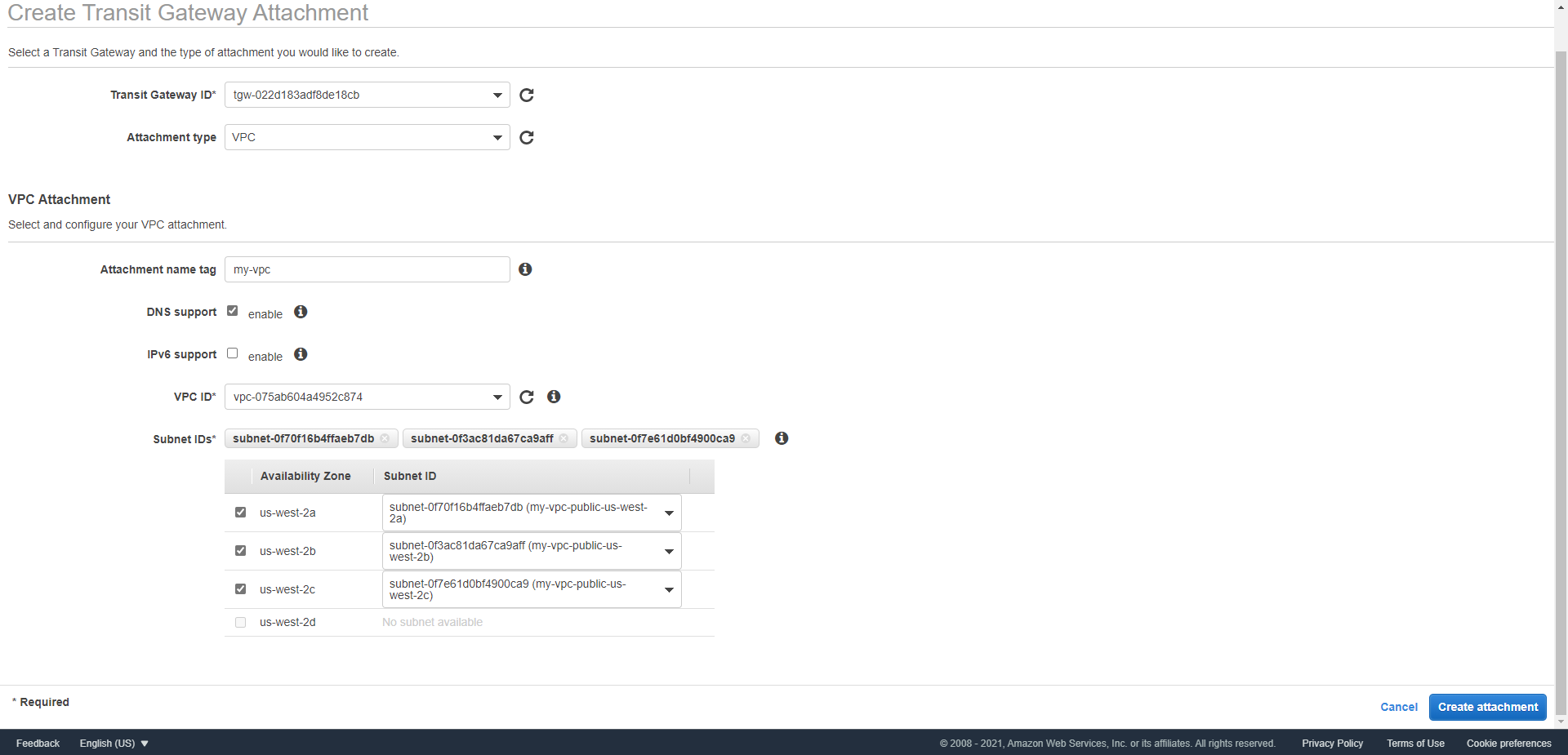
步骤四：创建 VPC 的中转网关连接

在导航窗格中，选择 Transit Gateway Attachments (中转网关挂载)。

对于 Attachment type (连接类型)，选择 VPC。

于 Subnet IDs (子网 ID)，为中转网关要用于路由流量的每个可用区域选择一个子网。您必须至少选择一个子网。只能为每个可用区域选择一个子网。

对两个账号都执行一次



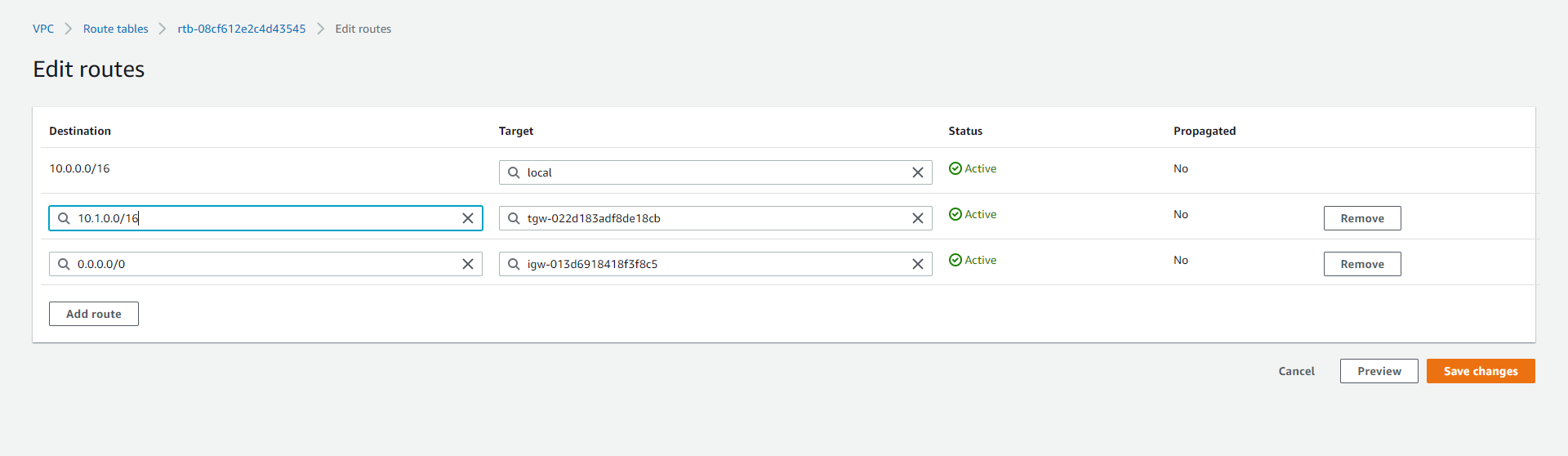
步骤五：向 VPC 路由表中添加路由

在导航窗格中，选择路由表。

选择 Routes (路由) 选项卡，然后选择 Edit routes (编辑路由)。

选择 Add route (添加路由)。

在 Destination (目的地) 列中，输入目的地VPC的cidr。对于 Target（目标），请选择中转网关挂载 ID。



步骤六：测试中转网关

确认中转网关已成功创建，方法是：通过连接到每个 VPC 中的一个 EC2 实例，然后在它们之间发送数据，如 ping 命令。(使用私有IP发送ping)

