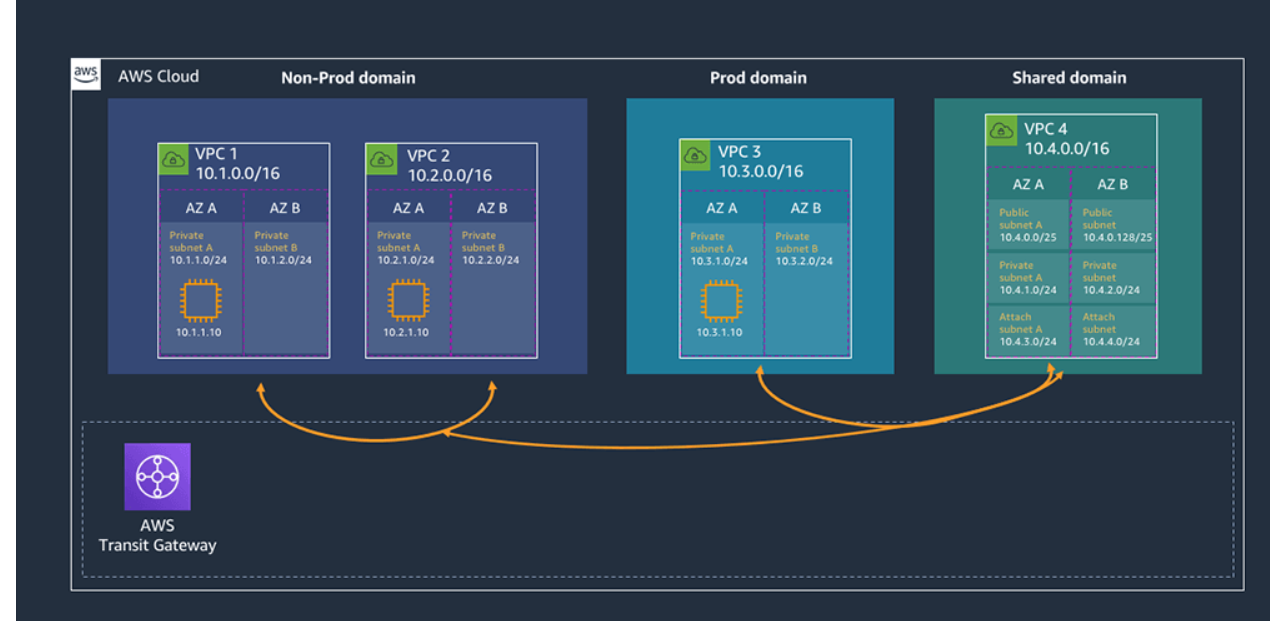
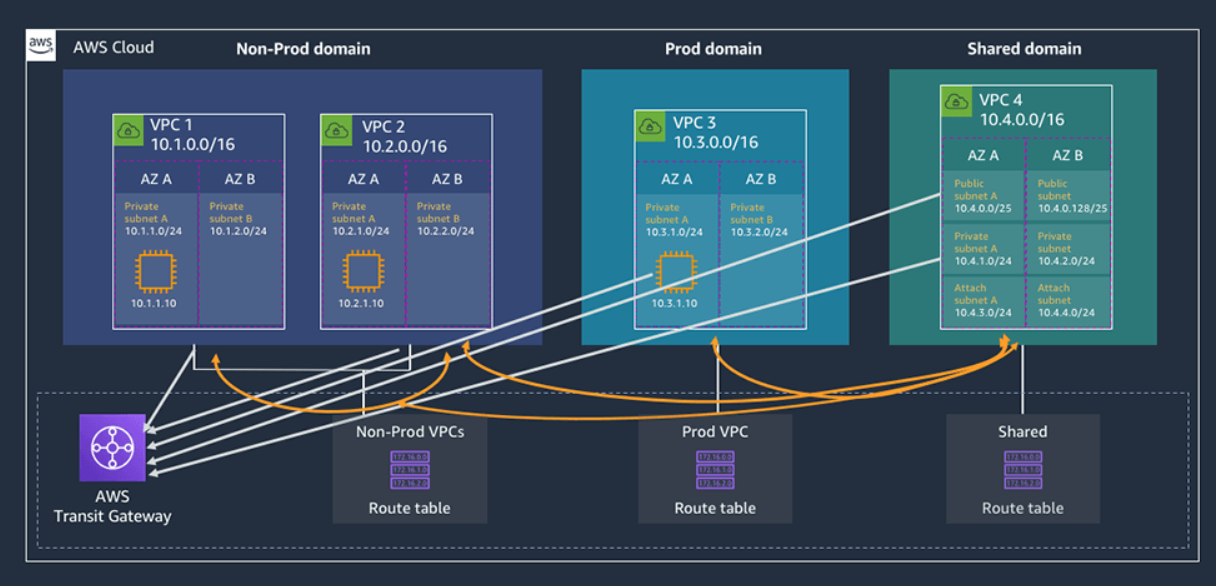
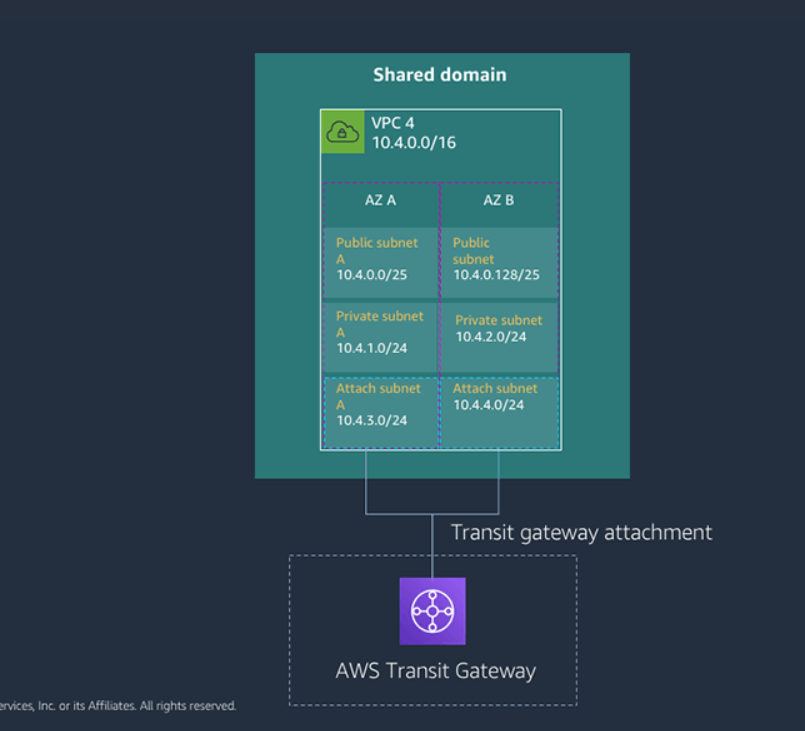
Transit gateway configuration:

2 attach subnets on different availability zone per vpc

The shared domain will have 2 attach subnets, 2 private subnets and 2 public subnets







Routing behaviour in the attach subnet:

You can have a routing table for the attach subnet that can redirect the traffic to a natgw, firewall appliance, another vpc,

**Transit Gateway creation:**

Name TAG

Description

ASN Number: must be unique and private (64512-65534)

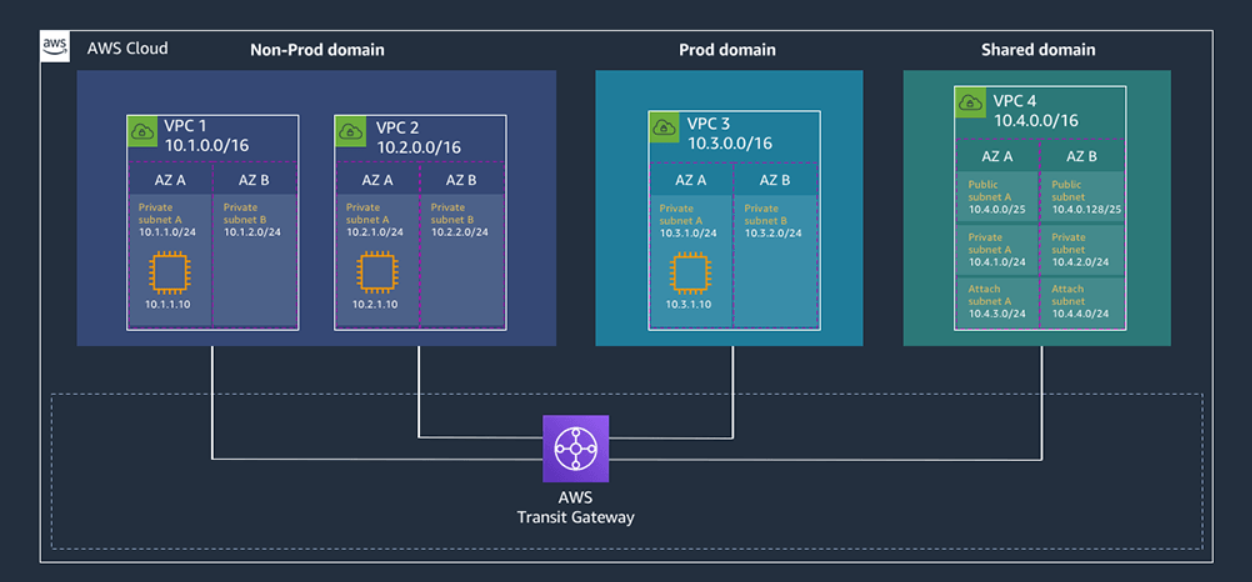
DNS Support: enable

VPN ECMP support: enable

Default route table association: disable

Default route table propagation: disable

Auto accept shared attachments: disable



**Transit gateway attachments: (one attachment per vpc)**

Transit gateway id

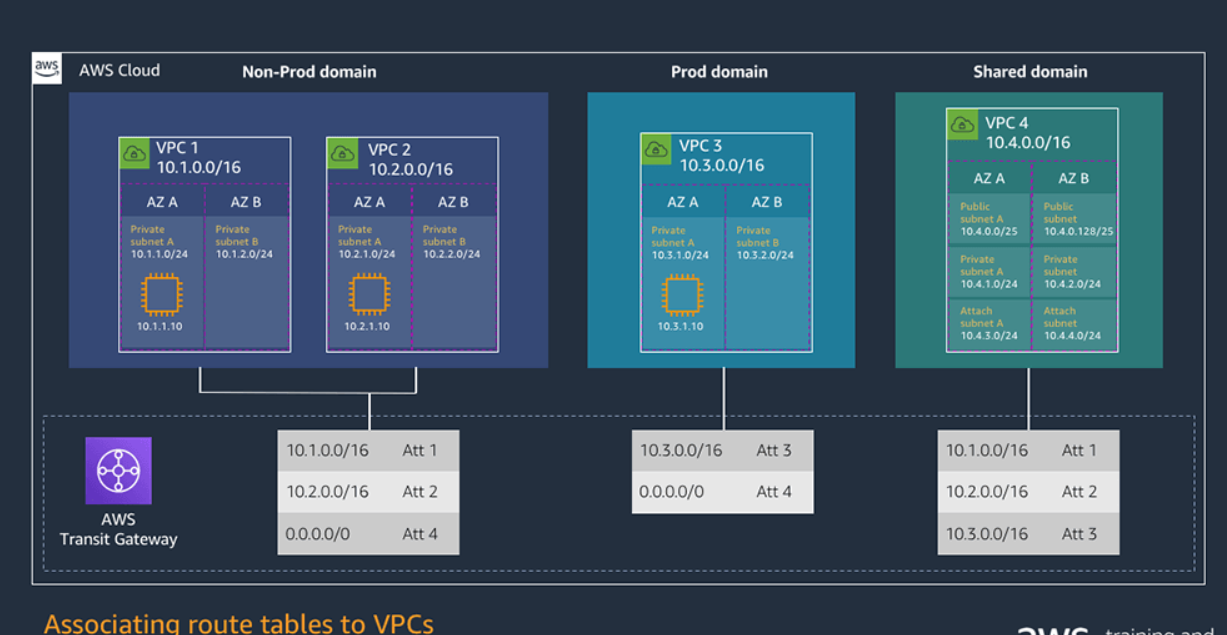
Attachment type (VPC, VPN…)

Name tag

DNS support

VPC ID

Subnet IDs: one attachment per AZ (Subnets in the spoke vpc)



**Create transit gateway route table (ONE PER VPC OR PER DOMAIN)**

Name

Transit gateway ID

**Associate the VPCs to the routing tables**

Transit gateway ID

Transit gateway route table ID

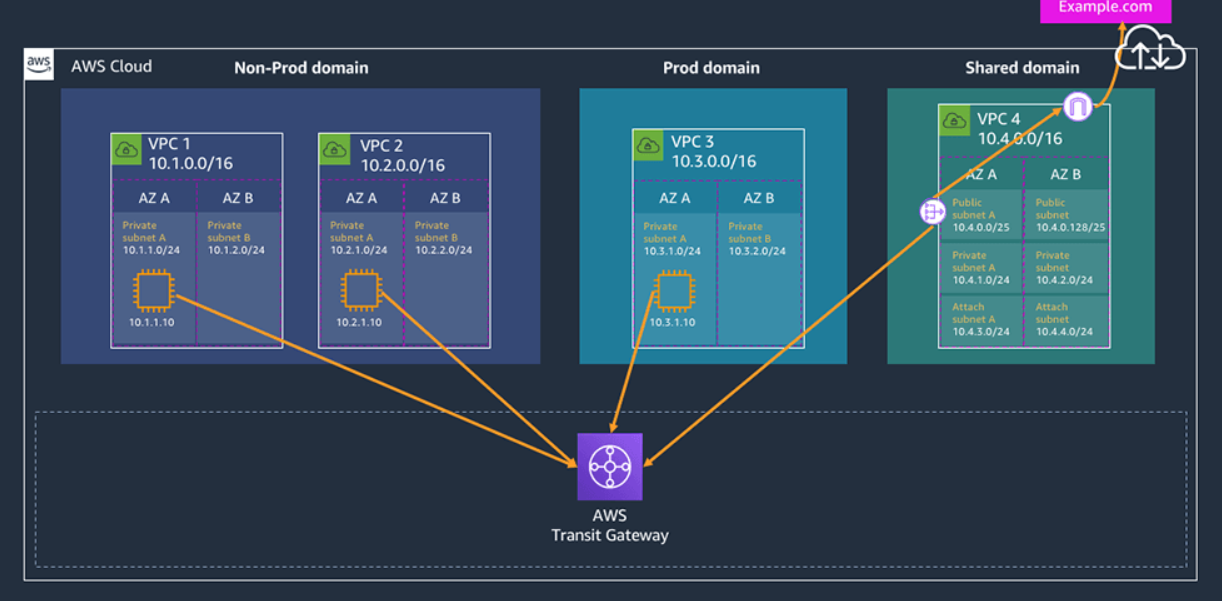
Chose attachment to associate (Attachment ID)

**Propagating VPC CIDRs into the TGW route tables**

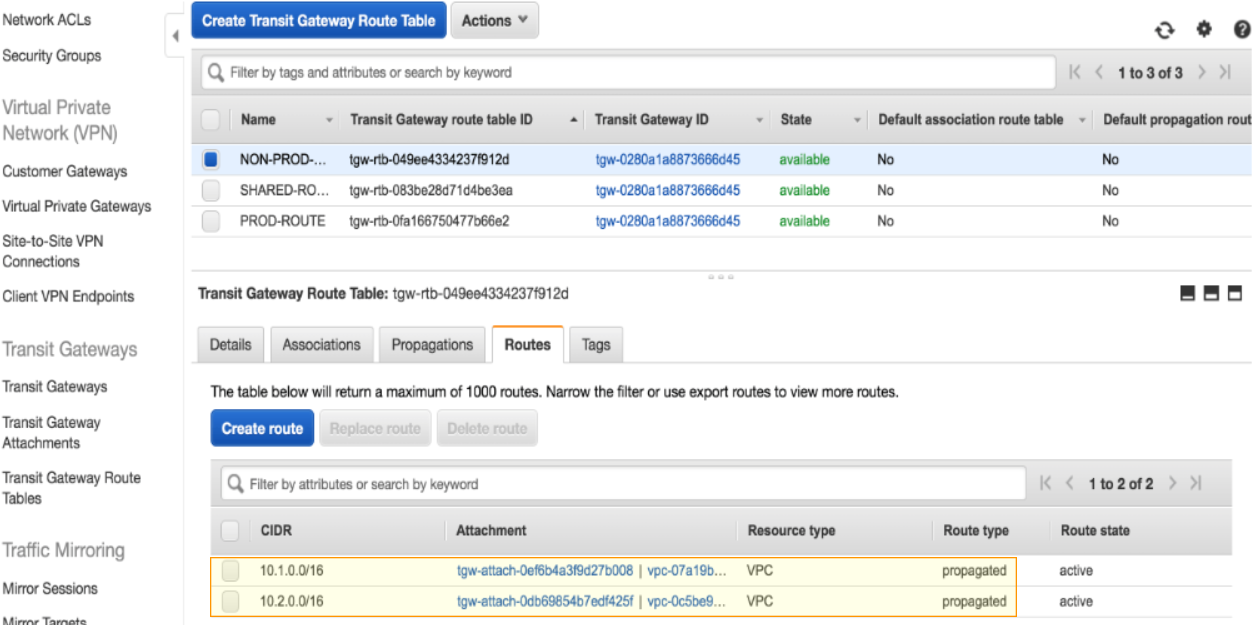
Transit gateway ID

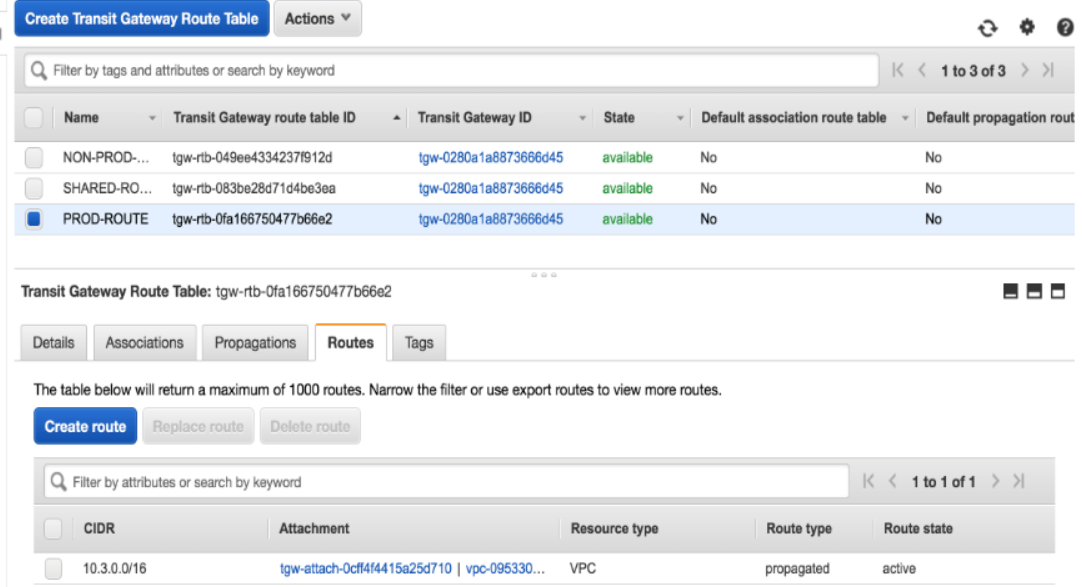
Transit gateway route table ID

Chose attachment to propagate (Attachment ID)



**Create static default routes on the spoke tgw route tables to the hub network vpc (Shared domain)**





**Create routes in the TGW route tables**

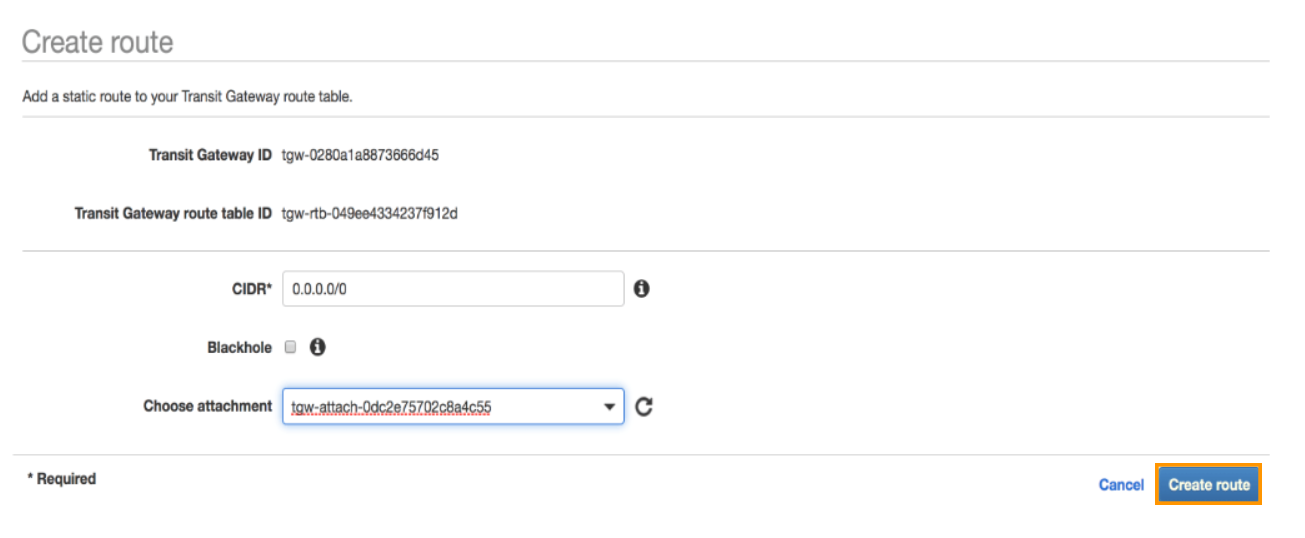
Transit gateway ID

Transit gateway route table id

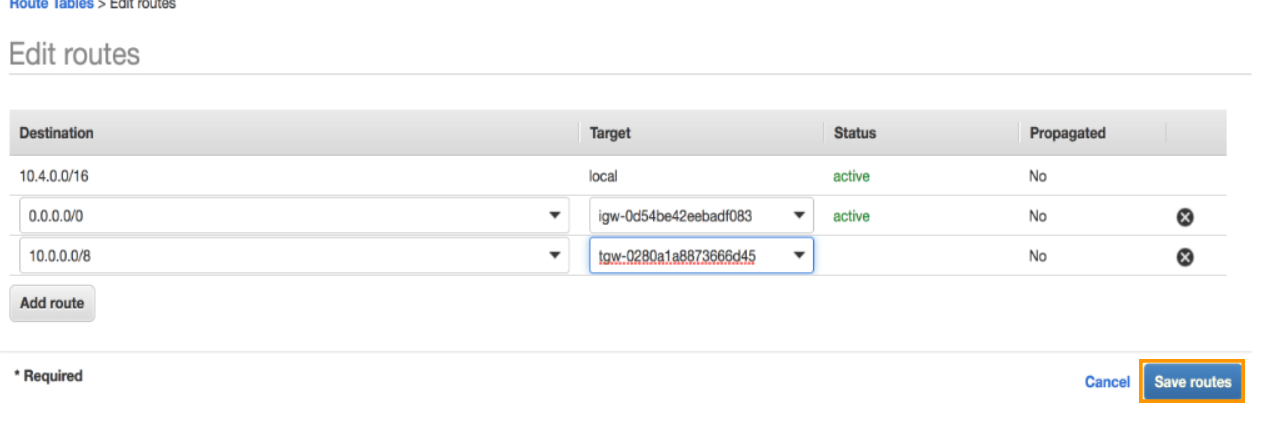
CIDR

Blackhole

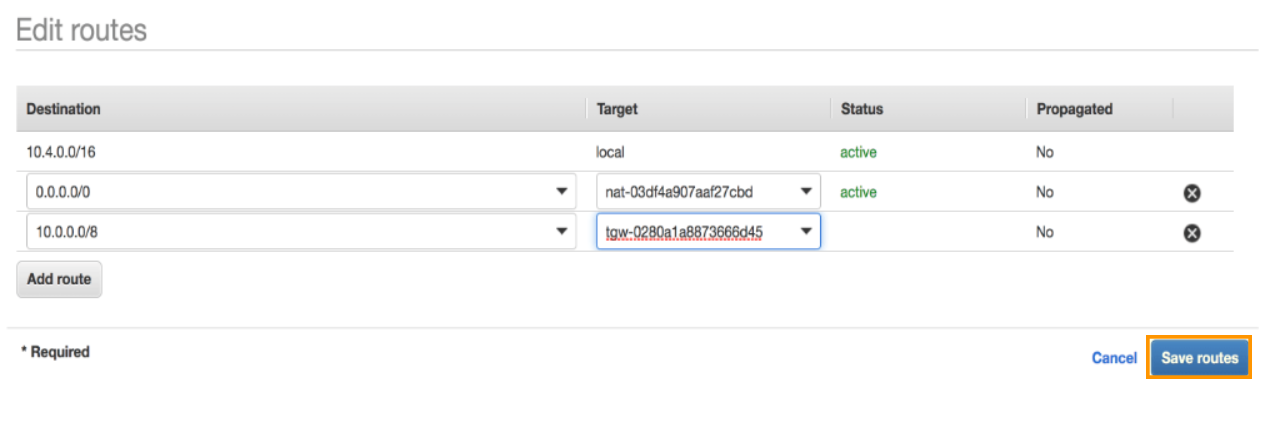
Choose attachment

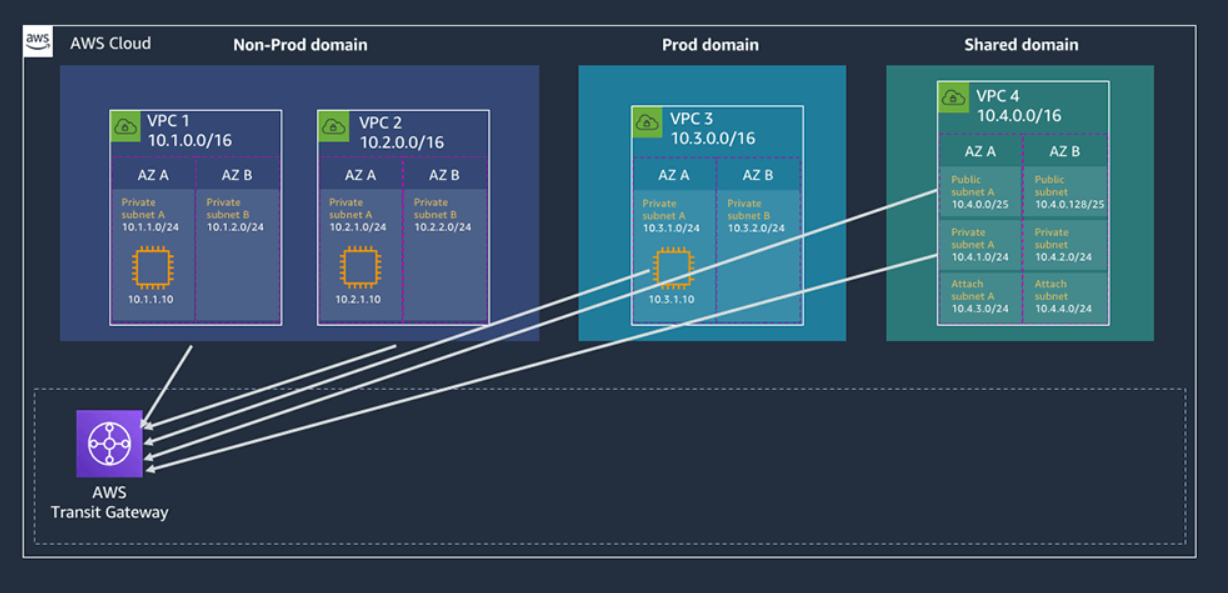


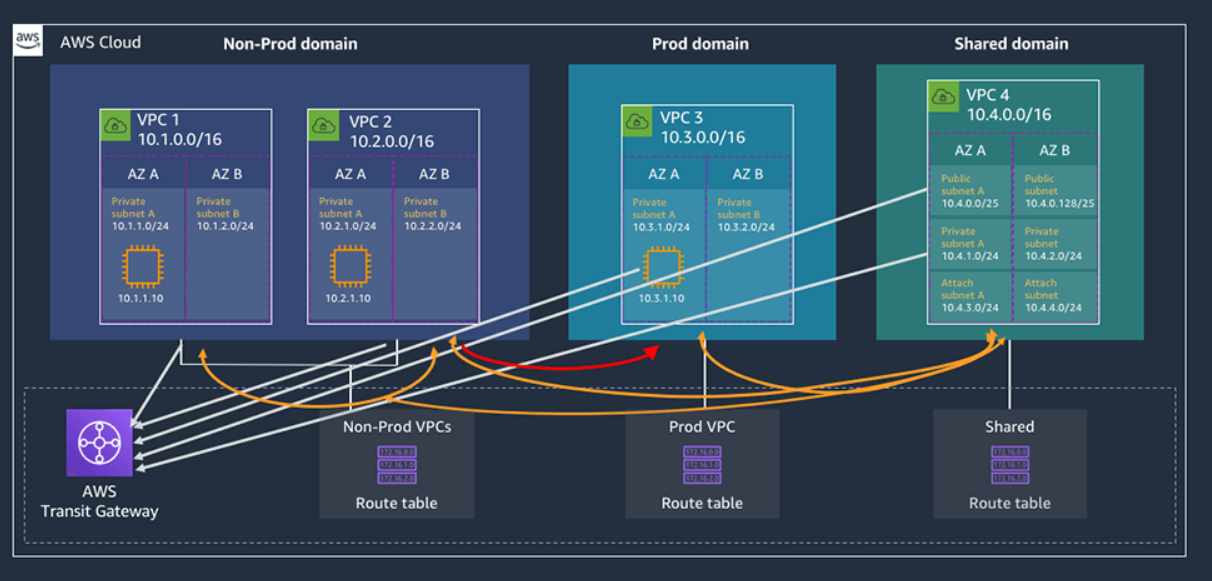
**Static route on public subnet in the hub vpc (shared vpc)**



**Static route on the private subnet in the hub vpc (shared vpc)**







**Creating a blackhole in the prod domain**

