VPC Connectivity Options

At the core of the lesson

You will learn how to differentiate the options for VPC connectivity.

VPC connectivity scenarios and solutions

If You Must:	Consider Using:	Solution Category
Connect a private subnet to the internet	• Network address translation (NAT) gateway • NAT instance	• Amazon Elastic Compute Cloud (Amazon EC2) instance connectivity
Connect a VPC to another VPC	VPC peering	VPC to VPC
Connect a VPC to an external network	• AWS Site-to-Site VPN • AWS Direct Connect plus VPN	• Network to VPC • Virtual private network (VPN) connectivity
Connect a VPC to Amazon Web Services (AWS) services without leaving the AWS network	• AWS PrivateLink • VPC gateway endpoint	• VPC to VPC • VPC gateway endpoint
Connect a VPC to multiple VPCs and external networks	AWS Transit Gateway	• Network to VPC • VPC to VPC

Connect a private subnet to the internet

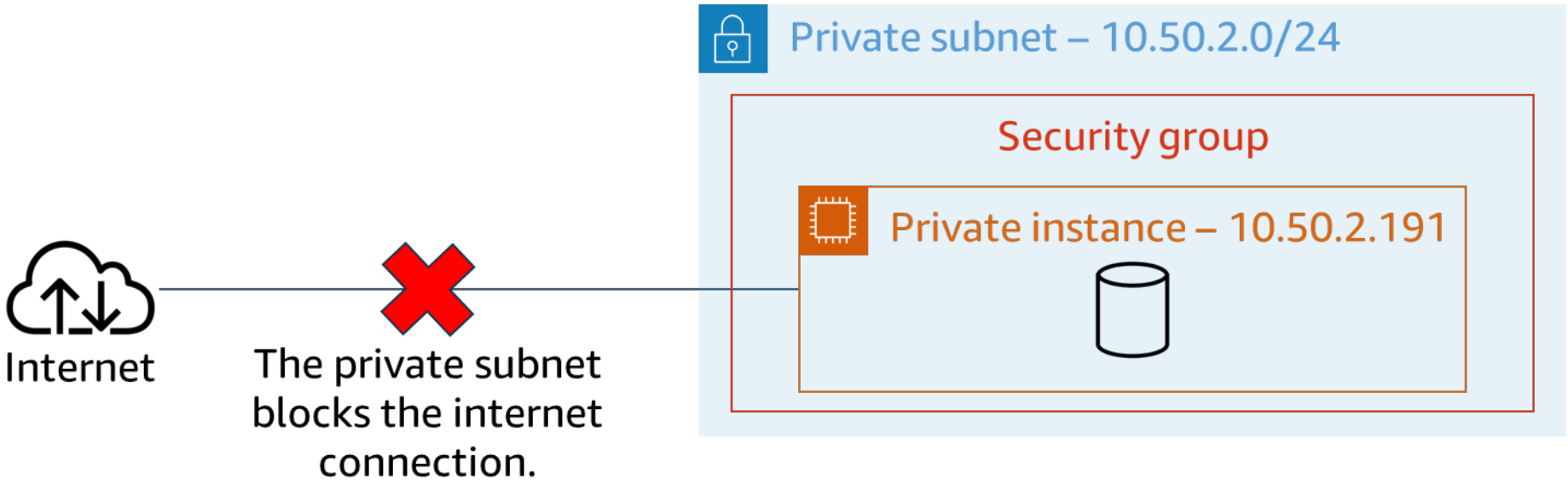
Network address translation

Challenge

An EC2 instance in a private subnet must connect to the internet.

Solutions

- NAT gateway
- NAT instance



NAT gateway characteristics and creation steps

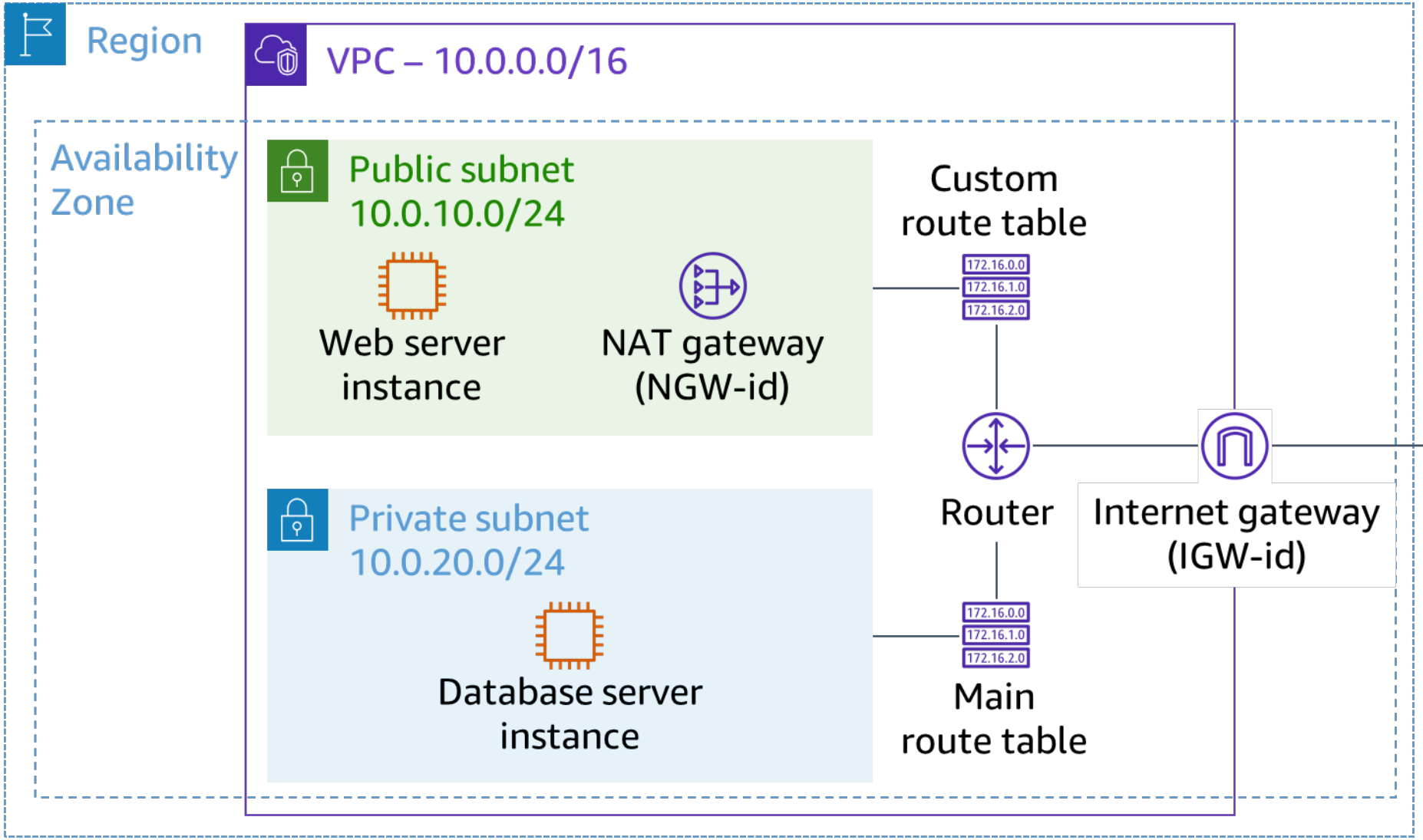
Characteristics

- Is an AWS managed service
- Is implemented with built-in redundancy within an Availability Zone
- Requires an Elastic IP address
- Supports the following protocols:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Internet Control Message Protocol (ICMP)

Creation steps

1. Choose the public subnet where the gateway will reside.
2. Assign an Elastic IP address to the gateway.
3. Update the route tables of the private subnets that will use the gateway.

Architecture of a VPC with a NAT gateway



Custom route table

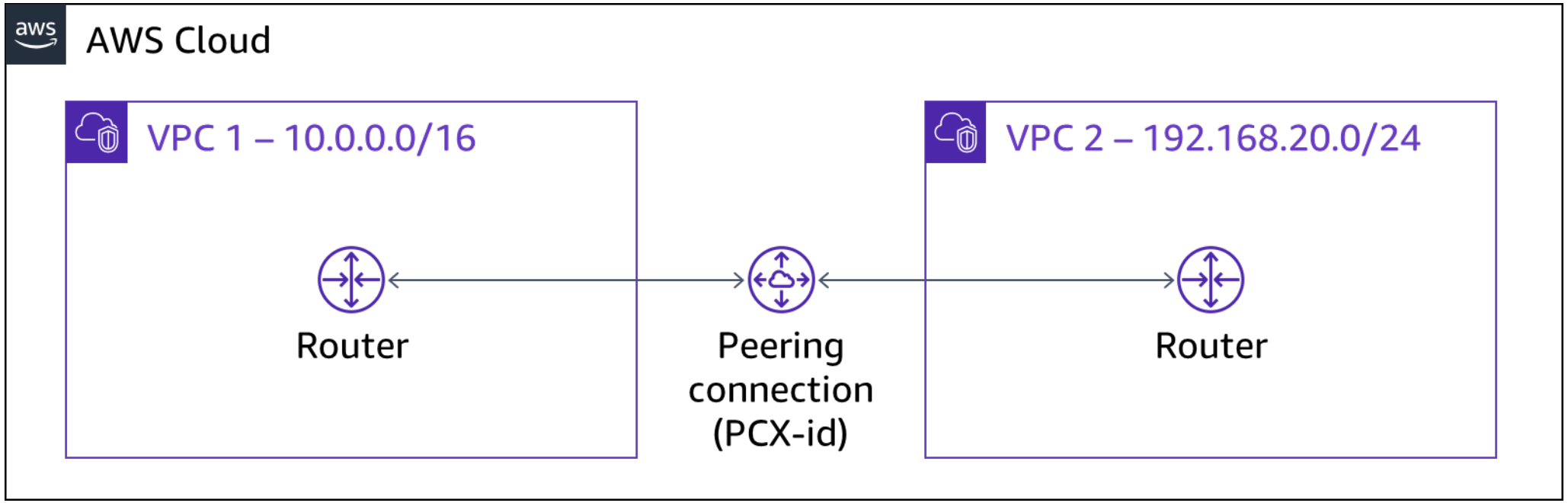
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW-id

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NGW-id

Connect a VPC to another VPC

VPC peering



VPC 1 route table

Destination	Target
10.0.0.0/16	local
192.168.20.0/24	PCX-id

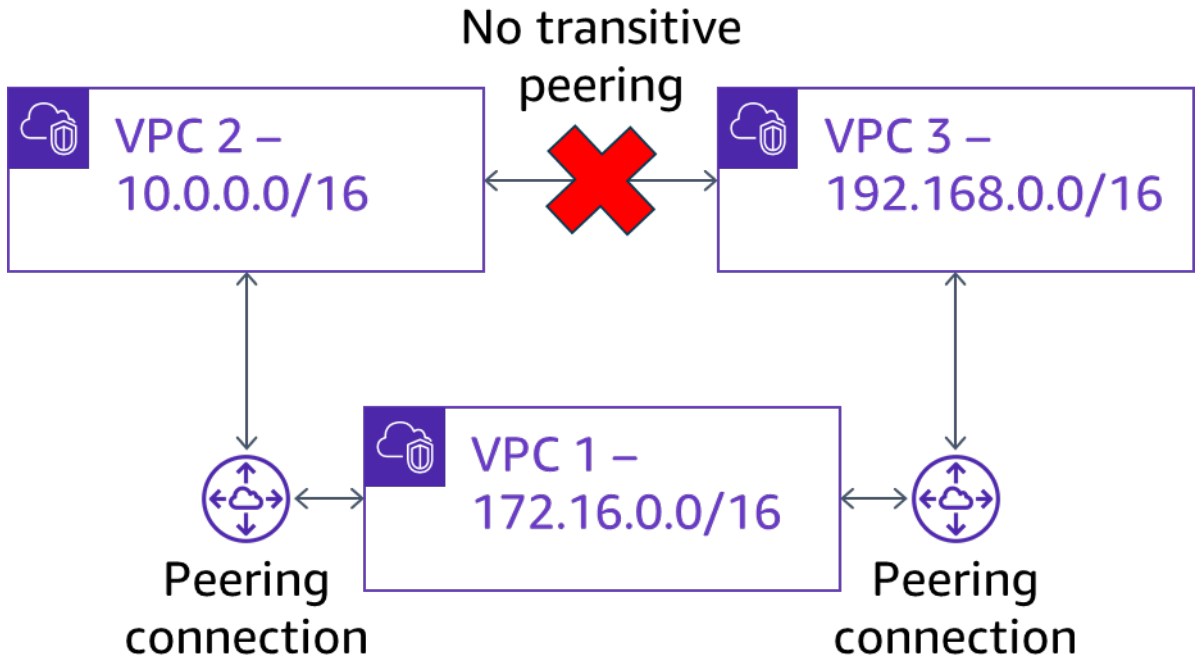
VPC 2 route table

Destination	Target
192.168.20.0/24	local
10.0.0.0/16	PCX-id

VPC peering limitations

The VPC peering limitations include the following:

- No overlapping IP address ranges.
- No transitive peering, edge routing, or internet gateway access.
- No NAT routing between VPCs.
- No Domain Name System (DNS) lookup resolution of private IP addresses.
- No cross-referencing of peer security groups across Regions.



Creating a VPC peering connection

The following are the steps for creating a VPC peering connection:

1. The owner of the requester VPC sends a VPC connection request.
2. The owner of the accepter VPC accepts the VPC connection request.
3. Both owners add route table entries in both participating VPCs.
4. If necessary, owners adjust security group rules in both participating VPCs.
5. If necessary, owners turn on DNS hostname resolution for VPC connection.

Creating a VPC peering connection request

Command

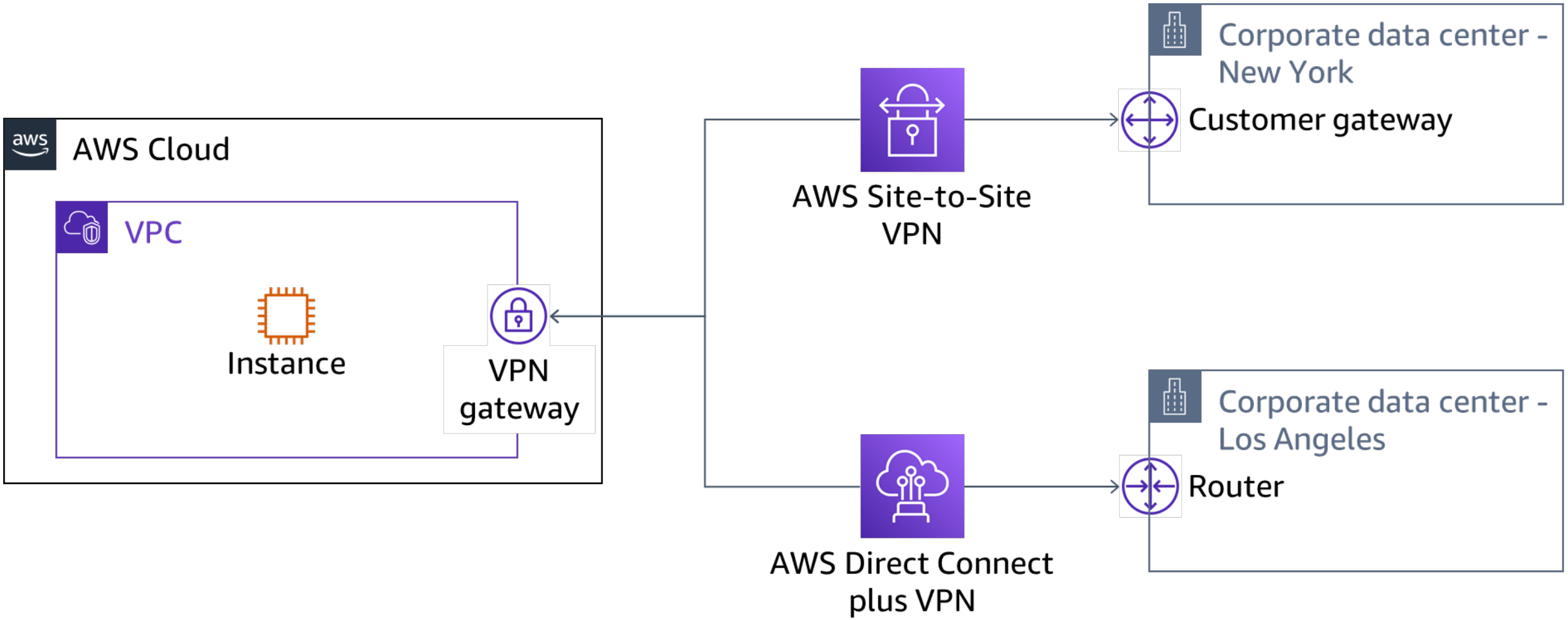
```
aws ec2 create-vpc-peering-connection \
--vpc-id vpc-1a2b3c4d \
--peer-vpc-id vpc-11122233
```

Result

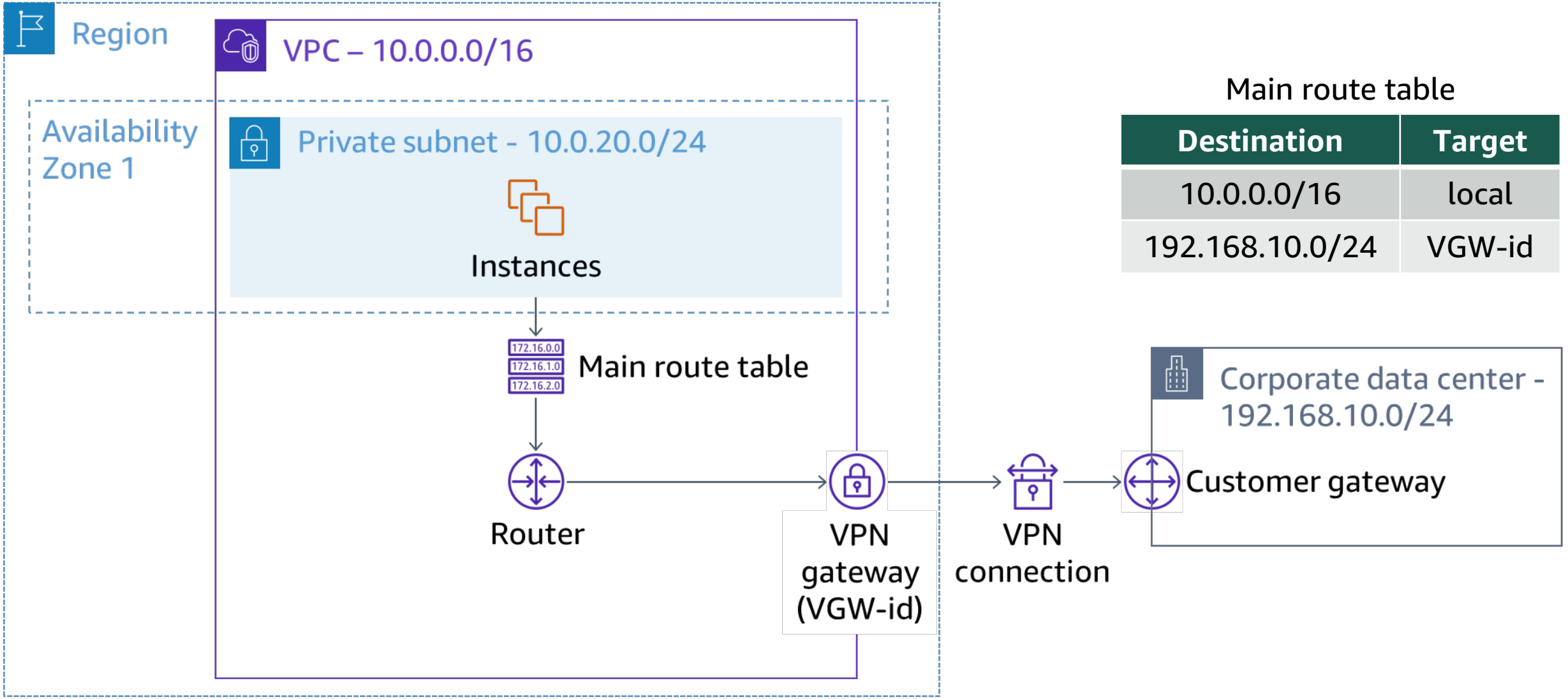
```
{
    "VpcPeeringConnection": {
        "Status": {
            "Message": "Initiating Request to 444455556666",
            "Code": "initiating-request"
        },
        "Tags": [],
        "RequesterVpcInfo": {
            "OwnerId": "444455556666",
            "VpcId": "vpc-1a2b3c4d",
            "CidrBlock": "10.0.0.0/28"
        },
        "VpcPeeringConnectionId": "pcx-111aaa111",
        "ExpirationTime": "2023-04-02T16:13:36.000Z",
        "AccepterVpcInfo": {
            "OwnerId": "444455556666",
            "VpcId": "vpc-11122233"
        }
    }
}
```

Connect a VPC to an external network

VPN connection options



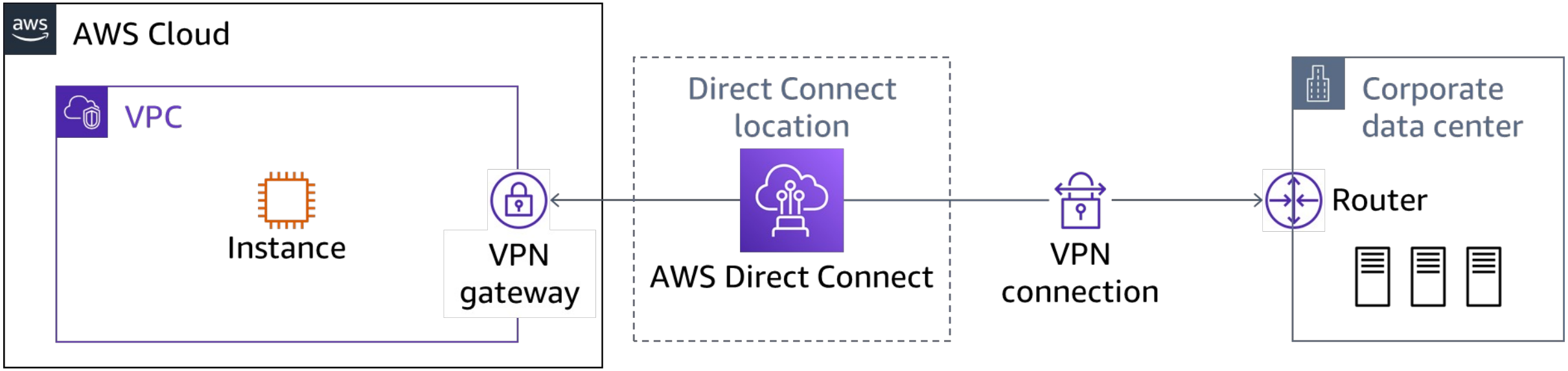
AWS Site-to-Site VPN



Main route table

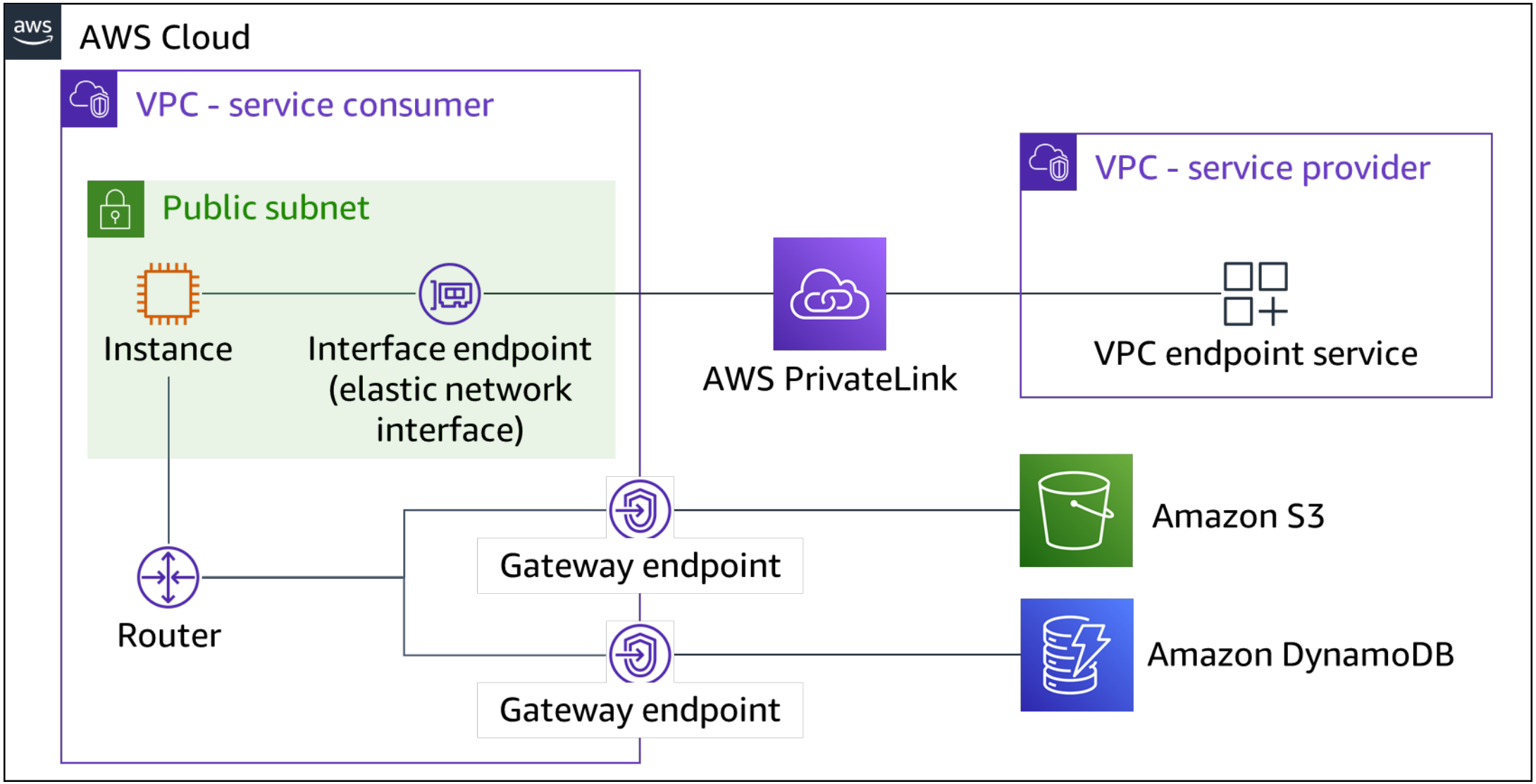
Destination	Target
10.0.0.0/16	local
192.168.10.0/24	VGW-id

AWS Direct Connect plus VPN

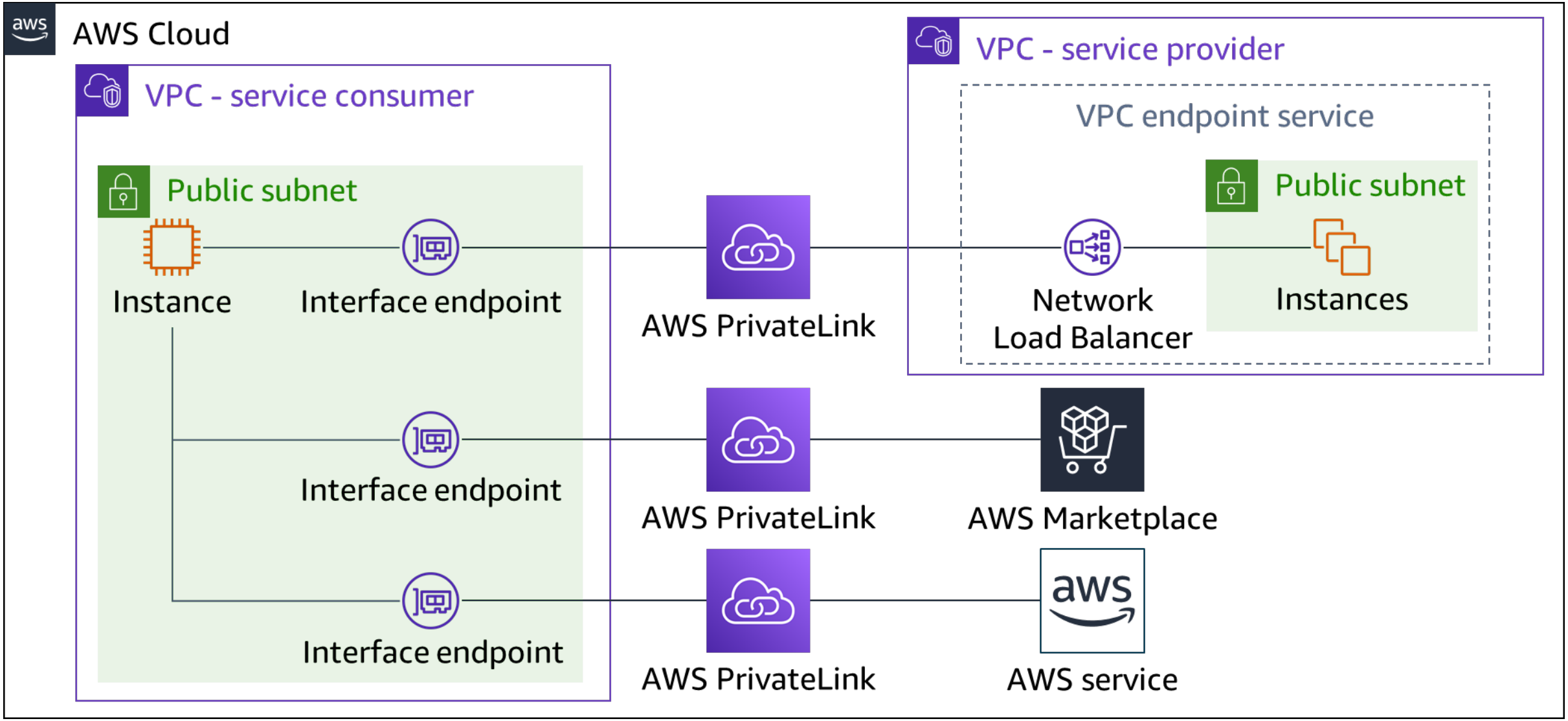


Connect a VPC to AWS services

VPC endpoints

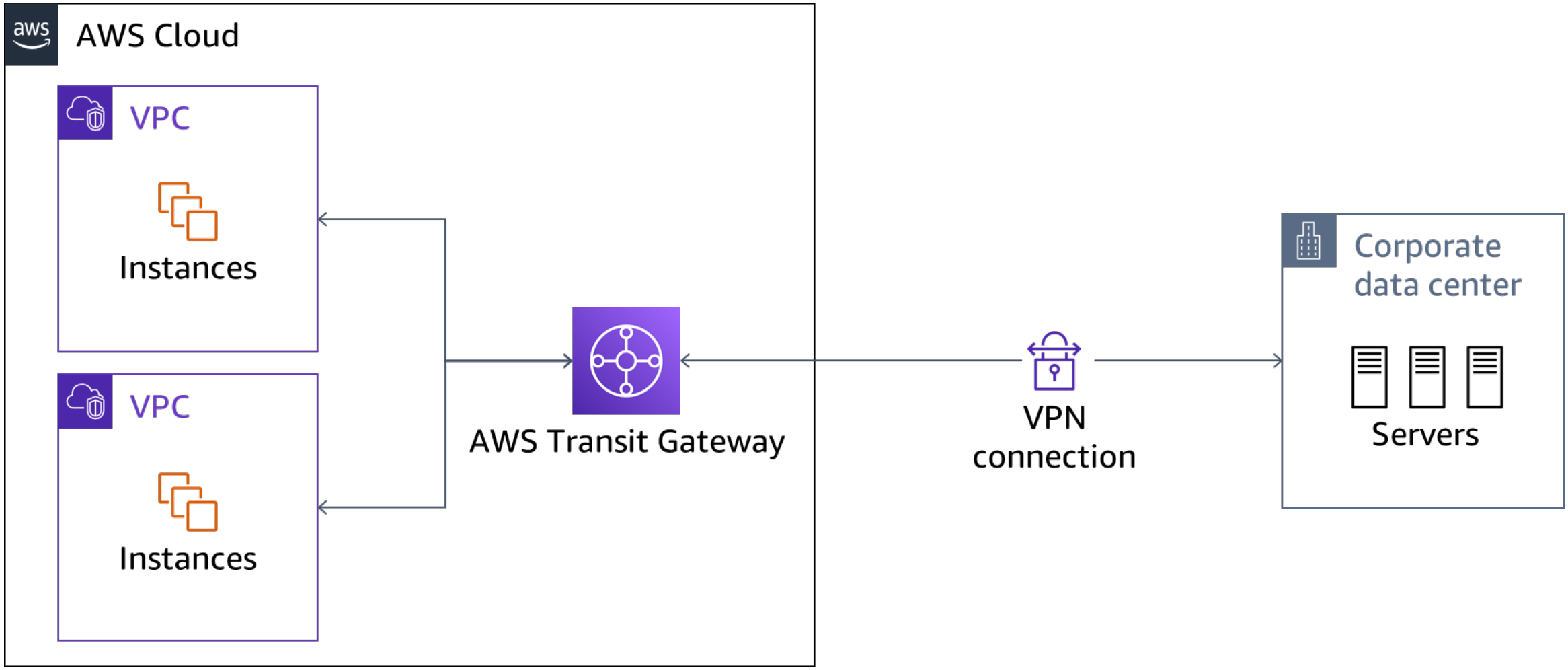


AWS PrivateLink interface endpoints



Connect a VPC to multiple VPCs and external networks

AWS Transit Gateway



Checkpoint questions

1. A network administrator wants to connect instances in a VPC to on-premises resources over the internet. The data communication must be encrypted. Which VPC connectivity solution should the administrator use?
2. What is the difference between a VPC interface endpoint and a VPC gateway endpoint?
3. Why is Transit Gateway the preferred solution for connecting multiple VPCs and VPNs?

Key ideas

- A NAT device forwards traffic from an instance that is in a private subnet to the internet or other AWS services and then sends the response back to the instance.
- VPC peering connects two VPCs so that you route traffic between them using private addresses.
- A Site-to-Site VPN connection establishes a secure connection between your on-premises equipment and your VPCs.
- A VPC endpoint privately connects your VPC to supported AWS services and to services that are powered by PrivateLink without leaving the AWS network.
- Transit Gateway establishes a network transit hub that you can use to interconnect your VPCs and on-premises networks without using the public internet.

Thank you

Corrections, feedback, or other questions?
Contact us at https://support.aws.amazon.com/#/contacts/aws-training.
All trademarks are the property of their owners.