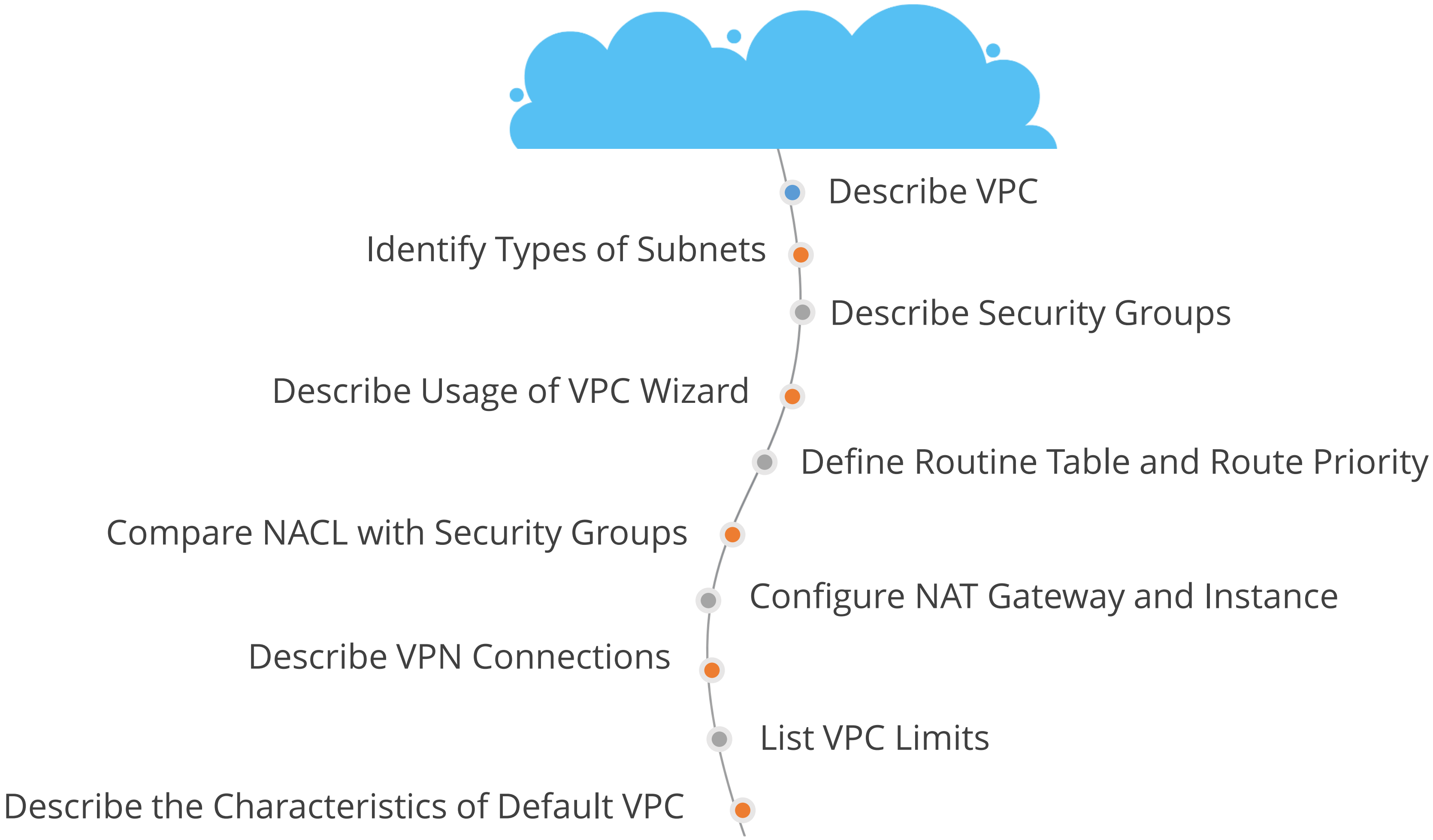
AWS Certified Developer Associate

Lesson 10: VPC

What You’ll Learn



- Describe VPC
- Identify Types of Subnets
- Describe Security Groups
- Describe Usage of VPC Wizard
- Define Routine Table and Route Priority
- Compare NACL with Security Groups
- Configure NAT Gateway and Instance
- Describe VPN Connections
- List VPC Limits
- Describe the Characteristics of Default VPC

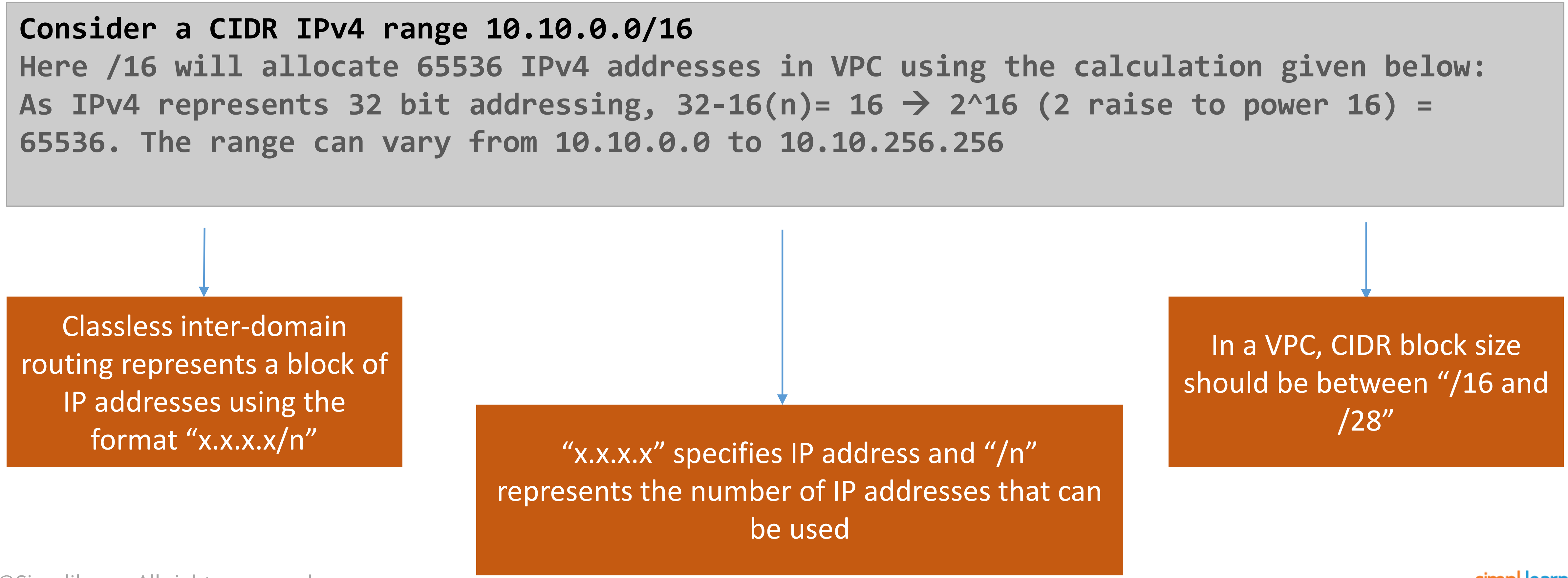
Basic Concepts of VPC

VPC Overview

- Sets up a logically isolated AWS cloud unit to launch your resources
- Contains one or more subnets
- Public subnet enables resources to connect to the Internet
- Private subnet does not allow resources to connect to the Internet
- Use default VPC when VPC is not needed

Classless Inter-domain Routing

For choosing a VPC and creating its subnets, you need to select the range of **private IP address** of the VPC and its subnets. This IP range will be further allocated to all the resources inside this VPC.



Consider a CIDR IPv4 range 10.10.0.0/16

Here /16 will allocate 65536 IPv4 addresses in VPC using the calculation given below: As IPv4 represents 32 bit addressing, 32-16(n)= 16 → 2^16 (2 raise to power 16) = 65536. The range can vary from 10.10.0.0 to 10.10.256.256

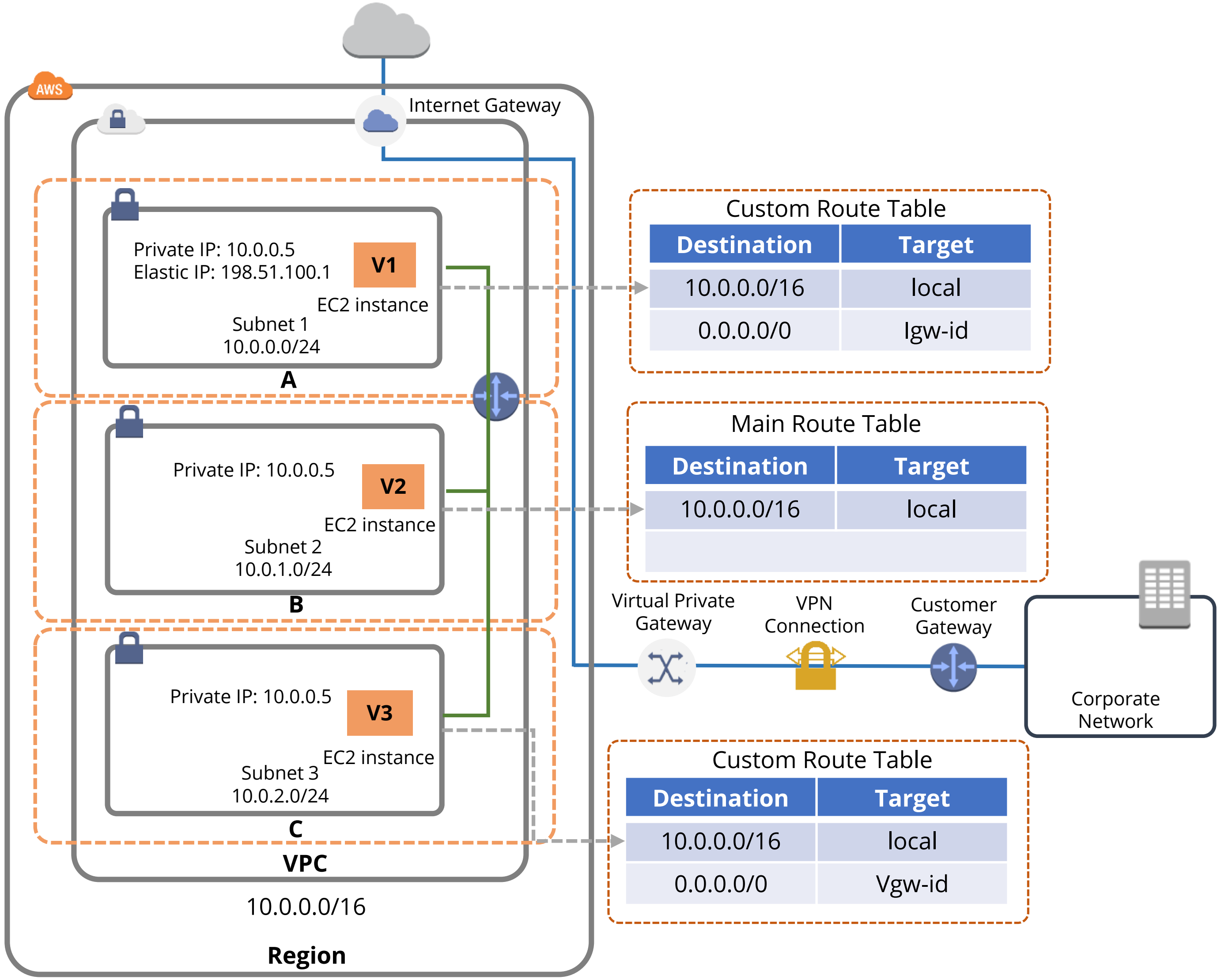
Classless inter-domain routing represents a block of IP addresses using the format “x.x.x.x/n”

“x.x.x.x” specifies IP address and “/n” represents the number of IP addresses that can be used

In a VPC, CIDR block size should be between “/16 and /28”

Subnets

- A subnet uses a subset of the IP addresses available to the VPC
- Subnets cannot span zones
- Each availability zone has one or more subnets
- The routing table controls the allowed routes
- Associate a custom route table while creating subnet



Custom Route Table

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

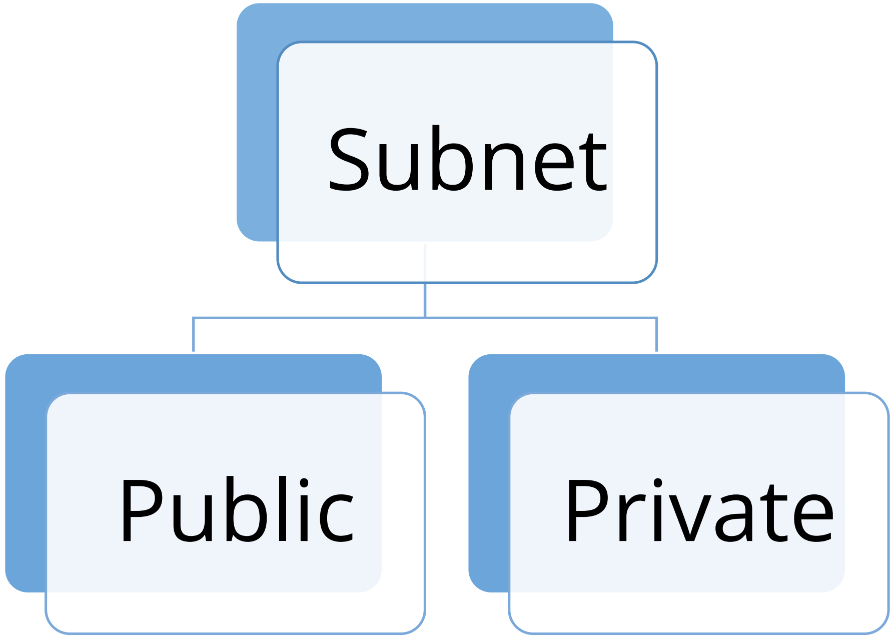
Main Route Table

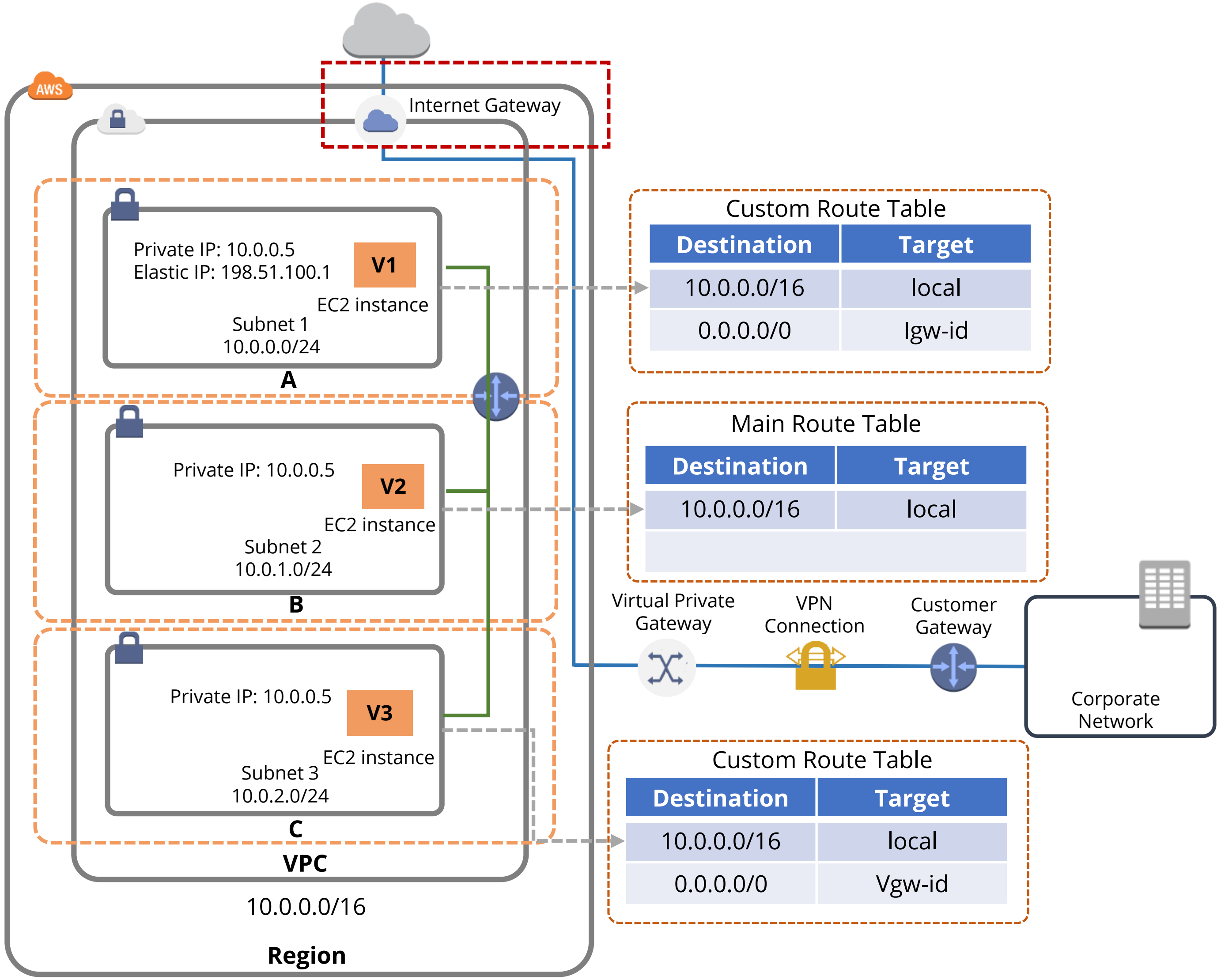
Destination	Target
10.0.0.0/16	local

Custom Route Table

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

Subnet Types





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

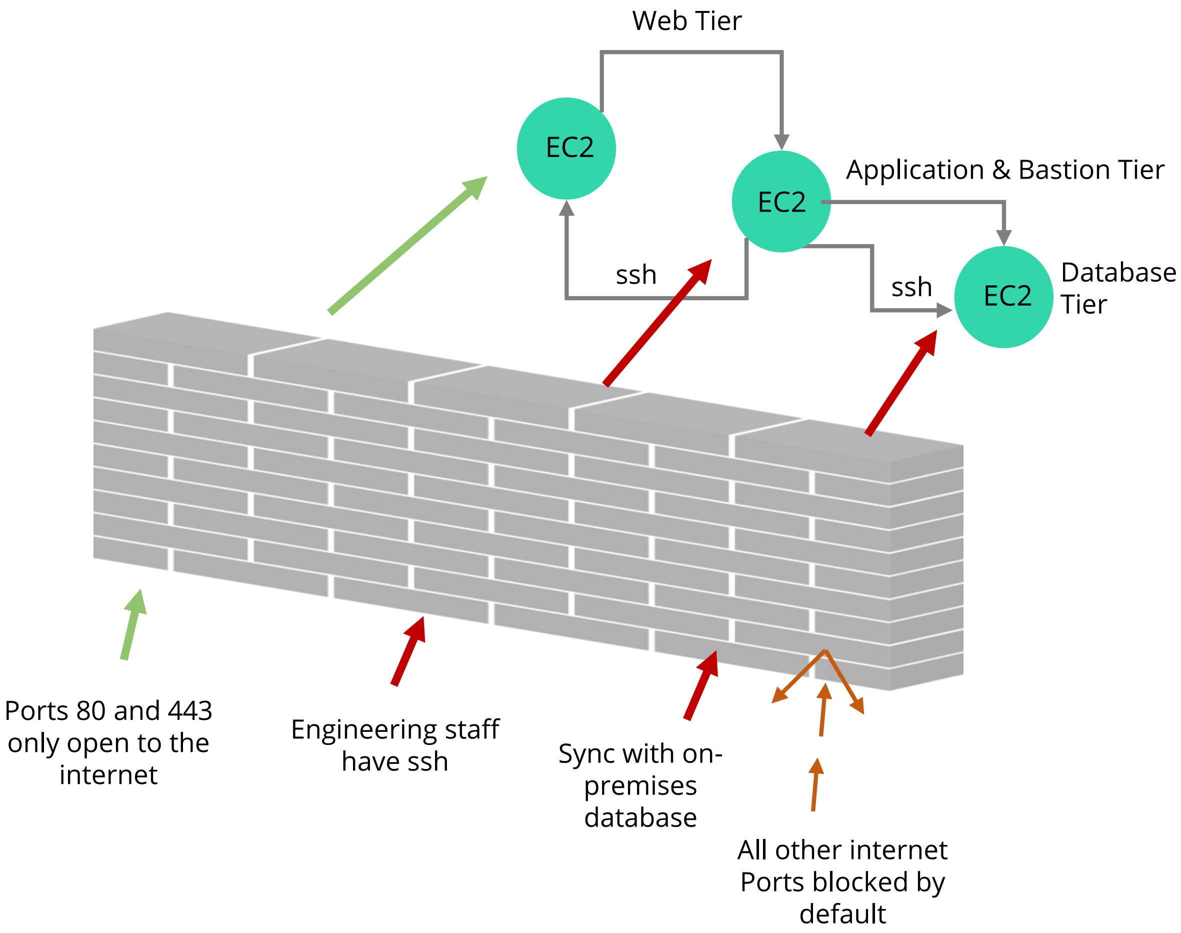
Custom Route Table

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

If the subnet is configured to route traffic to a virtual private gateway, it is called a "VPC Only" subnet.

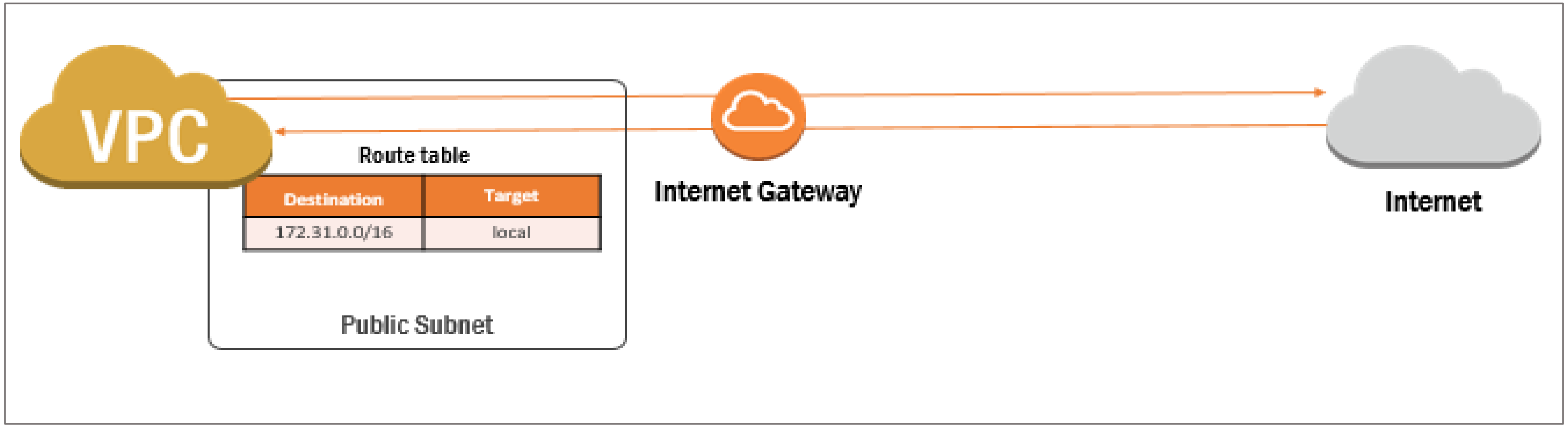
Security Groups

- Virtual firewall controls incoming and outgoing traffic
- A default security group allows traffic only from associated instances
- An instance can have multiple security groups attached
- Rules within a security group can be modified anytime
- Can be identified as source or destination



Web Tier
EC2
EC2
Application & Bastion Tier
ssh
ssh
EC2
Database Tier
Ports 80 and 443 only open to the internet
Engineering staff have ssh
Sync with on-premises database
All other internet Ports blocked by default

Internet Gateway

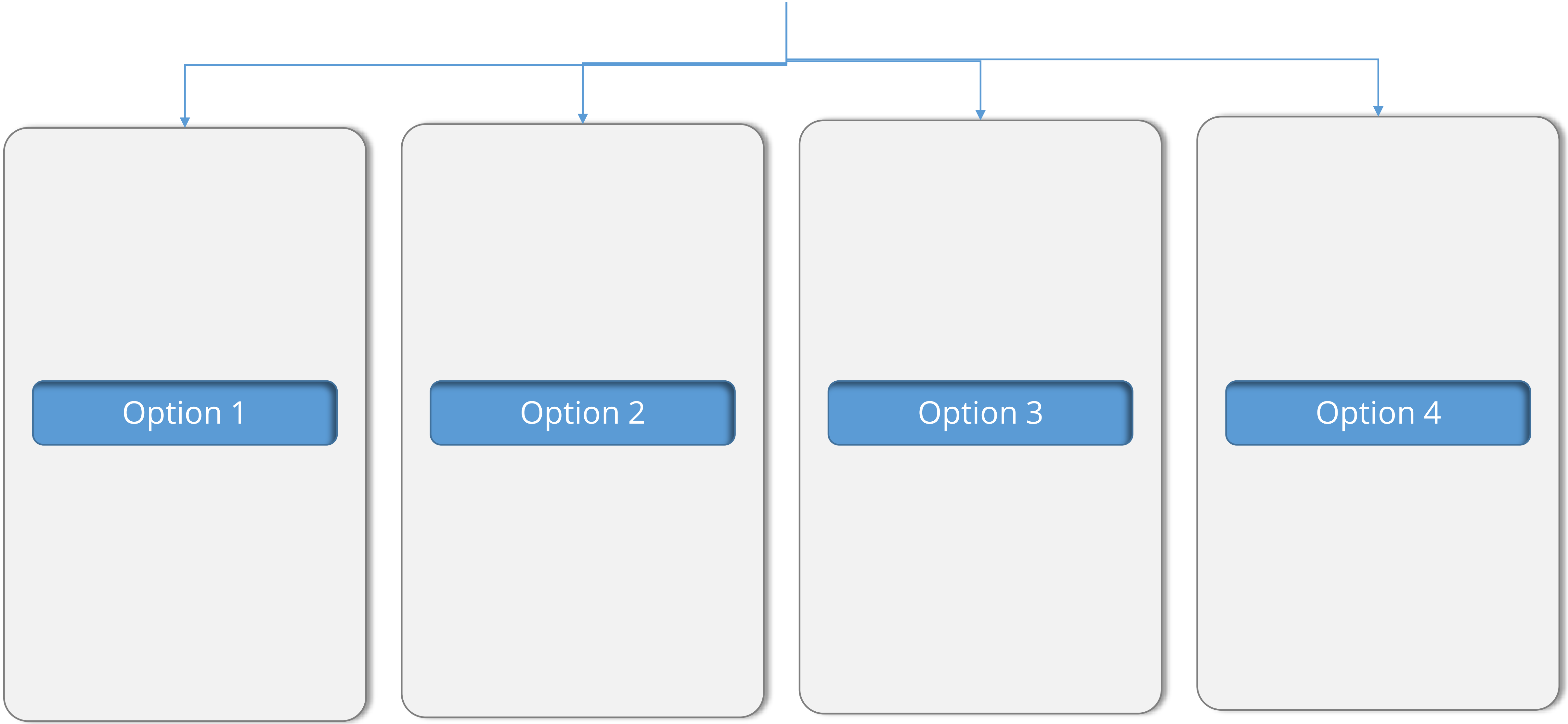


Destination	Target
172.31.0.0/16	local

Gateway is a device which connects two networks. One such gateway is Internet Gateway which connects instances in VPC with the Internet.

Internet gateway is a must for any VPC to allow its resources to communicate with the Internet.

VPC Wizard



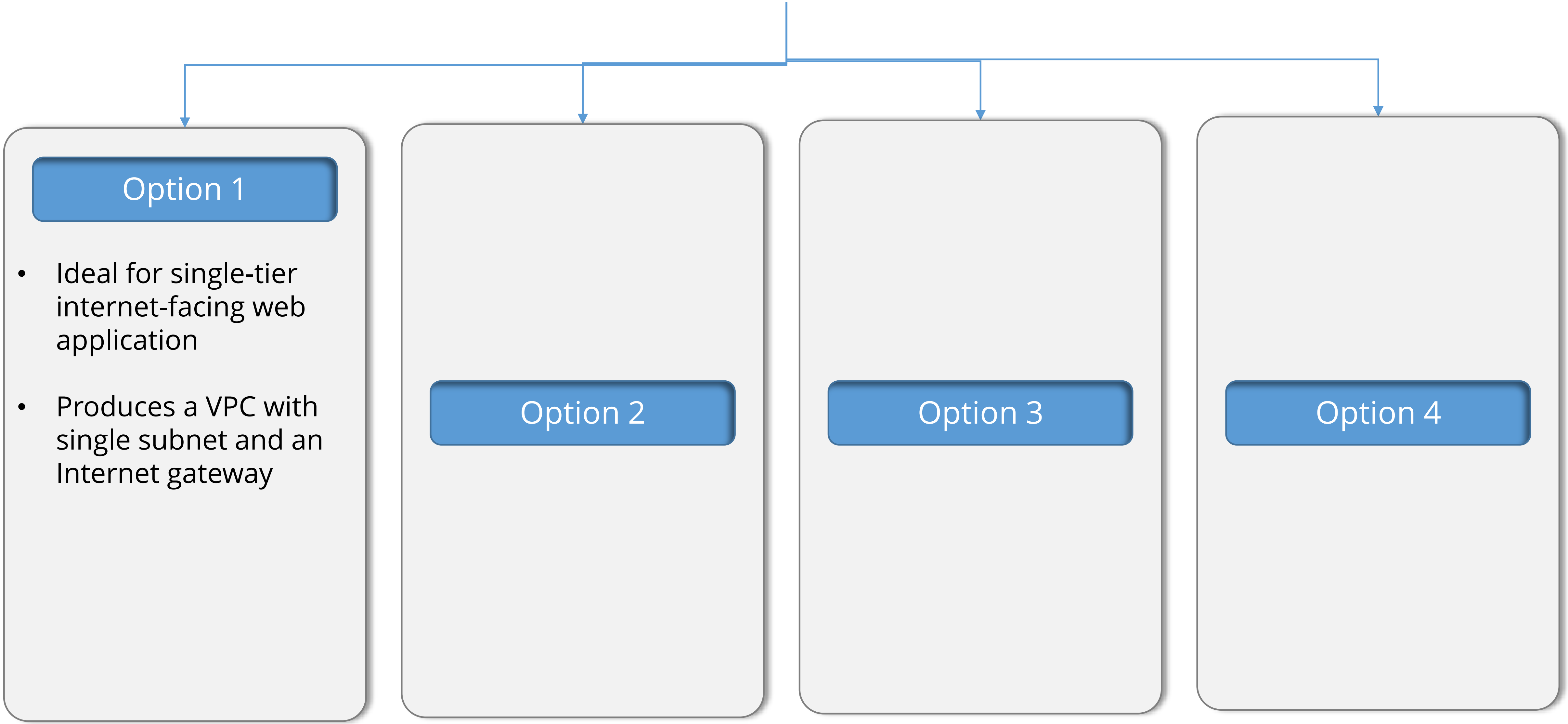
Option 1

Option 2

Option 3

Option 4

VPC Wizard



Option 1

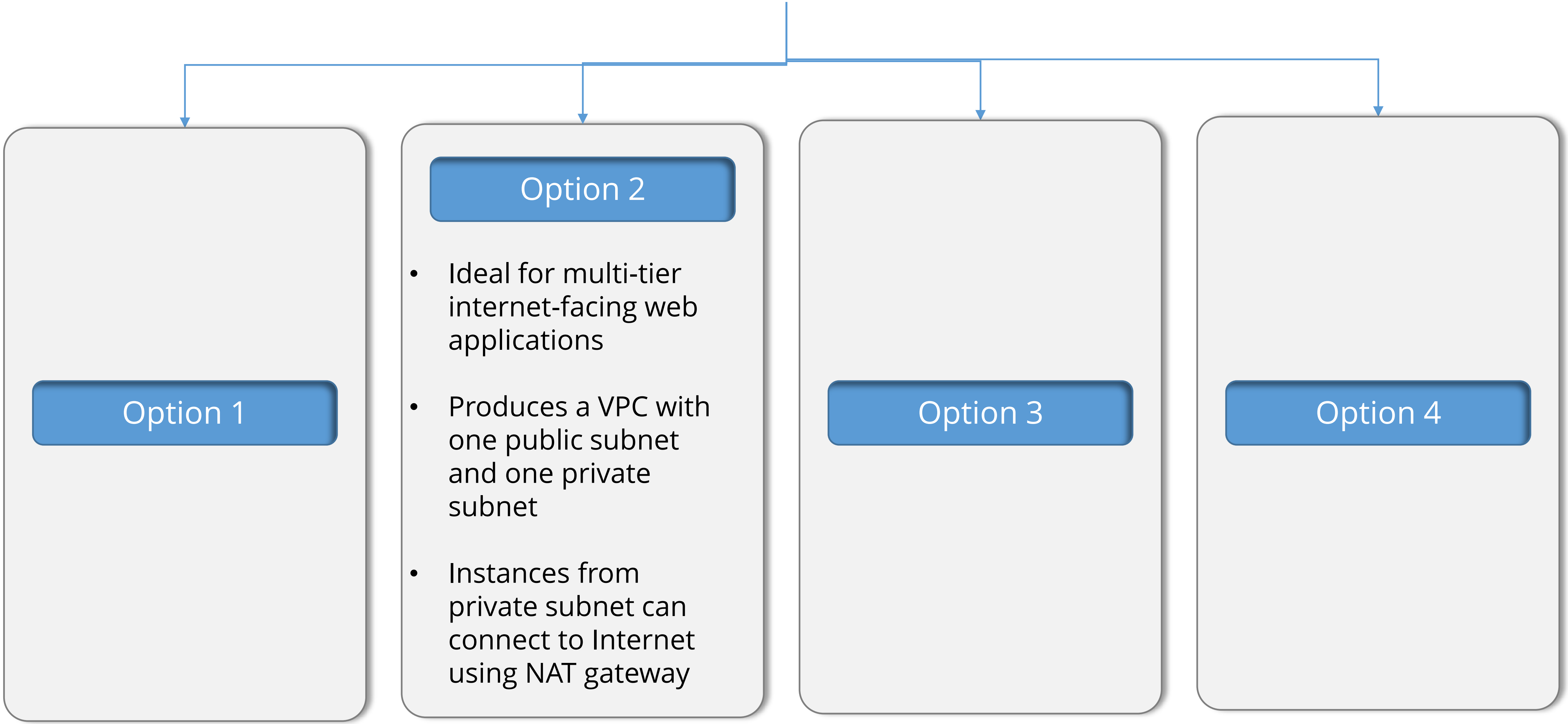
- Ideal for single-tier internet-facing web application
- Produces a VPC with single subnet and an Internet gateway

Option 2

Option 3

Option 4

VPC Wizard



Option 1

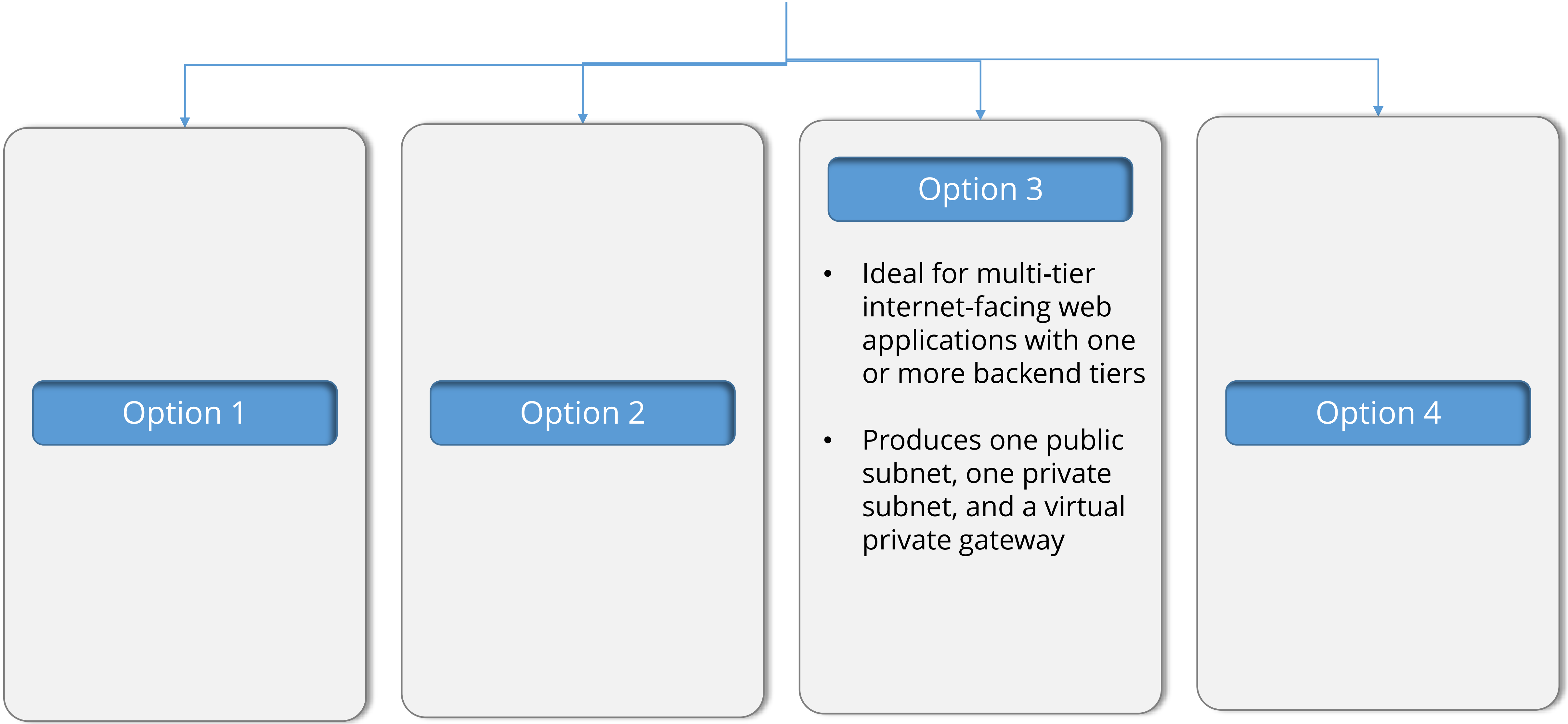
Option 2

- Ideal for multi-tier internet-facing web applications
- Produces a VPC with one public subnet and one private subnet
- Instances from private subnet can connect to Internet using NAT gateway

Option 3

Option 4

VPC Wizard



Option 1

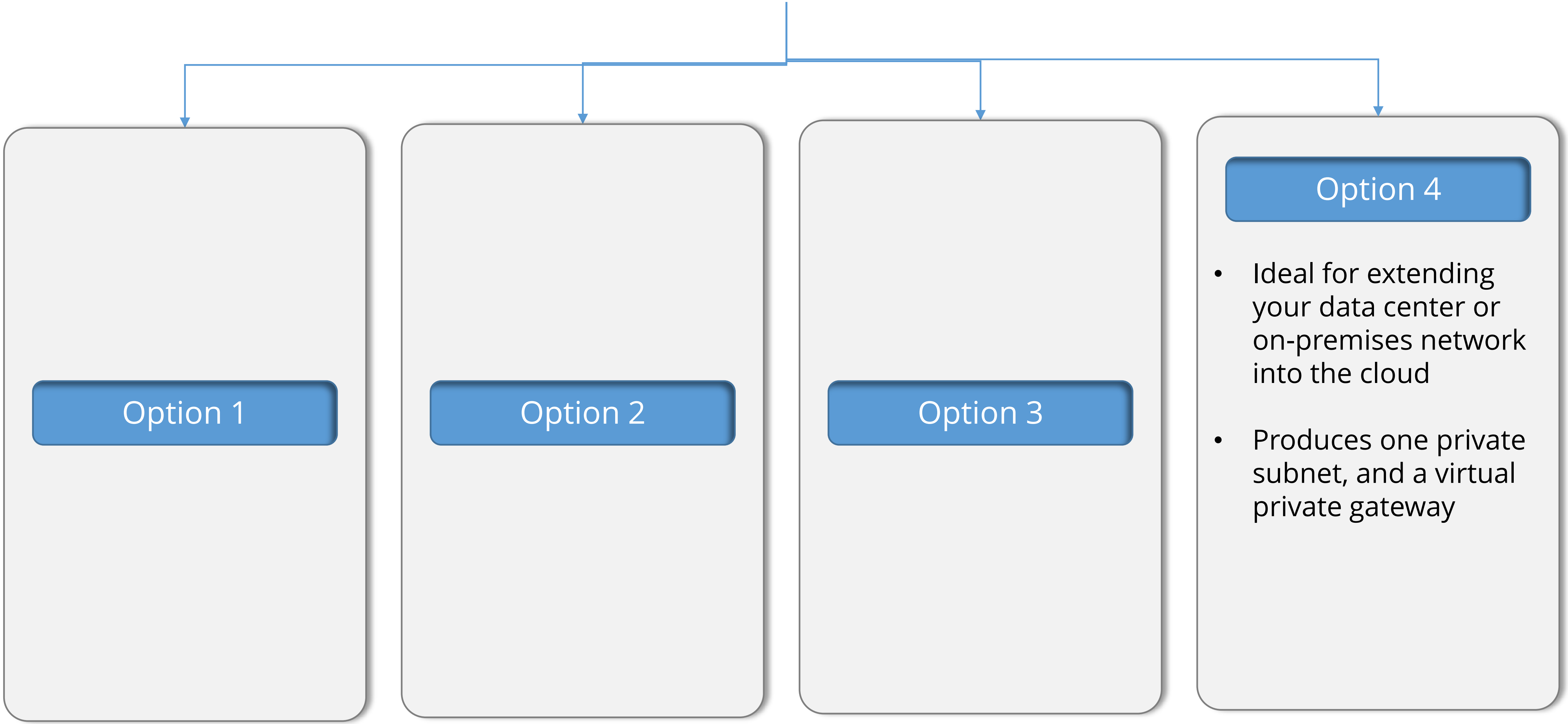
Option 2

Option 3

- Ideal for multi-tier internet-facing web applications with one or more backend tiers
- Produces one public subnet, one private subnet, and a virtual private gateway

Option 4

VPC Wizard



Option 1

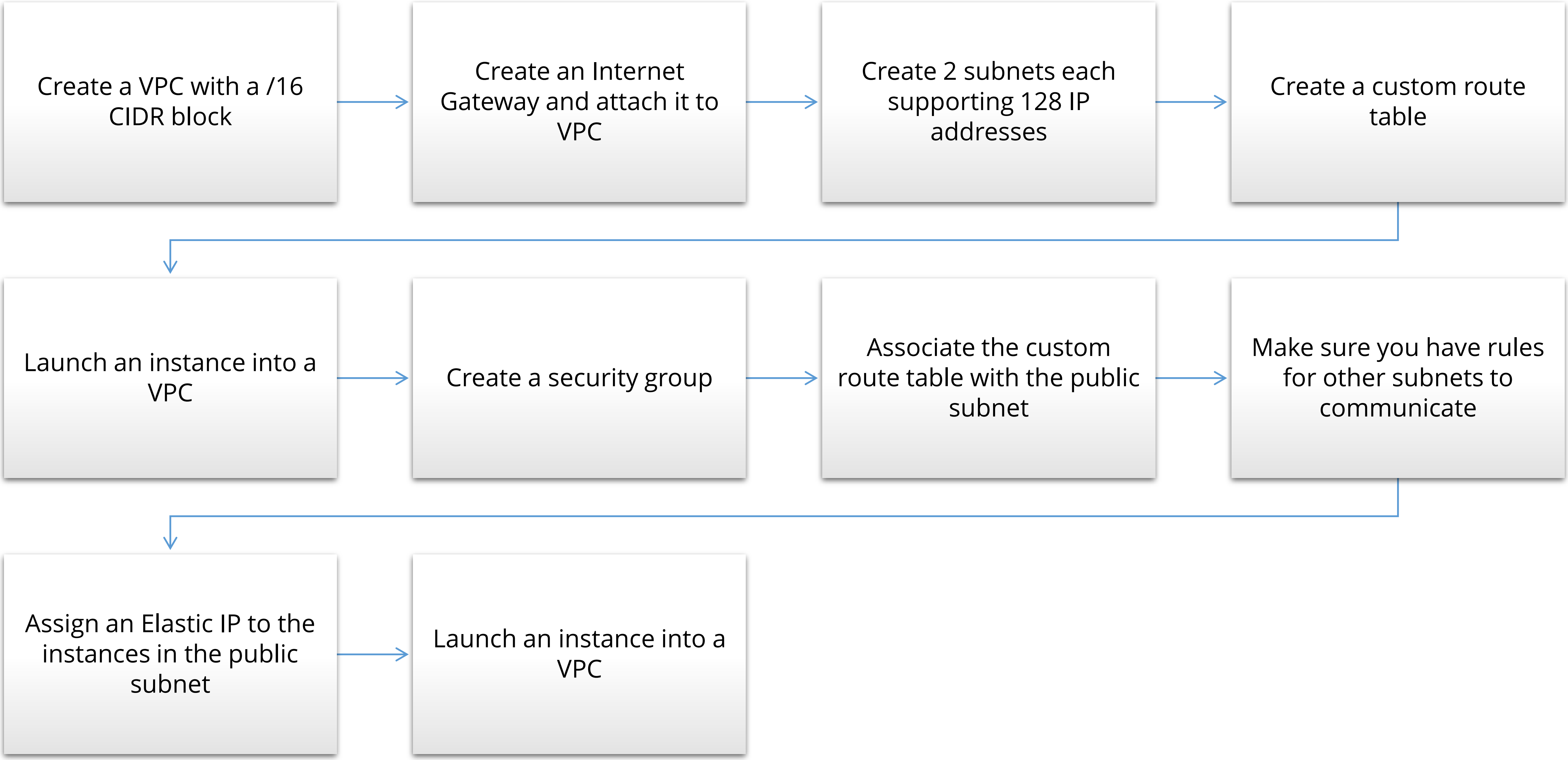
Option 2

Option 3

Option 4

- Ideal for extending your data center or on-premises network into the cloud
- Produces one private subnet, and a virtual private gateway

Manual VPC Creation



Create a VPC with a /16 CIDR block

Create an Internet Gateway and attach it to VPC

Create 2 subnets each supporting 128 IP addresses

Create a custom route table

Launch an instance into a VPC

Create a security group

Associate the custom route table with the public subnet

Make sure you have rules for other subnets to communicate

Assign an Elastic IP to the instances in the public subnet

Launch an instance into a VPC

Knowledge Check

KNOWLEDGE CHECK

What is the use of the Internet Gateway? (Choose 2)

a. Allows communication between instances in your private subnet and Internet

b. Allows communication between instances in your VPC and Internet

c. Performs network-address translation for instances that have public IP addresses

d. Performs network-address translation for instances that have private IP addresses

KNOWLEDGE CHECK

What is the use of the Internet Gateway? (Choose 2)

a. Allows communication between instances in your Private Subnet and Internet

b. Allows communication between instances in your VPC and Internet

c. Performs network address translation for instances that have public IP addresses

d. Performs network address translation for instances that have private IP addresses

The correct answer is **b and c**

Explanation: Internet Gateway is a highly scalable VPC component that allows communication between instances in your VPC and the Internet. Internet Gateway should be the target in your subnet's routing table. In addition, Internet Gateway performs network-address translation for instances that have public IP addresses.

VPC – Deep Dive

IP Addressing

- Private IP address is used to communicate and send traffic between instances in the same VPC
- Selected from the address range of the subnet CIDR block
- In EC2-classic, Private IP address remains with an instance when it’s stopped and restarted
- Additional private IP is known as secondary private IP address

Private

Public

Elastic

IP Addressing

- Public IP addresses are reachable over the Internet
- Instances that are launched in the default subnet receive a public IP address
- Public IP address comes from Amazon’s pool of available public IPs
- Cannot manually associate or disassociate a public IP address

Private

Public

Elastic

IP Addressing

- Elastic IP address is a static, Public IP address
- Elastic IP provides the flexibility to attach and detach from an instance
- It is a paid service from AWS

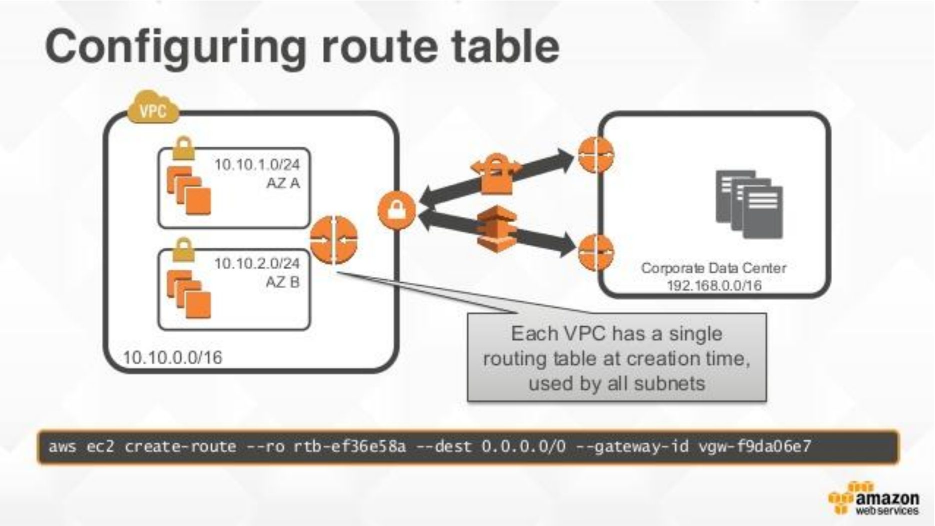
Private

Public

Elastic

Route Tables

- Contains a set of rules to determine where network traffic is routed in a VPC
- Each VPC comes with the main route table by default
- Each route in a table specifies a destination CIDR and a target
- The routing table associated with a subnet needs to be updated if there are any changes in status



Configuring route table

Each VPC has a single routing table at creation time, used by all subnets

```
aws ec2 create-route --ro rtb-ef36e58a --dest 0.0.0.0/0 --gateway-id vgw-f9da06e7
```

Route Priority

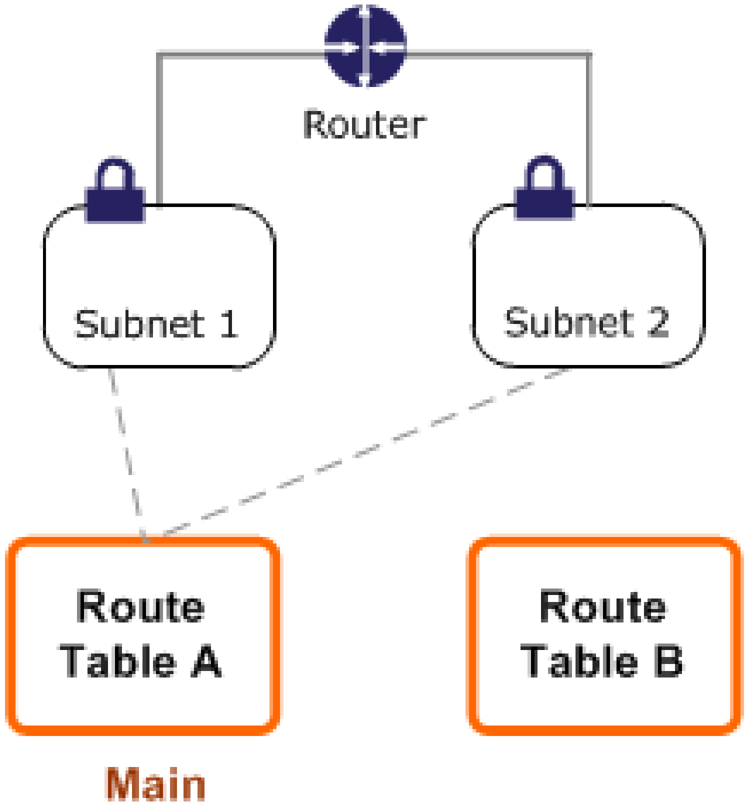
Specific routing policy or the longest prefix in your route table that matches the traffic determines how to route the traffic

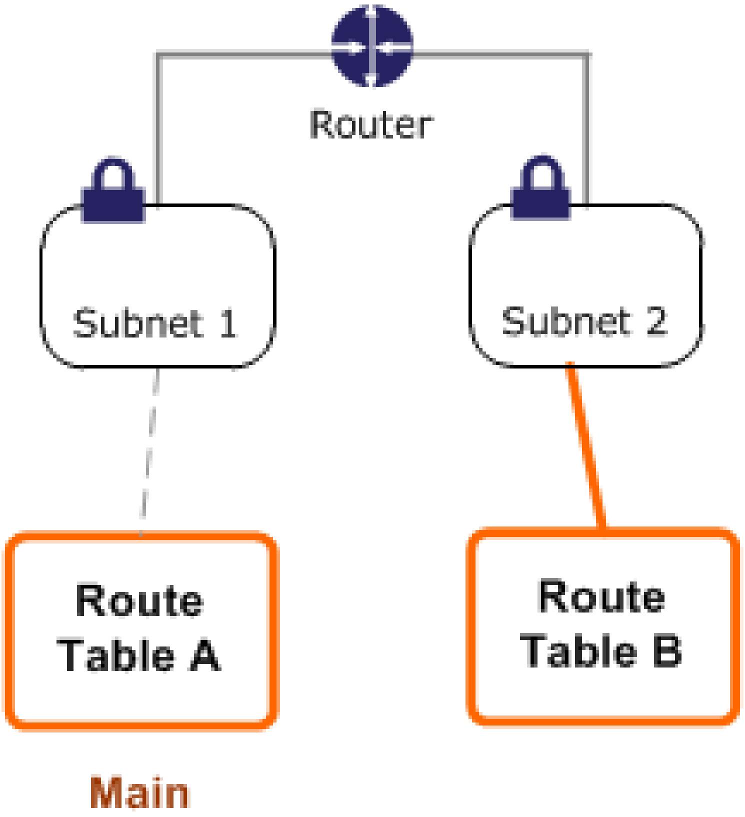
Virtual private gateways are mainly used for connecting data centers to cloud over an IPsec VPN tunnel

When a virtual private gateway is attached to a VPC, routes representing the VPN will automatically appear as decided routes

When overlapping routes within a VPN, follow the route specified on the VPN connection from the most preferred to the least preferred

Main vs. Custom Routing table





Network Access Control Lists

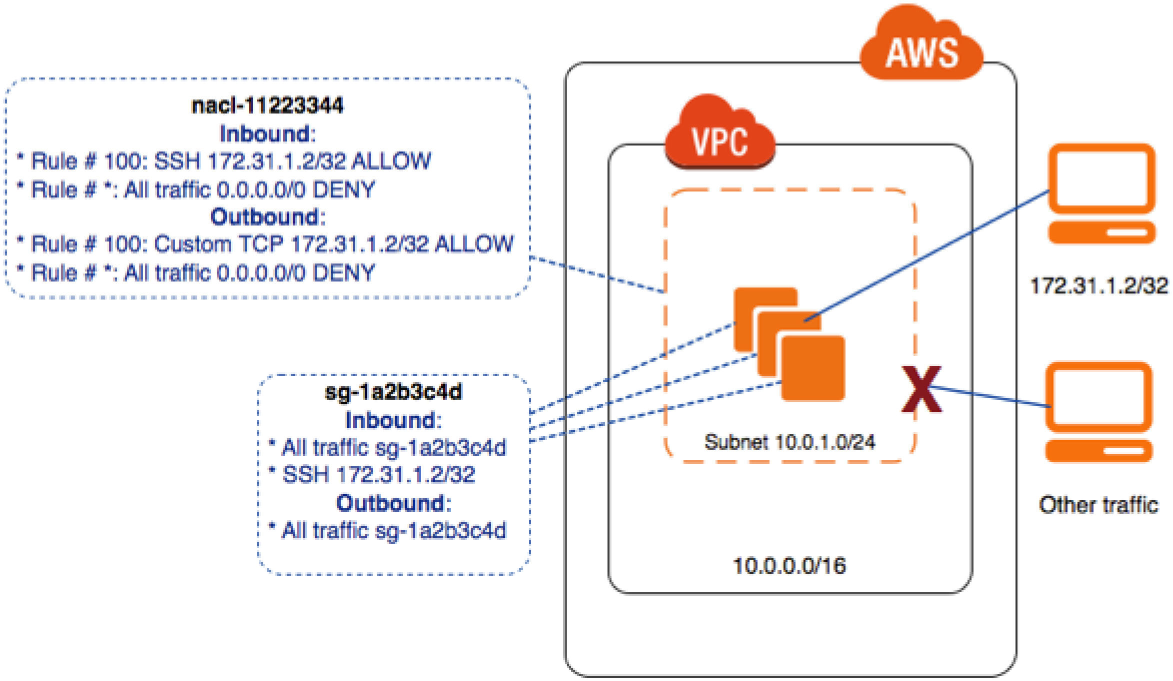
Optional layer of security for VPC

Every VPC comes with a modifiable default network ACL

A subnet can be associated with only one network ACL

Multiple subnets can use the same network ACL

Network ACLs are stateless

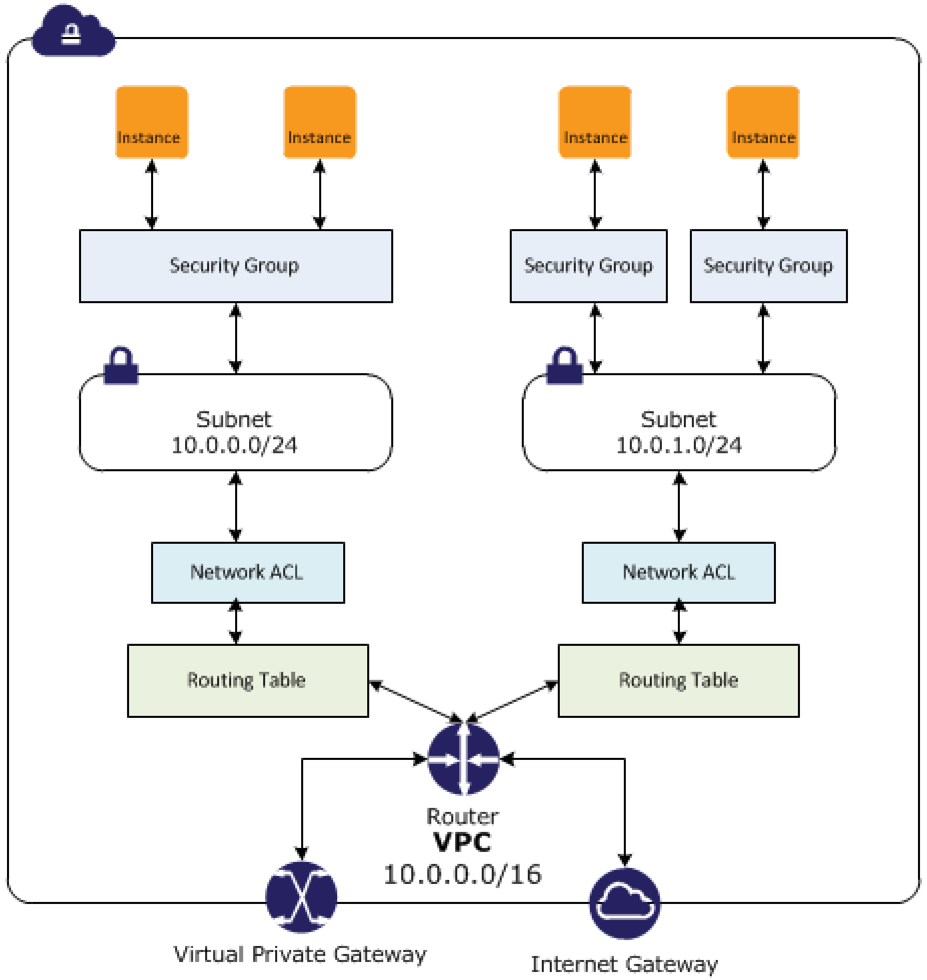


nacl-11223344
Inbound:
* Rule # 100: SSH 172.31.1.2/32 ALLOW
* Rule # *: All traffic 0.0.0.0/0 DENY
Outbound:
* Rule # 100: Custom TCP 172.31.1.2/32 ALLOW
* Rule # *: All traffic 0.0.0.0/0 DENY

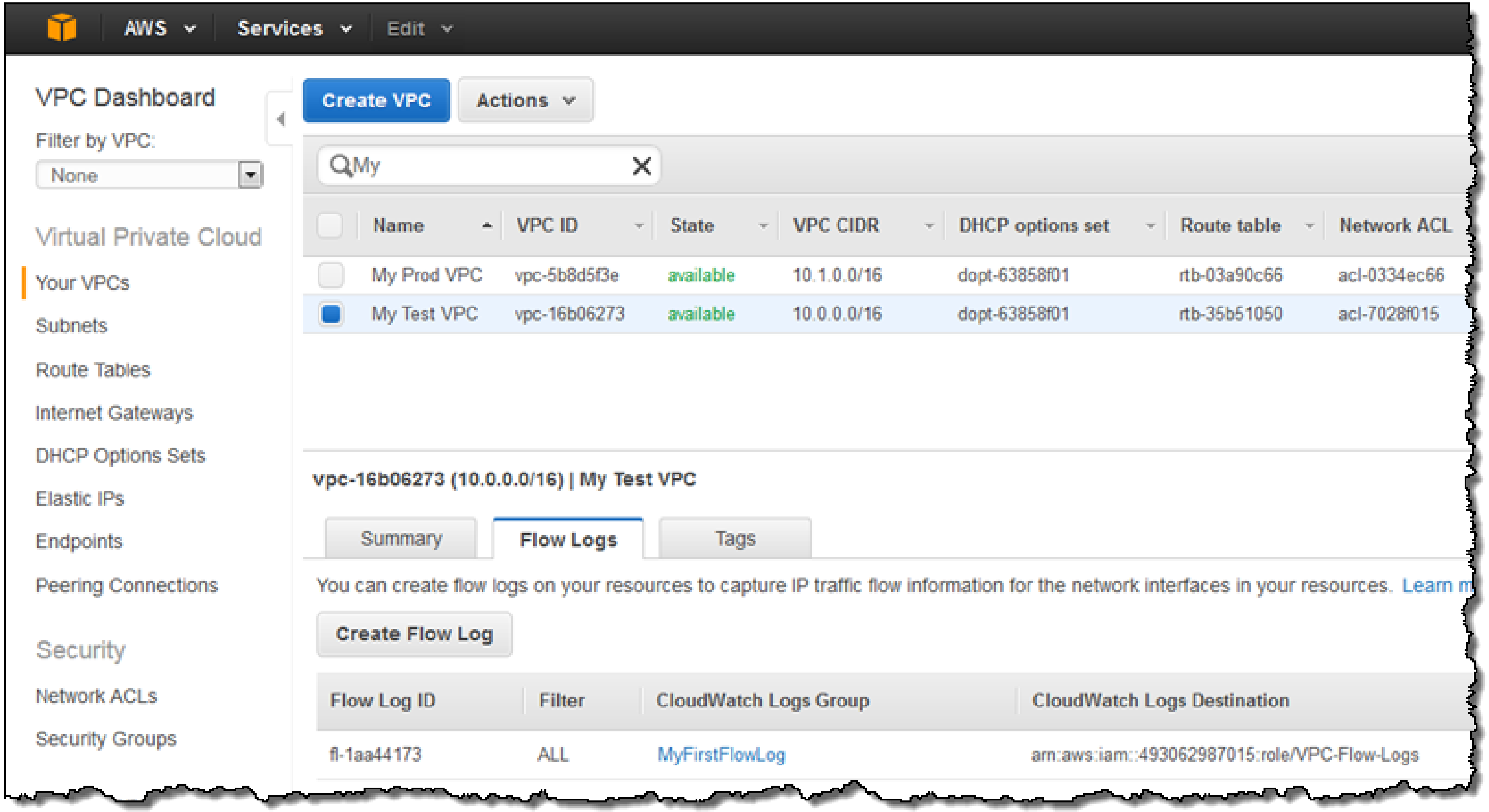
sg-1a2b3c4d
Inbound:
* All traffic sg-1a2b3c4d
* SSH 172.31.1.2/32
Outbound:
* All traffic sg-1a2b3c4d

Network ACLs vs. Security Groups

Security Groups	Network ACL
Supports instance-level firewall rules	Supports subnet-level firewall rules
Supports only “allow” rules	Supports “allow” and “deny” rules
Stateful	Stateless
Evaluates all available rules before allowing traffic	Evaluates in a sequence starting from the lowest
Must be specified while launching	Need not be specified
Instance can use multiple security groups	Subnet can use only one network ACL at a time



Flow Logs



□	Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL
□	My Prod VPC	vpc-5b8d5f3e	available	10.1.0.0/16	dopt-63858f01	rtb-03a90c66	acl-0334ec66
☑	My Test VPC	vpc-16b06273	available	10.0.0.0/16	dopt-63858f01	rtb-35b51050	acl-7028f015

vpc-16b06273 (10.0.0.0/16) | My Test VPC

You can create flow logs on your resources to capture IP traffic flow information for the network interfaces in your resources. Learn m

Flow Log ID	Filter	CloudWatch Logs Group	CloudWatch Logs Destination
fl-1aa44173	ALL	MyFirstFlowLog	arn:aws:iam::493062987015:role/VPC-Flow-Logs

Knowledge Check

KNOWLEDGE CHECK

How do network ACLs differ from security groups? (Choose 2)

a. NACL is stateless

b. NACL is stateful

c. NACL supports subnet level

d. NACL supports instance level

KNOWLEDGE CHECK

How do network ACLs differ from security groups? (Choose 2)

a. NACL is stateless

b. NACL is stateful

c. NACL supports subnet level

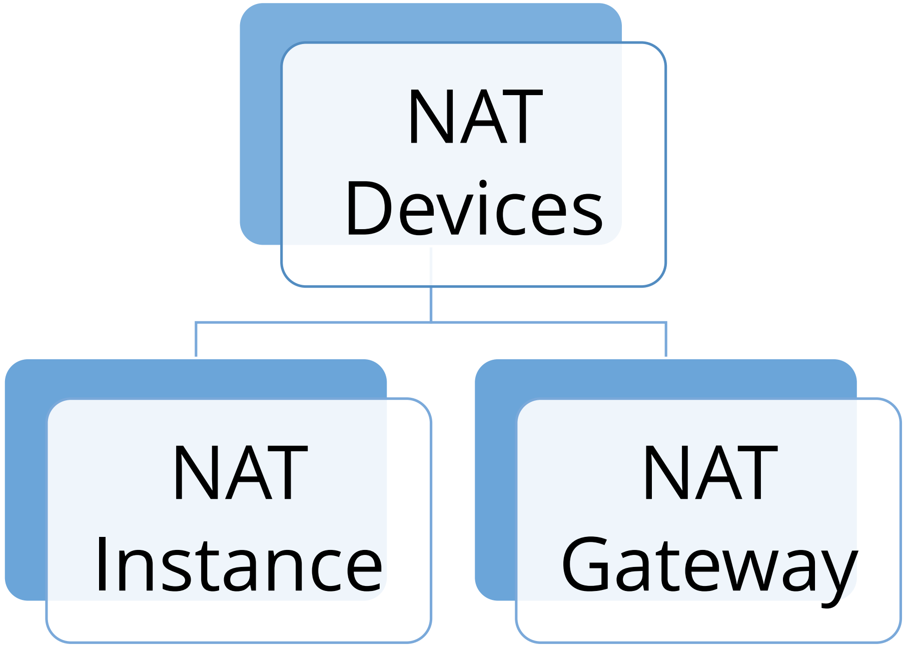
d. NACL supports instance level

The correct answer is **NACL is stateless & NACL supports subnet level**

Explanation: Security groups are stateful. When you use a rule to allow inbound or outbound traffic, the same rule is used for return traffic. Network ACLs are stateless. You need to explicitly specify inbound and outbound rules separately. Security groups support instance-level firewall rules. Network ACLs support subnet level firewall rules.

VPC – NAT, VPN, and Peering

Network Address Translation (NAT)



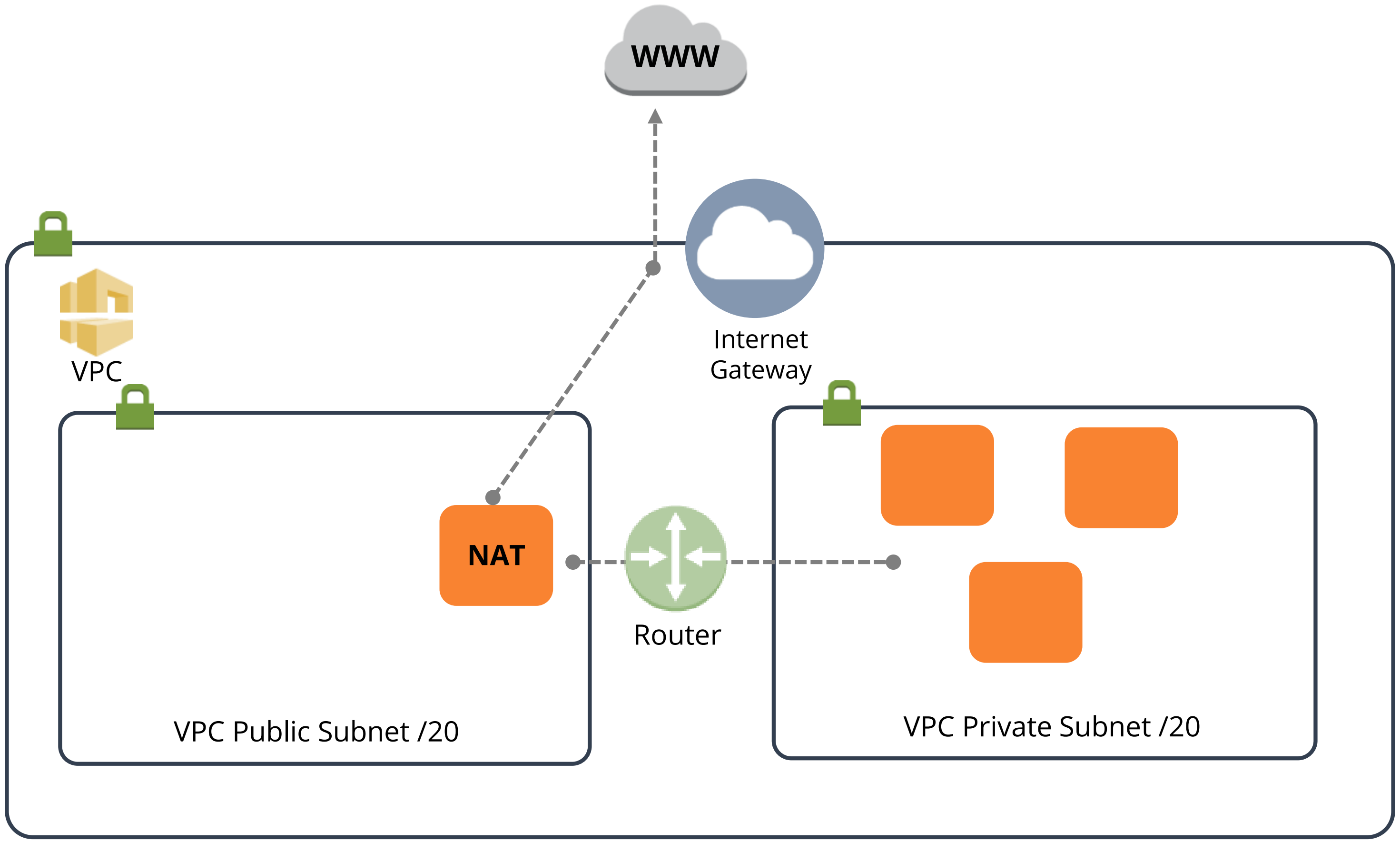
NAT Devices

NAT Instance

NAT Gateway

- Used to enable instances in a private subnet
- Forwards requests from instances to the Internet
- Replaces source IP address with NAT device’s address

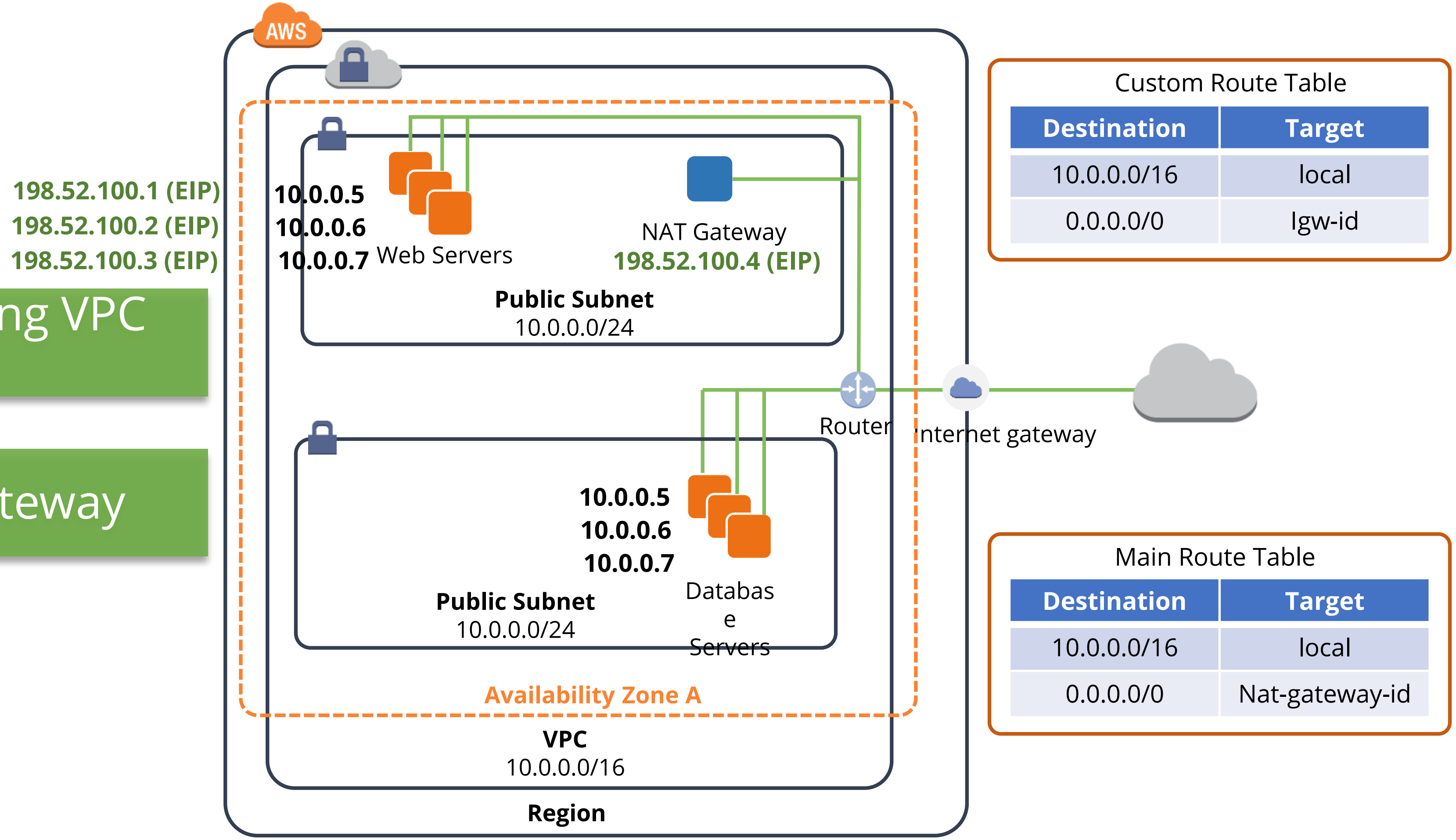
NAT Gateway


WWW
Internet Gateway
VPC
NAT
Router
VPC Public Subnet /20
VPC Private Subnet /20

NAT Gateway Configuration

1. Create a NAT gateway using VPC console

2. Create a route for 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	Nat-gateway-id

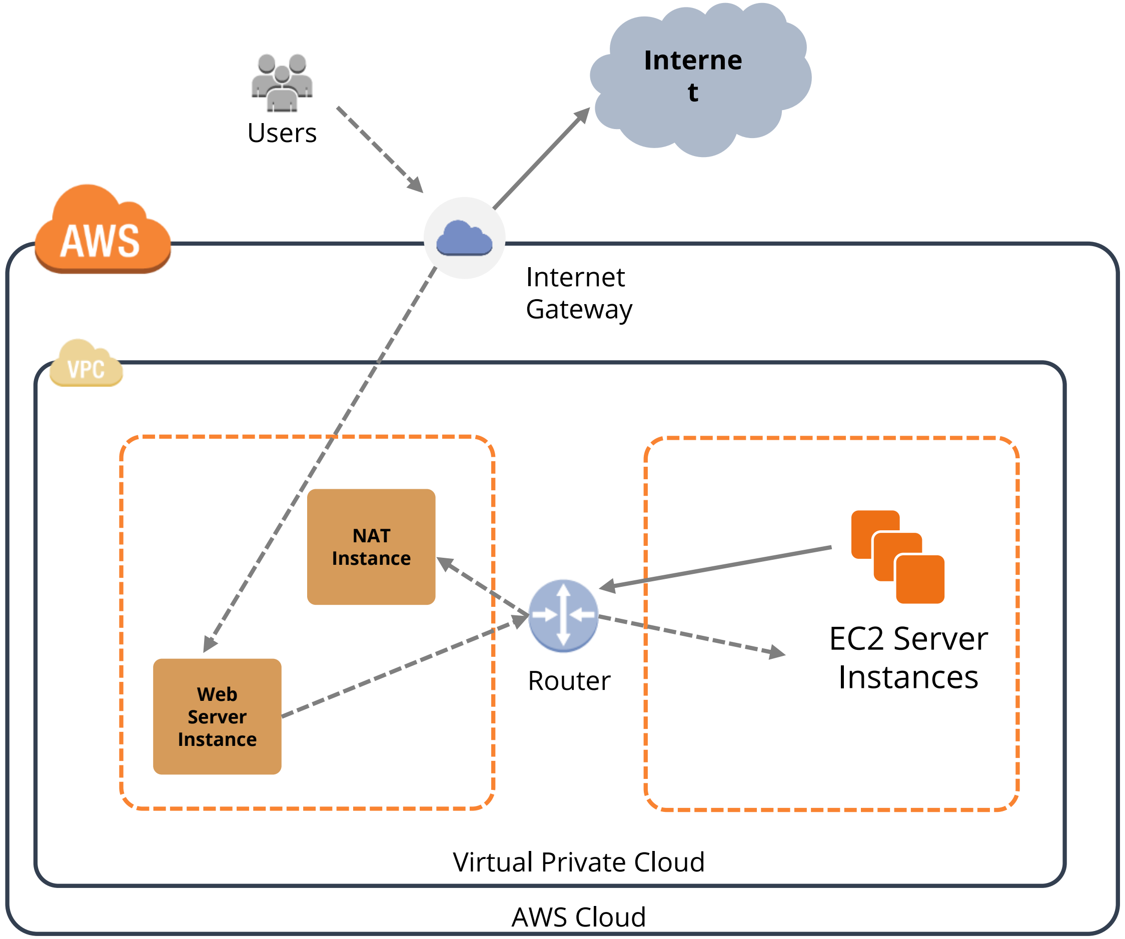
NAT Instance Configuration

NAT Launched from NAT AMI

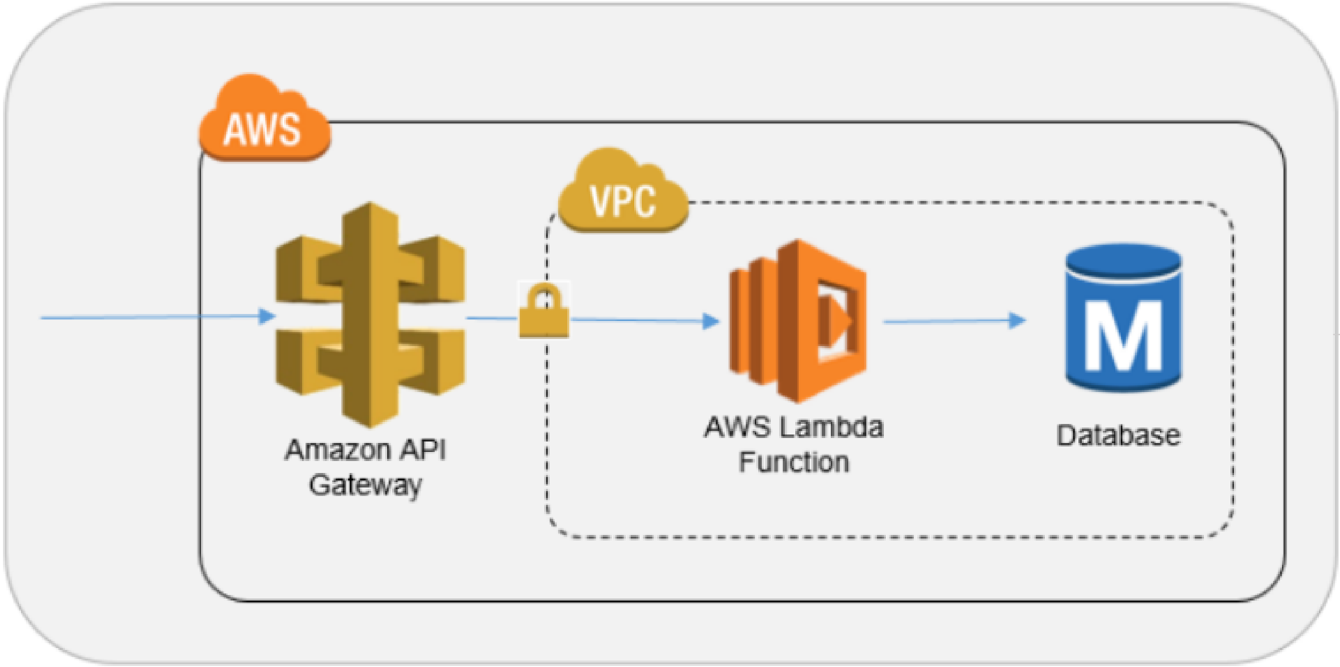
NAT Can be associated with customized security group

NAT Sends traffic to the Internet gateway of VPC

NAT Must disable “source and destination checks”



VPN Connections



To connect to private subnet of VPC from your datacenter, VPN is the most secure option

VPN allows you to become part of that network virtually and connect the private network in your VPC from your remote network by establishing a secure tunnel over the Internet

The following connectivity options are available with you:

- AWS Managed VPN
- AWS VPN CloudHub
- Third-party software VPN appliance

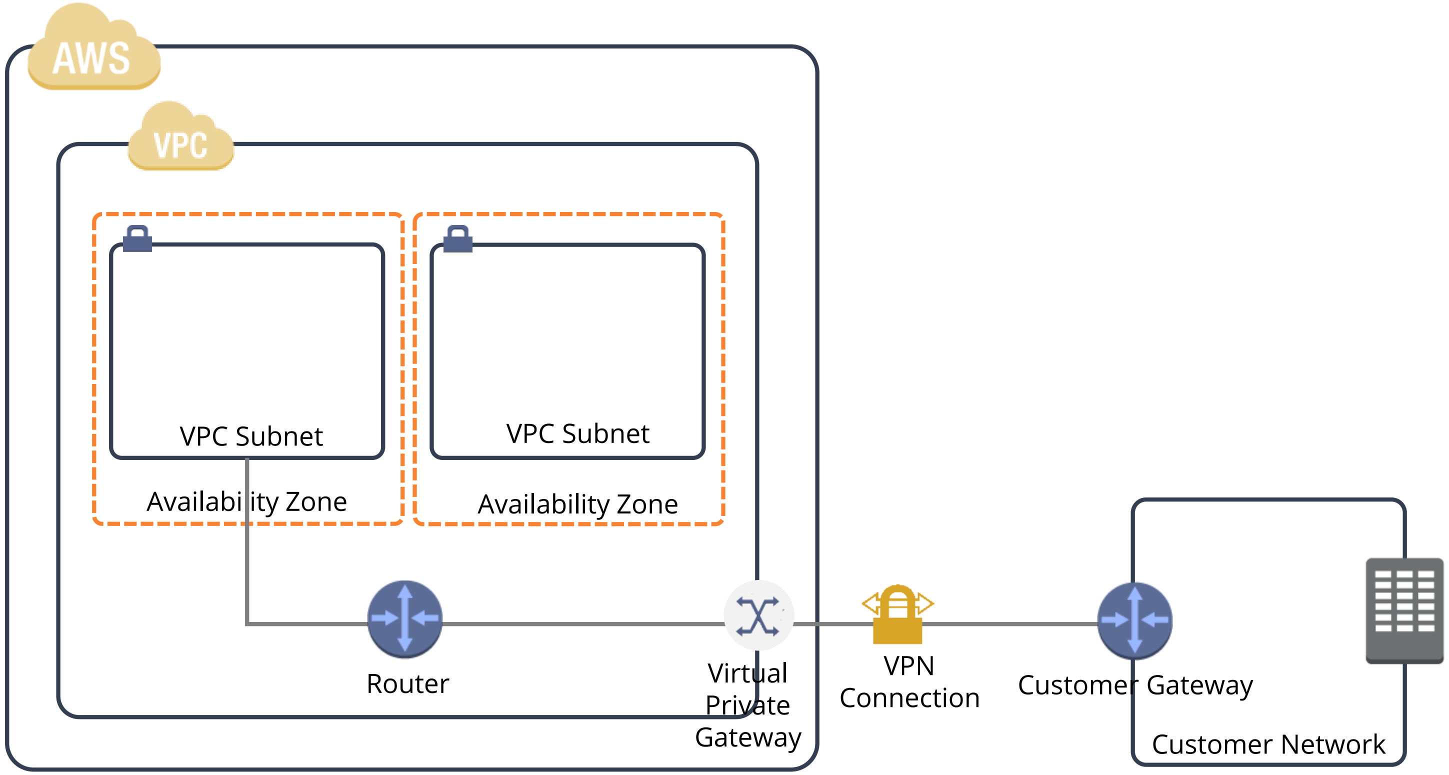
VPN Connections

1. AWS Hardware VPN

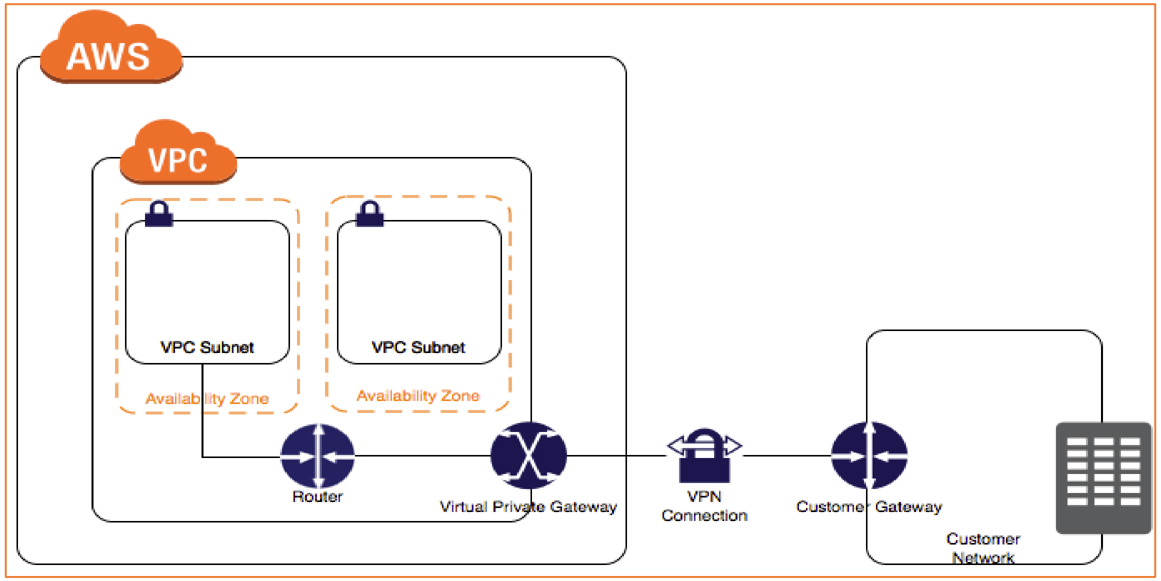
2. AWS Direct Connect

3. AWS VPN Cloud Hub

4. Software VPN



VPN Gateways



For establishing a VPN connection, two gateways are required:

Virtual Private Gateway

- At VPC side, it serves as an endpoint between tunnel and VPC

Customer Gateway

- At office network side, it serves as an endpoint between tunnel and office network

VPC Limitations

5 VPCs are allowed per region

200 subnets are allowed per VPC

5 Elastic IP addresses are allowed per region

5 Internet gateways are allowed per region

50 VPCs can have peering connections up to 50 other VPCs in the same region

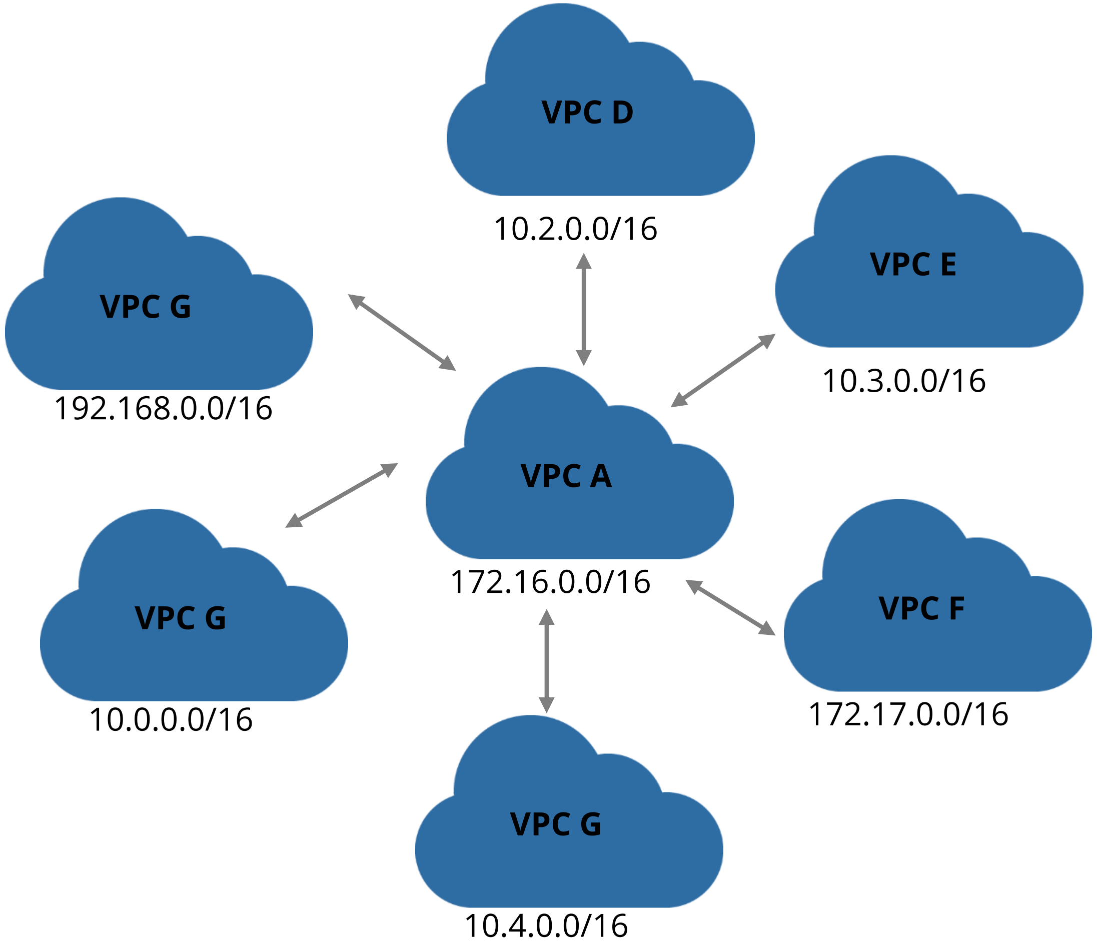
5 virtual private gateways are allowed per region

VPC Peering

- Enables resource communication using private IP address

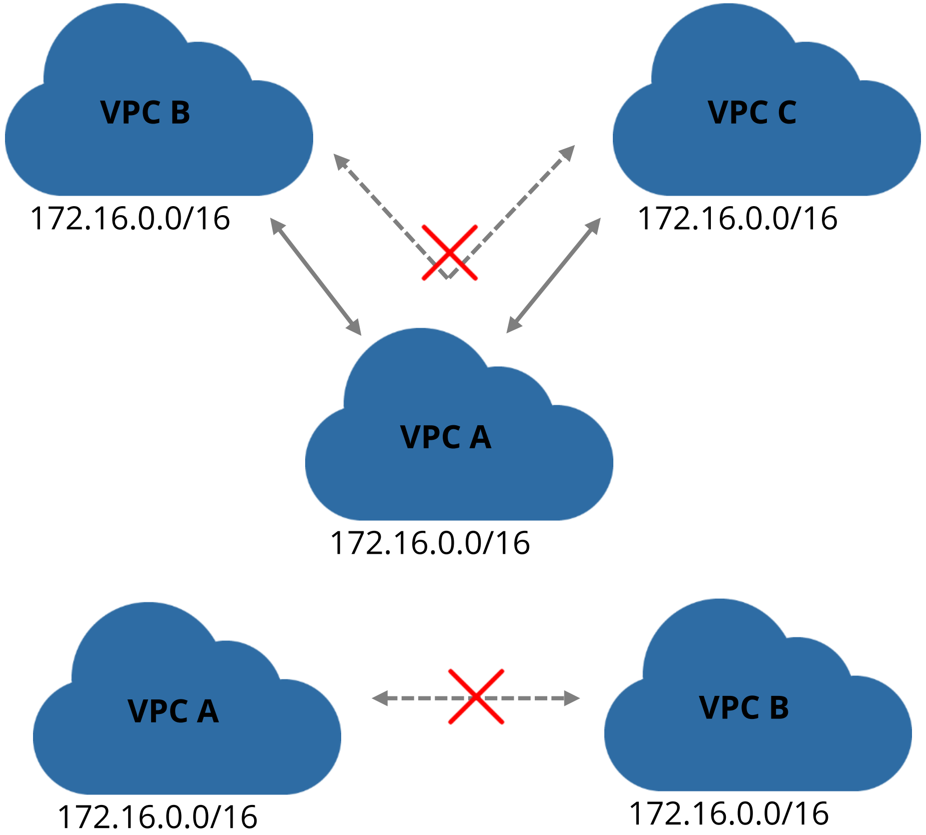
- Can be peered in different AWS accounts

- Only 2 VPCs per connection

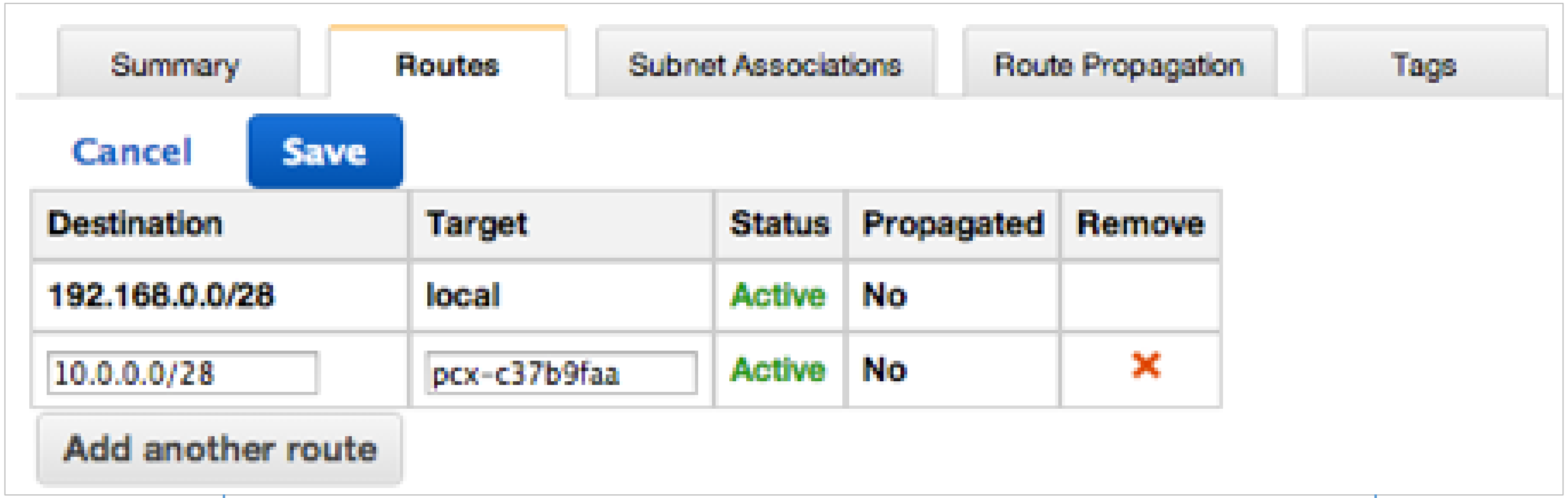


VPC Peering (Contd.)

- Transitivity peering relationship is not supported by VPC peering
- No access to other VPCs
- No connection between VPCs with matching/overlapping CIDR blocks
- No connection between VPCs in different regions



Route Table for Peering Connection

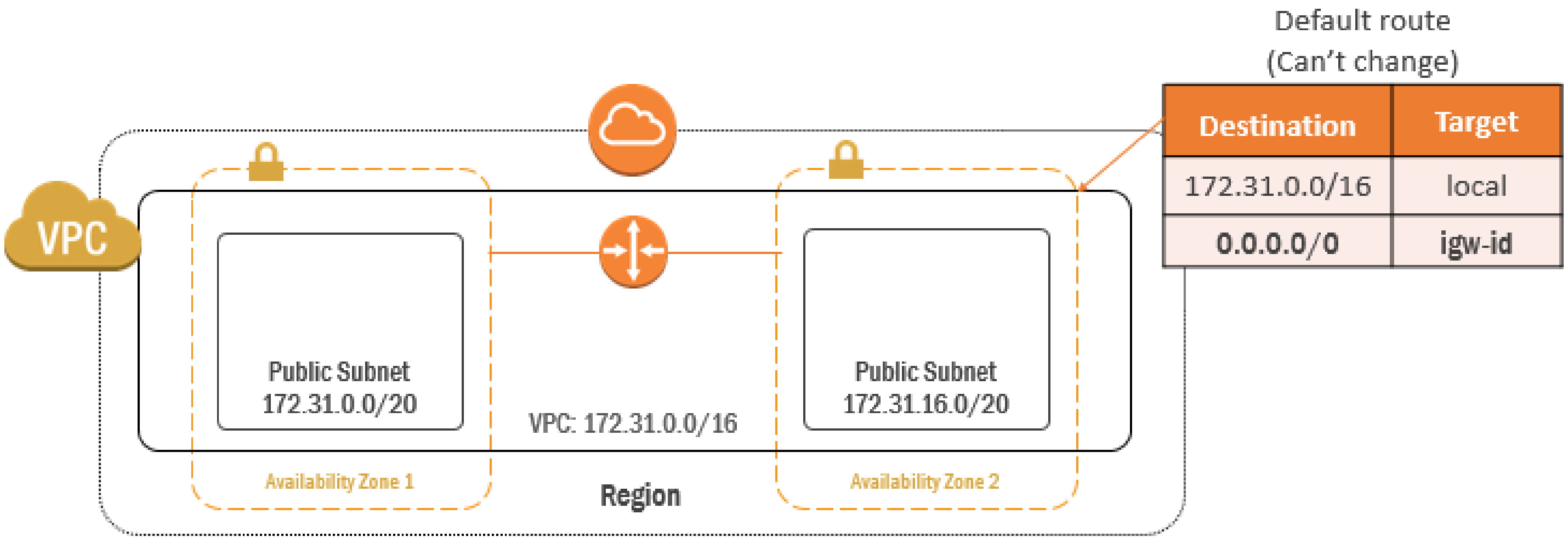


Destination	Target	Status	Propagated	Remove
192.168.0.0/28	local	Active	No	
10.0.0.0/28	pcx-c37b9faa	Active	No	✕

For allowing one instance in VPC-A to communicate with VPC-B in a peer VPC using private IP addresses, route table should have an entry to allow flow of traffic.

Route table of both VPCs should include last entry

Default VPC

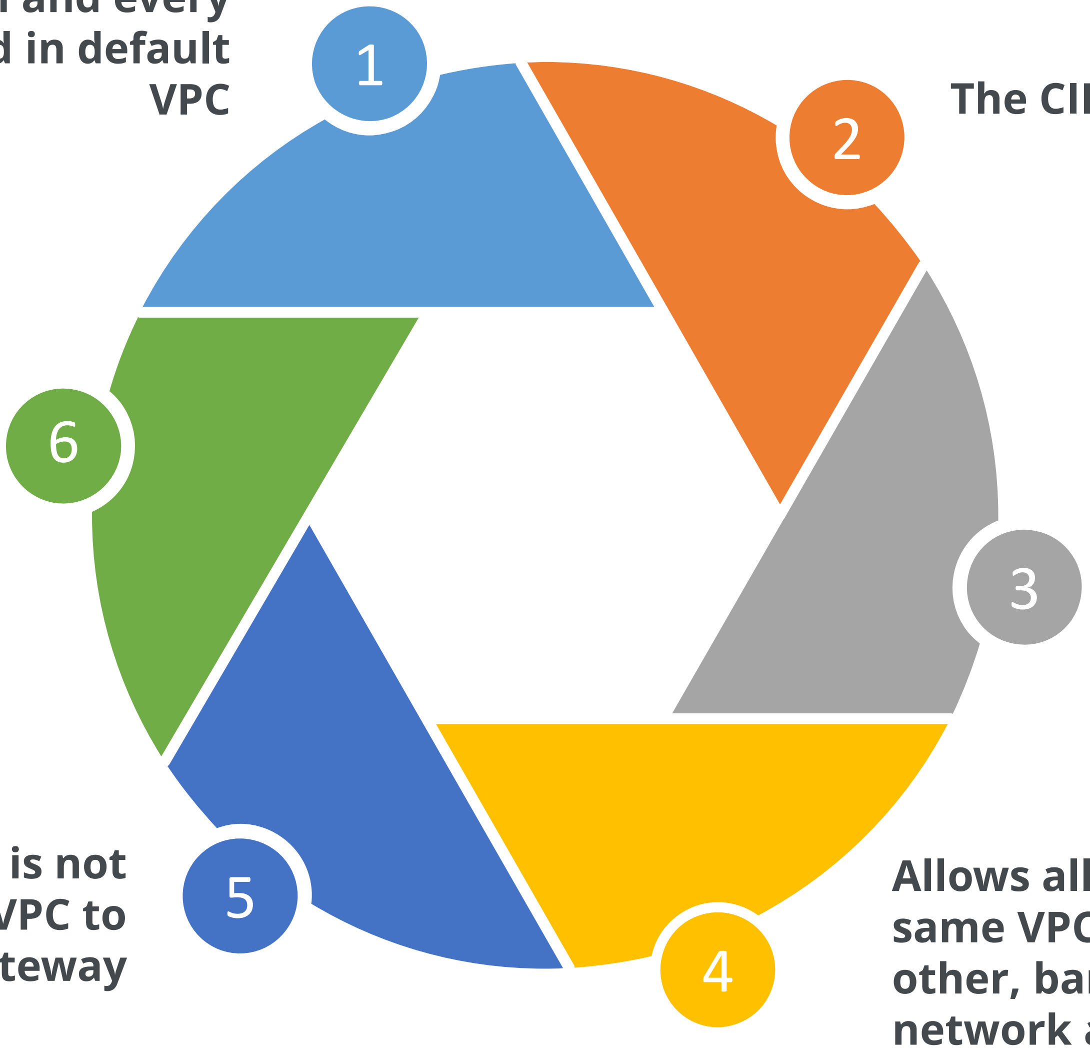


Default route
(Can’t change)

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	**igw-id**

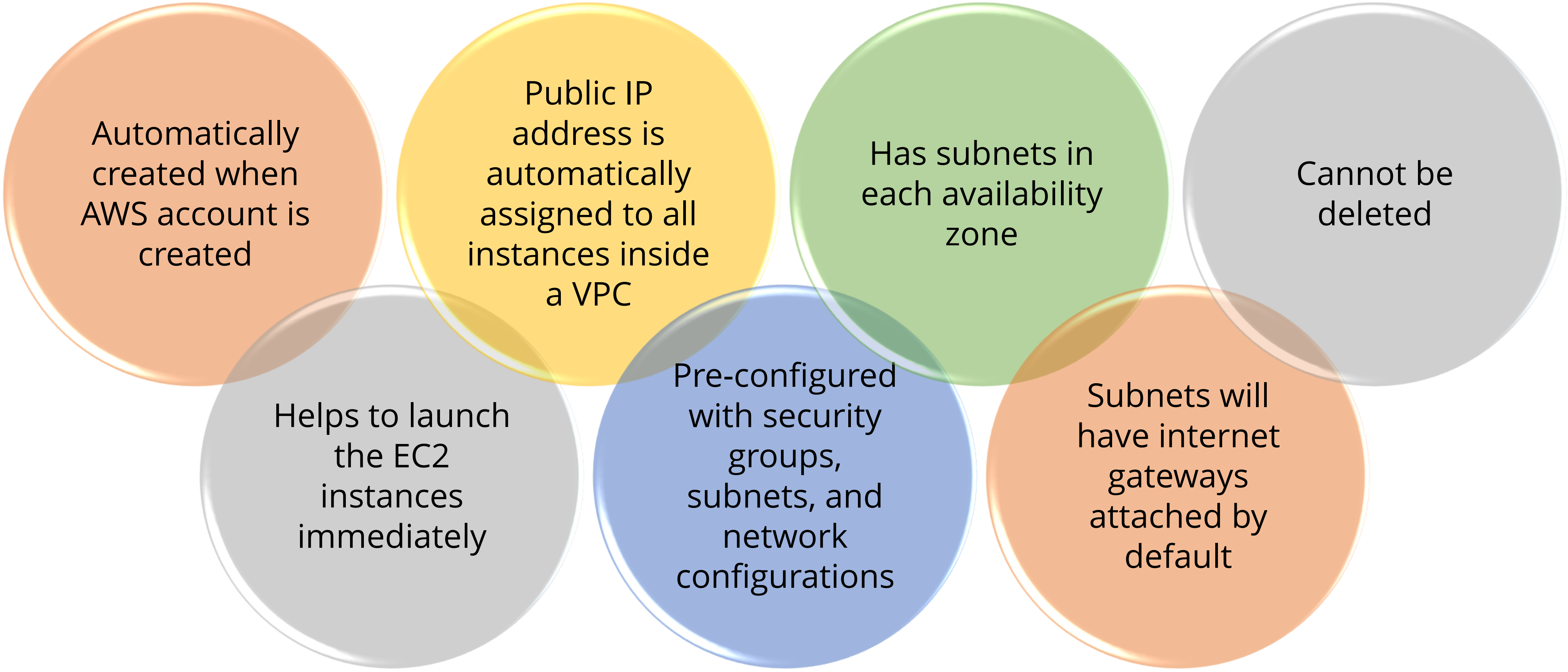
Default VPC is available by default in your account

Default VPC Features



1. By default, each and every resource is launched in default VPC
2. The CIDR supported is 172.31.0.0/16
3. Subnets created in default VPC automatically inherit the rules defined within default and main route table
4. Allows all the instances within the same VPC to communicate with each other, barring any rules defined in network access control lists
5. Sends all the traffic that is not targeting instances in VPC to Internet Gateway
6. A custom route table can be created and can be associated with default VPC in case a private subnet is to be added with default VPC

Default VPC Characteristics



- Automatically created when AWS account is created
- Public IP address is automatically assigned to all instances inside a VPC
- Has subnets in each availability zone
- Cannot be deleted
- Helps to launch the EC2 instances immediately
- Pre-configured with security groups, subnets, and network configurations
- Subnets will have internet gateways attached by default

Knowledge Check

KNOWLEDGE CHECK

Select two valid requirements of an EC2 instance to function as a NAT instance (Choose 2)

a. Must disable “source and destination checks”

b. Must enable “source and destination checks”

c. Must have public IP

d. Mush have private IP

KNOWLEDGE CHECK

Select two valid requirements of an EC2 Instance to function as a NAT instance (Choose 2)

a. Must disable “source and destination checks”

b. Must enable “source and destination checks”

c. Must have public IP

d. Mush have private IP

The correct answer is **Must disable “source and destination checks” & Must have public IP**

Explanation: By default, the function of a NAT instance is to send and receive traffic when the source or destination is not doing it by itself. Therefore, you must disable “source and destination checks” on the NAT instance. Also make sure to have either public or Elastic IP attached to the NAT instance.

Practice Assignment: Amazon VPC

To create a VPC using the Amazon VPC wizard

Create Your Own VPC

You need to create a VPC that can be used as your private space in the cloud.

Prerequisites:
AWS Account

Task:
To create a VPC using the Amazon VPC wizard.

Quiz

QUIZ

1

How many Internet gateways can be attached to a VPC?

a. 5

b. 1

c. 10

d. 2

QUIZ

1

How many Internet gateways can be attached to a VPC?

a. 5

b. 1

c. 10

d. 2

The correct answer is **1**

Explanation: Internet gateway is a highly scalable VPC component that allows communication between instances in your VPC and the Internet. Internet gateway should be the target in your subnet's routing table. Only one per VPC is allowed.

QUIZ 2	Can you attach more than one route table with a subnet?

a. Yes

b. No

QUIZ 2	Can you attach more than one route table with a subnet?

a. Yes

b. No

The correct answer is **No**

Explanation: You can’t have more than one route table for a subnet, but multiple subnets can use the same route table.

QUIZ 3	Where do you install a NAT gateway?

a. Outside a subnet

b. In a public subnet

c. In a private subnet

d. In an Internet gateway

QUIZ

3

Where do you install a NAT gateway?

a. Outside a subnet

b. In a public subnet

c. In a private subnet

d. In an Internet gateway

The correct answer is **In a public subnet**

Explanation: A NAT gateway needs a public subnet to reside in. So, we need to first create a public subnet and then a NAT gateway, followed by updating the routing table associated with private subnets to route internet traffic to the NAT gateway.

QUIZ

4

What is an important component that hardware VPN uses?

a. Virtual Public Gateway

b. Virtual Private Gateway

c. Virtual Elastic Gateway

d. Software Appliance

QUIZ

4

What is an important component that hardware VPN uses?

a. Virtual Public Gateway

b. Virtual Private Gateway

c. Virtual Elastic Gateway

d. Software Appliance

The correct answer is **Virtual Private Gateway**

Explanation: AWS hardware VPN provides secure IPSec connections between your VPC and your remote network. It uses the Virtual Private Gateway at your VPC's end to connect with VPN.

QUIZ

5

Is it possible to peer two VPCs from different regions?

a. Yes

b. No

QUIZ

5

Is it possible to peer two VPCs from different regions?

a. Yes

b. No

The correct answer is **No**

Explanation: You cannot create a VPC peering connection between VPCs in different regions.

Key Takeaways

- VPCs can span multiple availability zones, but subnets can't span zones
- Routing table controls the routes for outbound traffic. Custom routing table can also be attached at the time of creating a subnet, otherwise it defaults to the main table
- The default security group allows inbound traffic only from other instances associated with the same group, and allows all outbound traffic from the instance
- Specific routing policy or the longest prefix in your route table that matches the traffic determines how to route the traffic
- Virtual Private Gateways are mainly used for connecting data centers to the cloud over an IPsec VPN tunnel
- ACLs are an optional layer of security for the VPC, they act as a firewall for controlling inbound and outbound subnet traffic
- NAT instance enables instances in a private subnet to connect and receive traffic from the Internet or another AWS service

This concludes “VPC”.

The next lesson is “AWS Route 53”