AWS SysOps Administrator – Associate Level

TECHNOLOGY

Amazon Virtual Private Cloud (VPC)

simplilearn

Learning Objectives

By the end of this lesson, you will be able to:

- Describe and build a VPC
- Configure and launch a NAT instance
- Establish a network ACL
- Create a VPC endpoint
- Build a VPC flow log

TECHNOLOGY

Introduction to VPC

What Is VPC?

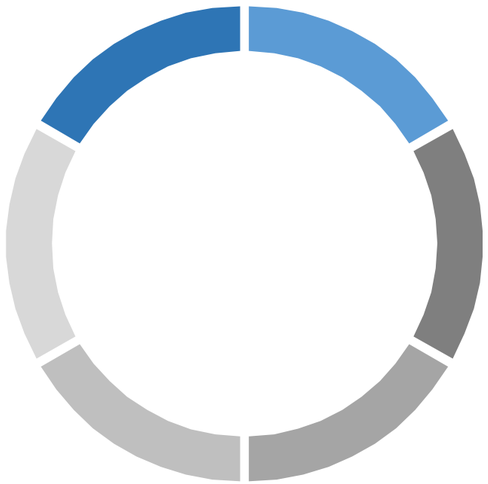
Amazon VPC is a service that helps the users to launch AWS resources into a defined virtual network. It provides users with complete control of the virtual networking environment.

Characteristics of VPC:

- Simple
- Customizable
- Secure

VPC: Uses

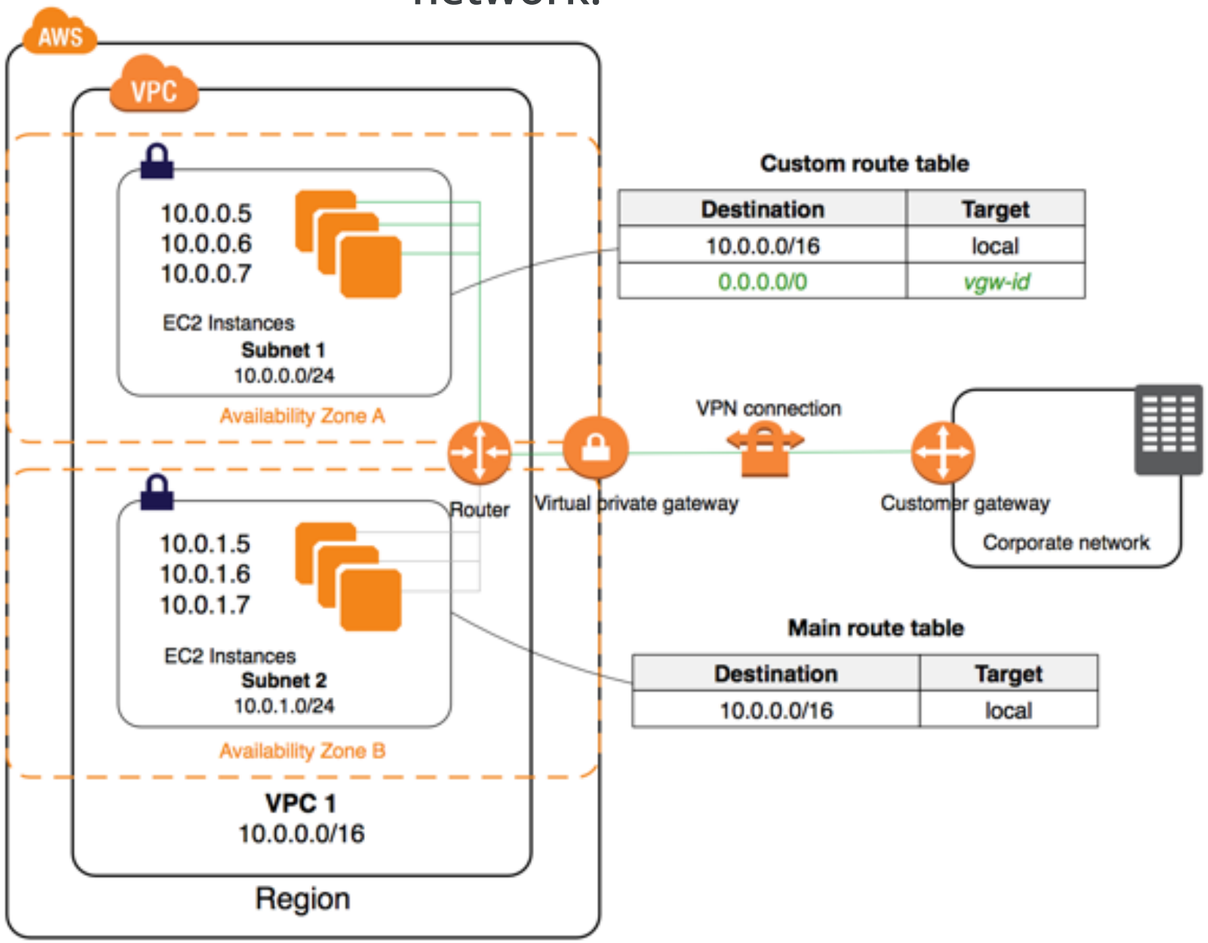
- To perform an inline traffic inspection
- To connect cloud applications to the data center securely
- To extend the corporate network into the cloud



- To host a public-facing website
- To host a multi-tier application
- For disaster recovery

Working of VPC

The following diagram shows how VPC works to access a corporate or home network.



Source: https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html

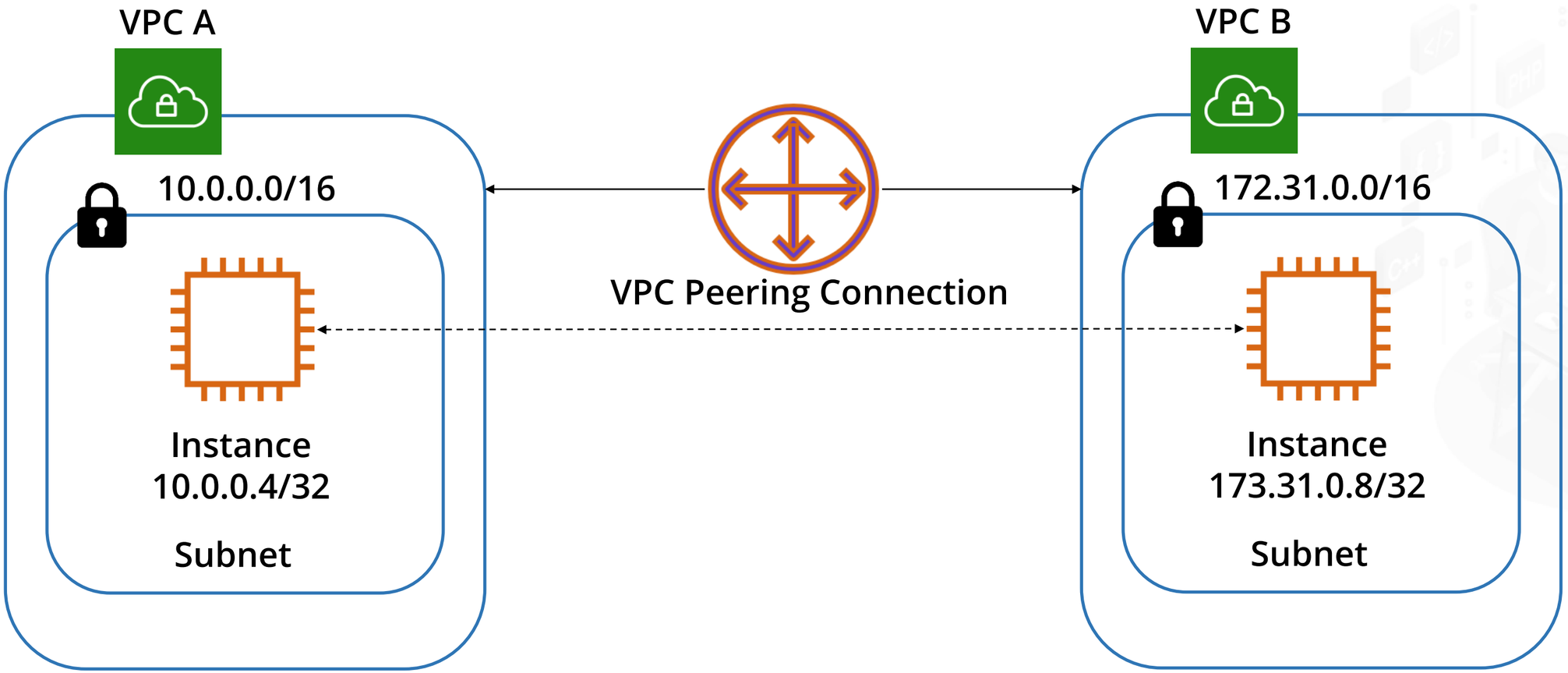
Default vs. Custom VPC

Parameters	Default VPC	Custom VPC
Creation	By default	User-created VPC
Assigned to user	Assigned when an instance is launched without allocating a subnet	Not assigned when an instance is launched without allocating a subnet
IPV4 Address	Uses both public and private IPv4 addresses	Uses just a private IPv4 address
Internet access	By default	Does not have access by default
Internet gateway	Internet gateway included	Internet gateway not included
Number of VPCs per region	One	5 by default

VPC Peering

VPC Peering

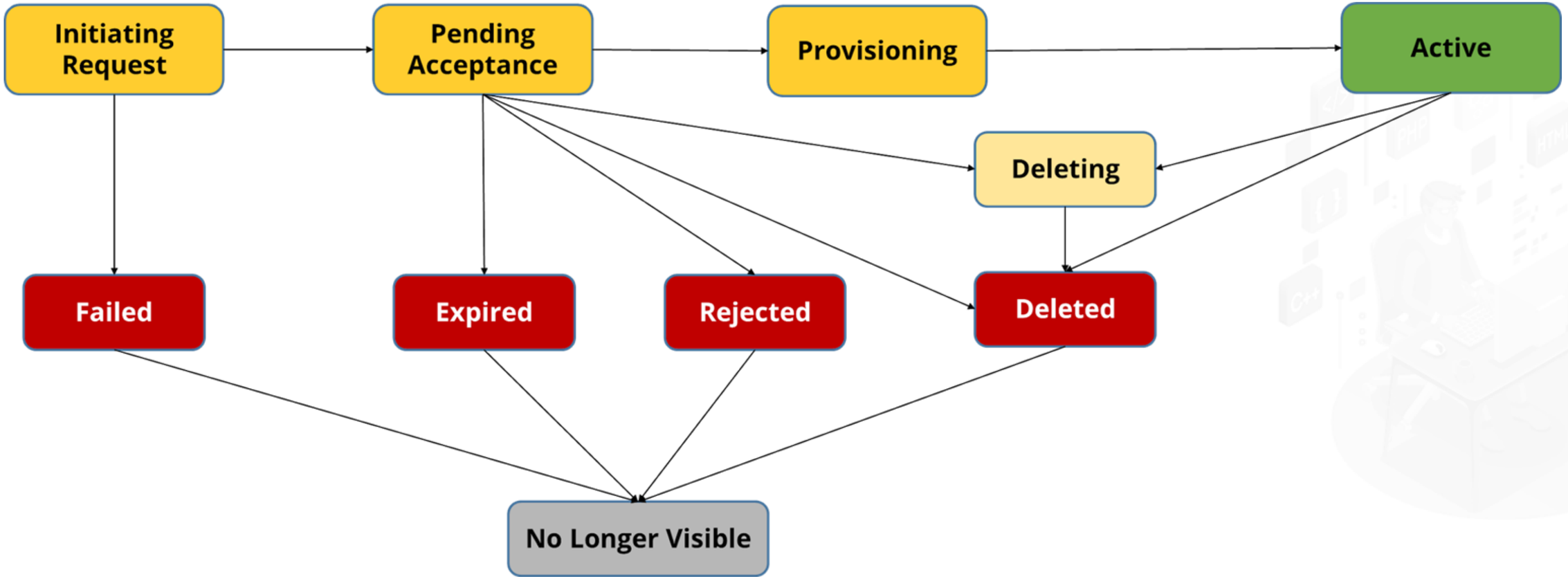
VPC peering is defined as a network connection established between two VPCs that allows to route the traffic between them with private IPV4 and IPV6 addresses.



VPC Peering: Advantages

1. Helps in facilitating the transfer of data
2. Allows other VPCs to access resources that are present in one of the VPCs
3. Does not rely on a separate piece of physical hardware
4. Has no single point of failure for communication or a bandwidth bottleneck

VPC Peering Lifecycle



VPC Peering: Limitations

- Cannot create a VPC peering connection between VPCs overlapping IPv4 or IPv6 CIDR blocks
- Has a quota on the number of active and pending VPC peering connections used
- Does not support transitive peering relationships
- Cannot have more than one VPC peering connection between the same two VPCs, simultaneously
- Does not support unicast reverse path forwarding
- Cannot query the Amazon DNS server in a peer VPC

Creating a Custom VPC

Duration: 10 Min.

Problem Statement:

Create a custom VPC.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create a custom VPC are as follows:

1. Login to AWS lab

1. Navigate to **VPC Management Console**

1. Create a custom VPC

1. Edit and increase the range of hosts

TECHNOLOGY

Network Address Translation (NAT)

Network Address Translation (NAT)

NAT devices are used to enable instances in a private subnet to connect to the internet or other AWS services.

A NAT device is used to forward traffic from the private subnet instances to the internet or AWS services, and then send the response back to the instances.

Network Address Translation (NAT)

There are two types of NAT devices:

- NAT Gateway
- NAT Instances

NAT Instances

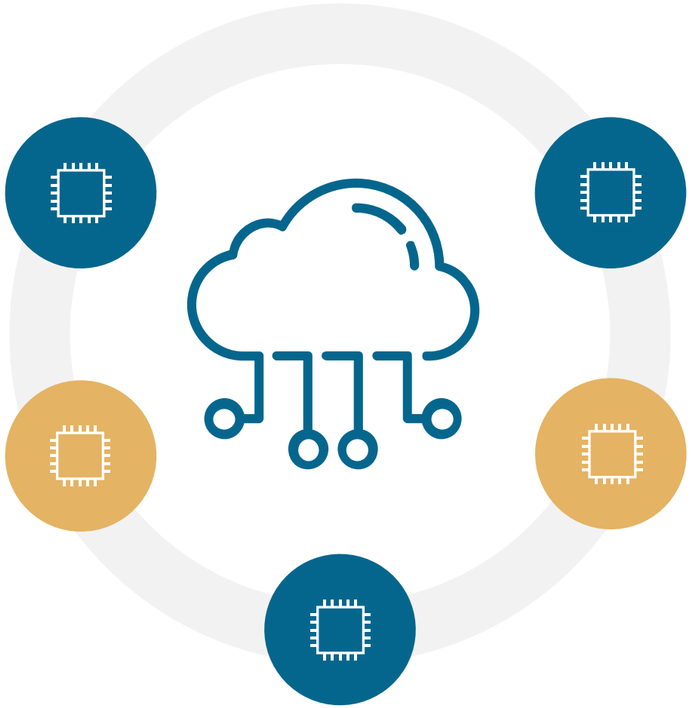
- Are instances in a public subnet that allow instances in a private subnet initiate outbound IPv4 traffic to AWS services

- Prevent instances from receiving inbound traffic initiated by someone on the internet

NAT Instances: Characteristics

Allow instances in the private subnet to connect to the internet

Must be launched in a public subnet



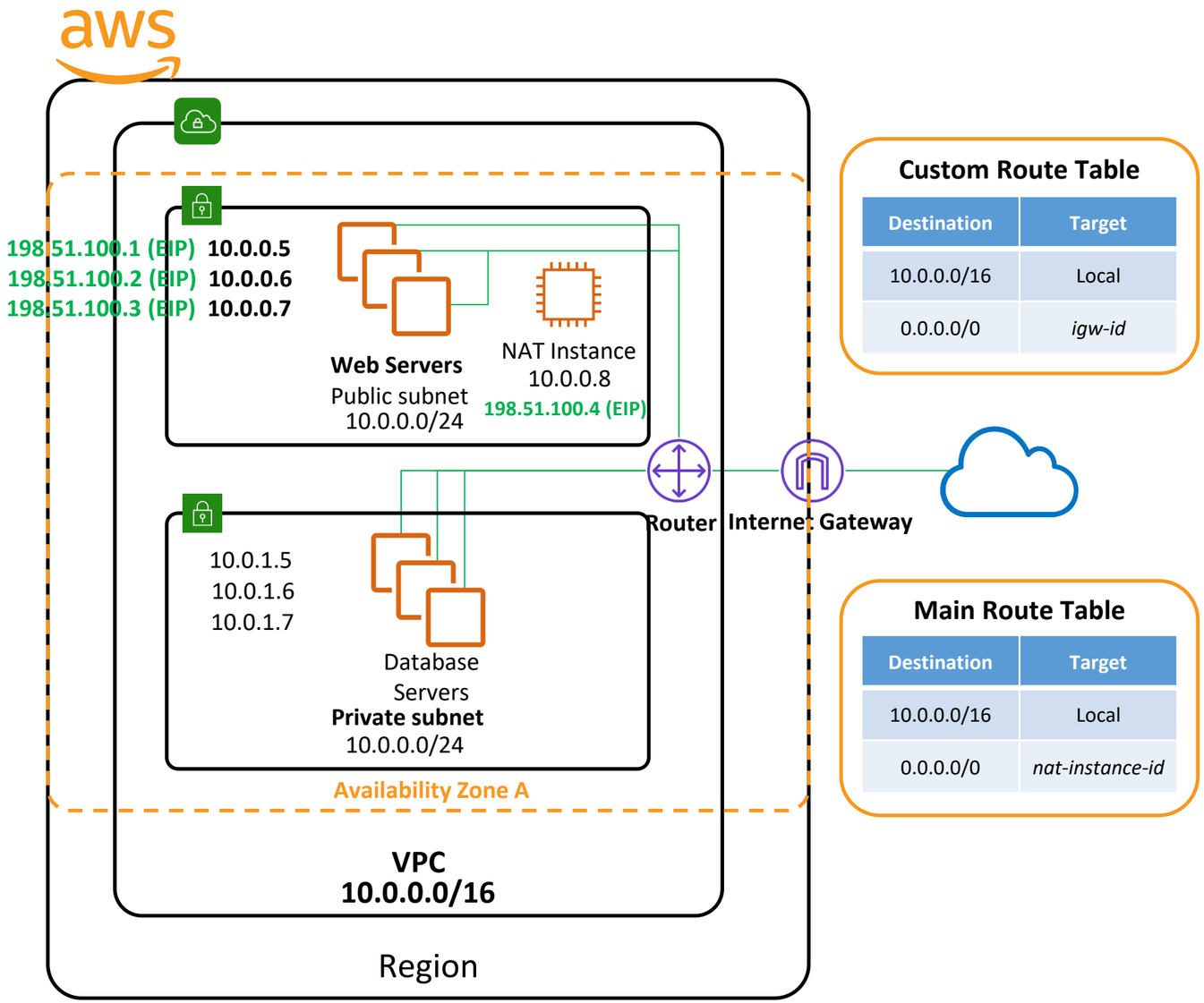
Must have EC2 flag disabled

Must have elastic IP attached

Route tables must be configured to route traffic from private subnets to NAT instances

NAT Instances

The following diagram shows the working of NAT instances.



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-instance-id*

Creating and Launching NAT

Duration: 10 Min.

Problem Statement:

Create and launch a NAT instance.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create and launch a NAT instance:

1. Create a custom VPC

1. Create a public and private subnet

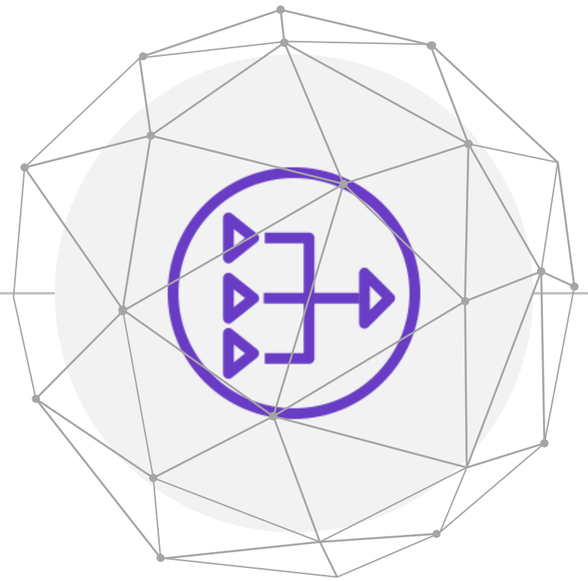
1. Create a public NAT instance

NAT Gateway

NAT gateway is a device that is used to enable instances in a private subnet to connect to the internet. It prevents the internet from initiating a connection with those instances.

Characteristics of NAT gateway:

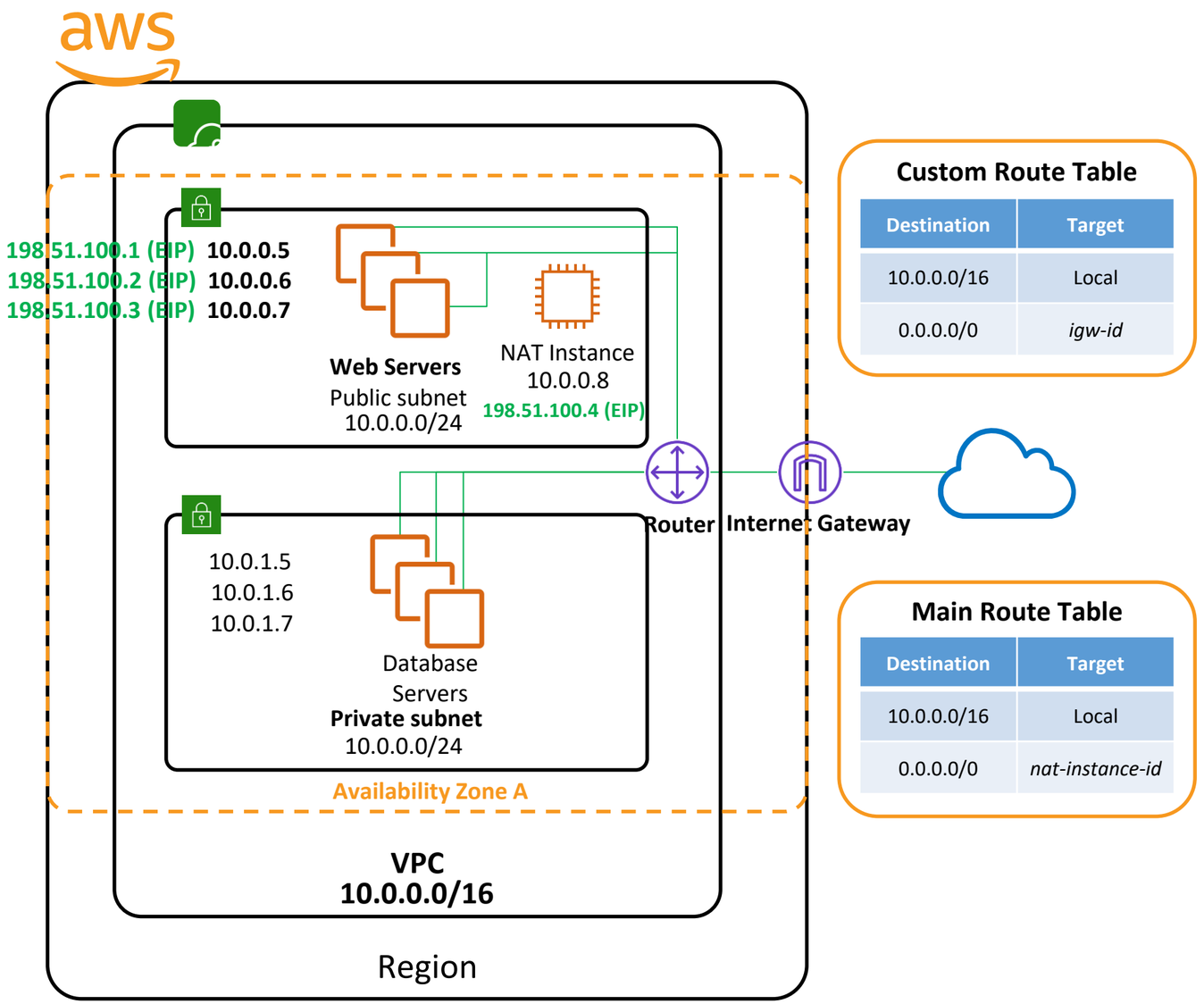
- An AWS-managed NAT with a higher bandwidth
- Created in a specific AZ
- No security group to be managed



- Pay per hour for usage and bandwidth
- IGW required
- Cannot be accessed by a ClassicLink connection associated with VPC

NAT Gateway

The following diagram shows the working of 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-instance-id*

Creating Network ACL (NACL)

Duration: 10 Min.

Problem Statement:

Create a network ACL and edit the inbound and outbound rules.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create a network ACL:

1. Create a network ACL (NACL)

1. Edit the inbound and outbound rules

VPC Flow Logs

VPC Flow Logs

VPC flow logs are used to capture information about the IP traffic going to and from the network interfaces in your VPC.

It can be published to Amazon S3 or CloudWatch.

Once the log is created, the data can be retrieved and viewed in the chosen destination.

Default format of VPC flow logs:

<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action> <log-status>

VPC Flow Logs: Uses

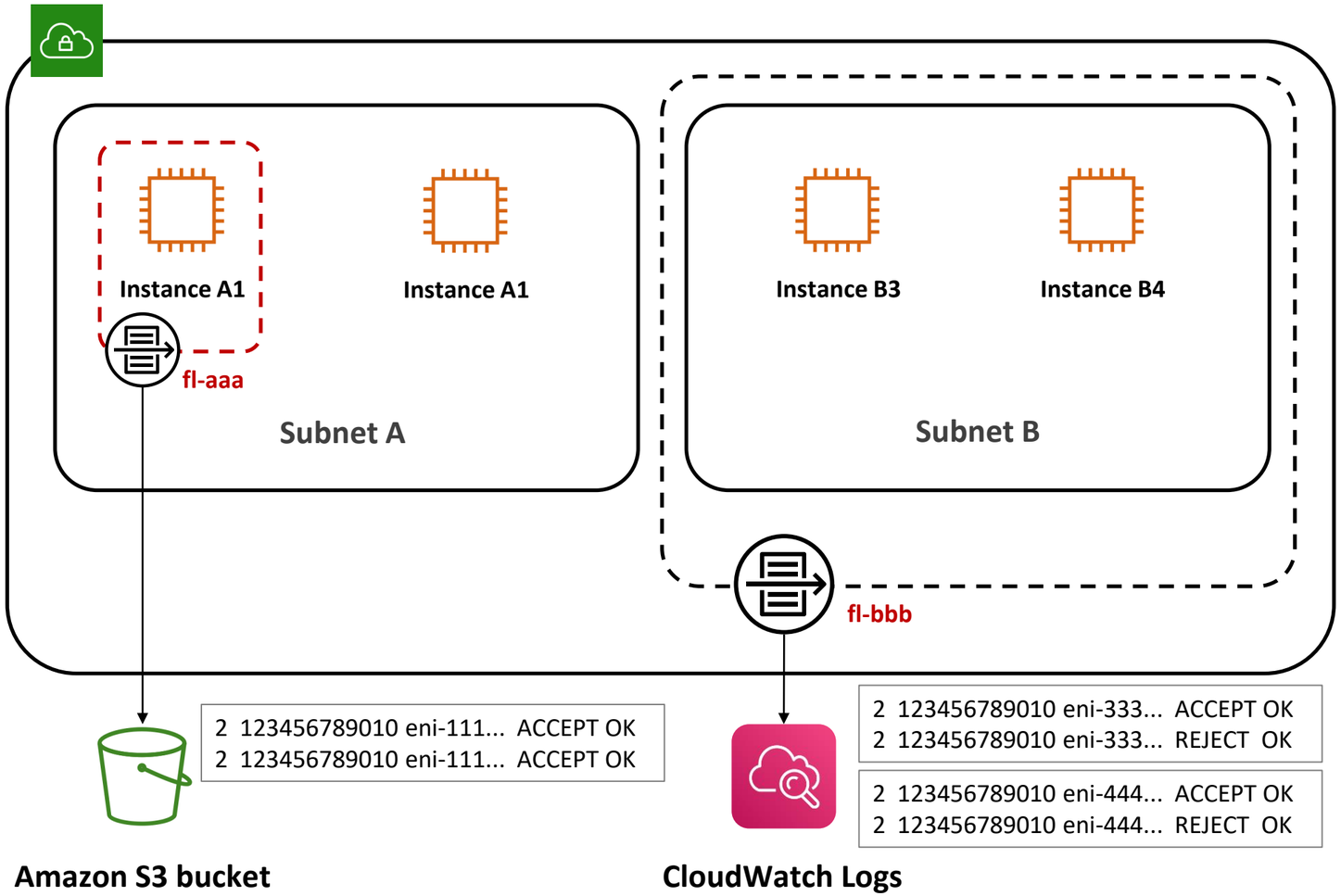
To diagnose overly restrictive security group rules

To determine the direction of the traffic to and from the network interfaces

To monitor and troubleshoot the connectivity issues

VPC Flow Logs

The following diagram shows the working of VPC flow logs.



VPC Flow Logs: Limitations

Cannot enable them for network interfaces that are in the EC2-Classic platform

Cannot change their configuration or the flow log record format

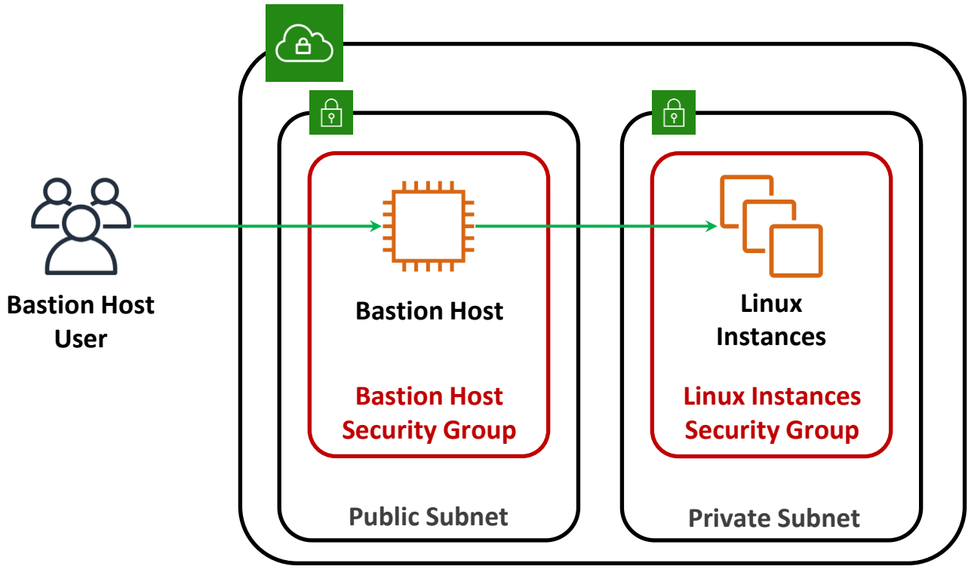
Cannot enable them for VPCs peered with your VPC unless the peer VPC is in your account

Do not capture all IP traffic

Bastion Hosts

Bastion hosts are used to SSH into a private instance.

Bastion host is in the public subnet which is then connected to all other private subnets.



The bastion host security group must be tightened.

Note: Bastion hosts allow us to connect to them via secure protocols, like SSH or RDP, whereas NAT device allows the traffic to flow out of the VPC.

Creating a VPC Endpoint

Duration: 10 Min.

Problem Statement:

Create a VPC endpoint to enable a private instance access different AWS services.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create a VPC endpoint:

1. Select **Amazon VPC** from the **Services**

1. Create a VPC endpoint

1. Choose category

1. Enable DNS

Creating a VPC Flow Log

Duration: 10 Min.

Problem Statement:

Create a VPC flow log, and monitor it using CloudWatch.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create VPC logs:

1. Create a VPC flow log
2. Monitor the VPC flow log using CloudWatch

Cleaning a VPC

Duration: 10 Min.

Problem Statement:

Clean a VPC and delete the used VPCs.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to clean VPC:

1. Navigate to VPC Management Console
2. Clean a VPC
3. Delete an instance
4. Delete VPC

Key Takeaways

- Amazon VPC is a service that helps users launch AWS resources into a defined virtual network.
- VPC peering allows other VPCs to access resources that are present in one of them.
- A NAT device is used to forward traffic from private subnet instances to the internet or AWS services.
- VPC flow logs are used to capture information about the IP traffic going to and from the network interfaces in your VPC.
- Bastion hosts are used to SSH into a private instance.

Create a VPC and NAT to Perform Bidirectional Monitoring

Problem Statement:

Perform Bidirectional monitoring using NAT and VPC.

Background of the problem statement:

As a senior SysOps engineer, you have been assigned a critical project where you have to create a VPC and NAT instances.

LESSON-END PROJECT