

Cloud



Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud

Cloud



Caltech

**Center for Technology &
Management Education**

AWS Certified SysOps Administrator – Associate Level



Networking

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



A Day in the Life of an AWS Administrator

You are employed as a networking engineer in a company. Your company is seeking a few network solutions provided by AWS and has asked you to recommend a few services based on the following criteria:

- The organization would like to deploy its resources in a logically isolated virtual network that is exclusively specified by them.
- Also, a solution that allows servers in private subnets to connect to the internet, other VPCs, or on-premises networks should be available.
- The organization would also like to ensure that the network and subnets are secure.
- In addition, the company wants to have a variety of cloud network connectivity and security alternatives.

To achieve all the above along with some additional features, you will be learning a few concepts in this lesson that will help you find solutions for the above-given scenario.

Introduction to VPC

What Is VPC?

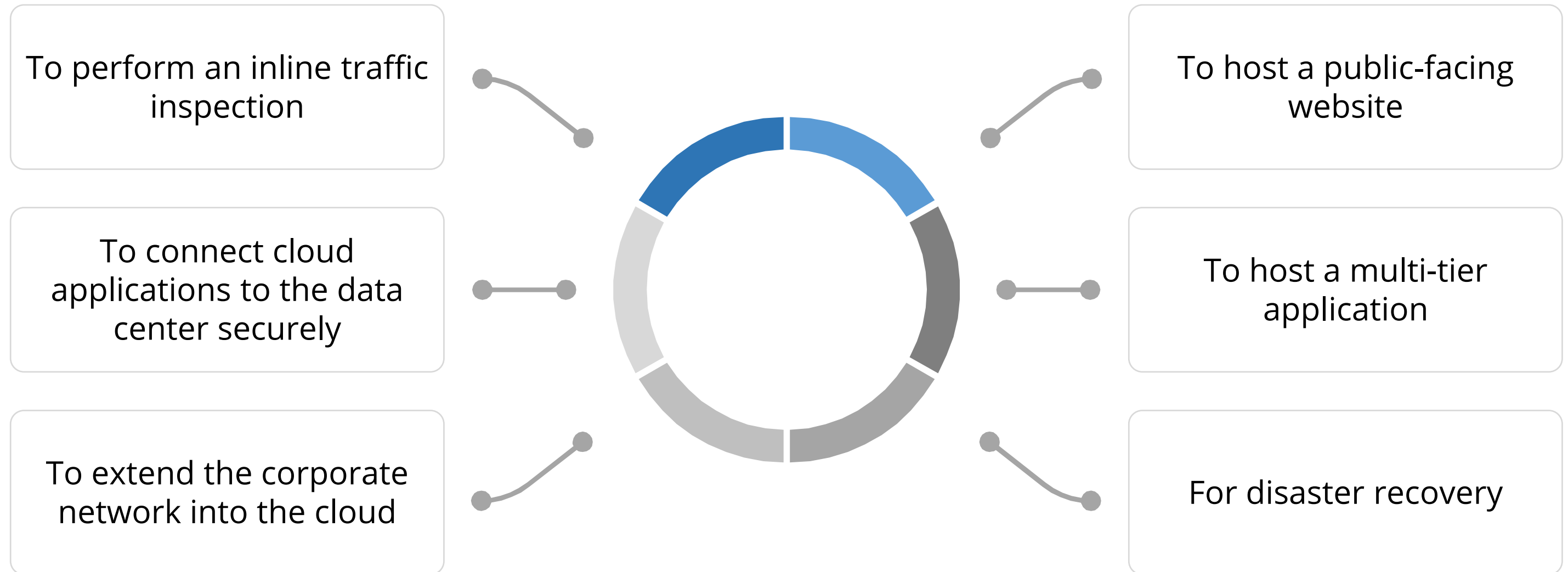
Amazon VPC is a service that helps the users to launch AWS resources into a defined virtual network. It provides users with complete control of the virtual networking environment.

Characteristics of VPC:

- Simple
- Customizable
- Secure

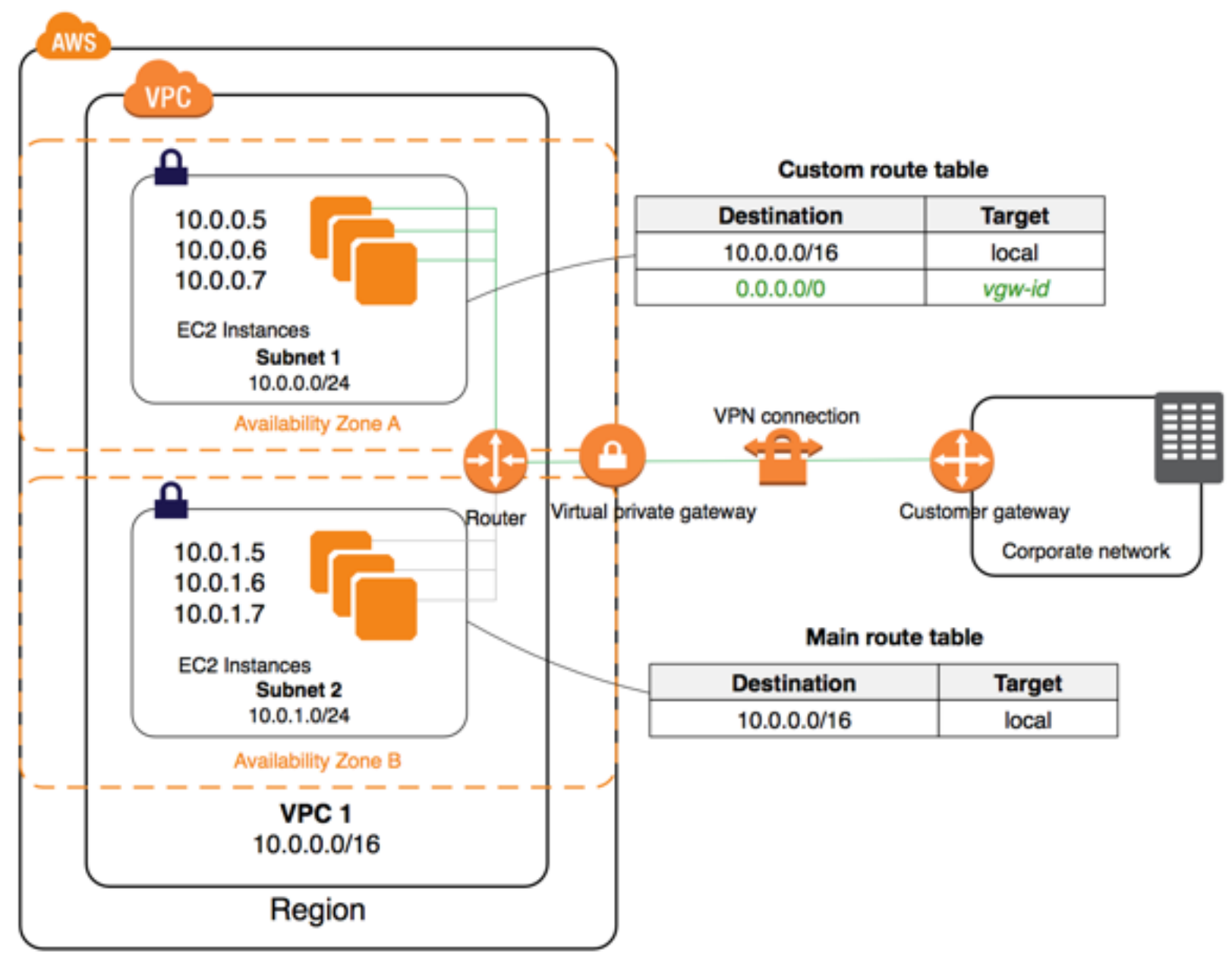


VPC: Uses



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

Assisted Practice

Create a Custom VPC

Duration: 10 Min.

Problem Statement:

You are given a project to create a custom VPC so that a default route table, Network Access Control List, and a default security group will also be automatically created.

Assisted Practice: Guidelines

Steps to create a custom VPC are as follows:

1. Login to AWS lab
2. Navigate to **VPC Management Console**
3. Create a custom VPC
4. Edit and increase the range of hosts

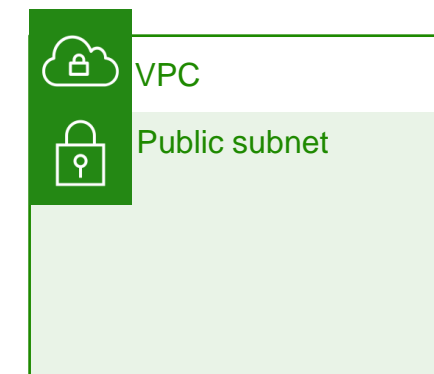
Overview of Subnet

A logical subdivision of an IP network is referred to as a subnet, and the practice of dividing a network into two or more networks is called subnetting.

AWS provides two types of subnetting:

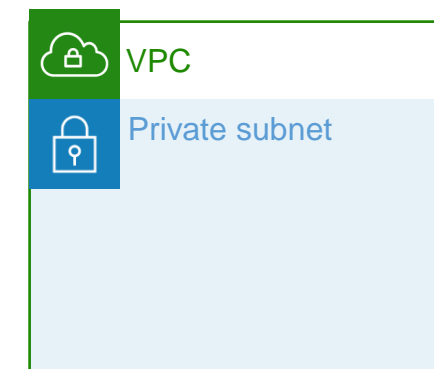
Public:

Allows the internet to access the machine



Private:

Restricts the internet to access the machine



Internet Gateways

An internet gateway is a VPC component that allows communication between a user's VPC and the internet. It is horizontally scaled, redundant, and highly available.

An internet gateway serves two purposes:

- Provides an internet-routable traffic target in a user's VPC route tables
- Performs Network Address Translation (NAT) for instances with public IPv4 addresses



Note

An internet gateway supports IPv4 and IPv6 traffic.

Route Table

A route table is defined by a set of rules called routes that control where the network traffic from your subnet or gateway is directed.

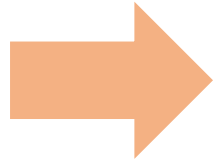
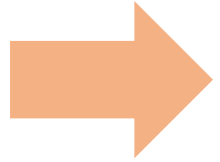
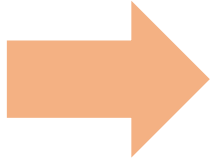
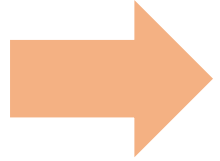
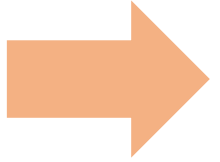
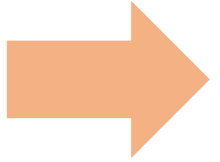
172.16.0.0

172.16.1.0

172.16.2.0

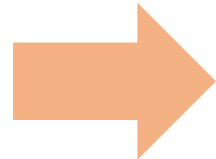
Route Table: Concepts

The key concepts for route tables are as follows.

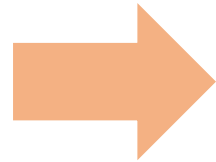
-  **Main route table:** Default route table that comes with the VPC
-  **Custom route table:** A route table created by a user
-  **Edge association:** A route table that routes inbound VPC traffic to an appliance
-  **Route table association:** The connection between a route table and a subnet, internet gateway, or virtual private gateway
-  **Subnet route table:** A route table that is linked to a certain subnet
-  **Gateway route table:** A route table that's associated with an internet gateway or virtual private gateway

Route Table: Concepts

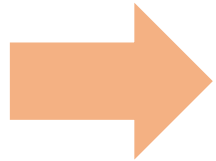
The key concepts for route tables are as follows.



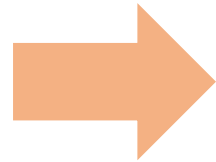
Local gateway route table: A route table that's associated with an Outposts local gateway



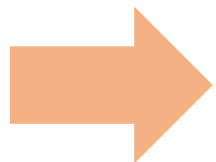
Destination: The range of IP addresses where a user wants traffic to go



Propagation: Route propagation allows a virtual private gateway to automatically propagate routes to the route tables



Target: The gateway, network interface, or connection through which to send the destination traffic



Local route: A default route for communication within the VPC

Egress-Only Internet Gateway

An egress-only internet gateway is a horizontally scaled, redundant, and highly available VPC component that:

- Allows outbound communication over IPv6 from instances in your VPC to the internet
- Prevents the internet from initiating an IPv6 connection with your instances

Note

An egress-only internet gateway is for use with IPv6 traffic only.

Network Address Translation (NAT)

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



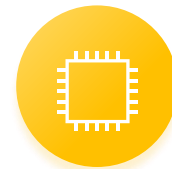
A NAT device is used to forward traffic from the private subnet instances to the internet or AWS services, and then send the response back to the instances.

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



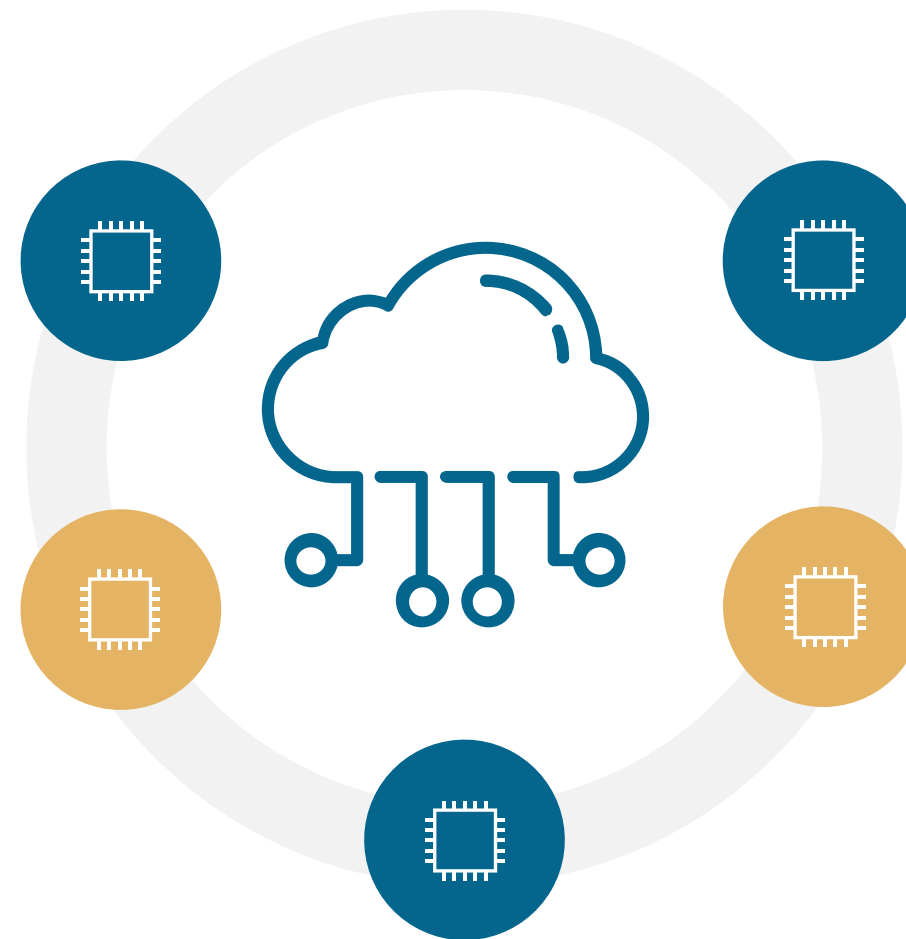
Prevent instances from receiving inbound traffic initiated by someone on the internet



NAT Instances: Characteristics

Allow instances in the private subnet to connect to the internet

Must be launched in a public subnet



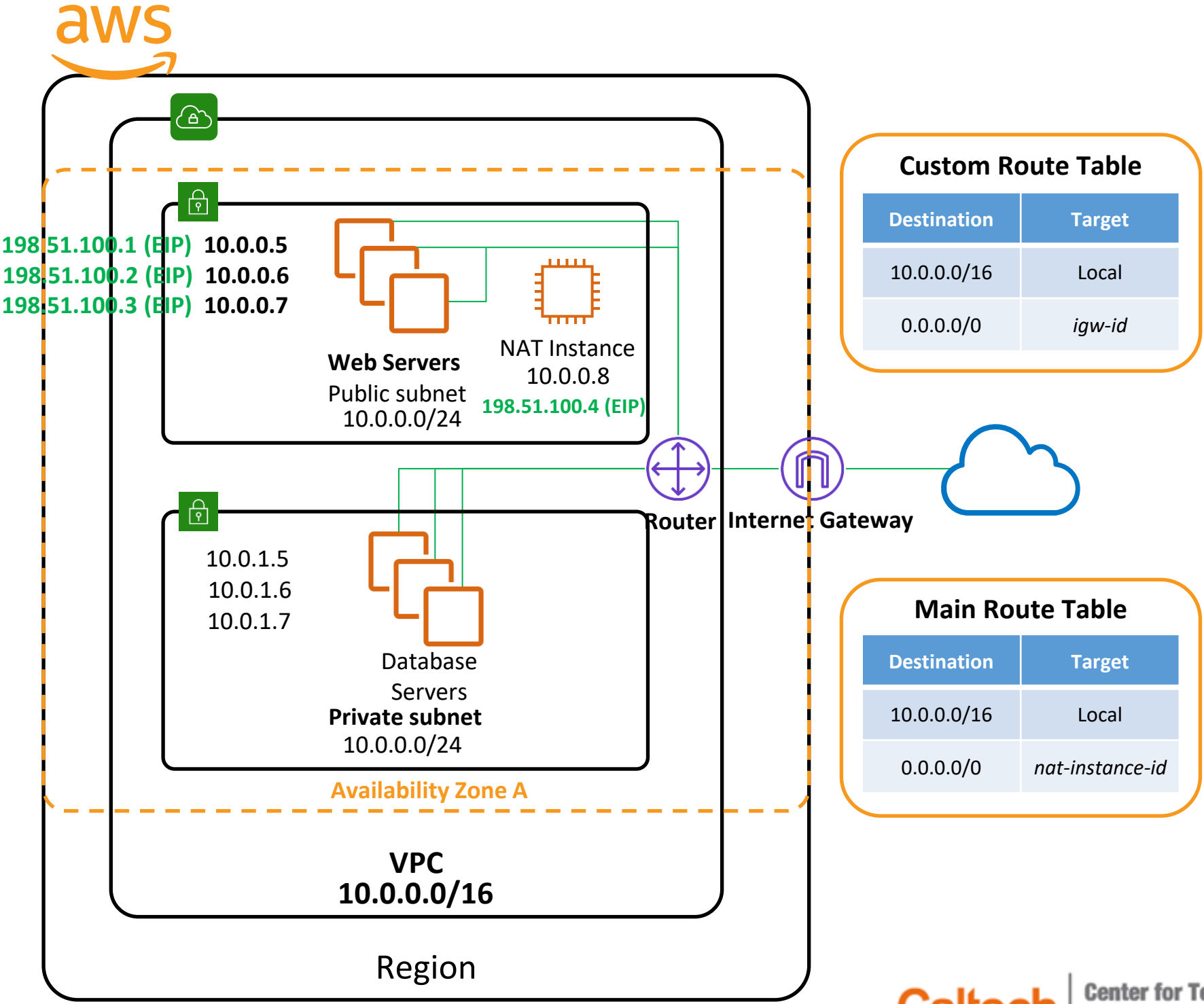
Must have EC2 flag disabled

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.

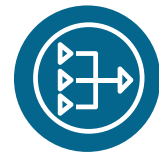


NAT Gateway

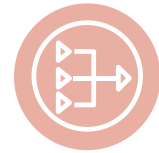
NAT gateway is a device that is used to enable instances in a private subnet to connect to the internet. It prevents the internet from initiating a connection with those instances.

Characteristics of NAT gateway:

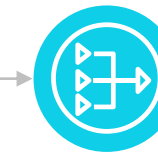
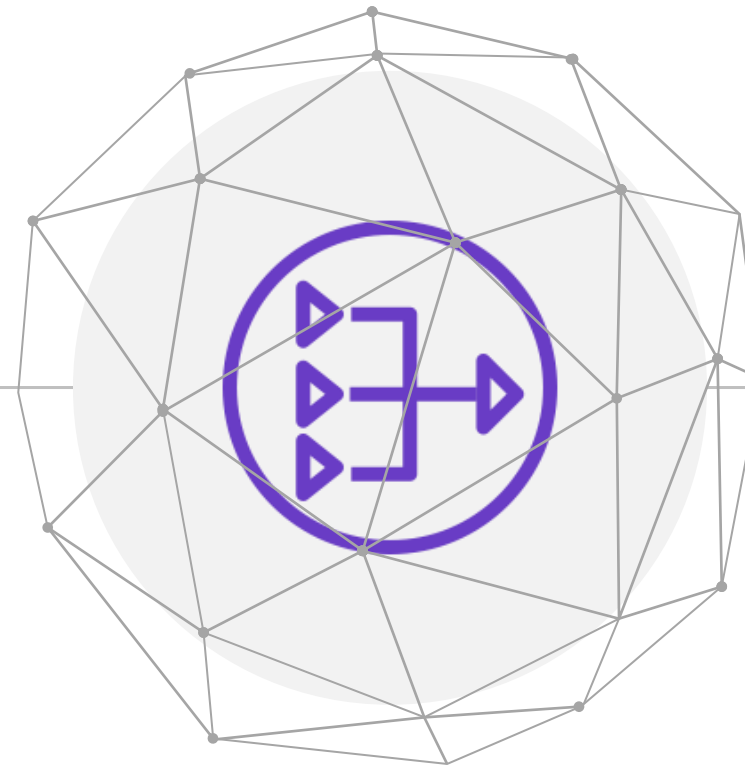
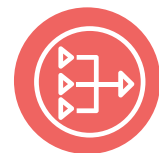
An AWS-managed NAT with a higher bandwidth



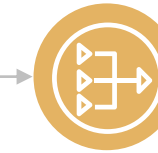
Created in a specific AZ



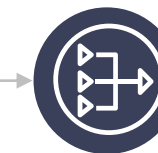
No security group to be managed



Pay per hour for usage and bandwidth



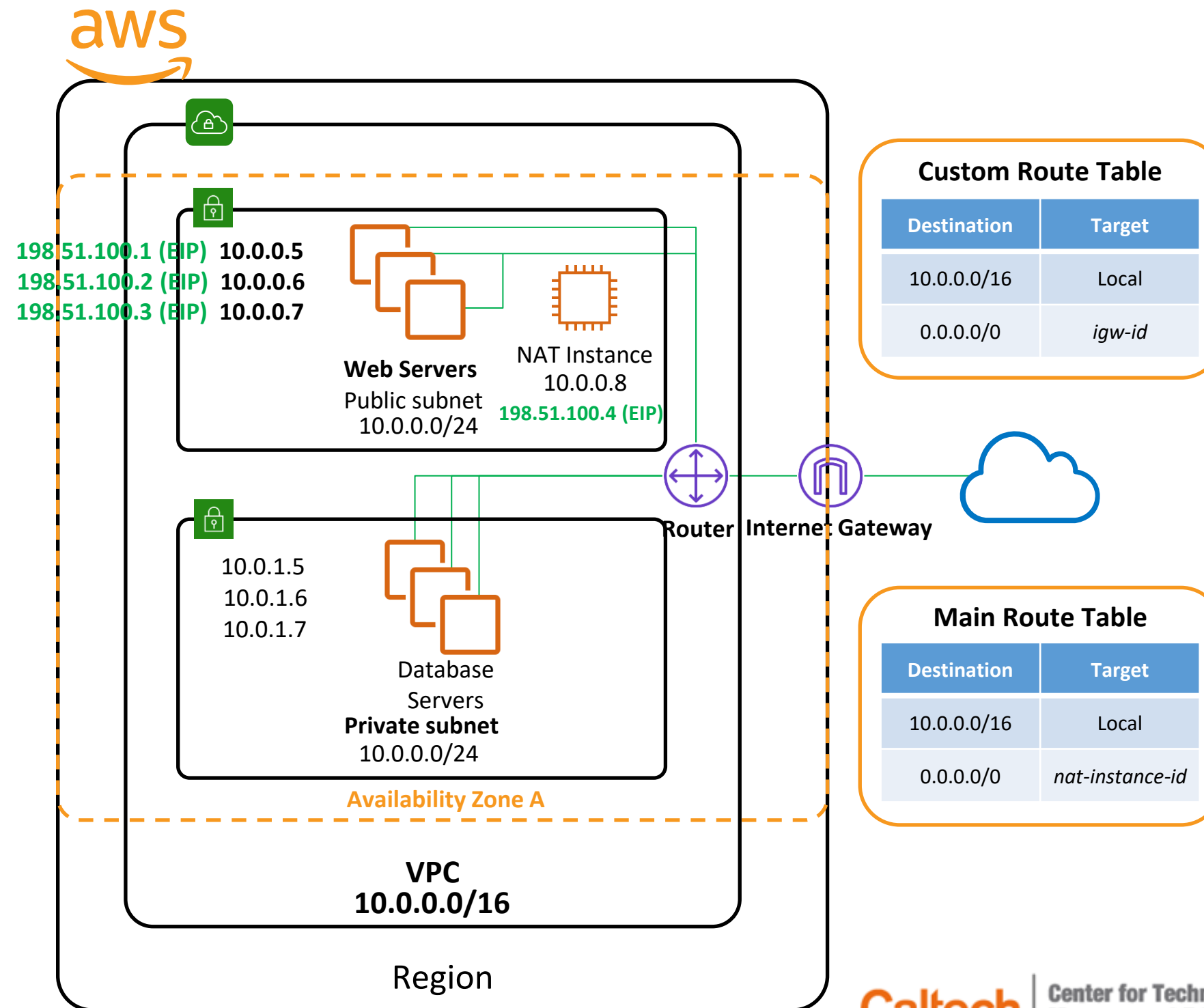
IGW required



Cannot be accessed by a ClassicLink connection associated with VPC

NAT Gateway

The following diagram shows the working of NAT gateway.



Assisted Practice

Configure and Launch a NAT Instance

Duration: 10 Min.

Problem Statement:

You are given the task to configure and launch NAT to allow instances in private subnets to connect to the internet, other VPCs, or on-premises networks.

Assisted Practice: Guidelines

Steps to create and launch a NAT instance:

1. Create a custom VPC
2. Create a public and private subnet
3. Create a public NAT instance

Security Groups

What Is a Security Group?

A security group is a virtual firewall to control traffic on an instance.

- Security groups (SGs) are associated with EC2 instances to provide port access and protocol-level security.
- Each security group contains a set of rules that filters inbound and outbound traffic of an EC2 instance.
- A security group can restrict outside access to your instance, and security rules can filter any malicious requests.

SG Rules

A rule in a security group is the condition that helps a user filter any malicious requests to an instance.

- AWS security groups are stateful.
- Each rule comprises five fields, namely: type, protocol, port range, source, and destination.
- These fields apply to both inbound and outbound rules of the security group.

Provisioning Security Group

Security groups can be created through AWS CLI or AWS Management Console.

Steps to create security groups without creating an EC2 instance:

- Log in to AWS Management Console
- Select EC2 service
- Select **Security Groups** from the menu on the left
- Click on the **Create Security Group** button
- Enter the name and description of the security group
- Select a VPC
- Add the rules

Network Access Control List (ACL)

A Network Access Control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

- A VPC comes with a default network ACL that can be modified.
- A custom network ACL can be created and associated with a subnet.
- Each subnet in a VPC must be associated with a network ACL.
- A user can associate a network ACL with multiple subnets.



Network Access Control List (ACL)

- An ACL for a network is a numbered list of rules. To determine whether traffic is allowed in or out of any subnet associated with the network ACL, we analyze the rules in order, starting with the lowest numbered rule.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Responses to approved inbound traffic are subject to the rules for outbound traffic since network ACLs are stateless.



Network Access Control List (ACL) Rules

A user can modify the default network ACL by adding or removing rules or can establish new network ACLs for VPC.

The following are the parts of a network ACL rule:

- | | |
|---------------|---------------|
| ● Rule Number | ● Port Range |
| ● Type | ● Source |
| ● Protocol | ● Destination |
| ● Allow/Deny | |

Assisted Practice

NACL Creation

Duration: 10 Min.

Problem Statement:

You are given a project to create an NACL that helps to provide a firewall that secures the VPCs and subnets. It helps provide a security layer that controls and efficiently manages the traffic that moves around in the subnets.

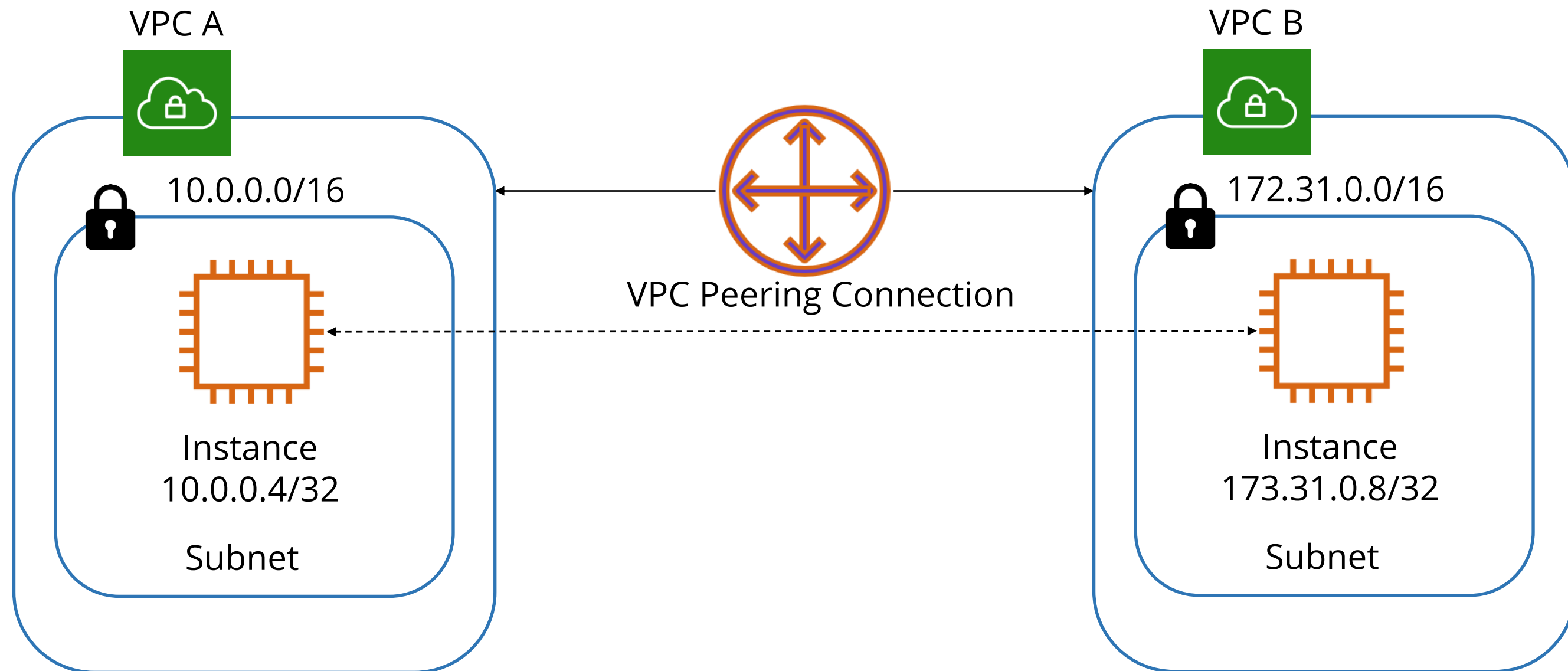
Assisted Practice: Guidelines

Steps to create a network ACL:

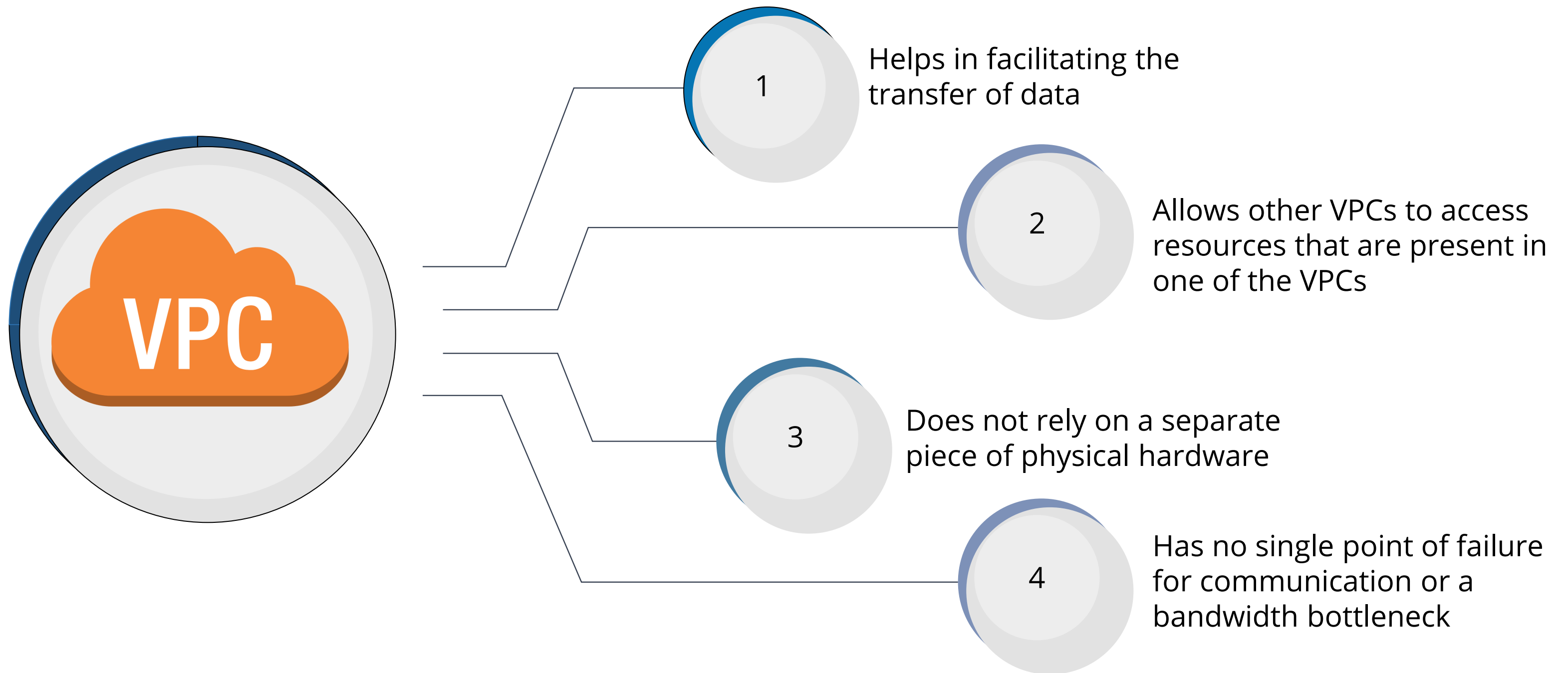
1. Create a network ACL (NACL)
2. Edit the inbound and outbound rules

VPC Peering

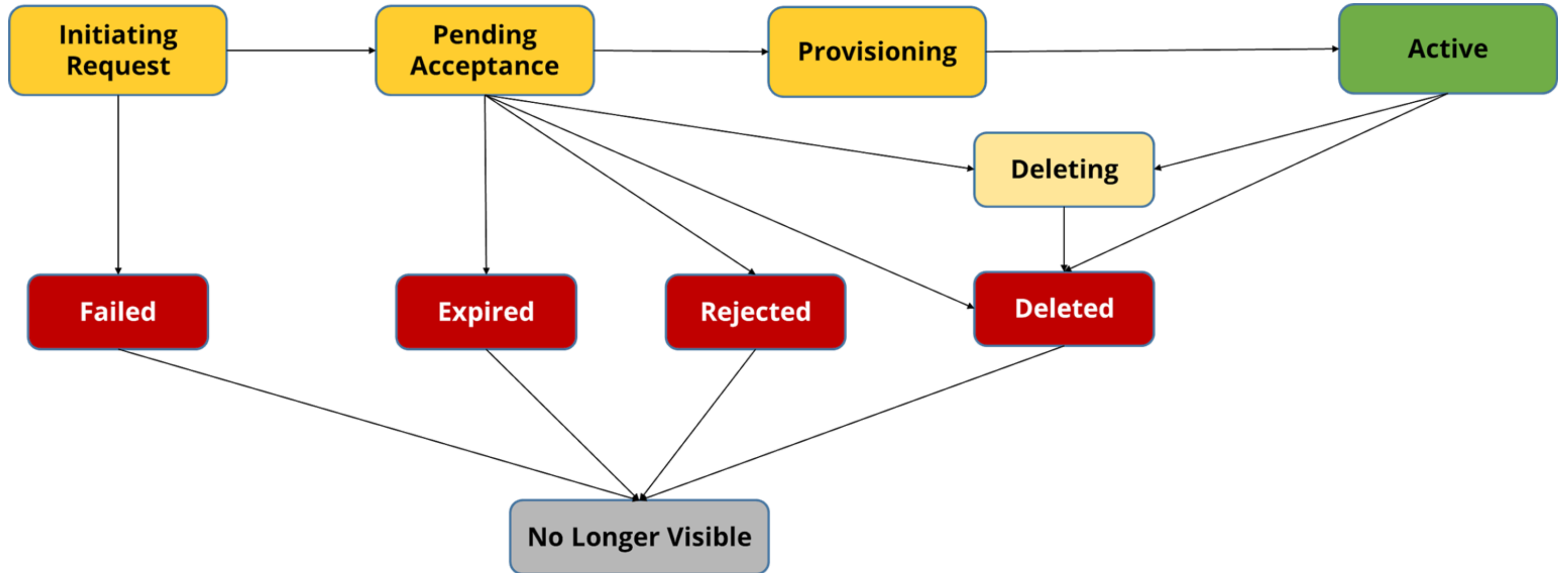
VPC peering is defined as a network connection established between two VPCs that allows to route the traffic between them with private IPV4 and IPV6 addresses.



VPC Peering: Advantages



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

Assisted Practice

Create a VPC Endpoint

Duration: 10 Min.

Problem Statement:

You are given the task to create a VPC endpoint that allows you to privately connect your VPC to supported AWS services.

Assisted Practice: Guidelines

Steps to create a VPC endpoint:

1. Select **Amazon VPC** from the **Services**
2. Create a VPC endpoint
3. Choose category
4. Enable DNS

Interpret 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



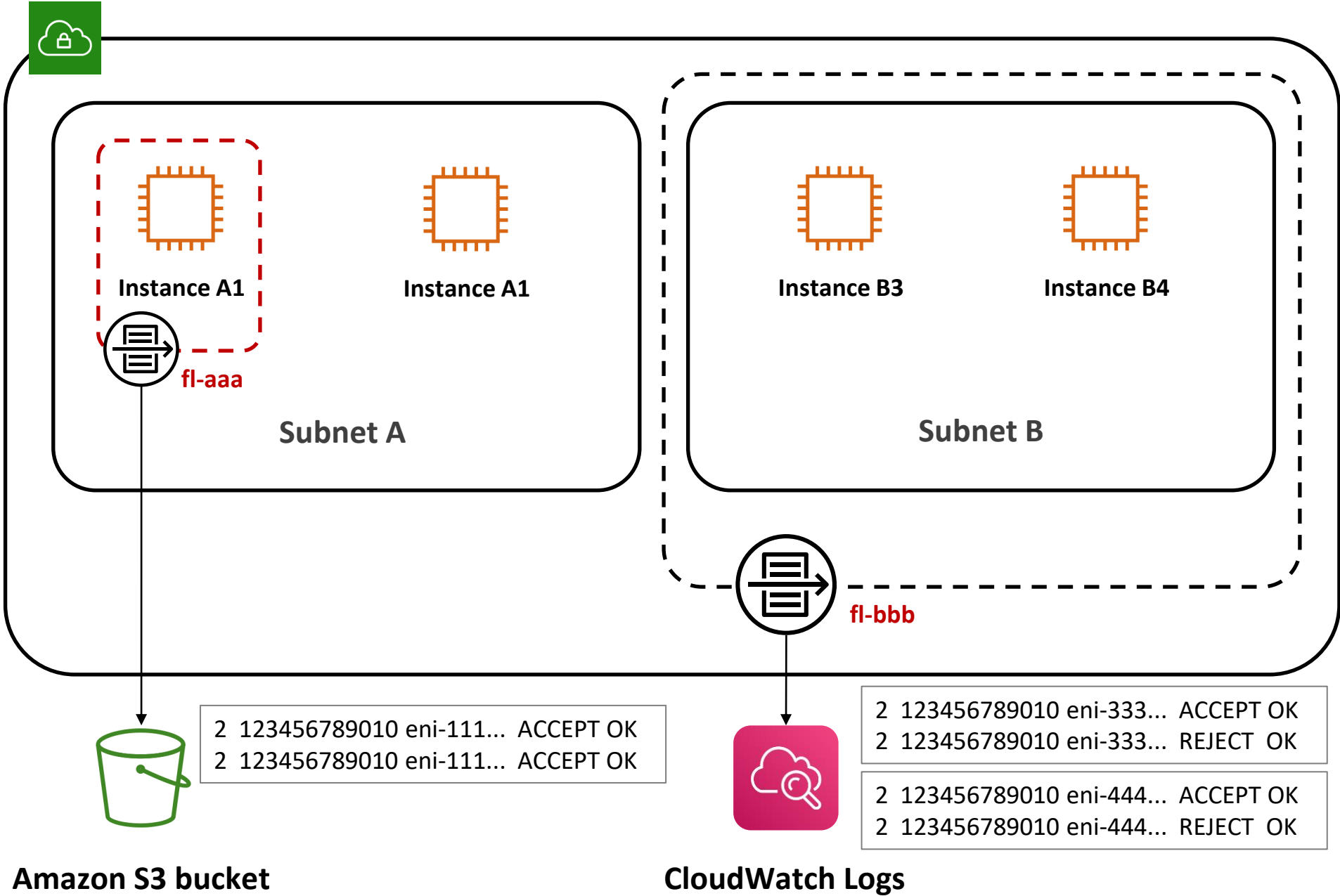
To determine the direction of the traffic to and from the network interfaces



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



Assisted Practice

Create a VPC Flow Log

Duration: 10 Min.

Problem Statement:

You are given the task to create a VPC Flow log that will enable you to capture information about the IP traffic going to and from network interfaces in your VPC.

Assisted Practice: Guidelines

Steps to create VPC logs:

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

Elastic Load Balancer Access Logs

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer.

Each log contains information such as:

- Time the request was received
- The client's IP address
- Latencies
- Request paths
- Server responses

A user can use these access logs to analyze traffic patterns and troubleshoot issues.

Assisted Practice

Clean a VPC

Duration: 10 Min.

Problem Statement:

You are given the task to clean up your VPC as it is no longer required.

Assisted Practice: Guidelines

Steps to clean VPC:

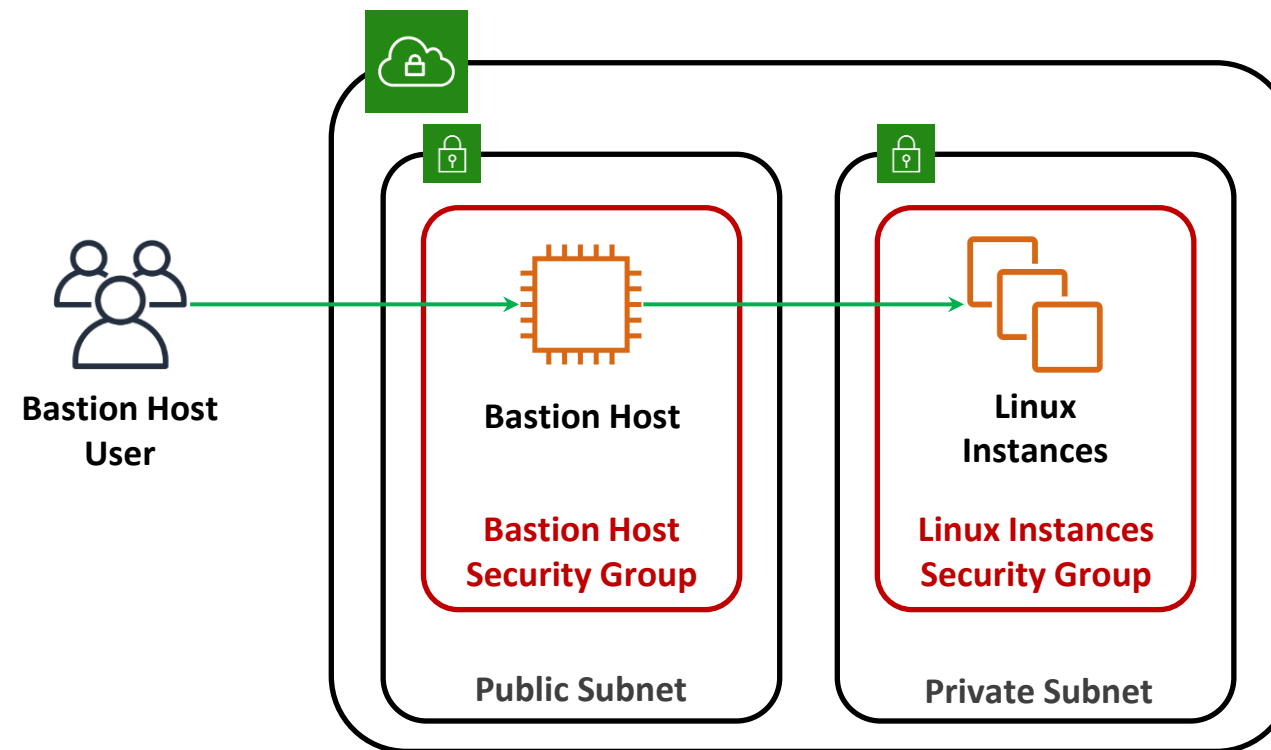
1. Navigate to VPC Management Console
2. Clean a VPC
3. Delete an instance
4. Delete VPC

Bastion Hosts

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.

Network Connectivity

AWS Site-to-Site VPN

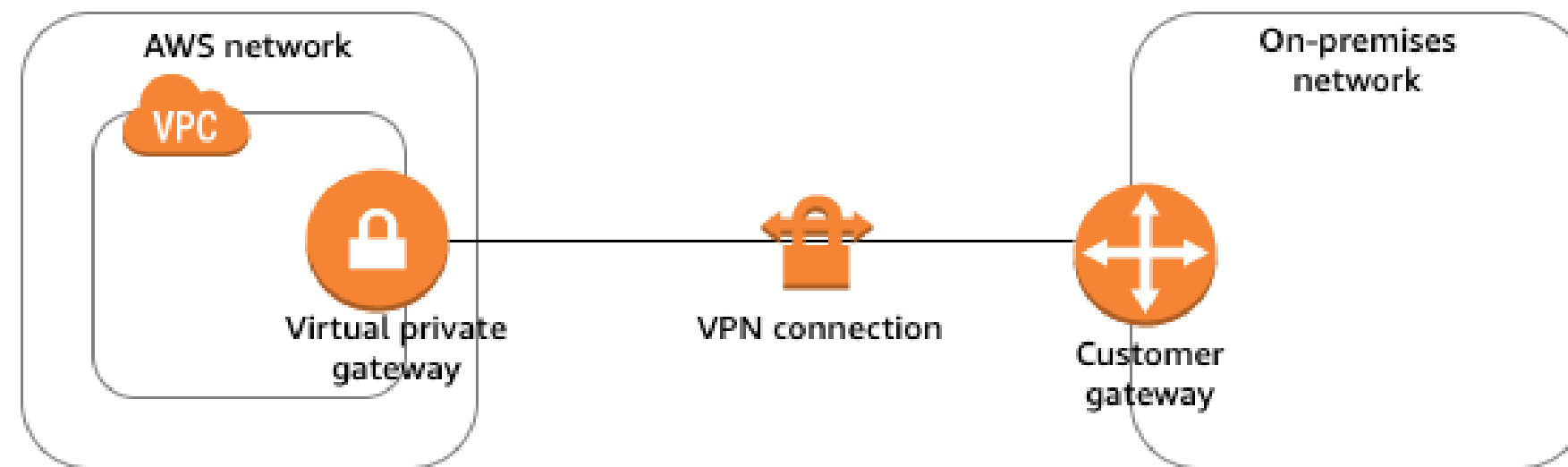
A Site-to-Site VPN connection establishes two VPN tunnels between an AWS virtual private gateway or transit gateway and a remote (on-premises) customer gateway (which represents a VPN device).

A Site-to-Site VPN connection consists of the following components:

- Virtual private gateway
- Transit gateway
- Customer gateway device
- Customer gateway

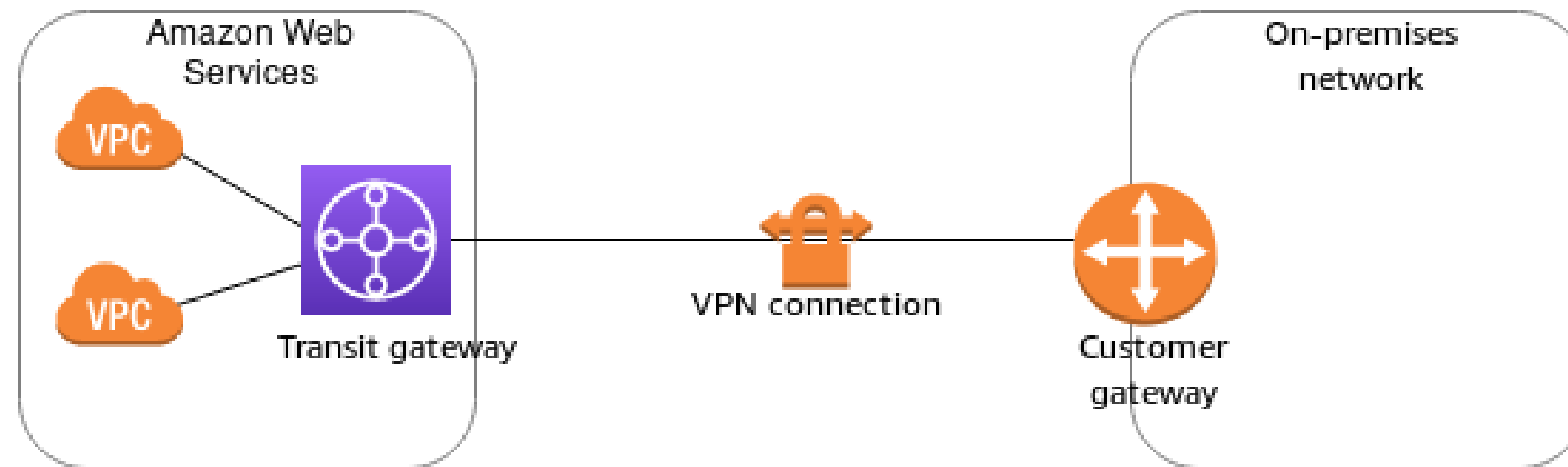
Virtual Private Gateway

A virtual private gateway is the VPN concentrator on the Amazon side of a Site-to-Site VPN connection. A user creates a virtual private gateway and attaches it to the VPC where the Site-to-Site VPN connection will be established.



Transit Gateway

A Transit Gateway is a transit hub that you can use to interconnect your Virtual Private Clouds (VPC) and on-premises networks.



Customer Gateway Device and Customer Gateway

Customer Gateway Device

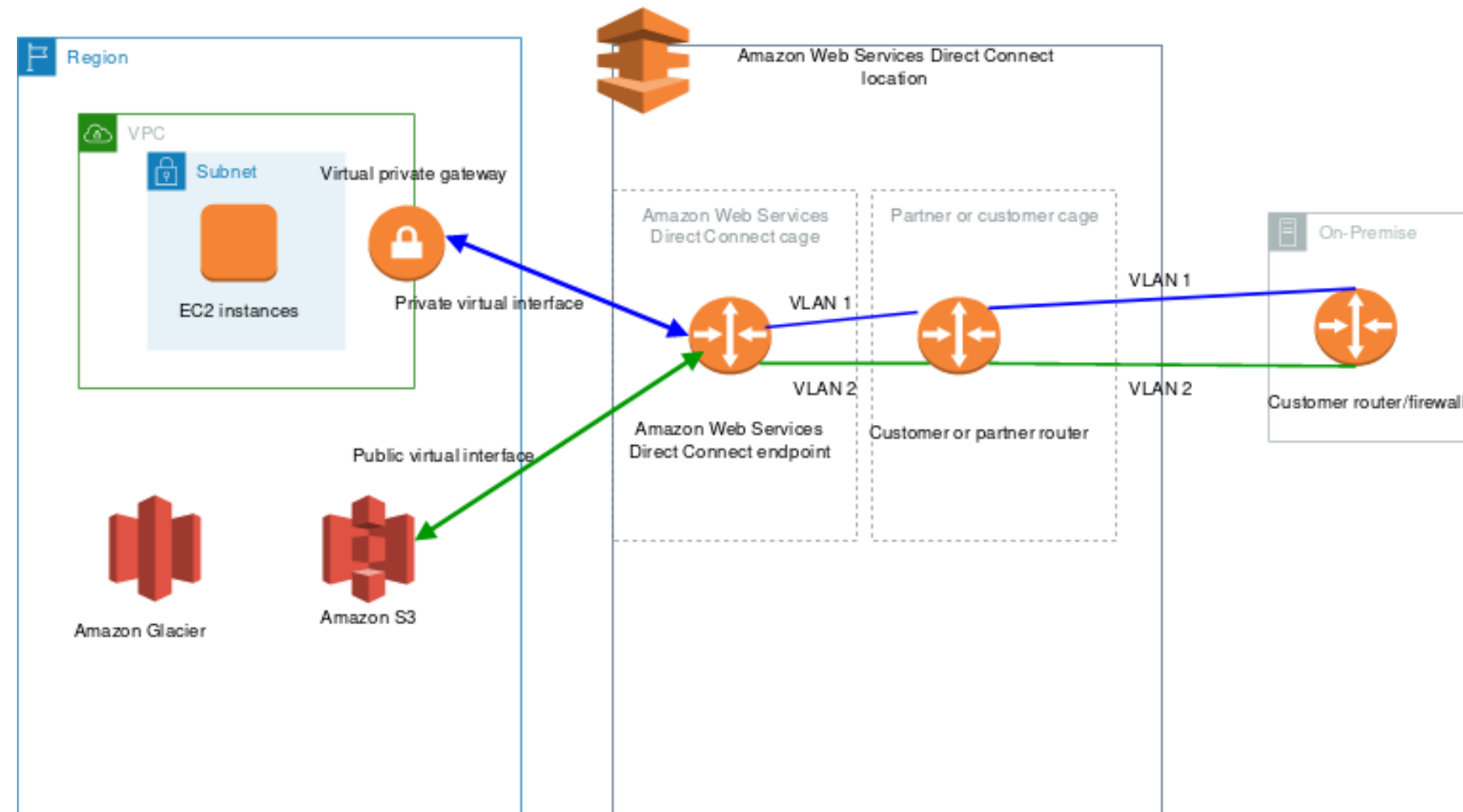
A customer gateway device is a physical device or software application on your side of the Site-to-Site VPN connection. A user configures the device to work with the Site-to-Site VPN connection.

Customer Gateway

A customer gateway is a resource that a user creates in AWS that represents the customer gateway device in his on-premises network. When the user creates a customer gateway, he provides information about his device to AWS.

Direct Connect

AWS Direct Connect uses a regular Ethernet fiber-optic cable to connect your internal network to an AWS Direct Connect facility.



AWS Direct Connect Components

AWS Direct Connect requires the following key components:

Connections

To build a network connection from on-premises to an AWS Region, create a connection at an AWS Direct Connect location.

Virtual Interfaces

To gain access to AWS services, create a virtual interface.

AWS Direct Connect Gateways

It enables a user to connect multiple Virtual Private Clouds (VPCs).

AWS Direct Connect gateways can be associated with any of the following gateways:

- A transit gateway when a user has multiple VPCs in the same Region
- A virtual private gateway to extend a user's Local Zone

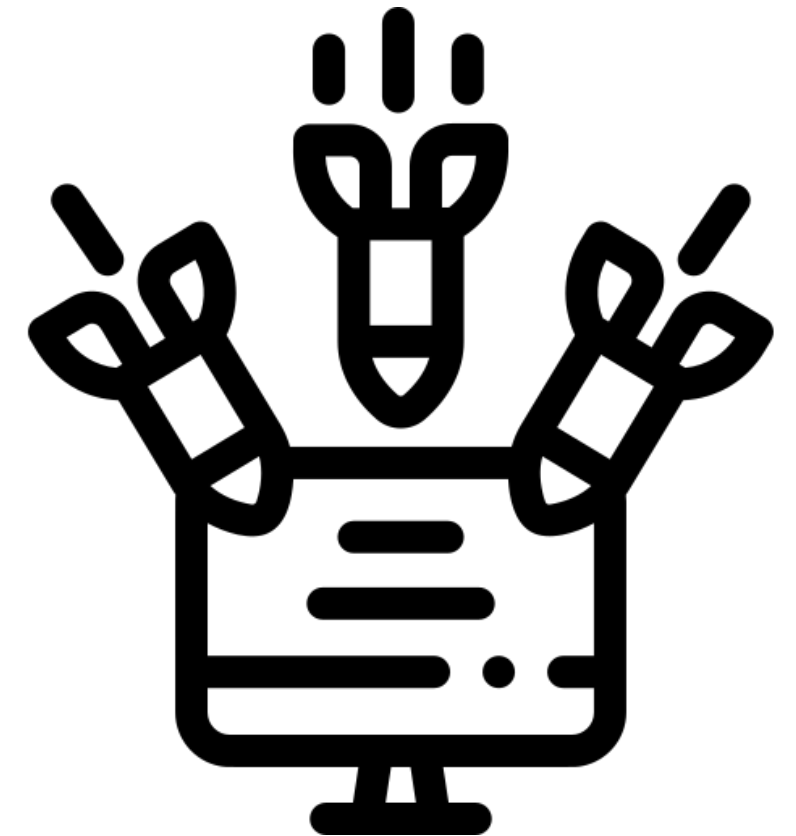
A Direct Connect gateway is a globally available resource.

Network Security

What Is DDoS?

A Distributed Denial-of-Service (DDoS) attack is a malicious act to disturb the normal traffic of a server, a service, or a network.

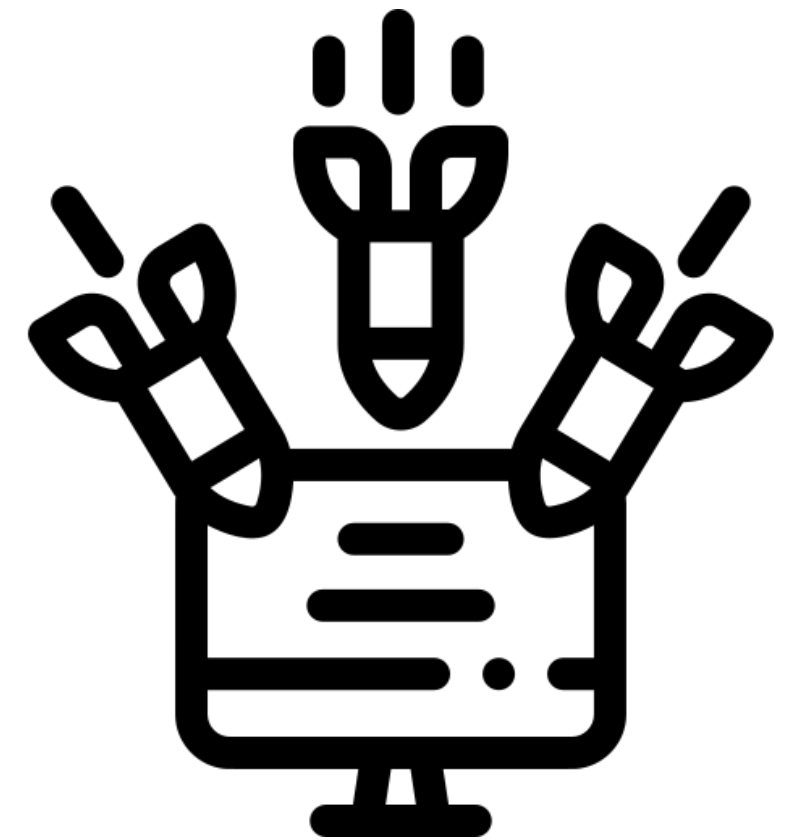
- Attackers generate large volumes of packets or requests which overload the target system.
- It can also be done by multiple mechanisms, such as a combination of reflection and amplification techniques and also by using large botnets.
- In DDoS, attackers use multiple sources to generate attacks.
- A DDoS attack makes an application or a website unavailable to the end user.



Types of DDoS Attacks

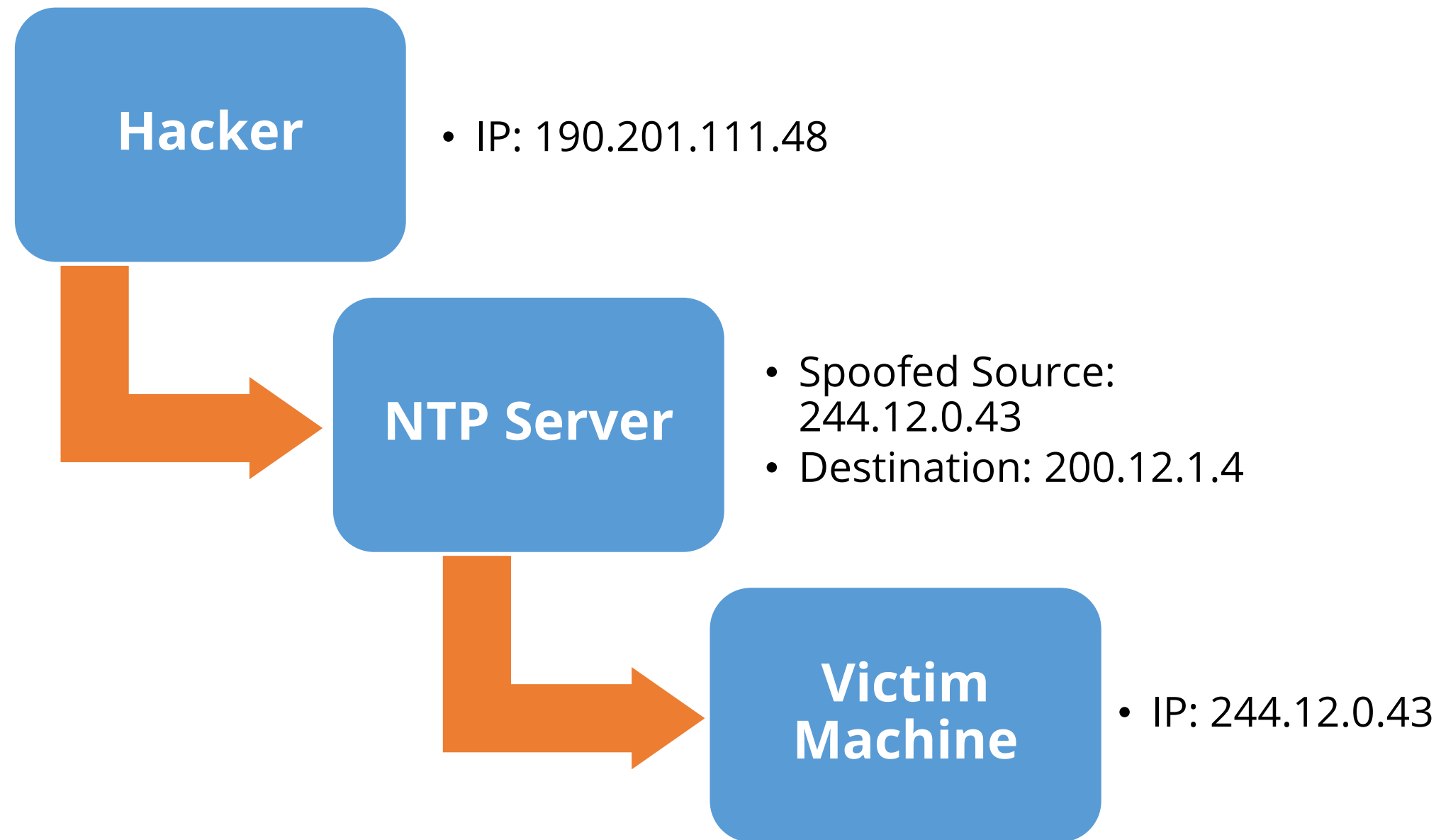
Amplification or Reflection

- It includes NTP, SSDP, DNS, Chargen, and SNMP attacks.
- In this attack, the attacker sends a request to a third-party server, such as NTP, using a spoofed IP address.
- Here, the server responds to this request with a larger payload than the initial request.
- Example: If the attacker sends a request of 64 bytes, the server responds with up to 3500 bytes of traffic.
- Attackers can use multiple third-party servers and make the server busy with a huge payload.
- These attacks are also called infrastructure layer attacks.



Types of DDoS Attacks

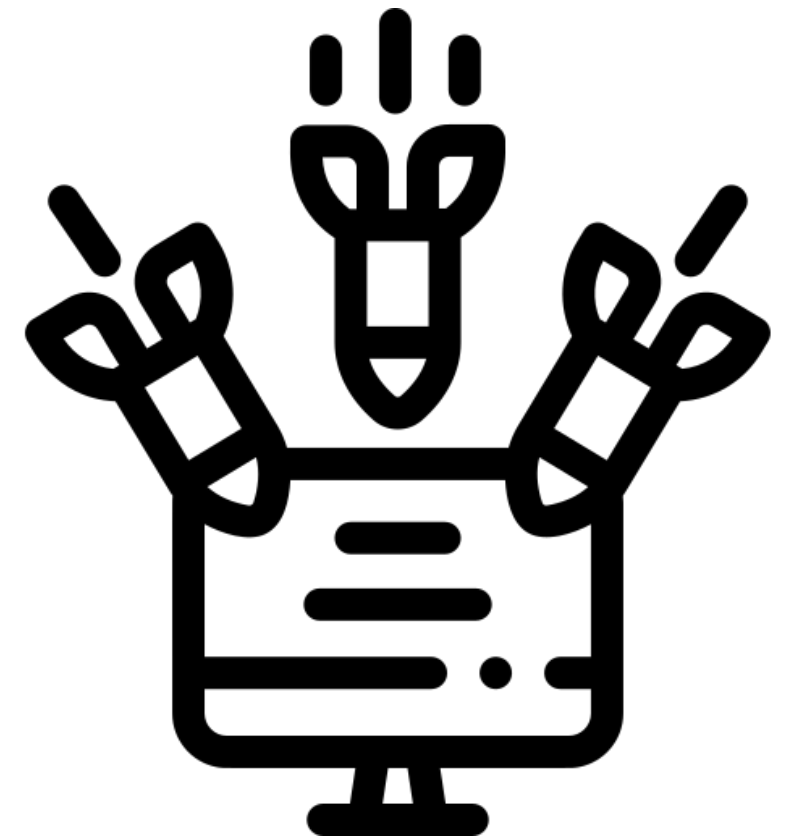
A representation of amplification or reflection is given below:



Types of DDoS Attacks

Application Attacks (L6 and L7)

- These attacks occur on layers 6 and 7 of the OSI model.
- They tend to focus on particularly expensive parts of an application thereby making it unavailable for real users.
- Example: A flood of HTTP requests to a login page or an expensive search API are the most common ways to attack layers 6 and 7.
- These attacks are also called application layer attacks.



Mitigating DDoS

The ways to mitigate DDoS attacks are as follows:

- Reduce the attack surface area using ALBs with web application files
- Scale the system to handle the attack using Auto Scaling groups
- Safeguard exposed resources
- Learn the behavior of an application to analyze if it acts abnormally
- Create a plan for attacks



AWS Shield

AWS Shield is a managed Distributed Denial-of-Service (DDoS) protection service that safeguards applications running on AWS.

- AWS Shield provides detection and automatic mitigation mechanism to reduce application downtime.
- There are two levels of AWS Shield subscriptions: Standard and Advanced protection.
- Standard subscription is free and can be used for applications hosted on services, like **CloudFront**, for protection against the most common DDoS attacks.



Source: <https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

AWS Shield

- For applications hosted over services, such as EC2 and ELBS, the advanced-level subscription is helpful.
- AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks.



Source: <https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

Benefits of AWS Shield

- Seamless integration and deployment: By default, the Standard protection is automatically enabled for the resources, and the Advanced one can be enabled in the service configurations. No routing changes are required.
- Customizable protection: Users can write customized rules with AWS WAF and deploy them immediately.



Source: <https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

Benefits of AWS Shield

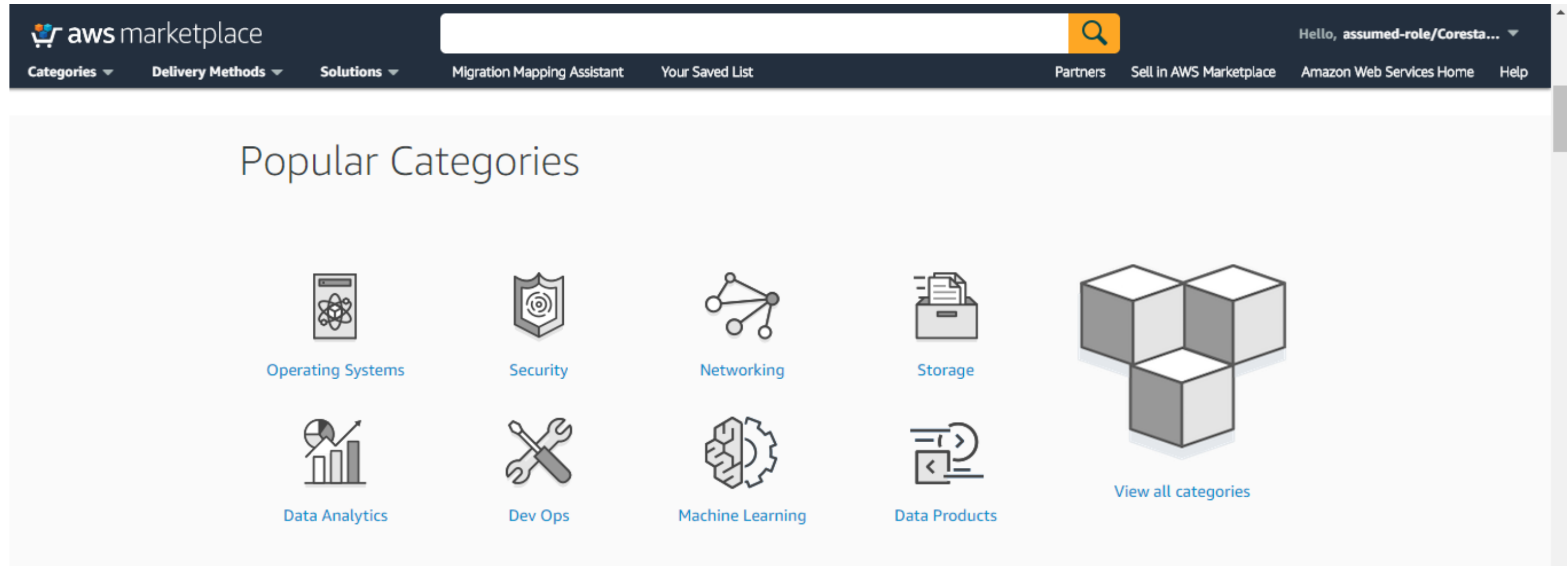
- Managed protection and attack visibility: AWS Shield is an always-on monitoring and protection mechanism and enables access to DRT for manual mitigation of risks. It provides a dashboard to keep an eye on the activities that are occurring to mitigate attacks.
- Cost-efficient: AWS Shield Standard is automatically enabled and is free of cost. AWS Shield Advanced provides AWS WAF and AWS firewall manager free of cost.



Source: <https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

AWS Marketplace

AWS marketplace is an online portal for purchasing products or services for your applications or projects.



Source: <https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

AWS Marketplace Security Products

AWS marketplace contains products for security purposes with all types of testing and protection tools. Examples of penetration testing tools are given below:

The screenshot shows the AWS Marketplace interface with a search for 'penetration testing'. The left sidebar contains filters for Vendors, Operating System, and Pricing Plan. The main content area displays three product listings: PurpleLeaf - Penetration Testing as a Service (PTaaS), Evolve Security Automation, and another Evolve Security Automation listing. The bottom of the page shows a shopping cart icon and a navigation bar with logos for Caltech, Center for Technology & Management Education, and simplilearn.

aws marketplace penetration testing

Categories ▾ Delivery Methods ▾ Solutions ▾ Migration Mapping Assistant Your Saved List Partners Sell in AWS Marketplace

Vendors

- ☐ SAINT (4)
- ☐ Evolve Security Automation (2)
- ☐ Cymulate - Breach and Attack Simulation (2)
- ☐ Cognosys Inc. (2)
- ☐ PurpleLeaf (1)
- ☐ foreseei (1)
- ☐ Guardicore (1)
- ☐ Fortinet Inc. (1)
- ☐ Kali Linux (1)
- ☐ Dimatas Technologies (1)
- [Show more](#)

Operating System

- ☒ All Windows
- ☒ All Linux/Unix

Pricing Plan

- ☐ Bring Your Own License (4)
- ☐ By Units (4)
- ☐ Annual (2)
- ☐ Free (2)
- ☐ Hourly (2)

PurpleLeaf - Penetration Testing as a Service (PTaaS)

Sold by [Virtue Security](#)

PurpleLeaf is a service-backed continuous penetration testing platform. Our platform allows customers to receive ongoing manual penetration testing combined with network and cloud vulnerability scanning. By purchasing PurpleLeaf through the AWS marketplace, your dedicated dashboard is created...

Linux/Unix, Other 2020.2 - 64-bit Amazon Machine Image (AMI)

evolve **Evolve Security Automation**

Version 2.1.0.0 | Sold by [Threat Intelligence Pty Ltd](#)

Evolve is the world's first Security Automation Cloud. The Evolve Marketplace offers over 350 specialist security automation workflows delivering on-demand automated specialist security capabilities including: - Automated Penetration Testing (BAS) - Automated Incident Response (SOAR) - Automated...

Linux/Unix, Ubuntu 2019.11.13 - 64-bit Amazon Machine Image (AMI)

evolve **Evolve Security Automation**

Version 2.1.0.0 | Sold by [Threat Intelligence Pty Ltd](#)

Starting from \$15.00/mo for software + AWS usage fees

Evolve is the world's first Security Automation Cloud. The Evolve Marketplace offers over 350 specialist security automation workflows delivering on-demand automated specialist security capabilities including: - Automated Penetration Testing (BAS) - Automated Incident Response (SOAR) - Automated...

Linux/Unix, Ubuntu 2019.11.13 - 64-bit Amazon Machine Image (AMI)

cart.png

Caltech | Center for Technology & Management Education | simplilearn

What Is AWS WAF?

AWS WAF is a web application firewall that lets you monitor HTTP and HTTPS requests that are forwarded to CloudFront, an ALB, or an API gateway.

- Users can configure restrictions and put conditions for the approval of access.
- Control access can be achieved using conditions, such as what IP addresses are allowed to make requests or what parameters are required in the query string.
- Using the above information, ALB or CloudFront decides whether to give permission to receive data or to send 403 error code.



AWS WAF Operations

AWS WAF allows three basic operations:

- Allows all requests except the excluded ones
- Rejects all requests except the approved ones
- Allows requests that match the specified conditions



AWS WAF Conditions

Conditions that a user can specify using characteristics of web requests:

- IP address for the origin of a request
- Country for the origin of a request
- Header values
- Mandatory strings to be present in the query
- Length of the requests
- Presence of SQL code in the query
- Presence of scripts, such as cross-site scripting, in the query string



WAF Integration

Services with which WAF integrates and doesn't integrate:

- WAF integrates with:
 - Application load balancer
 - CloudFront
 - API Gateway
- WAF doesn't integrate with:
 - Classic load balancer
 - Network load balancer

Note: WAF is a layer 7 service, and it needs application visibility. As a result, it doesn't integrate with classic and network load balancers.



Content Delivery

Amazon CloudFront

Fast content delivery network service that securely delivers data and applications globally with high-transfer speed

Integrated with AWS (both physical locations) connected to the AWS global infrastructure

It works seamlessly with services (DDos and Shield) to run custom codes and customize user experience



Benefits of Amazon CloudFront

- 1 Fast and Global
- 2 Security at the Edge
- 3 Highly Programmable
- 4 Deep Integration with AWS



Set up CloudFront to Deliver Network

1

Specify the origin servers from which CloudFront will get files to distribute over locations

2

Upload the files to the origin servers

3

Create CloudFront distribution to inform servers to get the user request files

4

Assigns a domain name to the new distribution that is returned as a response

5

Sends distribution configuration to all of its edge locations and points of presence

Cache Hit Ratios

The ratio of requests served from edge locations is known as cache hit ratio

More requests from edge locations imply better performance

Reduced load on origin server and latency

Improving Cache Hit Ratios

Improve cache hit ratios by:

- Specifying how long CloudFront caches your objects
- Caching based on query string parameters
- Caching based on cookie values and cookie requests
- Removing accept-encoding header when compression is not needed
- Serving media content by using HTTP



Improving
Cache Hit
Ratios

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.

