


AWS Virtual Private Cloud (VPC)

Khalid Bin Sattar





Agenda

- Overview of Amazon VPC.
 - Introduction to Amazon VPC.
 - Introduction to Subnet.
 - Basic Concepts of VPC.
 - Amazon VPC Advance Features.
 - Working with VPC & Subnets.
 - Amazon VPC Networking Concepts.
 1. Network Interface.
 2. Route Tables.
 3. Internet Gateways.
 4. NAT (Network Address Translation).
 - VPN Connections.
 - Amazon VPC Limitation.
 - Amazon VPC Pricing.
 - Demo and Scenarios.
- 



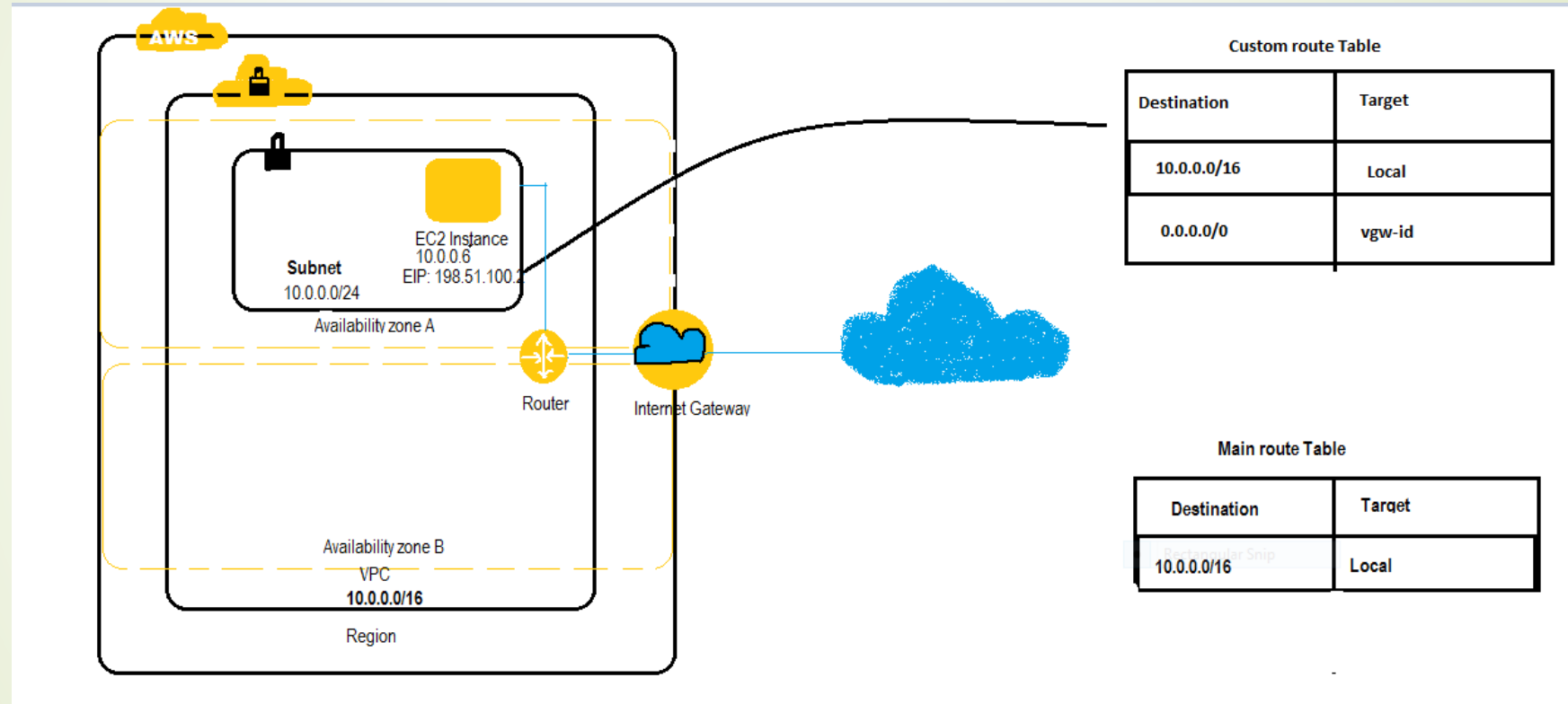
Overview of Amazon VPC

What Is Amazon VPC?

A virtual private cloud (VPC) is a virtual network that closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of Amazon Web Services (AWS).

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.

Architecture of Amazon VPC





Amazon VPC Concepts

VPCs and Subnets

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings.

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.

Amazon VPC Concepts

Supported Platforms:- The original release of Amazon EC2 supported a single, flat network that's shared with other customers called the EC2-Classic platform. Older AWS accounts still support this platform, and can launch instances into either EC2-Classic or a VPC. Accounts created after 2013-12-04 support EC2-VPC only.

By launching your instances into a VPC instead of EC2-Classic, you gain the ability to:

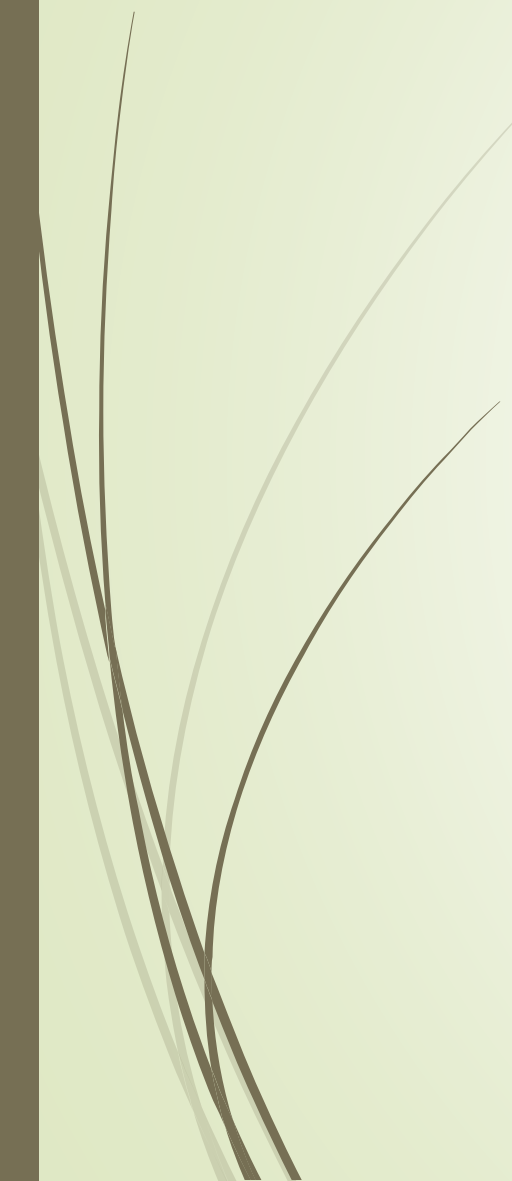
- Assign static private IPv4 addresses to your instances that persist across starts and stops.
- Optionally associate an IPv6 CIDR block to your VPC and assign IPv6 addresses to your instances.
- Assign multiple IP addresses to your instances.
- Define network interfaces, and attach one or more network interfaces to your instances.



Amazon VPC Concepts

Supported Platforms:-

By launching your instances into a VPC instead of EC2-Classic, you gain the ability to:

- Change security group membership for your instances while they're running.
 - Control the outbound traffic from your instances (egress filtering) in addition to controlling the inbound traffic to them (ingress filtering)
 - Add an additional layer of access control to your instances in the form of network access control lists (ACL)
 - Run your instances on single-tenant hardware.
- 



Amazon VPC Concepts

Default and Nondefault VPCs:-

If your account supports the EC2-VPC platform only, it comes with a default VPC that has a default subnet in each Availability Zone. A default VPC has the benefits of the advanced features provided by EC2-VPC, and is ready for you to use. If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC. You can launch instances into your default VPC without needing to know anything about Amazon VPC.

Regardless of which platforms your account supports, you can create your own VPC, and configure it as you need. This is known as a nondefault VPC. Subnets that you create in your nondefault VPC and additional subnets that you create in your default VPC are called nondefault subnets.



Amazon VPC Concepts

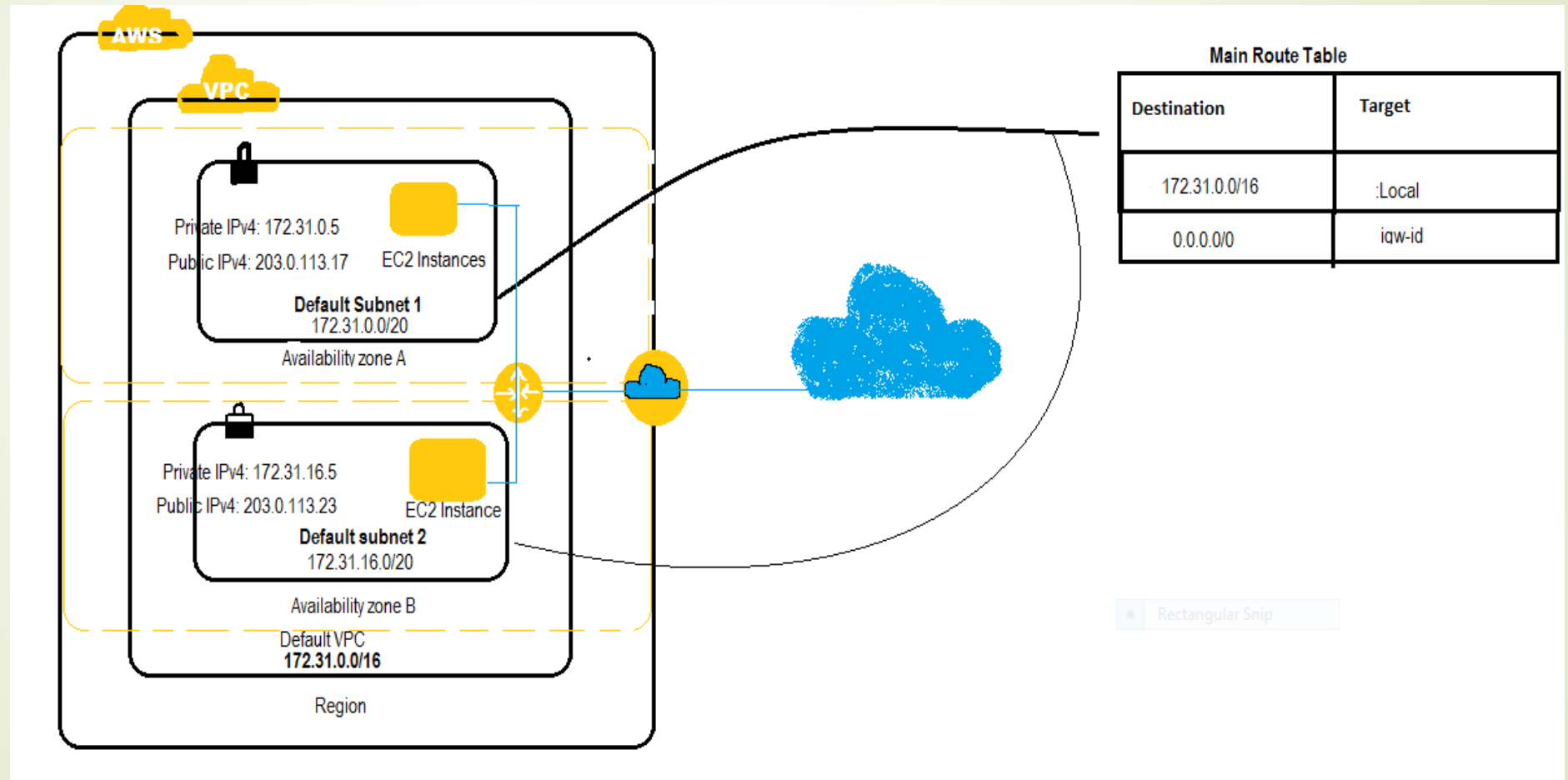
Accessing the Internet:-

You control how the instances that you launch into a VPC access resources outside the VPC.

Your default VPC includes an Internet gateway, and each default subnet is a public subnet. Each instance that you launch into a default subnet has a private IPv4 address and a public IPv4 address. These instances can communicate with the Internet through the Internet gateway. An Internet gateway enables your instances to connect to the Internet through the Amazon EC2 network edge.

Amazon VPC Concepts

Accessing the Internet:-





Amazon VPC Concepts

Accessing the Internet:-

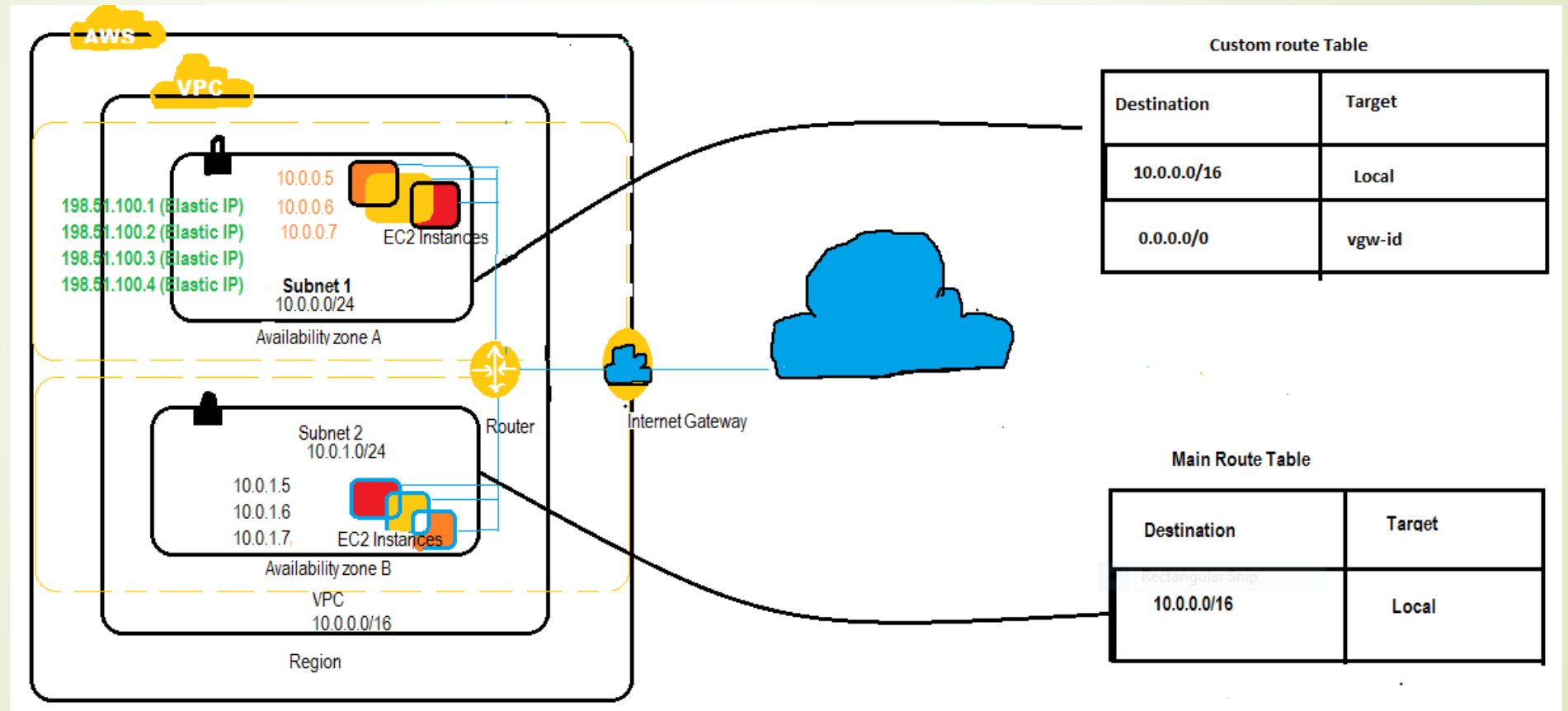
By default, each instance that you launch into a nondefault subnet has a private IPv4 address, but no public IPv4 address, unless you specifically assign one at launch, or you modify the subnet's public IP address attribute. These instances can communicate with each other, but can't access the Internet.

You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance.

Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) device for IPv4 traffic. NAT maps multiple private IPv4 addresses to a single public IPv4 address. A NAT device has an Elastic IP address and is connected to the Internet through an Internet gateway. You can connect an instance in a private subnet to the Internet through the NAT device, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

Amazon VPC Concepts

Accessing the Internet:-





Amazon VPC Concepts

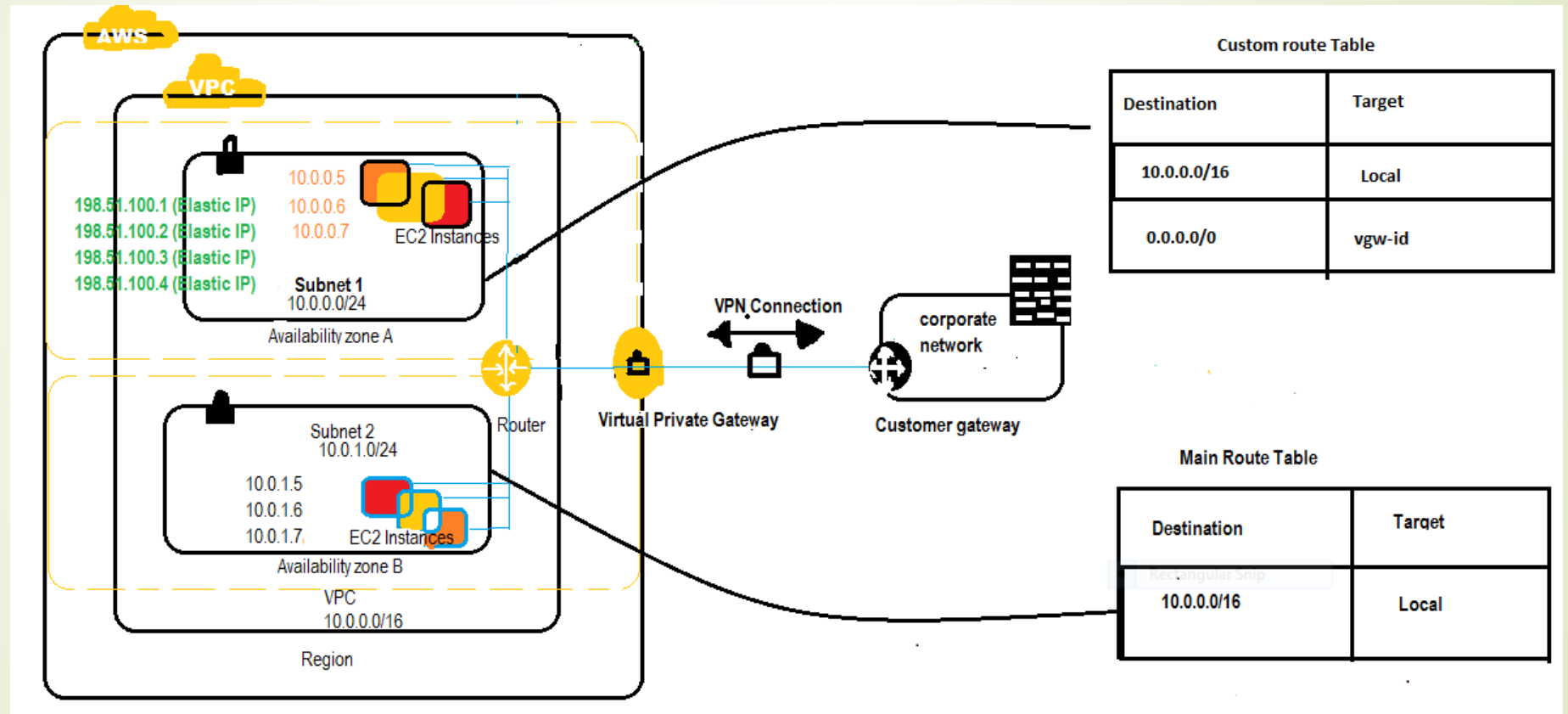
Accessing a Corporate or Home Network:-

You can optionally connect your VPC to your own corporate data center using an IPsec hardware VPN connection, making the AWS cloud an extension of your data center.

A VPN connection consists of a virtual private gateway attached to your VPC and a customer gateway located in your data center. A virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection. A customer gateway is a physical device or software appliance on your side of the VPN connection.

Amazon VPC Concepts

Accessing a Corporate or Home Network:-





Amazon VPC Concepts

VPC and Subnet Basics:-

- A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.
- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. This is the primary CIDR block for your VPC.
- A VPC spans all the Availability Zones in the region. After creating a VPC, you can add one or more subnets in each Availability Zone. When you create a subnet, you specify the CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. AWS assigns a unique ID to each subnet.
- You can also optionally assign an IPv6 CIDR block to your VPC, and assign IPv6 CIDR blocks to your subnets.



Amazon VPC Concepts

VPC and Subnet Sizing:-

Amazon VPC supports IPv4 and IPv6 addressing, and has different CIDR block size limits for each. By default, all VPCs and subnets must have IPv4 CIDR blocks—you can't change this behavior. You can optionally associate an IPv6 CIDR block with your VPC.

VPC and Subnet Sizing for IPv4:-

When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses). After you've created your VPC, you can associate secondary CIDR blocks with the VPC.

Amazon VPC Concepts

VPC and Subnet Sizing:-

When you create a VPC, AWS recommends that you specify a CIDR block (of /16 or smaller) from the private IPv4 address ranges as specified in RFC 1918:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
- The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset (for multiple subnets). The allowed block size is between a /28 netmask and /16 netmask. If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.

For example, if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).



Amazon VPC Concepts

VPC and Subnet Sizing:-

VPC and Subnet Sizing for IPv6:-

- You can associate a single IPv6 CIDR block with an existing VPC in your account, or when you create a new VPC. The CIDR block uses a fixed prefix length of /56. You cannot choose the range of addresses or the IPv6 CIDR block size; AWS assigns the block to your VPC from Amazon's pool of IPv6 addresses.
- If you've associated an IPv6 CIDR block with your VPC, you can associate an IPv6 CIDR block with an existing subnet in your VPC, or when you create a new subnet. A subnet's IPv6 CIDR block uses a fixed prefix length of /64.
- For example, you create a VPC and specify that you want to associate an IPv6 CIDR block with the VPC. Amazon assigns the following IPv6 CIDR block to your VPC: 2001:db8:1234:1a00::/56. You can create a subnet and associate an IPv6 CIDR block from this range; for example, 2001:db8:1234:1a00::/64.
- You can disassociate an IPv6 CIDR block from a subnet, and you can disassociate an IPv6 CIDR block from a VPC. After you've disassociated an IPv6 CIDR block from a VPC, you cannot expect to receive the same CIDR if you associate an IPv6 CIDR block with your VPC again later.



Amazon VPC Concepts

Subnet Security:-

- AWS provides two features that you can use to increase security in your VPC: security groups and network ACLs. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets. In most cases, security groups can meet your needs; however, you can also use network ACLs if you want an additional layer of security for your VPC.
- By design, each subnet must be associated with a network ACL. Every subnet that you create is automatically associated with the VPC's default network ACL. You can change the association, and you can change the contents of the default network ACL.
- You can create a flow log on your VPC or subnet to capture the traffic that flows to and from the network interfaces in your VPC or subnet. You can also create a flow log on an individual network interface. Flow logs are published to CloudWatch Logs.



Amazon VPC Concepts

Working with VPCs and Subnets:-

The following procedures are for manually creating a VPC and subnets. You also have to manually add gateways and routing tables. Alternatively, you can use the Amazon VPC wizard to create a VPC plus its subnets, gateways, and routing tables in one step.

Topics:-

1. Creating a VPC
2. Creating a Internet Gateway and Associate with VPC.
3. Creating a Subnet in VPC.
4. Associating a Secondary IPv4 CIDR Block with Your VPC.
5. Associating an IPv6 CIDR Block with Your VPC.
6. Associating an IPv6 CIDR Block with Your Subnet.
7. Launching an Instance into Your Subnet.
8. Deleting Your Subnet.
9. Disassociating an IPv4 CIDR Block from Your VPC.
10. Disassociating an IPv6 CIDR Block from Your VPC or Subnet.
11. Deleting Your VPC.



Amazon VPC Concepts

IP Addressing in Your VPC:-

- IP addresses enable resources in your VPC to communicate with each other, and with resources over the Internet. Amazon EC2 and Amazon VPC support the IPv4 and IPv6 addressing protocols.
- By default, Amazon EC2 and Amazon VPC use the IPv4 addressing protocol. When you create a VPC, you must assign it an IPv4 CIDR block (a range of private IPv4 addresses). Private IPv4 addresses are not reachable over the Internet. To connect to your instance over the Internet, or to enable communication between your instances and other AWS services that have public endpoints, you can assign a globally-unique public IPv4 address to your instance.
- You can optionally associate an IPv6 CIDR block with your VPC and subnets, and assign IPv6 addresses from that block to the resources in your VPC. IPv6 addresses are public and reachable over the Internet.
- Your VPC can operate in dual-stack mode: your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 addresses are independent of each other; you must configure routing and security in your VPC separately for IPv4 and IPv6.



Amazon VPC Concepts

Private IPv4 Addresses:-

- Private IPv4 addresses (also referred to as private IP addresses) are not reachable over the Internet, and can be used for communication between the instances in your VPC. When you launch an instance into a VPC, a primary private IP address from the IPv4 address range of the subnet is assigned to the default network interface (eth0) of the instance. Each instance is also given a private (internal) DNS hostname that resolves to the private IP address of the instance.
- You can assign additional private IP addresses, known as secondary private IP addresses, to instances that are running in a VPC. Unlike a primary private IP address, you can reassign a secondary private IP address from one network interface to another. A private IP address remains associated with the network interface when the instance is stopped and restarted, and is released when the instance is terminated.



Amazon VPC Concepts

Public IPv4 Addresses:-

- All subnets have an attribute that determines whether a network interface created in the subnet automatically receives a public IPv4 address. Therefore, when you launch an instance into a subnet that has this attribute enabled, a public IP address is assigned to the primary network interface (eth0) that's created for the instance. A public IP address is mapped to the primary private IP address through network address translation (NAT).
- A public IP address is assigned from Amazon's pool of public IP addresses; it's not associated with your account. When a public IP address is disassociated from your instance, it's released back into the pool, and is no longer available for you to use. You cannot manually associate or disassociate a public IP address. Instead, in certain cases, AWS release the public IP address from your instance, or assign it a new one
- If you require a persistent public IP address allocated to your account that can be assigned to and removed from instances as you require, use an Elastic IP address instead.
- If your VPC is enabled to support DNS hostnames, each instance that receives a public IP address or an Elastic IP address is also given a public DNS hostname.



Amazon VPC Concepts

IPv6 Addresses:-

- You can optionally associate an IPv6 CIDR block with your VPC and subnets.
- When your instance receives an IPv6 address during launch, the address is associated with the primary network interface (eth0) of the instance. You can disassociate the IPv6 address from the primary network interface. AWS do not support IPv6 DNS hostnames for your instance.
- An IPv6 address persists when you stop and start your instance, and is released when you terminate your instance. You cannot reassign an IPv6 address while it's assigned to another network interface—you must first unassign it.
- You can assign additional IPv6 addresses to your instance by assigning them to a network interface attached to your instance. The number of IPv6 addresses you can assign to a network interface, and the number of network interfaces you can attach to an instance varies per instance type.
- IPv6 addresses are globally unique, and therefore reachable over the Internet. You can control whether instances are reachable via their IPv6 addresses by controlling the routing for your subnet, or by using security group and network ACL rules.



Amazon VPC Concepts

Security:-

Amazon VPC provides features that you can use to increase and monitor the security for your VPC:

- Security groups :- Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.
- Network access control lists (ACLs) :- Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
- Flow logs :- Capture information about the IP traffic going to and from network interfaces in your VPC.



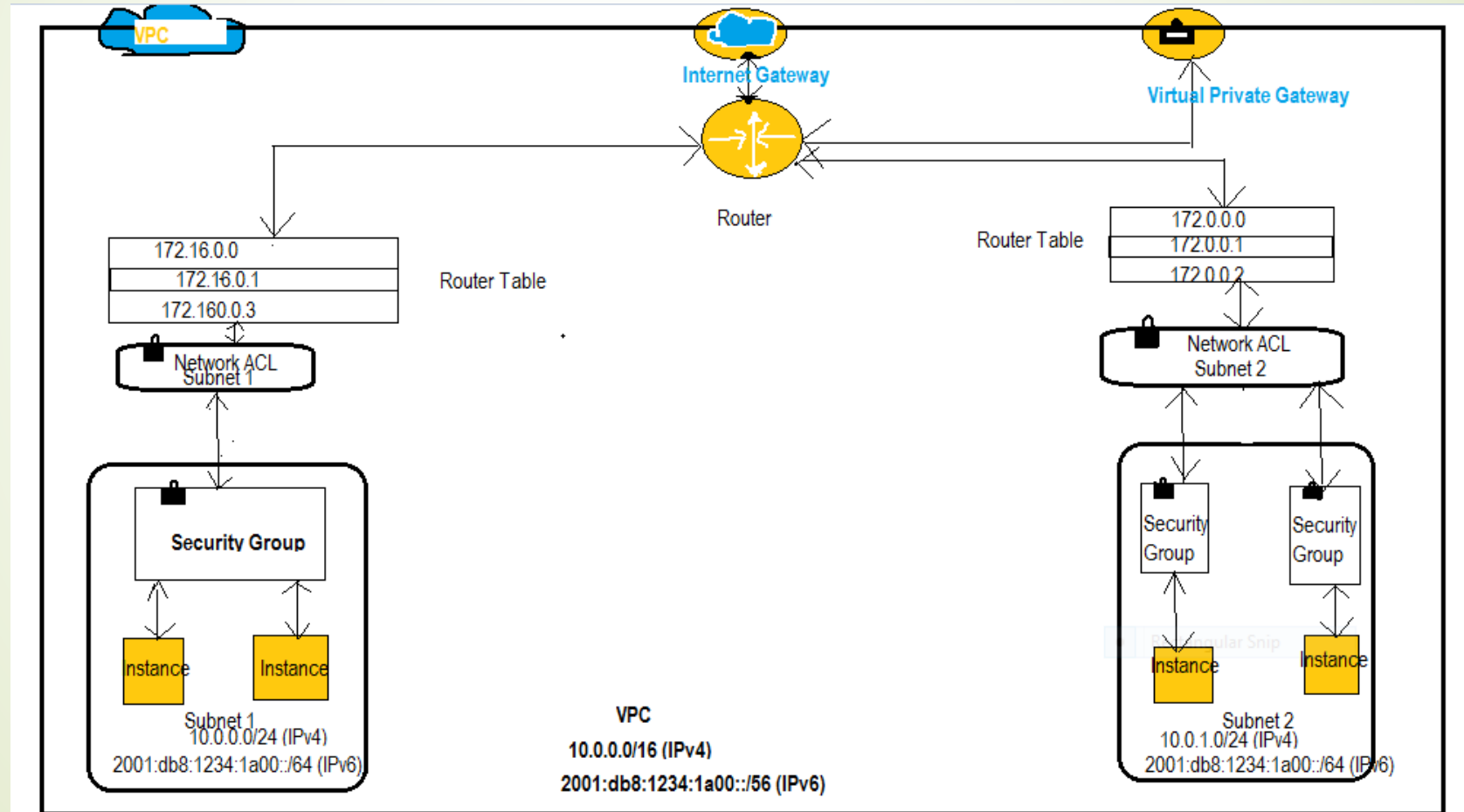
Amazon VPC Concepts

Security:-

- When you launch an instance in a VPC, you can associate one or more security groups that you've created. Each instance in your VPC could belong to a different set of security groups. If you don't specify a security group when you launch an instance, the instance automatically belongs to the default security group for the VPC.
- You can secure your VPC instances using only security groups; however, you can add network ACLs as a second layer of defense.
- You can monitor the accepted and rejected IP traffic going to and from your instances by creating a flow log for a VPC, subnet, or individual network interface. Flow log data is published to CloudWatch Logs, and can help you diagnose overly restrictive or overly permissive security group and network ACL rules.

Amazon VPC Concepts

Security:-





Amazon VPC Concepts

Security Groups for Your VPC:-

- A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.
- For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.
- You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.



Amazon VPC Concepts

Security Group Basics:-

1. You have limits on the number of security groups that you can create per VPC, the number of rules that you can add to each security group, and the number of security groups you can associate with a network interface.
2. You can specify allow rules, but not deny rules.
3. You can specify separate rules for inbound and outbound traffic.
4. When you create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group.
5. By default, a security group includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed.
6. Security groups are stateful :- if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.



Amazon VPC Concepts

Working with Security Groups:-

This section shows you how to work with security groups using the Amazon VPC console.

Topics:-

- Creating a Security Group.
- Adding, Removing, and Updating Rules.
- Changing an Instance's Security Groups.
- Deleting a Security Group.



Amazon VPC Concepts

Network ACLs:-

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. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Network ACL Basics:-

The following are the basic things that you need to know about network ACLs:

- Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL.



Amazon VPC Concepts

Network ACL Basics:-

- You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.
- A network ACL contains a numbered list of rules that AWS evaluate in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. AWS recommends that you start by creating rules with rule numbers that are multiples of 100, so that you can insert new rules where you need to later on.
- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

Amazon VPC Concepts

Network ACL Rules:-

You can add or remove rules from the default network ACL, or create additional network ACLs for your VPC. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets it's associated with.

The following are the parts of a network ACL rule:

- Rule number. Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that may contradict it.
- Protocol. You can specify any protocol that has a standard protocol number. If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.
- [Inbound rules only] The source of the traffic (CIDR range) and the destination (listening) port or port range.
- [Outbound rules only] The destination for the traffic (CIDR range) and the destination port or port range.
- Choice of ALLOW or DENY for the specified traffic.

Amazon VPC Concepts

Default Network ACL:-

The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated. Each network ACL also includes a rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule.

The following is an example default network ACL for a VPC that supports IPv4 only.

Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY
Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
100	All IPv4 traffic	all	all	0.0.0.0/0	ALLOW
*	All IPv4 traffic	all	all	0.0.0.0/0	DENY



Amazon VPC Concepts

Default Network ACL:-

If you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC, AWS automatically add rules that allow all IPv6 traffic to flow in and out of your subnet. AWS also add rules whose rule numbers are an asterisk that ensures that a packet is denied if it doesn't match any of the other numbered rules. You can't modify or remove these rules.

Amazon VPC Concepts

Default Network ACL:-

Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
101	All IPv6 traffic	All	All	::/0	ALLOW
*	All traffic	All	All	0.0.0.0/0	DENY
*	All IPv6 traffic	All	All	::/0	DENY
Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
100	All traffic	all	all	0.0.0.0/0	ALLOW
101	All IPv6 traffic	all	all	::/0	ALLOW
*	All traffic	all	all	0.0.0.0/0	DENY
*	All IPv6 traffic	all	all	::/0	DENY



Amazon VPC Concepts

Working with Network ACLs:-

This section shows you how to work with network ACLs using the Amazon VPC console.

Topics:-

1. Determining Network ACL Associations.
2. Creating a Network ACL.
3. Adding and Deleting Rules.
4. Associating a Subnet with a Network ACL.
5. Disassociating a Network ACL from a Subnet.
6. Changing a Subnet's Network ACL.
7. Deleting a Network ACL.



Amazon VPC Concepts

VPC Flow Logs:-

- VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.
- Flow logs can help you with a number of tasks; for example, to troubleshoot why specific traffic is not reaching an instance, which in turn can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.
- There is no additional charge for using flow logs; however, standard CloudWatch Logs charges apply.

Amazon VPC Concepts

Flow Logs Basics:-

- You can create a flow log for a VPC, a subnet, or a network interface. If you create a flow log for a subnet or VPC, each network interface in the VPC or subnet is monitored. Flow log data is published to a log group in CloudWatch Logs, and each network interface has a unique log stream. Log streams contain flow log records, which are log events consisting of fields that describe the traffic for that network interface.
- To create a flow log, you specify the resource for which you want to create the flow log, the type of traffic to capture (accepted traffic, rejected traffic, or all traffic), the name of a log group in CloudWatch Logs to which the flow log will be published, and the ARN of an IAM role that has sufficient permission to publish the flow log to the CloudWatch Logs log group. If you specify the name of a log group that does not exist, AWS attempt to create the log group for you. After you've created a flow log, it can take several minutes to begin collecting data and publishing to CloudWatch Logs. Flow logs do not capture real-time log streams for your network interfaces.
- You can create multiple flow logs that publish data to the same log group in CloudWatch Logs. If the same network interface is present in one or more flow logs in the same log group, it has one combined log stream. If you've specified that one flow log should capture rejected traffic, and the other flow log should capture accepted traffic, then the combined log stream captures all traffic.



Amazon VPC Concepts

Flow Logs Basics:-

- If you launch more instances into your subnet after you've created a flow log for your subnet or VPC, then a new log stream is created for each new network interface as soon as any network traffic is recorded for that network interface.
- You can create flow logs for network interfaces that are created by other AWS services; for example, Elastic Load Balancing, Amazon RDS, Amazon ElastiCache, Amazon Redshift, and Amazon WorkSpaces. However, you cannot use these services' consoles or APIs to create the flow logs; you must use the Amazon EC2 console or the Amazon EC2 API. Similarly, you cannot use the CloudWatch Logs console or API to create log streams for your network interfaces.
- If you no longer require a flow log, you can delete it. Deleting a flow log disables the flow log service for the resource, and no new flow log records or log streams are created. It does not delete any existing flow log records or log streams for a network interface. To delete an existing log stream, you can use the CloudWatch Logs console. After you've deleted a flow log, it can take several minutes to stop collecting data.

Amazon VPC Concepts

Flow Log Limitations:-

- You cannot enable flow logs for network interfaces that are in the EC2-Classic platform. This includes EC2-Classic instances that have been linked to a VPC through ClassicLink.
- You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account.
- You cannot tag a flow log.
- After you've created a flow log, you cannot change its configuration; for example, you can't associate a different IAM role with the flow log. Instead, you can delete the flow log and create a new one with the required configuration.
- None of the flow log API actions (ec2:*FlowLogs) support resource-level permissions. If you want to create an IAM policy to control the use of the flow log API actions, you must grant users permission to use all resources for the action by using the * wildcard for the resource element in your statement.
- If your network interface has multiple IPv4 addresses and traffic is sent to a secondary private IPv4 address, the flow log displays the primary private IPv4 address in the destination IP address field.



Amazon VPC Concepts

Flow Log Limitations:-

Flow logs do not capture all types of IP traffic. The following types of traffic are not logged:

- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
- Traffic generated by a Windows instance for Amazon Windows license activation.
- Traffic to and from 169.254.169.254 for instance metadata.
- DHCP traffic.
- Traffic to the reserved IP address for the default VPC router.



Amazon VPC Concepts

Working With Flow Logs:-

You can work with flow logs using the Amazon EC2, Amazon VPC, and CloudWatch consoles.

Topics:-

- Creating a Flow Log
- Viewing Flow Logs
- Deleting a Flow Log



Amazon VPC Networking Concepts

Elastic Network Interfaces:-

An elastic network interface (referred to as a network interface in this documentation) is a virtual network interface that can include the following attributes:

- a primary private IPv4 address
- one or more secondary private IPv4 addresses
- one Elastic IP address per private IPv4 address
- one public IPv4 address, which can be auto-assigned to the network interface for eth0 when you launch an instance
- one or more IPv6 addresses
- one or more security groups
- a MAC address
- a source/destination check flag
- a description



Amazon VPC Networking Concepts

Elastic Network Interfaces:-

- You can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. A network interface's attributes follow it as it is attached or detached from an instance and reattached to another instance. When you move a network interface from one instance to another, network traffic is redirected to the new instance.
- Each instance in your VPC has a default network interface (the primary network interface) that is assigned a private IPv4 address from the IPv4 address range of your VPC. You cannot detach a primary network interface from an instance. You can create and attach an additional network interface to any instance in your VPC. The number of network interfaces you can attach varies by instance type.



Amazon VPC Networking Concepts

Route Table:-

A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.

Route Table Basics:-

- Your VPC has an implicit router.
- Your VPC automatically comes with a main route table that you can modify.
- You can create additional custom route tables for your VPC.
- Each subnet must be associated with a route table, which controls the routing for the subnet. If you don't explicitly associate a subnet with a particular route table, the subnet is implicitly associated with the main route table.
- You cannot delete the main route table, but you can replace the main route table with a custom table that you've created.
- Each route in a table specifies a destination CIDR and a target.

Amazon VPC Networking Concepts

Route Table Basics:-

- CIDR blocks for IPv4 and IPv6 are treated separately. For example, a route with a destination CIDR of 0.0.0.0/0 (all IPv4 addresses) does not automatically include all IPv6 addresses. You must create a route with a destination CIDR of ::/0 for all IPv6 addresses.
- Every route table contains a local route for communication within the VPC over IPv4. If your VPC has more than one IPv4 CIDR block, your route tables contain a local route for each IPv4 CIDR block. If you've associated an IPv6 CIDR block with your VPC, your route tables contain a local route for the IPv6 CIDR block. You cannot modify or delete these routes.
- When you add an Internet gateway, an egress-only Internet gateway, a virtual private gateway, a NAT device, a peering connection, or a VPC endpoint in your VPC, you must update the route table for any subnet that uses these gateways or connections.
- There is a limit on the number of route tables you can create per VPC, and the number of routes you can add per route table.



Amazon VPC Networking Concepts

Main Route Tables:-

- When you create a VPC, it automatically has a main route table. On the Route Tables page in the Amazon VPC console, you can view the main route table for a VPC by looking for Yes in the Main column. The main route table controls the routing for all subnets that are not explicitly associated with any other route table. You can add, remove, and modify routes in the main route table.
- You can explicitly associate a subnet with the main route table, even if it's already implicitly associated. You might do that if you change which table is the main route table, which changes the default for additional new subnets, or any subnets that are not explicitly associated with any other route table.



Amazon VPC Networking Concepts

Custom Route Tables:-

- Your VPC can have route tables other than the default table. One way to protect your VPC is to leave the main route table in its original default state (with only the local route), and explicitly associate each new subnet you create with one of the custom route tables you've created. This ensures that you explicitly control how each subnet routes outbound traffic.
- The main route table came with the VPC, and it also has a route for the VPN-only subnet. A custom route table is associated with the public subnet. The custom route table has a route over the Internet gateway.



Amazon VPC Networking Concepts

Route Table Association:-

- The VPC console shows the number of subnets explicitly associated with each route table, and provides information about subnets that are implicitly associated with the main route table.
- Subnets can be implicitly or explicitly associated with the main route table. Subnets typically won't have an explicit association to the main route table, although it might happen temporarily if you're replacing the main route table.
- You might want to make changes to the main route table, but to avoid any disruption to your traffic, you can first test the route changes using a custom route table. After you're satisfied with the testing, you then replace the main route table with the new custom table.

Amazon VPC Networking Concepts

Route Table Association:-

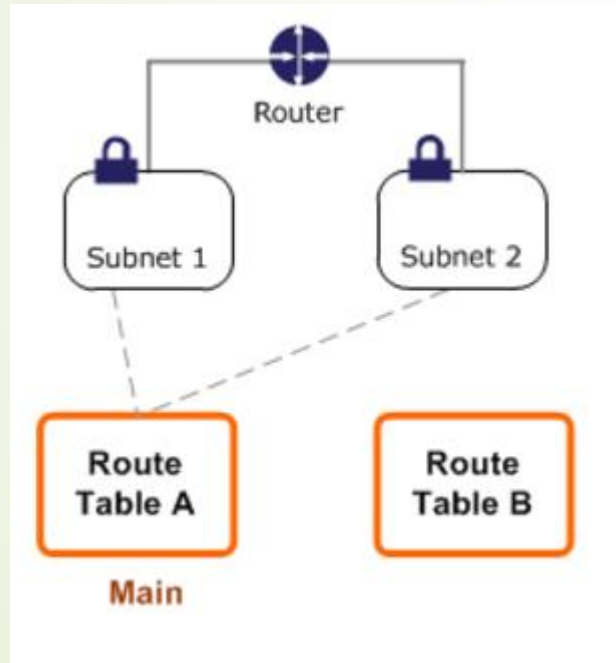


Fig. 1

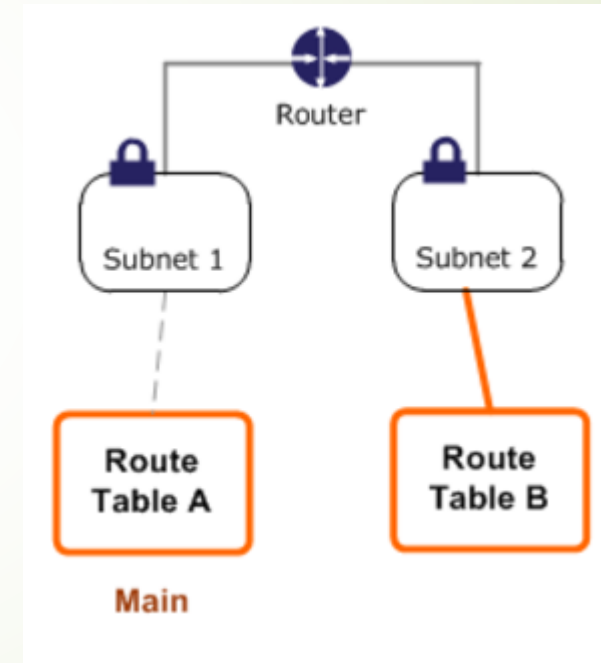


Fig. 2

Amazon VPC Networking Concepts

Route Table Association:-

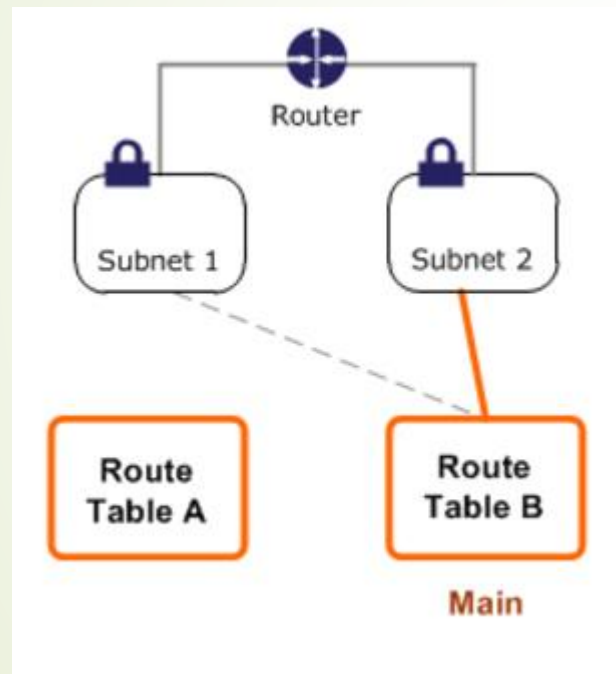


Fig. 3

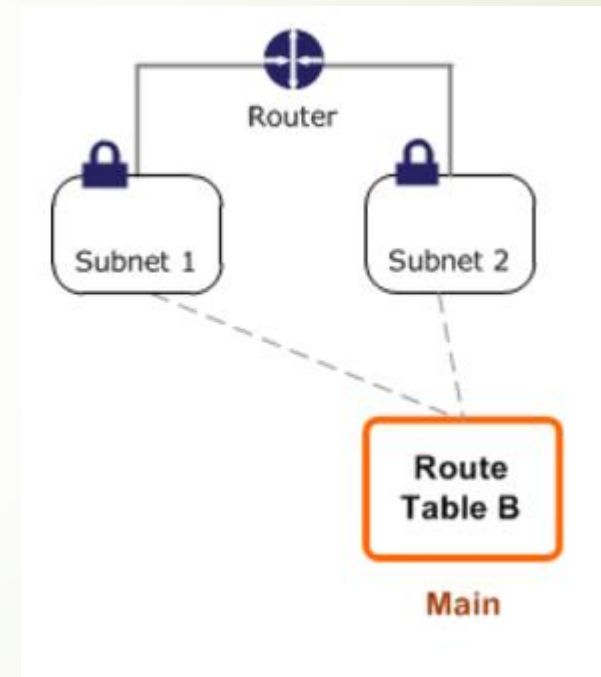


Fig. 4



Amazon VPC Networking Concepts

Internet Gateways:-

- An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- An Internet gateway serves two purposes: to provide a target in your VPC route tables for Internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.
- An Internet gateway supports IPv4 and IPv6 traffic.



Amazon VPC Networking Concepts

Enabling Internet Access:-

To enable access to or from the Internet for instances in a VPC subnet, you must do the following:

- Attach an Internet gateway to your VPC.
- Ensure that your subnet's route table points to the Internet gateway.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.



Amazon VPC Networking Concepts

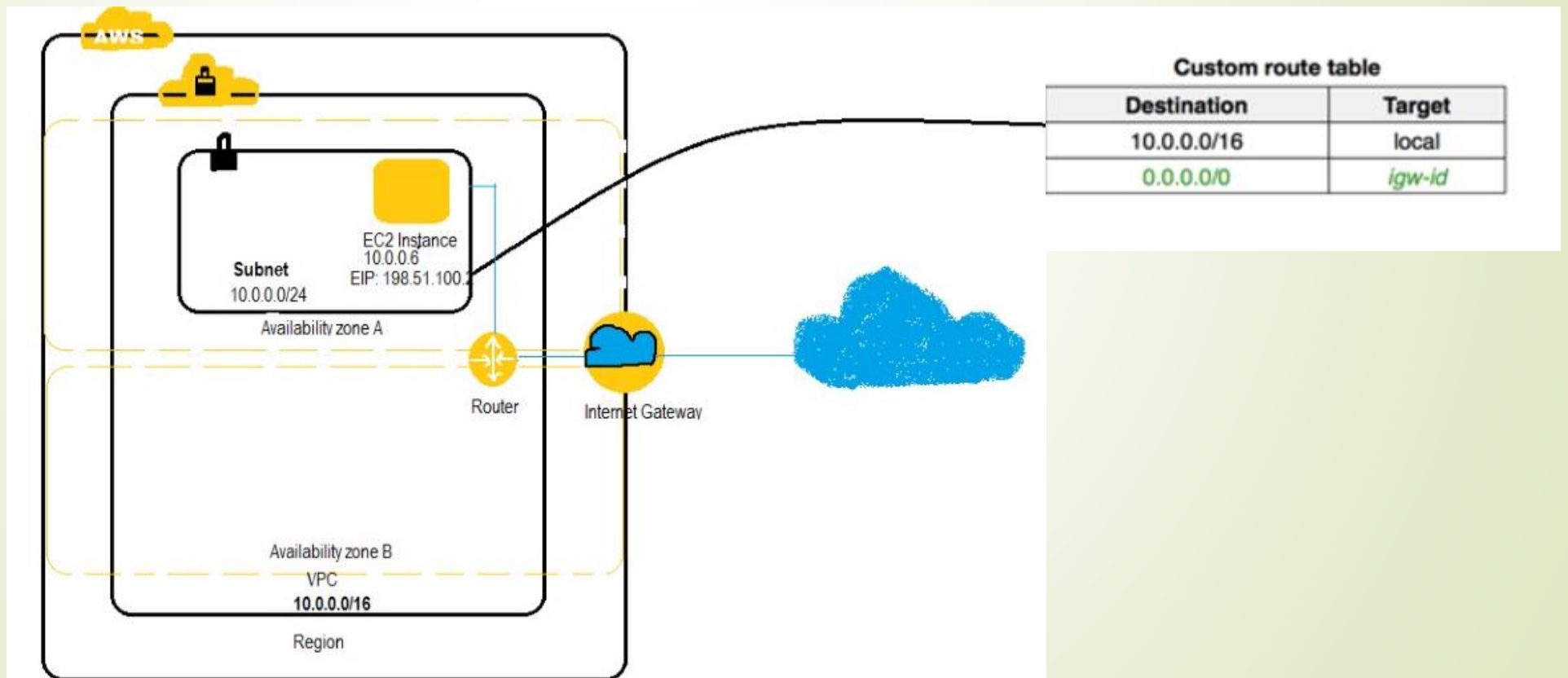
Enabling Internet Access:-

- To use an Internet gateway, your subnet's route table must contain a route that directs Internet-bound traffic to the Internet gateway.
- To enable communication over the Internet for IPv4, your instance must have a public IPv4 address or an Elastic IP address that's associated with a private IPv4 address on your instance. Your instance is only aware of the private (internal) IP address space defined within the VPC and subnet. The Internet gateway logically provides the one-to-one NAT on behalf of your instance, so that when traffic leaves your VPC subnet and goes to the Internet, the reply address field is set to the public IPv4 address or Elastic IP address of your instance, and not its private IP address.
- To enable communication over the Internet for IPv6, your VPC and subnet must have an associated IPv6 CIDR block, and your instance must be assigned an IPv6 address from the range of the subnet. IPv6 addresses are globally unique, and therefore public by default.

Amazon VPC Networking Concepts

Architecture of Internet Gateway and VPC:-

In the following diagram, Subnet in the VPC is associated with a custom route table that points all Internet-bound IPv4 traffic to an Internet gateway. The instance has an Elastic IP address, which enables communication with the Internet.





Amazon VPC Networking Concepts

Creating a VPC with an Internet Gateway:-

How to manually create a public subnet to support Internet access.

Topics:-

- Creating a Subnet.
- Attaching an Internet Gateway.
- Creating a Custom Route Table.
- Updating the Security Group Rules.
- Adding Elastic IP Addresses.
- Detaching an Internet Gateway from Your VPC.
- Deleting an Internet Gateway.

Amazon VPC Networking Concepts

NAT(Network Address Translation):-

- You can use a NAT device to enable instances in a private subnet to connect to the Internet (for example, for software updates) or other AWS services, but prevent the Internet from initiating connections with the instances. A NAT device forwards traffic from the instances in the private subnet to the Internet or other AWS services, and then sends the response back to the instances. When traffic goes to the Internet, the source IPv4 address is replaced with the NAT device's address and similarly, when the response traffic goes to those instances, the NAT device translates the address back to those instances' private IPv4 addresses.
- AWS offers two kinds of NAT devices—a NAT gateway or a NAT instance. AWS recommend NAT gateways, as they provide better availability and bandwidth over NAT instances. The NAT Gateway service is also a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI. You can choose to use a NAT instance for special purposes.



Amazon VPC Networking Concepts

NAT Gateways:-

- You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
- You are charged for creating and using a NAT gateway in your account. NAT gateway hourly usage and data processing rates apply. Amazon EC2 charges for data transfer also apply.
- NAT gateways are not supported for IPv6 traffic—use an egress-only internet gateway instead.



Amazon VPC Networking Concepts

NAT Gateway Basics:-

- To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside.
- You must also specify an Elastic IP address to associate with the NAT gateway when you create it. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet.
- Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone. You have a limit on the number of NAT gateways you can create in an Availability Zone.
- If you no longer need a NAT gateway, you can delete it. Deleting a NAT gateway disassociates its Elastic IP address, but does not release the address from your account.



Amazon VPC Networking Concepts

NAT Gateway Characteristics:-

- A NAT gateway supports bursts of up to 10 Gbps of bandwidth. If you require more than 10 Gbps bursts, you can distribute the workload by splitting your resources into multiple subnets, and creating a NAT gateway in each subnet.
- You can associate exactly one Elastic IP address with a NAT gateway. You cannot disassociate an Elastic IP address from a NAT gateway after it's created. To use a different Elastic IP address for your NAT gateway, you must create a new NAT gateway with the required address, update your route tables, and then delete the existing NAT gateway if it's no longer required.
- A NAT gateway supports the protocols like TCP, UDP, and ICMP.



Amazon VPC Networking Concepts

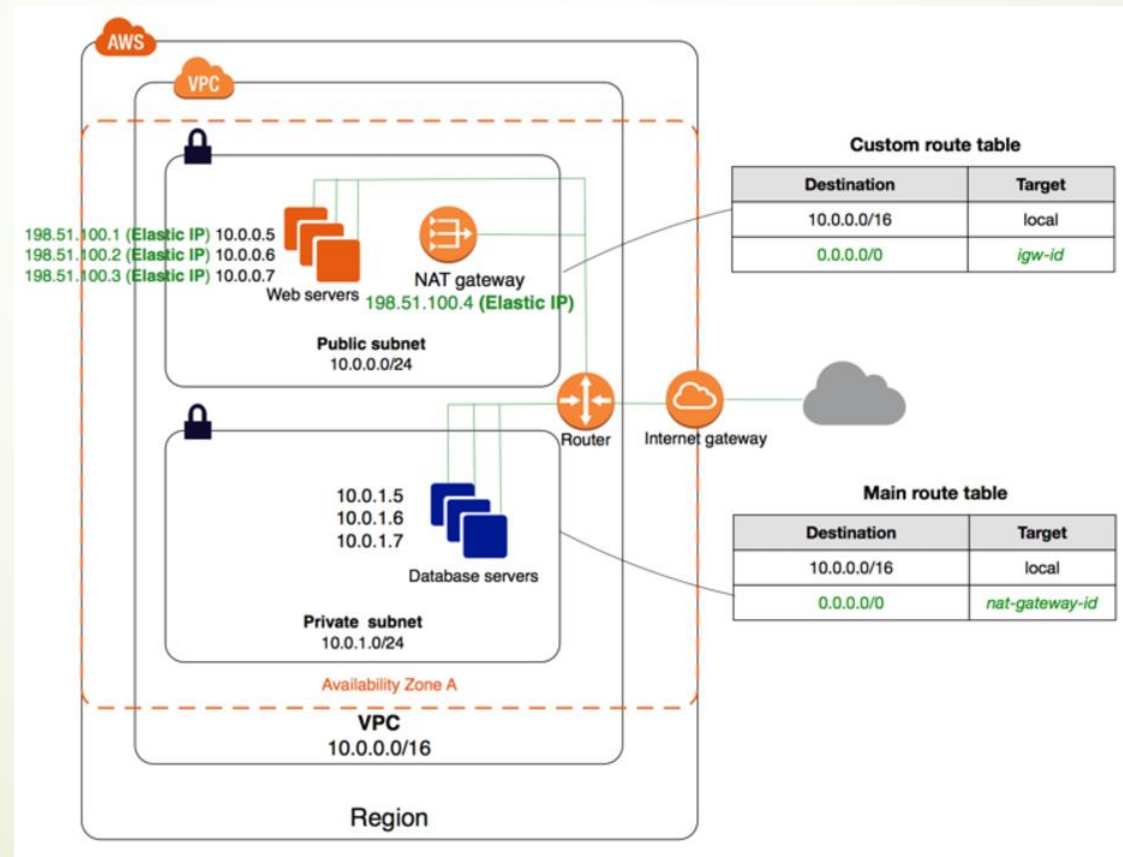
NAT Gateway Characteristics:-

- You cannot associate a security group with a NAT gateway. You can use security groups for your instances in the private subnets to control the traffic to and from those instances.
- You can use a network ACL to control the traffic to and from the subnet in which the NAT gateway is located. The network ACL applies to the NAT gateway's traffic. A NAT gateway uses ports 1024–65535.
- When a NAT gateway is created, it receives a network interface that's automatically assigned a private IP address from the IP address range of your subnet. You can view the NAT gateway's network interface in the Amazon EC2 console.
- A NAT gateway cannot be accessed by a ClassicLink connection associated with your VPC.

Amazon VPC Networking Concepts

Architecture of a VPC with a NAT gateway:-

The main route table sends internet traffic from the instances in the private subnet to the NAT gateway. The NAT gateway sends the traffic to the internet gateway using the NAT gateway's Elastic IP address as the source IP address.





Amazon VPC Networking Concepts

Working with NAT Gateways:-

You can use the Amazon VPC console to create, view, and delete a NAT gateway. You can also use the Amazon VPC wizard to create a VPC with a public subnet, a private subnet, and a NAT gateway.

Topics:-

- Creating a NAT Gateway
- Updating Your Route Table
- Deleting a NAT Gateway
- Testing a NAT Gateway



Amazon VPC Limits

The following tables list the limits for Amazon VPC resources per region for your AWS account. Unless indicated otherwise, you can request an increase for these limits by using the Amazon VPC Limits form. If you want to increase a limit that applies per resource, AWS increase the limit for all resources in the region; for example, the limit for security groups per VPC applies to all VPCs in the region.

Topics:-

- VPC and Subnets.
- Elastic IP Addresses (IPv4).
- Flow Logs.
- Gateways.
- Network ACLs.
- Network Interfaces.
- Route Tables.
- Security Groups.



Amazon VPC Limits

1. VPCs per region

The Default limit of VPC per Region is 5. To increase this limit, submit a request.

The limit for internet gateways per region is directly correlated to this one. Increasing this limit increases the limit on internet gateways per region by the same amount.

2. Subnets per VPC

The Default limit of Subnets per VPC is 200. To increase this limit, submit a request.

3. IPv4 CIDR blocks per VPC

This limit is made up of your primary CIDR block plus 4 secondary CIDR blocks. To increase this limit, submit a request.

4. Elastic IP addresses per region

The Default limit of Elastic IP addresses per region is 5. This is the limit for the number of VPC Elastic IP addresses you can allocate within a region. This is a separate limit from the Amazon EC2 Elastic IP address limit. To increase this limit, submit a request.



Amazon VPC Limits

5. Flow logs per single network interface, single subnet, or single VPC in a region

You can effectively have 6 flow logs per network interface if you create 2 flow logs for the subnet, and 2 flow logs for the VPC in which your network interface resides. This limit cannot be increased.

6. Customer gateways per region

The Default limit of Customer gateways per region is 50. To increase this limit, contact AWS Support.

7. Network ACLs per VPC

The Default limit Network ACLs per VPC is 200. You can associate one network ACL to one or more subnets in a VPC. This limit is not the same as the number of rules per network ACL.



Amazon VPC Limits

8. Network interfaces per instance

This limit varies by instance type. For more information, see [IP Addresses Per ENI Per Instance Type](#).

9. Route tables per VPC

The Default limit of Route tables per VPC is 200. Including the main route table. You can associate one route table to one or more subnets in a VPC. To increase this limit, submit a request.

10. Security groups per VPC (per region)

The Default limit of Security groups per VPC (per region) is 500. To increase this limit, submit a request.

How to Convert .pem Key Pair to .ppk key pair



AWS Virtual Private Cloud Pricings





Amazon VPC(Virtual Private Cloud)Demonstration

Demonstration of Creating AWS VPC and its components using AWS Management Console.



Amazon EC2 Demonstration

Demonstration of AWS EC2 by following ways:-

1. AWS Management Console.
2. AWS CLI (Command Line Interface).
3. AWS SDK (Software development Kits).

