KR Network Cloud Technologies PVT. LTD.

VPC (Virtual Private Cloud)

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Amazon VPC is the networking layer for Amazon EC2. 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 specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.

Example:

- Some Servers are publicly accessible.
- Some Servers are on private subnet. (Not reachable over internet)
- Some Servers are reachable only from on premises/Corporate data center. (Using VPN)

VPC Terminology:

1. IP Addresses

There are five classes of IP addresses in networking.

Class IP Address range

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

Class	Private IP Address Range	Public IP Address Range
Class A	10.0.0.0 – 10.255.255.255	1.0.0.0 – 9.255.255.255 11.0.0.0 – 126.255.255.255
Class B	172.16.0.0 – 172.31.255.255	128.0.0.0 – 172.15.255.255 172.32.0.0 – 191.255.255.255
Class C	192.168.0.0 – 192.168.255.255	192.0.0.0 – 192.167.255.255 192.169.0.0 – 223.255.255.255

Types of IP Addresses in AWS

Private IP Addresses:

- Private IPv4 addresses (also referred to as private IP addresses in this topic) 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.
- 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.

Public IP Addresses:

- A public IP address is an IPv4 address that's reachable from the Internet. You can use public addresses for communication between your instances and the Internet.
- A public IP address is mapped to the primary private IP address through network address translation (NAT).
- When you launch an instance in EC2-Classic, we automatically assign a public IP address to the instance from the EC2-Classic public IPv4 address pool. And it’s not in our control, generally managed by Amazon network team.

Elastic IP Addresses:

- An Elastic IP address is a static IPv4 address designed for dynamic cloud computing.
- An Elastic IP address is associated with your AWS account.
- With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
- An Elastic IP address is a public IPv4 address, which is reachable from the Internet.

2. Subnets

- 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.
- Assign static private IP addresses to your instances that persist across starts and stops
- Assign multiple IP addresses to your instances
- 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).

3. Route Tables

- A route table contains a set of rules, called routes that are used to determine where network traffic is directed.
- Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet
- A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

4. Internet Gateway

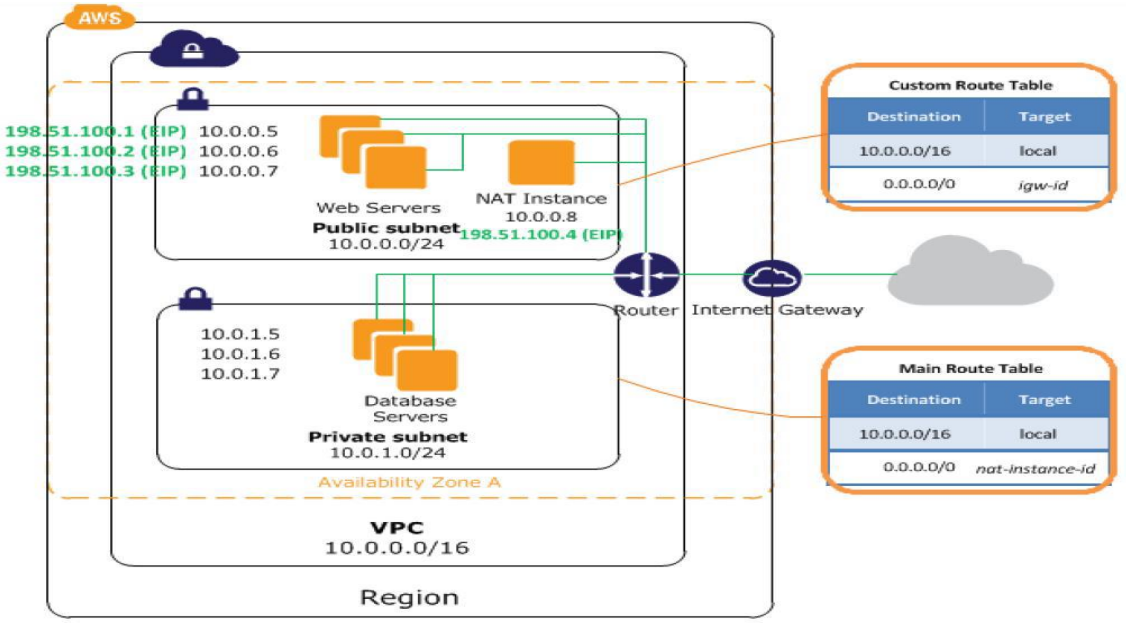
- An Internet gateway is a highly available VPC component that allows communication between instances in your VPC and the Internet.
- It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- An Internet gateway serves two purposes: to provide a target in your VPC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

5. 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 IP 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 IP addresses.

6. NAT Instance

- AWS provides two options: NAT instances and NAT Gateways to solve this problem as they allow instances to gain Internet access when deployed in private subnets.
- A NAT Instance is an Amazon Linux Amazon Machine Image (AMI) that is designed specifically to accept instances in a private subnet, translate source IP address to public IP address of the NAT instance, and then forward the traffic to the Internet Gateway.
- Here's what you must do to allow instances internet access through the IGW via NAT Instances.



7. Security Group

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 can be assigned to a different set of security groups.

If you launch an instance using the Amazon EC2 API or a command line tool and you don't specify a security group, the instance is automatically assigned to the default security group for the VPC. If you launch an instance using the Amazon EC2 console, you have an option to create a new security group for the instance.

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. This section describes the basic things that you need to know about security groups for your VPC and their rules.

Security group basics

The following are the basic characteristics of security groups for your VPC:

- You can specify allow rules, but not deny rules.
- You can specify separate rules for inbound and outbound traffic.
- Security group rules enable you to filter traffic based on protocols and port numbers.
- 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.

8. NACL (Network Access Control List)

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.

A network ACL contains a numbered list of rules. We evaluate the rules 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. We recommend that you start by creating rules in increments (for example, increments of 10 or 100) so that you can insert new rules where you need to later on.

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 that 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 might contradict it.

Type: The type of traffic; for example, SSH. You can also specify all traffic or a custom range.

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.

Port range: The listening port or port range for the traffic. For example, 80 for HTTP traffic.

Source: [Inbound rules only] The source of the traffic (CIDR range).

Destination: [Outbound rules only] The destination for the traffic (CIDR range).

Allow/Deny: Whether to allow or deny the specified traffic.

Ephemeral ports

The example network ACL in the preceding section uses an ephemeral port range of 32768-65535. However, you might want to use a different range for your network ACLs depending on the type of client that you're using or with which you're communicating.
The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system.

- Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000.
- Requests originating from Elastic Load Balancing use ports 1024-65535.
- Windows operating systems through Windows Server 2003 use ports 1025-5000.
- Windows Server 2008 and later versions use ports 49152-65535.
- A NAT gateway uses ports 1024-65535.
- AWS Lambda functions use ports 1024-65535.

The Well Known Ports are those from 0 through 1023.
The Registered Ports are those from 1024 through 49151
The Dynamic and/or Private Ports are those from 49152 through 65535

9. ENIC (Elastic Network Interface Card)

An elastic network interface (referred to as a network interface in this documentation) is a logical networking component in a VPC that represents a virtual network card. It can include the following attributes:

- Primary private IPv4 address
- 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
- MAC address
- Source/destination check flag
- Description

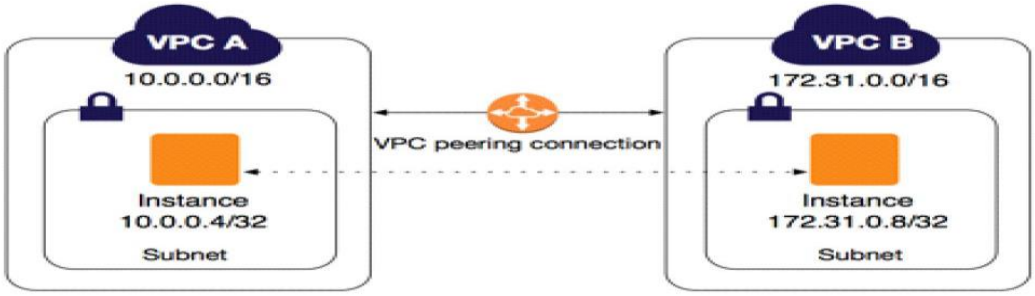
10. VPC Peering

Without Peer: Traffic goes over public internet
Benefit: Security & Cost.
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

VPC Peering Scenarios:

- Your company has a VPC for the finance department, and another VPC for the accounting department. The finance department requires access to all resources that are in the accounting department, and the accounting department requires access to all resources in the finance department.

- Your company has multiple IT departments, each with their own VPC. Some VPCs are located within the same AWS account and others in a different AWS account. You want to peer together all VPCs to enable the IT departments to have full access to each other's' resources.



11. Transit Gateway

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks.
Transit gateway concepts
The following are the key concepts for transit gateways:

Attachments — You can attach the following:

- One or more VPCs
- A Connect SD-WAN/third-party network appliance
- An AWS Direct Connect gateway
- A peering connection with another transit gateway
- A VPN connection to a transit gateway

Transit gateway Maximum Transmission Unit (MTU) — The maximum transmission unit (MTU) of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data that can be passed in a single packet. A transit gateway supports an MTU of 8500 bytes for traffic between

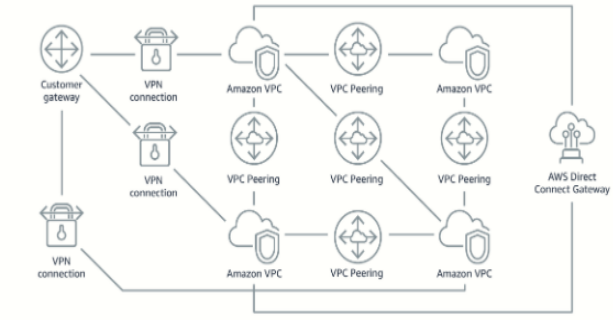
VPCs, AWS Direct Connect, Transit Gateway Connect, and peering attachments. Traffic over VPN connections can have an MTU of 1500 bytes.

Transit gateway route table — A transit gateway has a default route table and can optionally have additional route tables. A route table includes dynamic and static routes that decide the next hop based on the destination IP address of the packet. The target of these routes could be any transit gateway attachment. By default, transit gateway attachments are associated with the default transit gateway route table.

Associations — Each attachment is associated with exactly one route table. Each route table can be associated with zero to many attachments.

Route propagation — A VPC, VPN connection, or Direct Connect gateway can dynamically propagate routes to a transit gateway route table. With a Connect attachment, the routes are propagated to a transit gateway route table by default. With a VPC, you must create static routes to send traffic to the transit gateway . With a VPN connection or a Direct Connect gateway, routes are propagated from the transit gateway to your on-premises router using Border Gateway Protocol (BGP). With a peering attachment, you must create a static route in the transit gateway route table to point to the peering attachment.

Without AWS Transit Gateway



With AWS Transit Gateway