Virtual Private Cloud - VPC

Ponnam Phani Krishna
PONNAM.PHANI@GMAIL.COM

Virtual Private Cloud – VPC

Amazon Virtual Private Cloud (Amazon VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Amazon VPC makes it easy to customize your VPC's network configuration. You can create a public-facing subnet for your web servers that have access to the internet. It also lets you place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. Amazon VPC lets you to use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

By default, AWS will create a VPC for you in your particular region the first time you sign up for the service. This is called as the default VPC.

The default VPC is always created with a CIDR block of /16, which means it supports 65,536 IP addresses in it.

A default subnet is created in each AZ of your selected region. Instances launched in these default subnets have both a public and a private IP address by default as well.

An Internet Gateway is provided to the default VPC for instances to have Internet connectivity. A few necessary route tables, security groups, and ACLs are also created by default that enable the instance traffic to pass through to the Internet.

VPC Components:

- **Internet Gateways**
- **Subnet**
  - **Public Subnet**
  - **Private Subnet**
- **Route Tables & Routes**
- **Network Address Translation**
  - **NAT Instance**
  - **NAT Gateways**
- **Bastion Station / JumpServer**
- **Security Groups**
- **Network Access Control Lists (NACL)**
- **VPC Peering**

VPCs also have a few limits set on them by default. For example, you can have a maximum of ***five VPCs per region.*** Each VPC can have a max of ***one Internet gateway*** as well as one virtual private gateway. Also, each VPC has a limit of hosting a maximum of up to ***200 subnets per VPC***. You can increase these limit by simply requesting AWS to do so.

Source: *https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html*

Internet Gateway (IGW): An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

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. It does not cause availability risks or bandwidth constraints on your network traffic. There's no additional charge for having an internet gateway in your account.

Amazon EC2 instances within an Amazon VPC are only aware of their private IP addresses. When traffic is sent from the instance to the Internet, the IGW translates the reply address to the instance’s public IP address (or EIP address, covered later) and maintains the one-to-one map of the instance private IP address and public IP address.

When an instance receives traffic from the Internet, the IGW translates the destination address (public IP address) to the instance’s private IP address and forwards the traffic to the Amazon VPC.

Subnet: A subnet is a range of IP addresses in your VPC. You can launch AWS resources, such as EC2 instances, into a specific subnet. When you create a subnet, you specify the IPv4 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. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single zone.

A **public subnet** is one in which the associated route table directs the subnet’s traffic to the Amazon VPC’s IGW. All the instance in public subnet will get both Public and Private IP Addresses.

A **private subnet** is one in which the associated route table does not direct thesubnet’s traffic to the Amazon VPC’s IGW. All the instance in the private subnet will get Private IP addresses only, and hence no communication with the interent.

Route Tables: A route table is a logical construct within an Amazon VPC that contains a set of rules (called routes) that are applied to the subnet and used to determine where network traffic is directed.

Your VPC has an implicit router, and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.

Route: Each route in a table specifies a destination and a target. For example, to enable your subnet to access the internet through an internet gateway, add the appropriate route to your subnet route table.

Important Points about Route Tables and Routes:

- 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.
- You can also use route tables to specify which subnets are public (By routing the traffic through IGW) and which subnets are private (By not routing the traffic through IGW).
- Each subnet must be associated with a route table, which controls the routing for the subnet. If you don't associate a subnet with a particular route table, the subnet uses the main route table.

Network Address Translation (NAT): By Default, any instance that you launch into a private subnet in an amazon VPC is not able to communicate with the internet through the IGW. AWS provides NAT option to share the internet with the private subnet and it will not allow incoming traffic from the internet.

NAT Instance: A NAT Instance is an Amazon Linux AMI that is built on the latest version of amazon Linux, which reached the endo of support on December 32, 2020. AWS recommends that you migrate to a NAT Gateway or create your own NAT AMI on Amazon Linux2 as soon as possible.

NAT instance to be create in the public subnet and need to update the Private Subnet's route table with a new route which points all traffic through NAT Instance.

Note: For the NAT Instance Security group, we need to open 80, 443 from your private subnet.

NAT Gateway: A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.When you provision a NAT gateway, you are charged for each hour that your NAT gateway is available and each Gigabyte of data that it processes. For more information, see Amazon VPC Pricing.

Compare NAT Gateways & NAT Instances.

Bastion Host: A **bastion host** is a server whose purpose is to provide access to a private network from an external network, such as the Internet.

Security Groups: A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. 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

The Following are the characteristics of security Groups:

1. You can specify allow rules, but not deny rules.
2. You can specify separate rules for inbound and outbound traffic.
3. Security group rules enable you to filter traffic based on protocols and port numbers
4. 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.
5. When you first 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.
6. 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.
7. A security group can only be used in the VPC that you specify when you create the security group.

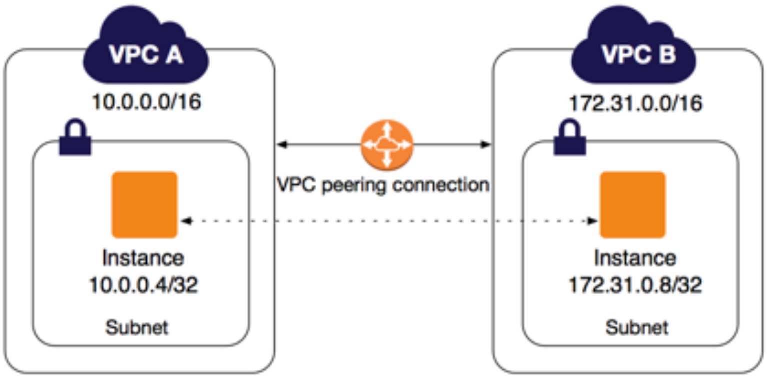
Network Access Control Lists (NACL): A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

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

The Following are the characteristics of NACL:

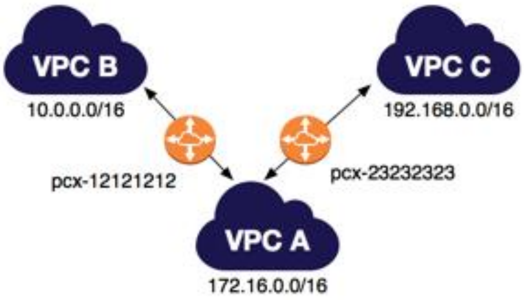
1. Your VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic.
2. You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
3. 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.
4. 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.
5. 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.
6. A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
7. Network ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

VPC Peering: A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).



it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

VPC Peering is a non-Transitive Peering. Means there will be no automatic peering between **VPC B & VPC C**



Pricing for a VPC Peering Connection:

If the VPCs in the VPC peering connection are within the same region, the charges for transferring data within the VPC peering connection are the same as the charges for transferring data across Availability Zones. If the VPCs are in different regions, inter-region data transfer costs apply.