Virtual Private Clouds

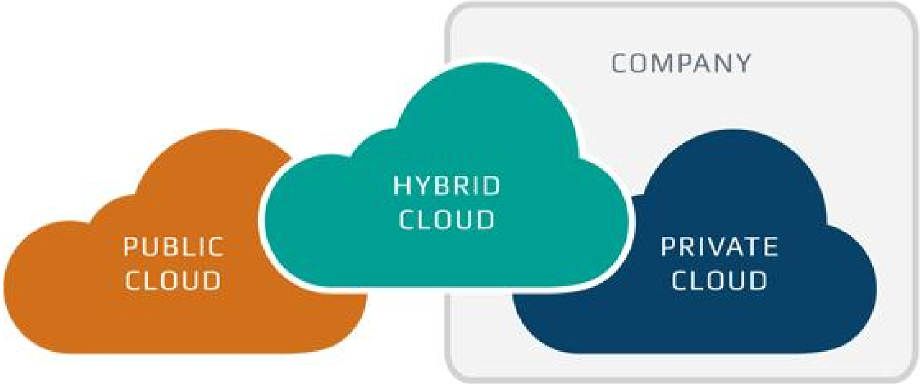
TJ Cloud Computing Club

January 2020

1 Deploying Cloud Computing

As you may know, cloud computing is the process of delivering some service over the Internet. With cloud computing, users can access files, applications, and web pages from any device connected to the Internet. How do you deploy a cloud computing service, though? There are generally three methods of doing this:

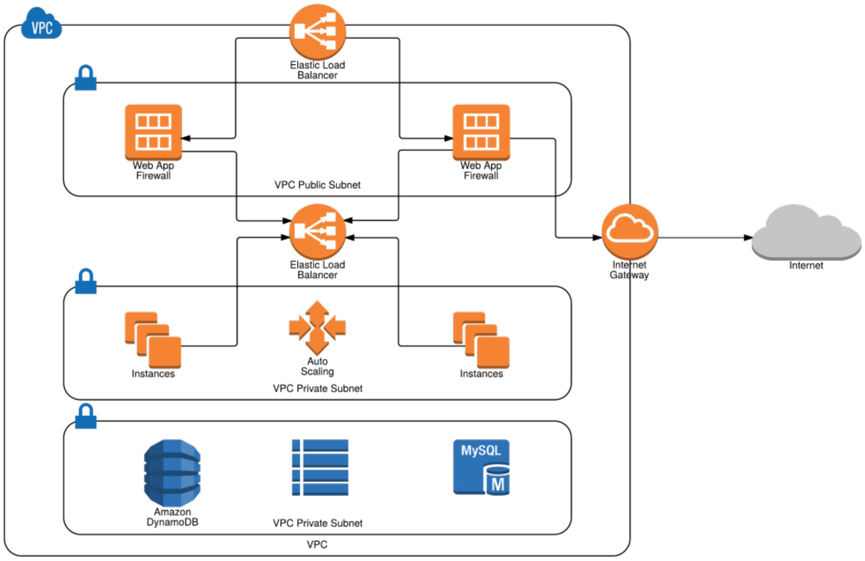
- Public Clouds: With public clouds, cloud resources such as servers and storage are owned and managed by a third-party cloud service provider, such as AWS or Microsoft Azure. Public clouds require no maintenance and are frequently used for cloud computing.
- Private Clouds: Private clouds are exclusively used by one organization or business and require much more maintenance as they are not managed by a third-party provider. They offer more options to customize network configurations and provide much greater security.
- Hybrid Clouds: This method combines the two previous methods by using both private and public clouds. Data and applications can move between public and private clouds, allowing for greater flexibility.



2 Why Use a Virtual Private Cloud?

Although hosting websites, applications, or virtual machines on a public cloud requires less maintenance and management, they are much more prone to attacks and bugs from outside sources. With a virtual private cloud, you can have much greater security and the choice to expose only a portion of your infrastructure to the Internet.

For example, you could have a database within your virtual private cloud and choose to not connect it directly to the internet. It would only be accessible through certain instances in your private cloud. Additionally, especially in the case of AWS, using a virtual private cloud is the best way to connect a private data center with instances from a cloud service provider. To control the virtual environment within the cloud, you can choose to add your own IP address range, subnets, route tables, and network gateways.



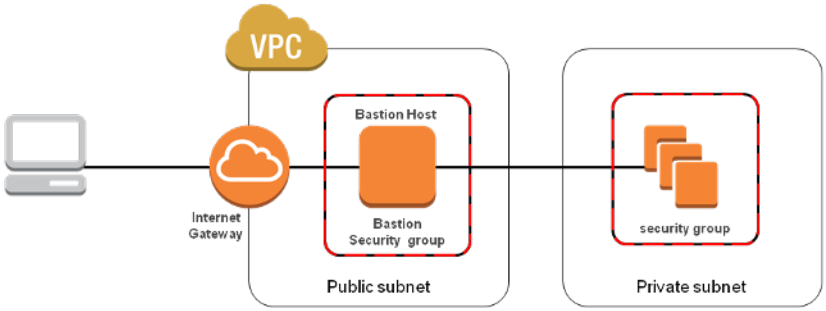
3 Subnets

Subnetworks, or subnets, are essential components of virtual private clouds. Subnets have their own specific IP range as a subdivision of the overall network. Why, you may ask, can there not just be one large network? This is because some components, as mentioned earlier, are better off without being exposed to Internet (such as databases), while others are. Additionally, a subnet cannot traverse more than a single availability zone, which is defined as a physical data center in a specific region. By having multiple subnets, it is possible to deploy your cloud in multiple availability zones. Lastly, these components greatly reduce the amount of network congestion that may result from one large network.

Subnets can be defined as either public subnets or private subnets according to what you want to expose to the outside world. Private subnets are generally used more for backend resources. They primarily use the NAT gatway to connect to the Internet, whereas public subnets use the Internet gateway.

3.1 Internet Gateway

The Internet gateway is how a public subnet connects to the Internet. This component does not have a specified IP address range and does not need to be managed. It allows for bi-directional communication between the outside world and instances within the VPC.



3.2 NAT Gateway

The Network Address Translation (NAT) gateway is similar to the Internet gateway in that it acts as a connection to Internet. It also does not have a specified IP range and requires no management. However, it differs from the Internet gateway as it attached to a private subnet. It allows the subnet to connect to the Internet, but prevents the Internet from initiating a connection with it first.

4 Route Tables

Each subnet in the virtual private cloud must be associated with a specific route table. This can either be a user-defined route table or a main route table that is created by default with a VPC. Route tables control the flow of network traffic by listing out the routes to particular network destinations. Every route in a route table must have a destination and a target. The destination is specified by a range of IP addresses, while the target indicates where the traffic for the specified destination should be sent (ex. the Internet gateway or a local subnet).

5 Differences in AWS, GCP, and Azure

As always, each of the main three cloud providers have their own method to implement VPCs. The names are as follows:

- AWS - Amazon VPC
- Google Cloud - GCP Virtual Private Cloud
- Microsoft Azure - Azure Virtual Network