International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 9, Issue 7, July 2020 **ISSN 2319 - 4847**

VPC: Virtual Private Cloud overview

Venkatesh A[1], Shivakumara T[2] and Sudarsanam P[3]

[1,2,3]BMS Institute of Technology and Management

ABSTRACT

The concept of cloud computing is not a new thing in the present scenario. People are so dependent on cloud so that, they cannot escape using internet to do their routine activities. When we have such a dependency on cloud, then security becomes more crucial. In this paper, we are using VPN(Virtual Private network) concept in cloud context and calling it as VPC(Virtual private Cloud) that is aimed at providing more security and more freedom to its user, especially during Covid-19 pandemic.
Keywords: *VPN, VPC, Private Cloud, Security*

1. INTRODUCTION

As more and more people started relying on cloud computing to access the digital resources ubiquitously from anywhere, cloud is posing a serious security concern. The main objective of this paper is to highlight the need for security for cloud users and organizations at large. Here, for my convenience, I'm considering the example of Amazon cloud to explain the virtual private cloud concepts. Key components of VPC are: Subnet, route table, internet gateway and endpoint, which we will be explaining in this paper briefly.

2. ACCESSING AMAZON VPC

The very basic thing is to know how to access Amazon web services using its portal and the next step is to learn how to manage the services and resources of Amazon AWS. Amazon AWS provides different ways to access its services viz: Amazon Management console, Amazon command-line interface, AWS To manage VPCs, one can use different interfaces. Below shown are some of the commonly used interfaces:

2.1 SUBNET:

Any given VPC can be logically sub-divided into smaller networks called subnets. Especially useful when you have too many domains or departments in your organization. In Amazon Web Services, user can create a public or a private subnet within a VPC. Using a public subnet user can connect to the internet, whereas a private subnet does not allow connection to the internet. However, users can still configure subnets to allow two way traffic for the instances. One can assign an IP address to an EC2 instance that will uniquely identify it in a subnet in VPC. As IP address has two sections: the network section or the routing prefix and the host. The network section or routing prefix identifies the subnet to which the EC2 instance communicates. The host part identifies the EC2 instance uniquely anywhere in the network across this globe.

2.2 ROUTE TABLE:

The main function of a route table is to route packets to destination route, which are used to determine direction of the data packets in the network. Each subnet within a VPC is associated with a routing table. VPC has a main route table and any subnet by default is associated with it. It is also possible to create custom route tables for subnets or VPCs. The entries of the main route table can also be customized. Each route in a route table has got target and destination device/node. For example – Traffic Destined for 10.0.0.34/28 is targetted for Internet Gateway (IGW).

2.3 INTERNET GATEWAY:

2.3.1 Public Subnet: Includes a route to outside world/Internet gateway.

2.3.2 Private Subnet: Its context is only the local network. It is helpful for security of data within a team or a company.

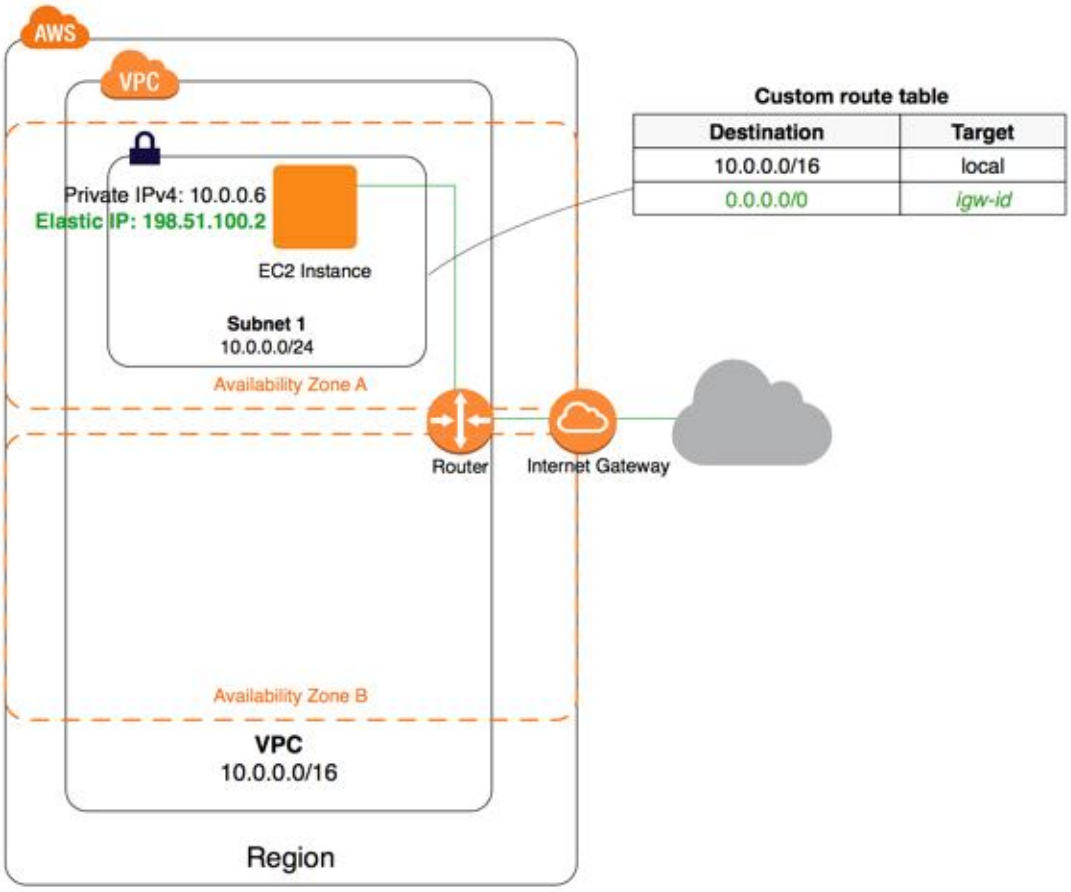

Figure-2: Virtual Private Cloud (VPC)

The Internet gateway is a logical device that connects both subnet and the Internet. Users can allow the gateway instances in their VPC to initiate outgoing connections, but can prevent incoming connections using a network address translation or NAT instances.

2.3.3 Transit Gateway:

A transit gateway is a network transit hub that one can use to interconnect their virtual private clouds (VPC) and on-premises networks. Important points about transit gateways:

- **Attachment** — one can attach a VPC, a P2P connection with another transit gateway, an AWS Direct Connect gateway or a VPN connection to a transit gateway.
- **Transit gateway route table** — Transit gateway has a common routing table and it can also have additional route tables. Dynamic and static routes inside the routing table decides the next hop based on the destination IP address of the packet. The target of these routes could be a VPC or a VPN connection. By default, transit gateway attachments are associated with the default or common transit gateway routing table.
- **Associations** — every attachment is associated with exactly one routing table. Each routing table can be associated with '0 to N' attachments.
- **Route propagation** — Transit gateway can dynamically get information from VPN or VPC. With a VPC, one needs to create a static route to send traffic to a transit gateway. When you have a VPN connection, routes are propagated from the transit gateway to your on-premises router using the Border Gateway Protocol (BGP). With a peering attachment, it is mandatory to create a static route in the transit gateway route table to point to the peering attachment.

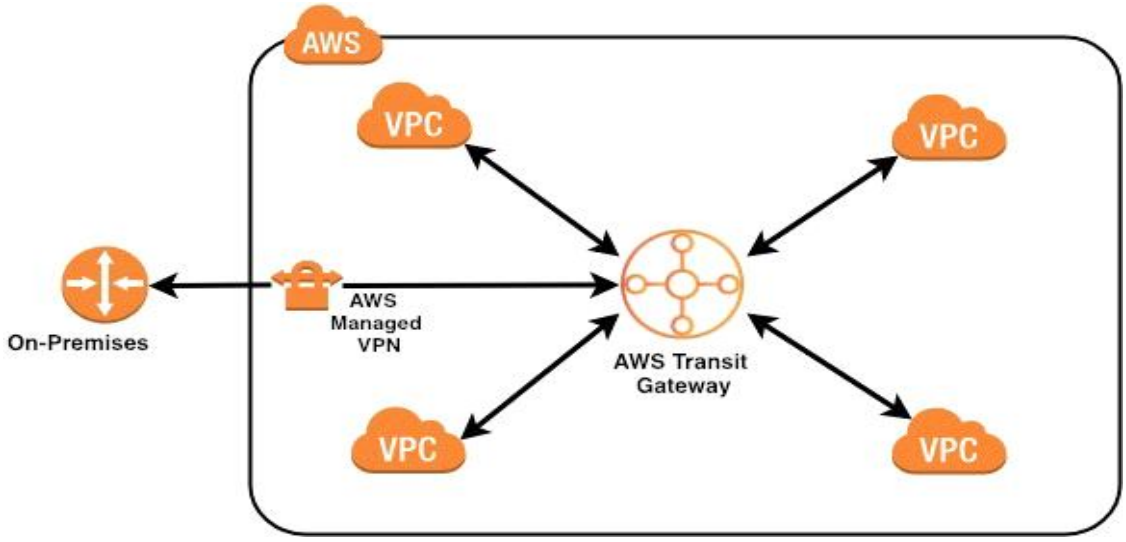

Figure 3: Virtual Private Cloud Connectivity for on premise setup

3.NEED FOR VPC

It is also possible for the organizations to ask their employees to work from home during pandemic situations just like now: Covid-19 pandemic, VPCs become very much useful to virtually connect remote teams and extract work. VPC provides more security as it is a private network.

4. CONCLUSION

After studying the VPC implementation using Amazon AWS, we are confident that cloud based VPC can provide secure communication and can protect company's data. It is every company's inside matter to deal with the private/public VPC needs. It is advisable to place your backend systems, such as database servers or application servers, in a private subnet with no internet access. Private VPCs just like VPN, provides secure way to connect to logical local virtual network in a secure manner using cloud computing. In Amazon AWS, one can implement several layers of security using access control lists and security groups, to help control access to Amazon EC2 instances in each subnet. Similar facilities are provided by most of the cloud vendors. Thus VPC has become mandatory for companies to allow their employees to work from home securely and seamlessly.

REFERENCES

[1] Josip Balen, Denis Vajak, Khaled Salah, "Comparative Performance Evaluation of Popular Virtual Private Servers," Journal of Internet Technology, vol. 21, no. 2 , pp. 343-356, Mar. 2020.
[2] Radhika, T & Subramanian, Sathish & Gouda, K C. (2015). A STUDY ON THE DIFFERENT ASPECTS OF THE VIRTUAL PRIVATE CLOUD. International Journal of Applied Engineering Research (IJAER) ISSN 1087-1090. 10. 343-34
[3] Palomares, Daniel & Migault, Daniel & Hendrik, & Laurent, Maryline. (2014). Elastic Virtual Private Cloud 10.1145/2642687.2642704.
[4] https://aws.amaon.com/console
[5] https://docs.aws.amazon.com
[6] https://en.wikipedia.org/wiki/Virtual_private_cloud

AUTHOR

Prof. Venkatesh. A received the B.Sc. in Computer Science and M.C.A. degree from Bangalore University and Visveswaraya Technological University in 2005 and 2008, respectively. Presently working as Assistant Professor in Dept. of Computer Applications, BMS Institute of Technology and Management, Bengaluru.. Pursuing Ph.D in the area of Wireless Sensor Networks. Interested in areas like: Cloud computing, Automation and Cyber Security.

Prof. Shivakumara T, working for Department of MCA, BMS Institute of Technology and Management, Bangalore as an Assistant Professor since 2008. He has completed his masters' degree (Master of Computer Applications) in 2007. Teaching the masters' degree computer applications courses prescribed by Visvesvaraya Technological University (VTU). Actively involved in teaching-learning process, as an outcome of it he was able to publish 3 text books, laboratory manuals, learning materials in coordination with co-authors in the same field. He has published few national conference papers and journals. His current research focuses on data and information security - data leakage prevention. He has been engaged to create awareness on cyber security-cyber safe Karnataka in association with cyber security center of excellence, Government of Karnataka, to school and college students. He is the member of ISTE chapter. Currently, pursuing PhD in Computer Applications under VTU and currently heading the National Service Scheme (NSS) Cell.

Dr. Sudarsanam P received the M.E (CSE), PhD. (CSE) degree from Anna University in 2009 and 2020, respectively. Presently working as Assistant Professor in Dept. of Computer Applications, BMS Institute of Technology anManagement, Bengaluru. The area of specialization is Computer Networks and Parallel computing.