Large Scale Integration of Site to Site VPN using AWS VPC Content and Delivery Network Web service

Heena Sejwal[1], Nidhi Sewal[2]
DPG Institute of Technology and Management
Sector 34, Gurugram, Haryana 122001

ABSTRACT

Amazon's cloud services are rapidly changing and changing the way organizations deal with IT infrastructure and what Internet services offer. Today, it is easy to find the power of a computer. The user can purchase it online and use the programs provided by the cloud companies to open and close the visual images. VPC offers greater security than traditional cloud rental offerings but allows consumers to take advantage of the high availability, flexibility, and cost effectiveness of the public cloud. Visualization still separates your information from other companies - travel and the network provider - helping to create a safer environment. VPC connects to remote networks via Virtual Private Network (VPN) connection. Suitable for companies seeking higher levels of security, privacy and control, such as health organizations and financial institutions that are subject to legal compliance. Businesses also find VPC ready for use by critical applications. In this paper we will be taking steps to launch EC2 Instances on Amazon VPC and build Our Connections (our Corporate or local network). In order to communicate we can establish a Site to Site VPN Secure connection between our devices in the building and VPC's VPN Tunnel which is a link installed where data can pass through a customer network to or from AWS. The information presented in this paper will be useful to professionals who intend to manage Communication Networks and Resources within AWS and to researchers who are committed to improving cloud computing.

INTRODUCTION

1. CLOUD COMPUTING

Cloud computing describes a way in which data and programs can be stored and accessed without having to store or access them on any virtual media. This is especially helpful for companies that require a large amount of disk space. Amazon Web Services offers a comprehensive set of cloud-based products including compute, storage, data, analytics, network, mobile, developer tools, management tools, IoT, security, and sought-after business applications available in seconds, at a fraction of the cost. -be-you-go. From Warehousing data to delivery tools, content delivery guides, more than 140 AWS resources are available. New services can be provided quickly, at no extra cost to the city. This allows businesses, startups, small and medium enterprises, and clients in the public sector to access building blocks that need to be responded to quickly in changing business needs.

1.1 Cloud Computing Deployment Models :-

Public Cloud Model allows the general public to access the program and services easily. Companies such as Google, Amazon and Microsoft offer cloud services online. There is a low level of security in the Public Cloud as data is available to users publicly online.

Private Cloud allows programs and services to be accessed within the organization. Private Cloud operates within a single organization. However, it can be controlled internally by the organization itself or by third parties. Ensures high security and privacy.

Hybrid Cloud Model

This model is a combination of private and public cloud. Non-critical activities are done

using a public cloud while important activities are done using a private cloud.

Community Cloud allows programs and services to be accessed by a group of organizations. Share infrastructure between several community organizations. It may be managed within organizations or by a third party.

1.2 ELASTIC COMPUTE CLOUD

Amazon Elastic Compute Cloud (Amazon EC2) is a Virtual Machine that offers more computing and cloud computing. Allows organizations to identify and configure virtual servers in Amazon data centers and integrate those used to build and host software applications. Organizations can select from a variety of operating systems and resource configurations (memory ,CPU, storage, and so on) that are optimal for the application profile of each workload. Amazon ec2 provides scalable computing capacity in the cloud .

1.3 VIRTUAL PRIVATE CLOUD

A VPC is a Virtual Network that closely resembles a traditional networking that we operate in our own data center, with the benefits of using the scalable infrastructure of AWS. To Simply say it is a virtual network or data center inside AWS for one client. It is logically isolated from other virtual network in the AWS cloud, Max 5 VPC can be created inside one region and 200 subnets in 1 VPC, We can allocate max 5 elastic IP's. Once we created a VPC,DHCP, NACL and Security Group will be created automatically. A VPC is confined to an AWS Region and does not extend between regions, Once the VPC is created, we cannot change its CIDR, block range and If you need a different CIDR size, create a new VPC. The different Subnets within a VPC cannot overlap, however we can expand our VPC CIDR by adding new/extra IP address ranges(except American Govt cloud & AWS China)

Components of VPC :

CIDR & IP Address Subnets,

- Implied router & routing table
- Internet gateway
- Security groups
- Network ACL
- Virtual private gateway
- Peering connections
- Elastic IP

Implied Router & Route Table

It is the central routing function, It connects the different AZ together and connects the VPC to the Internet Gateway, we can have upto 200 route tables per VPC, we can have upto 50 route entries per route table. Each subnet must be associated with only one route table at any given time, If we do not specify a subnet to route table association, the subnet will be associated with the default VPC Route table. We can also edit the main route table if we need, but we cannot delete main route table. However we can make a custom route table manually, make it the main route table then we can delete the former main, as it is no longer a main route table. We can associate multiple subnets with the same route table.

Internet Gateway An IGW is Virtual Router that connects a VPC to the internet, Default VPC is already attached with an IGW, if we create a new VPC then we must attach the IGW in order to access the internet. Ensure that our Subnet's Route table points to the internet gateway, It performs NAT between our Private and Public IPv4 Address, It supports both IPv4 and IPv6

NAT Gateway : Also does PAT(Port Address translation),we can use a Network Address Translation 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, Creation and usage of NAT gateway in an account is charged by AWS

VPC provides double level of Security

Security Groups : It is a Virtual firewall which works at ENI(Elastic Network Interface) level, upto 5 Security Groups per EC2 instances

interface can be applied, Can only have permit rules, cannot have deny rule, Stateful (if inbound allowed then automatically outbound is also allowed and vice versa) i.e return traffic is allowed then inbound traffic is also allowed, even if there are no rules to allow it.

Network ACL : It is a function performed on the implied router and provides an optional layer of security for our VPC that acts as a firewall for controlling traffic in and out of one or more subnets. Our VPC automatically comes with a modifiable default Network ACL. By default, it allows all inbound and outbound ipv4 traffic and if applicable,ipv6 traffic, We can create a Custom Network ACL and associate it with a subnet ,By default each Custom ACL rejects all incoming and outgoing traffic until we add rules,

VPC Peering : A VPC Peering connection is a networking connection between two VPC that enables us 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, We can create a VPC Peering Connection between our own VPC or with a VPC in Another AWS account. The VPC can be in different Region.

There are 2 types of VPC :-

Default VPC : Created in each AWS region when an AWS account is created, has default CIDR, Security Group, NACL and Route Table settings, it has an Internet Gateway by default.

Custom VPC : Is an AWS Account admin creates, AWS user creating custom VPC can decide the CIDR, has its own default Security Group, Network ACL, and Route Table, does not have an Internet Gateway by default, one needs to be created when needed.

Steps to follow for creating a VPC :

1.Create VPC
2.Subnet
3.Internet Gateway
4.Route Table

Public Subnet : If a Subnets Traffic is routed to an Internet Gateway, the subnet is known as Public Subnet, If we want our Instance in a public subnet to communicate with internet connection over ipv4, there must be a public ipv4 address or an Elastic IP address

Private Subnet : If a subnet does not have a route to the Internet Gateway, the subnet is known as a Private Subnet.

Note : While creating a VPC, we must specify an IPv4 CIDR block for the VPC. The allowed block size is between /16 to /28 and the first four & last IP address of a subnet cannot be assigned.

Virtual Private Gateway, Customer Gateway & Site-to-Site VPN connection

By default, Instances that we launch into an Amazon VPC can't Communicate with our own(our Corporate or home network) Network. To enable the communication we have to establish Site to Site VPN connection which is a Secure Connection between our on-premises equipment and our VPC's VPN Tunnel which is an encrypted link where data can pass through a customer network to or from AWS. Each VPN connection include two VPN tunnels which we be simultaneously used for high availability.

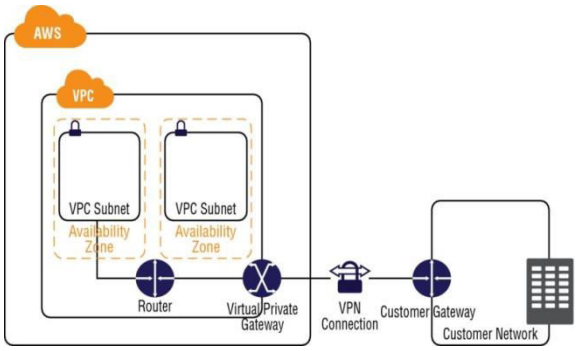


Fig.1 Site to Site VPN Connection

Customer Gateway is an AWS resource which provides information to AWS about our Customer Gateway Device

Customer Gateway Device is a physical or software app on customer side

Create AWS Account by Amazon Management Console Log in website using

https://AWS.amazon.com/console/ link, Click on sign up for a new Account.

Enter your details for signing up for a new account in AWS Management Console, it will ask for your User name and email-id after that once we click on Continue it will move to next page which asks for your actual Bank Account details which will deduct Rs2 from the account for verification of details provided by you are correct or not.

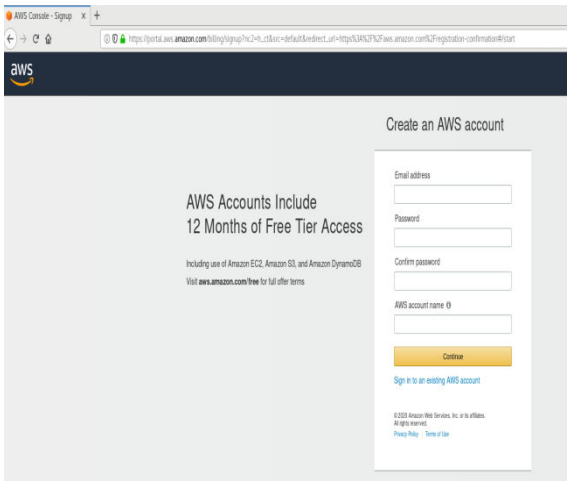


Fig.2. Create AWS account

Once AWS Account has been created, now Sign in using your User name and Password on AWS Management Console.

As we are establishing VPN connection between 2 Regions, so here we will take Mumbai Region for AWS Data Center and another Region as Singapore for Customer end.

1.Create VPC at Mumbai Region 10.1.0.0/16 as IPv4 CIDR value

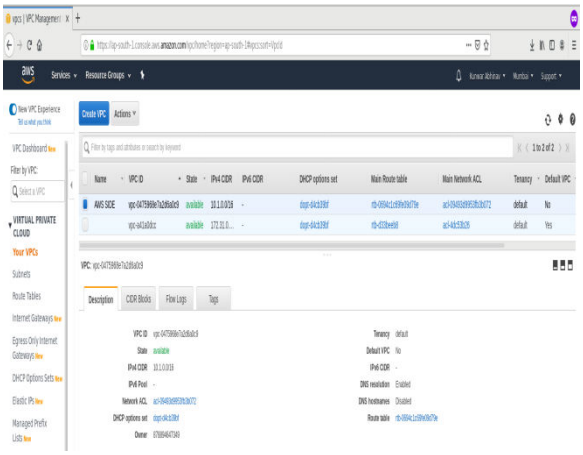
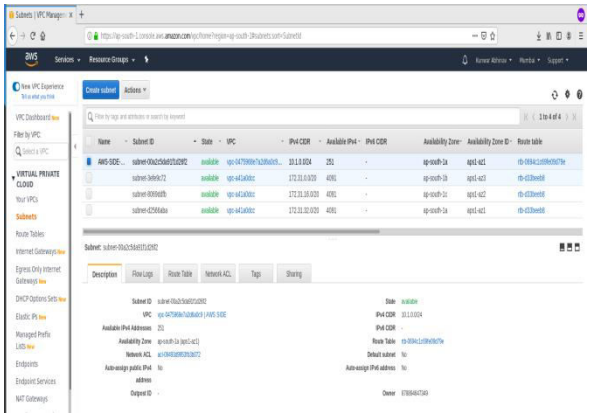


Fig.3.VPC at Mumbai Region

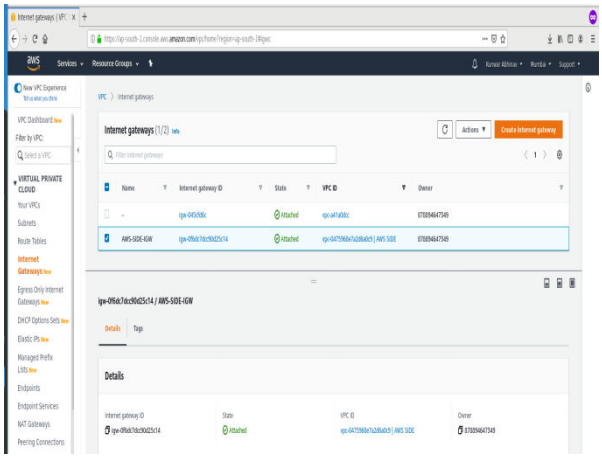
2. Create Subnet(AWS-SUBNET) for the Mumbai Region VPC(AWS SIDE) and



10.1.0.0/24 as IPv4 CIDR value

Fig.4 Subnet at Mumbai Region

3. Create Internet Gateway (AWS-SIDE-IGW) and attach it to AWS- SIDE VPC in Mumbai



Region

Fig.5 Internet Gateway in Mumbai Region

4. Create Route table named as AWS-ROUTE for the AWS-SIDE VPC and edit Routes by entering value as 0.0.0.0 and selecting Internet Gateway created in step 3

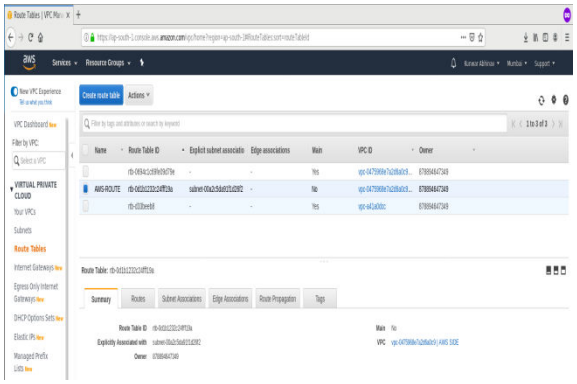


Fig.6 Route Table of VPC in Mumbai Region

5. Now select Singapore Region and open AWS Console for Singapore region in new tab and create VPC named as CUSTOMER-VPC providing 10.2.0.0/16 as CIDR IPv4 address.

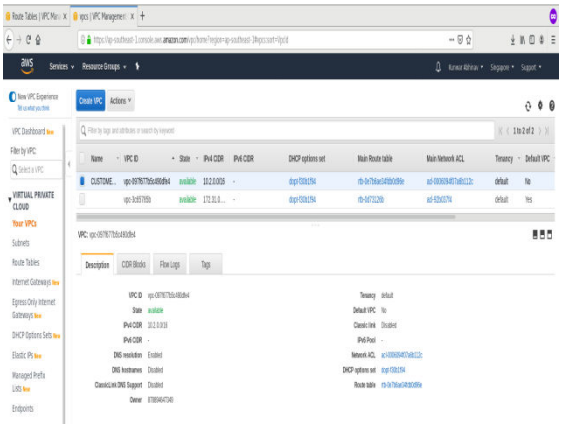


Fig.7 VPC Creation at Customer

6. Create Subnet for CUSTOMER- VPC providing 10.2.0.0/24 as CIDR IPv4 address using same steps followed above for AWS – SIDE VPC. Create Internet Gateway CUSTOMER- IGW and attach it to CUSTOMER- VPC, Create Route table for this VPC named as CUSTOMER-ROUTE and edit entries 0.0.0.0 and Internet Gateway in Routes and also associate Subnet which we created for this VPC i.e CUSTOMER – SUBNET.

7. After creating VPC in both Regions, Launch Linux EC2 Instance by selecting **Amazon Linux 2 AMI (HVM), SSD Volume Type** and choosing the
CUSTOMER-VPC network in Configure Instance details in Singapore Region.

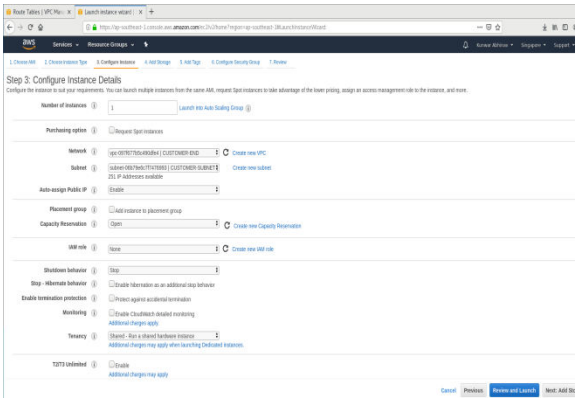


Fig. 8 Allocating Customer VPC network to EC2 instance in Singapore Region

8. For Add Storage tab, keep it as default and in tags tab enter name as Customer-Machine and create a new Security group as Customer-SG and selecting SSH, All TCP and All ICMP-IPv4 protocols and selecting source as either your subnet range or Anywhere to allow access to the ec2 instance.

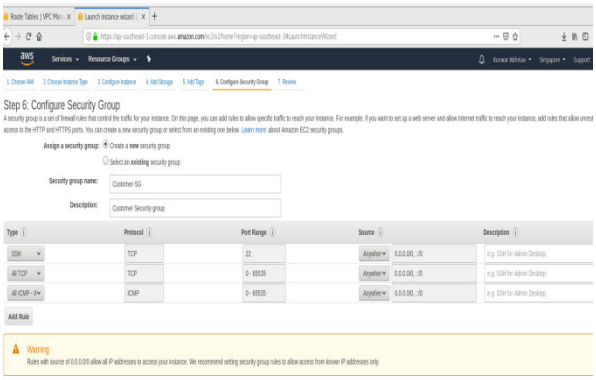


Fig 9. Assigning Security Group to EC2 Instance

Click on review and then launch Instance it will ask for Secure Private Key to access the instance once it is launched, create a new keypair file for this purpose and download it.
Click on Review → click on Launch
Once EC2 instance has been launched in Singapore region and becomes available after 2/2 status checks.

9. Go to Mumbai Region, click on Virtual Private Networks available in Services window,

click on Create Virtual Private Gateway and create a VPG named as AWS-SIDE-GW and attach it to
AWS-SIDE-VPC.

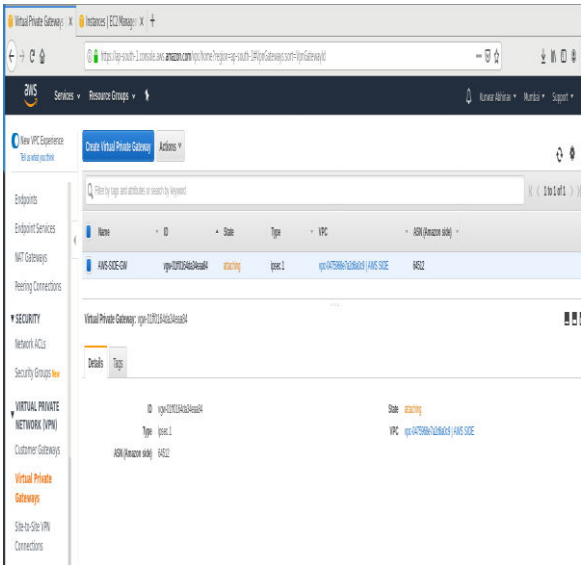


Fig 10. Creating Virtual Private Gateway

10. Click on Customer Gateway and create a new Customer Gateway named as CG-AWS-SIDE, Routing as static and mention **Public IP** of machine with which you want to establish connection I.e Customer-Machine in Singapore Region.

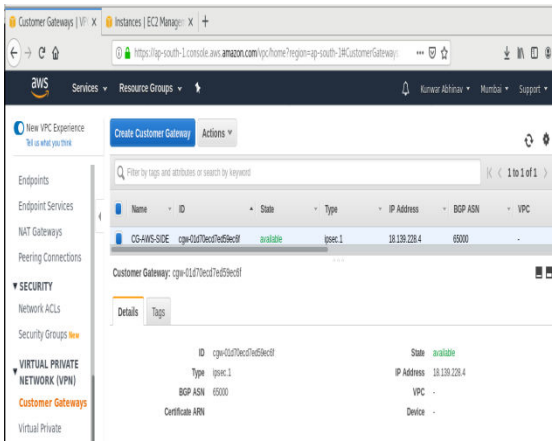


Fig. 11 Creating Customer Gateway in Mumbai Region

11. We will create Site-to-Site VPN Connection in Mumbai Region which will establish 2 Secure Tunnels for high Availability between the 2 Regions. For this click on create VPN Connection and name it as MUMBAI-SINGAPORE, in Target Gateway Type select Virtual Private Gateway and select VPG which we have created in step 9 and select existing Customer Gateway which we have created in step 10. In Routing Options select Static and enter Singapore side (**CUSTOMER-SUBNET**) value in **Static IP Prefixes**.

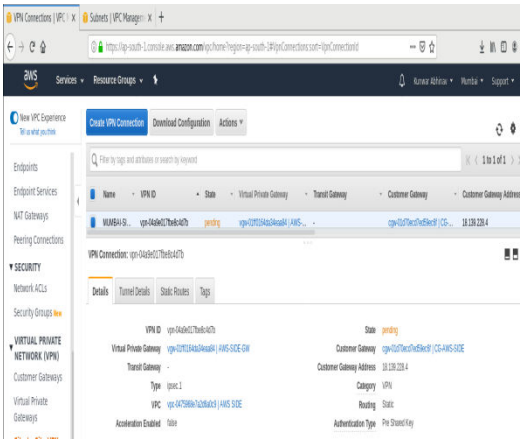


Fig. 12 Creating VPN Connection

Once VPN Connection become available we will Download Configuration file of this connection. For downloading configuration file select Vendor as Generic and then click on download.

12. Go to Route Tables within Mumbai Region and select AWS-ROUTE and select Route Propagation and choose CUSTOMER-SUBNET or we can manually edit Route entries by entering Customer-subnet CIDR values 10.2.0.0/16.

13. Now we will be installing VPN Software and Configuring VPN Connection in Customer-Machine (Singapore Region). For that we need to connect to EC2 instance which is Customer Machine and follow the below steps for Installation and Configuration.

GO TO PUTTY,CONNECT TO YOUR EC2
LOGIN AS- ec2-user
1. Commands for Installation of Openswan
ii. Change to root user:
$ sudo su -

ii. Install openswan:
$ yum install openswan -y
iii. In /etc/ipsec.conf uncomment following line if not already uncommented:
include /etc/ipsec.d/*.conf
iv. Update /etc/sysctl.conf to have following
net.ipv4.ip_forward = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
v. Restart network service:
$ service network restart
2.Command for /etc/ipsec.d/AWS-vpn.conf
conn Tunnel1
authby=secret
auto=start
left=%defaultroute
leftid=Customer end Gateway VPN public IP
right=AWS Virtual private gateway ID- public IP
type=tunnel
ikelifetime=8h
keylife=1h
phase2alg=aes128-sha1;modp1024
ike=aes128-sha1;modp1024
keyingtries=%forever
keyexchange=ike
leftsubnet=Customer end VPN CIDR
rightsubnet=AWS end VPN CIDR
dpddelay=10
dpdtimeout=30
dpdaction=restart_by_peer

leftid, right, leftsubnet and rightsubnet values will be changed as per Configuration file which we have downloaded from Site-to-Site VPN Connection.
3. Contents for /etc/ipsec.d/AWS-vpn.secrets
customer_public_ip AWS_vgw_public_ip: PSK "shared secret"
customer_public_ip AWS_vgw_public_ip and shared secret(pre-shared) key values will be edited according to Site-to-Site VPN Connection Configuration File downloaded in step 11.

4. Commands to enable/start ipsec service
$ chkconFig.ipsec on
$ service ipsec start
$ service ipsec status

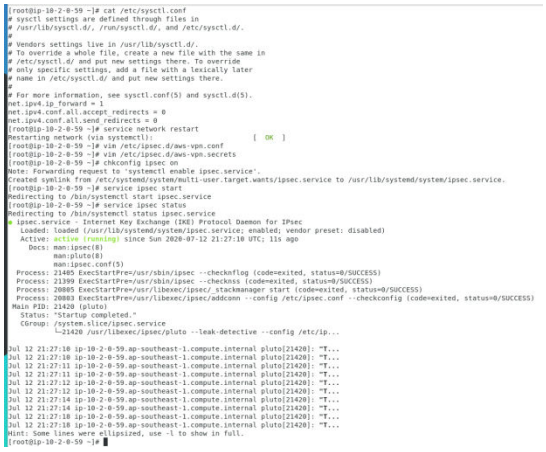


Fig. 13 Successful establishment of VPN Connection between AWS and Singapore Region

Status as active (running) will show successful VPN software establishment and VPN connection configuration between the 2 Region.

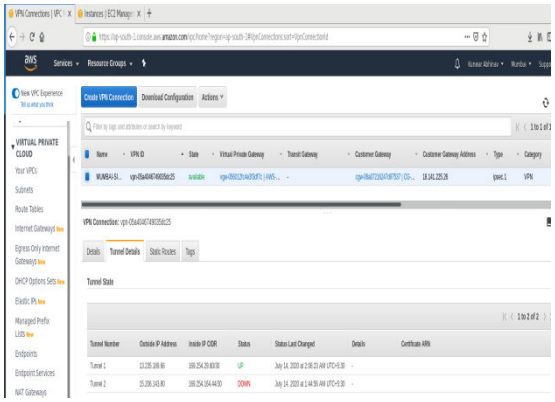


Fig. 14 Tunnel is UP

After the connection is in Active (running) state we will check for the Tunnels state which is up in Site-to-Site VPN Connection which shows successful secure VPN Connection tunnels creation.

14. Create a Linux EC2 instance in AWS Region (follow steps 7 and 8), name it as AWS-Side-Instance and select Network as AWS-SIDE VPC.

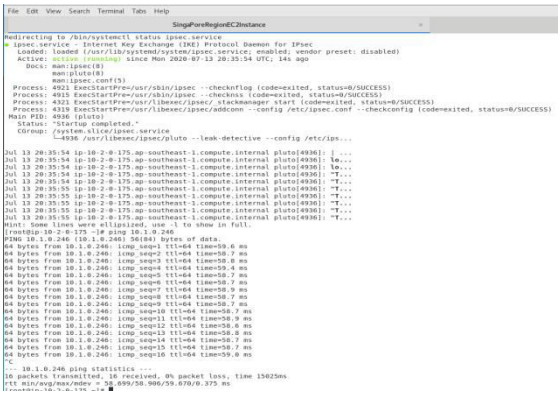


Fig. 15 Successful ping of AWS EC2 instance in Mumbai from Singapore Region.

For checking the configuration done by us. We will now check the VPN Connection between the 2 Regions by pinging AWS side ec2 instance private IP from EC2 instance in Singapore Region.

15. For Cross-checking purpose and confirming successful VPN Connection between both the regions, we will ping Singapore Region EC2 Private IP from Mumbai Region AWS EC2 instance.

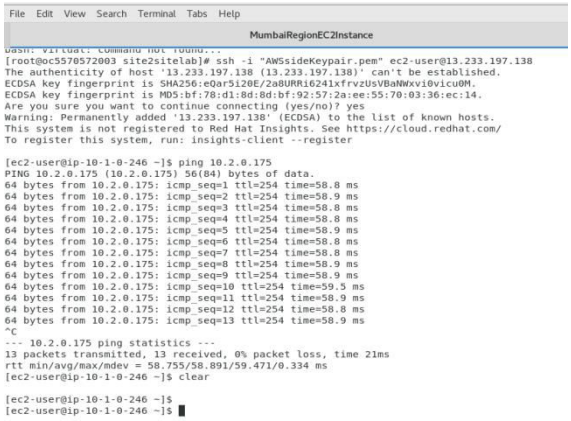


Fig 16 Successful pinging of Singapore Region from Mumbai for Cross checking

CONCLUSION

Your Virtual Private Cloud is set up and you now have a rock-solid Secure Site to Site VPN connection with which to reach it. A Virtual Private Cloud is a single-tenant concept that gives you the opportunity to create a private space within the public cloud's architecture. A VPC offers greater security than traditional multi-tenant public cloud offerings but still lets customers take advantage of the high availability, flexibility, and cost-effectiveness of the public cloud, it is ideal for companies seeking high levels of security, privacy and control, such as healthcare and financial organizations dealing with regulatory compliance. Businesses also find VPC ideal for running mission-critical applications

Unfortunately, you can see that these services are currently very intricate to set up and are aimed at Professionals, not casual users. I'm sure that this paper will also be helpful for average users and they will also take advantage of using AWS Services by creating one year free account and learning and experimenting by utilizing the Freely available AWS Resources.

REFERENCES

[1]. Sullivan B. (2016). "Amazon Web Services Public Cloud",[Online].Available:http://www.techweekeurope.co.uk/cloud/cloud-management/amazon-web-services-public-cloud-185687

[2]."Amazon Web Services(AWS)."https://AWS.amazon.com/marketplace

[3]. L. Wang, G. Laszewski, M. Kunze and J.Tao, —Cloud computing: a perspective study‖, J New Generation Computing, 2010,pp 1-11.

[4].https://en.wikipedia.org/wiki/Amazon_Web_Services

[5]. Cloud Application Architectures - O'Reilly - By George Reese.

[6]. Amazon Web Services Tutorial - by Jineshlalan.

[7]. Sushil Bhardwaj, Leena Jain, Sandeep Jain,Cloud computing: a study of

Infrastructure as a service (Iaas)‖ IJEIT 2010, 2(1), pp 1-4.

[8]. Rupinder Kaur, —Cloud computing‖,International Journal of Computer Science and Technology, IJCST Vol. 2, Issue 3,September 2011 .

[9]. Craig Balding, —Assessing the Security Benefits of Cloud Computing‖,http://cloudsecurity.org/blog/2008/07/21/assessing-the-security-benefits-of-cloud-computing.html

[10]. Getting Started with Amazon Redshift - by Stefan Bauer.

[11]. Learning AWS OpsWors - By Todd Rosner.