

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

> Heena Sejwal¹, Nidhi Sewal² 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, analytics, network, mobile, storage, data, 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 International Journal of Scientific Research in Engineering and Management (IJSREM) Volume: 04 Issue: 08 | August -2020

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

Subnets VPC Managern: X	+												1
€ ⇒ ¢ ≙	0 🛔 https://wj-s	nativ-1 console	ivis anazon.com/y	chanehegi	in-ap-south-1#subrets.sort	Subretif				- 🗟 🖞	± I	100	
aws Senice	s 🖌 Resource Group	s - 5								🗴 Kener Altera •	Reta •	Sepot •	l
New VPC Experience The end you think	Create subset	kcioes v										00	
VPC Dashbaard 🐜	Q. How by tags an	antes e se	ant) to knowed)({ 1m	4ef4)	
Filer by VPC.	Nare	- Sabret ID		State -	UPC .	PNICER -	Analabie IPv4 -	INI COR	Availability Zone-	Assilubility Zone ID -	Route table		
d section.	ANS-SDE	subret-00a	2/56/6011/28/2	nakte	1pc-0475903e7122050253.	10.1.0.024	251		ap-south-tax	aps1-az1	10-0634(2)(9)	605673e	
WIRTUAL PRINATE		sabret-3et	912	avalatie	spc-a41a0ttc	172.11.0029	401		ap-south-18	aps1-az3	rb-t3betH		
the VPCs		subret-808	outh	maistie	vpc-odla00cc	172,31,05,020	4081		10-1047-11	aps1-az2	rb-d3beet6		
Subrets		salmet d25	66838	sisiste	spc=64180000	172.31.32.020	4081		ap-scelt-1a	eps1-ez1	rb-03bed8		
Route Tables	Subret: subret-01e	0.564(1).09	2	-			0.01	-				85	1
Egress Only Internet Gateways	Description	Row Logs	Route Table	Network	AQL Taps	Shuring							
DHCP Options Sets www		Subret 10	sahrer 4062/50607	1282				Sale	NEDT				
Elastic Ps		(PC	10.475881.008	0c817WS 50	E			IPv4 CDR	30.10.004				
Managed Prefix	Analubie IP	vi Addesses	20 month is best or	-				Pri CDR	an Allow I allow the Party				
Lister		Network ACL	KIONESSISTER	4				Debuit subnet	No.				
Endpoints	Auto-analg	n public Pol	10				Artes	nige IPv6 address	10				
Endpoint Services		address											
N4T Gateways		Outpost ID						Owner	E7854547349				

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

🔒 literiet gateways (VPC - X - +	÷												1
€ → @ @	🖲 🔒 https://ip-south-1.consile.avs.ar	ador con Apo hone (region-ap-so)	ti-l≢pis						- 🛛 🕁	ź	R.		
evices +	Resource Groups 🗸 🖌							۵	Kenver Abhinav •	Natbi +	Supp	nt •	l
New VPC Experience Manufactures	(IPC) isternet patievojs												0
VPC Dashboard New	Internet gateways (1/2)	n					C	Actions 1	Create in	arnet gatewa	r.		
Q Select a VPC	Q, Filter internet johnneys									(1)	0		
VIRTUAL PRIVATE	Nama T	Internet gateway ID	7 State	Ŧ	VPC ID		Owner				7		
Your VPCs Subrets	0	iga 645chdix	() Attach	8	vpc-atta0dec		678894647549						
Route Tables	ANS-SIDE-KW	ign=066c76c90d25c14	⊘ Attach	¢.	vp:44759667a286a03 AVS 5	R	E78854647549						
latemet Gateways Inc												_	
Egress Only internet Gateways Inv	igw-016dc7dcc90x025c14 / AWS-S	DE-IGW								8		8	
DH CP Options Sets new	Details Tass												
Elastic Ps 🐜													
Managed Riefx Lists tee	Details												
Endpoints													
Endpoint Services NAT Galeways	internet gateway/D 🗗 igw-0f6dc7dx:90025c14	Stater Ø Attached			1PC ID 1pc 4475968e76286605	AWS SI	x	Owner 🗗 87885464	0349				

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

Route Tables VPC Marin X	Ŧ													
€ ⇒ ¢ ≙		() 🔒 https://ap-so	off+1 consideran	s anazon.co	niqohote?	egion-ap-south-]#	Rodel alles sof-mode la	961			🗟 🖞	ź	10 1	8 3
aws services	*.	Resource Groups	× 1							1	🗘 KennerAblicos 🔹	• Munitai • Supp		,
New VPC Experience Bill and a particle	1	Create route table	Actions *										0 (• 6
VPC Dashboard See		Q, Filter by Laps and	atchine or som	t ty knywció) ({ 1b	030f3 (
Fiber by VPC		Name -	Route Table I	0	• Exploit	abret associatio	Edge associations	Van	VPC D	Owner				
· · · · · ·			10-0634:3:65	1096798				Ns	vpc-0479988e7x208a0c9.	878854547348				
VIRTUAL PRIVATE		ANS-ROUTE	r6-06362233	2417238	sainet-0	1256671692		10	yp-0479968e7u288a0c9	678894647349				
Your VRCs			rth-dilibeebi					165	spr-silja0dz	878854647349				
Subnets														
Route Tables														
internet Gateways 🗤		Route Table: rb-0d3	b1222c34ff19e											80
Egress Only Internet Gateways two		Sureary	Routes	Sitre: A	accations	Edge Associations	Route Propagation	Taps						
OHCP Options Sets two														
Electic (PS New		Ri Explicitly Ass	exte Table D i di sociated with i si	hendelse berikelse	4014282				Main To VPC vpc-047586	60,260,9 105	SIDE			
Wanaged Prefix			Owner E	1854547349										

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.

🔒 Route Tables VPC Marx X	🔒 ips (VPC Management): X 🔸	F.							6
€ → @ @	0 🛔 https://up-southeast-1.o	rsole avs anaton com ly	pohane?regior=ap-southeast-14kpcc;	at=lipld			- 🗟 🕁	ź	N 0 8 E
allis Senites	🗸 Resource Groups 🔹 🕇						🗘 tanar Khaw •	Segger •	Suppt +
New VPC Experience Microsoft you think	Cross IPC Actors Y								000
VPC Dashboard Me	Q. File by lags and administra	which by improved						K (1	to 2 of 2 🔅 🕅
Filer by VPC	Name - VPC D	• S28	· INVICER INVICER	DHCP options set	Main Rou	te table	Main-Network ACL	Tenancy	- Default VPC
Queensive.	CUSTONE. 100-0978	TTb5c490die4 main	★ 112.005 ·	dop=131b1154	rts de Tale	x54100.0%	ad-00083407a6012c	default	10
VIRTUAL PRIVATE		750 evela	₽ 12224	dop/301154	10-10732	20	ad-5250574	delaalt	ю
Your VPCs	VPC: qc-05%7/b6x480de4			101					880
Subrets Route Tables	Description CDR Bloc	o Plon Lops	bp						
internet Gateways New Egress Only Internet Gateways See	UPC E State	nga GETTETTESa ABISHA Mashadin Mashadin			Tenancy Default VPC	istad No			
DHCP Options Sets 🗤	PHOD				Pró Pool	-			
Elastic PS See	DIS resolution	Enabled			Network ACL	x100540412			
Wataged Pieta Lists two	DNS kostname CassicLink.DNS Suppor Owner	Dualed Dualed ETES464T045			DHCP options set Route table	10-017540400056			

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.

E - C & G	a https://ap	-southeast-Learning and	negat.com/ccl/35	one ⁷ mpontap-southeast-IBLaurchinstanceWized		*	10.5
and a				2010 Contraction of the Contract			
Senios - I	Resource on the	uja v te		ų	GEAR APPENS *	Sappes -	Supp
L Chorse AMI L Chorse instance Type	3. Configure	Indance A, Add Scrapt	LANDAR C.D	Infigure Security Circup T. Review			
Step 3: Configure Instan	ice Details	5					
Configure the instance to suit your requir	reevents. You ca	e launch multiple instances (tom the same AM, o	equest. Spot instances to take advantage of the lower prising, assign an access management role to the instance, and more.			
Number of instances	(k)		Laureh wo Auto Sa	aling Grap 👔			
Purchasing option	0 Da	equest Spatiestances					
Metavork	(i) upor	ostristritiscellouillee CUSTI	NER END	C Create new VPC			
Subret	(i) (s.be) 251 F	ei-08278e8c711478983 CL P Addresses svalatie	STOMER-SUBNET	Create new subset			
Auto-assign Public IP	(j) Erab	ie .	,				
Placement group	() D4	lifivelance to placement gro	φ				
Capacity Reservation	(i) Opp	n	;	C Criste new Capado Reservation			
UAM role	() Nore		,	C Criste Her Will role			
Shutdown behavior	() (Sap						
Stop - Hibernate bohavior	 (i) Dr 	uble hibernation as an adde	ional skip behaver				
Enable termination protection	() 🗇	tect against accidental terr	rination				
Monitoring	() () A555	whie Chudiwach detailed in Ional charges apply	initaling				
Tenarcy	(i) Shan Addi	od - Ran a shared hardusre local charges may apply who	instance 3 In launching Dedicate	el instances.			
	(i) (i)er	while .					

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.

⊌tzj ⊻tili G Q Kanar Bibare - Sappare - Sapp
▲ Konar Hitter • Support • Support
in server and also threezer traffic to reach one instance with order they direct
de manues and allow between bodies to reach usure instances, add order their allows
n sene ann ann frienn cuns ar four yn roanne, au in an ann d
Description ()
20 e.g. SSH far Admin Desktop
x0 e.g. SSR for Admin Desktop
20 e.g. SSH far Admin Deskop

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 \rightarrow 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.

🔋 Virtual Private Gateways 🗆	X	Instances EC2 Manager X +								
€ → ሮ ≙		🕼 titpsåpsads Loosies	vs anzoncon lipchone	hegion=op-south-13	Apr&aangssot=1p	Geneyd			- 🛛 🟠	¥NO\$
aws senio	5 v	Resource Groups 🖌 🕴							🕽 KnerAlira	• Kerbä • Suppet •
Nev VPCExperience Billis with you this		Create Virtual Private Gateway	Actions V							0 ¢
Endpoints		${\bf Q}$ Film by tape and attributes a reso	ch by keywood) (101d1)
Endpoint Services	-	l kane -	D	• 强	lpe	- 190		• ASN (Amazon side) •		
NAT Gateways Rearing Connections		ANS-SIDE-GN	np=10134434ea84	nonj	psc.1	pp:0475886728603/A	NS SIZE	9512		
v SECURITY lietwork ACLs Security Groups New		Virtual Private Gateway: xpx-1157. Details Tags	Misleni)							
VIRTUAL PRIVATE Network (VPN)		D Tpe	gelittiskaskesk peri				Sale	ecity gr.4758672603-485	Œ	
Customer Gateways Virtual Private Gateways Sile-to-Site VPN		KSN (Anazon side)	ME							

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 it MUMBAIname as 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.

VPN Connections VPC	X	Subrets	VPC Managerii: X	+					
€ → @ ≙		0 4 Im	ps://ap-south-1.com	iste avs anzon	.com/ipch	one/hegion=ap-south-1#VgnCorrections sort=VgnCorrection)		- 🛛 🕁	± N ⊡ \$
aWS Servic	5 v	Resourc	eGroups 🗸 👌	ł				👃 Ruma Abinar 🔹	Nunbá • Support •
New VPC Experience Rel to what you think		Create VPI	N Connection	Download Config	pution	Actions *			0 Ø
Endpoints		Q, Filet	y tags and attributes	or seach by keyw	ú				$\ \langle$ (1010f1 \rangle
Endpoint Services	Ţ	Nan Nan	e - VPN E)	• San	+ Virtual Private Galeway + Transit Galeway		- Customer Gateway -	Customer Gateway Addre
NAT Gateways	NUMBALS., yp-Matellitheldith pering op/UtilisMaskaak/AUS., - op/UtilisMaskaak/AUS.,								18 139 229.4
Peering Connections		VPN Conne	ection: ipn-04a9el	0.7fbe8c4d7b					
V SECURITY									
Network ACLs		Details	Tunnel Details	Static Routes	Taps				
Security Groups tex									
VINTURE BARLINT			191	ID vpr-0439403	76864676		State	pending	
NETWORK (VPN)		1	Virtual Private Gates	way von-lottle	its Mession	RWS-SIDE-GW Dustomer	Gateway	ogwith/tecolwElect//CGANS-SI	ίξ.
Curtanar Colourum			Transit Gate	ny ·		Customer Galeria	Address	18 139 228 4	
cromite ogenelje			1	pe ipsec1			Category	VAN	
Virtual Private			y	PC VIC-UPSEE	elaxisads	AWS SIDE	Routing	State	
Gateways			Acceleration Enab	led falle		Automical	ion Type	Pre Stated Key	

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 = 1net.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 IDpublic 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.

I II II CARECULAS VIC. A	instances	EC2 Manageri X 🕂							
e) → @ @	0 🛔 ttp	i Rep-south-1 conside.ave	anazat con lochone hegines	p-south-1#liprC	onectors sof=lprContectorid		6	1 û	ź∦ 5
aws Services	 Resource 	Groups 🗸 🕨					₿ Ken	eer Abhinau 🔹	Nurba • Supp
New VPC Experience Tel scatter you think	Create VPI	Correction Doumlea	i Configuration Actions V						0
1. I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I	Q FRITE	tops and attributes or search	ty keyverd .						K < 1016
VIRTUAL PRIVATE	Barre	+ YPN D	• State • Vin	sei Prinzile Galerna	y · Transk Galeway	 Castorier Gideway 	Customer Gateway Address	· 1jpr	- Calegory
Your VPCs	N.A5	AISL VINESSORE IN	istats waiste ege	0802143307	:(#W5., -	speila/72/200	737(05., 183422528	iper.1	YPN
Subrets Route Tables	_	_		_		_	-		
Internet Gateways Inc	VPN Conne	diam: vpn-0564046749035	ét25						
Egress Only Internet Gateways Ima	Deals	Turnel Details State	Routes Tags						
Egress Only Internet Gateways Ima DHCP Options Sets Ima	Details Tunnel St	Turnel Details State	Houtes Taps						
Egress Only Internet Gateways Ion DHCP Options Sets Ion Elastic PS Ion	Details Tunnel St	Turnel Details State	Acutes Taps						
Egress Only Internet Gateways Imm DHCP Options Sets Imm Elastic Pis Imm Managed Perfix	Deals	Turnel Detuils Stats	anats lags						(102d2)
Egress Only Internet Gatessiys Ison DHCP Options Sets Ison Elastic P3 Ison Managed Perfix LLSS Ison Endocints	Disals Turnel St Turnel N	Turnel Details Statu atte atter Cuttale P	Houtes Tops	States	Satus Last Charged	Deals	Certificate ARM		< 1102012 >
Egress Only Internet Gateways Iwa DHCP Options Sets Iwa Bastic PA Iwa Nanaged Pedra Lists Iwa Entpoints Entpoints Entpoints	Disais Turnel St Turnel I Turnel 1	Turnel Details State	Address Inside IP COR 16 201 25 42 30 23	States UP	Status Last Changed July 14, 2020 at 218-221-040 UTC-5-28	Deals	Certificate ARM		(1020/2)

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.

							Mumb	NRagionEC	-2100	tanca	
							Mump	airegionec	. zins	tance	
uas r	III VI	LUGL	Comman	IU HOL	Tound.	1	4	e a i da Kau			07 130
The	outh	optic	12003 S.	host 11	la bas	550	120 (12	222 107	120	r.pem ecz-user@13.233.1	97.138
ECD	SA ke	v fin	acorio:	ie Si	10256.0	lar5	130 (13	233.19/	1 4 4	sy can t be established	
ECD	CA ka	y fin	gerprin	t is M	1A250.0	and 1	. 9d. 9d.	bf:02:57	122	00:55:70:07:26:00:14	
Are	VOU	sure i	Gerbitu	t to co	ntinue	500	necting	lves/no	12 1	.ee.55.70.03.50.ec.14.	
War	nina	Derm	anently	added	113 23	2 10	7 128'	(ECDSA)	to	the list of known hosts	
Thi	e eve	tem i	s not re	aduced	red to I	Red	Hat Ins	ights S	ee l	https://cloud_redbat_com	1
To	reals	ter ti	his syst	tem, ri	in: ins	ight	s-clien	t regi	ster	r	e .
	regis		113 393	cem, re		gine	a criten	e regi	3		
[ec	2-use	r@ip-	10-1-0-3	246 -19	s ping	10.2	.0.175				
PIN	G 10.	2.0.1	75 (10.)	2.0.17	5) 56(8	1) b	vtes of	data.			
64	bytes	from	10.2.0	175: 1	cmp se	1=1	ttl=254	time=58	.8 1	ns	
64	bytes	from	10.2.0	175: 1	cmp se	1=2	ttl=254	time=58	.9 1	ns	
64	bytes	from	10.2.0	175: 1	cmp se	1=3	ttl=254	time=58	.8 1	ns	
64	bytes	from	10.2.0	.175: 1	icmp se	1=4	ttl=254	time=58	.8 1	ns	
64	bytes	from	10.2.0	.175: 1	cmp se	1=5	ttl=254	time=58	.9 1	ns	
64	bytes	from	10.2.0	.175: 1	icmp se	1=6	ttl=254	time=58	.8 1	ns	
δ4	bytes	from	10.2.0	.175: 1	cmp_se	q=7	ttl=254	time=58	.8 1	ns	
64	bytes	from	10.2.0	.175: 1	cmp se	3=B	ttl=254	time=58	.9 1	ns	
δ4	bytes	from	10.2.0	.175: 1	cmp_se	q=9	ttl=254	time=58	.9 1	ns	
54	bytes	from	10.2.0	.175: 1	icmp_se	7=10	ttl=25	4 time=5	9.5	ms	
54	bytes	from	10.2.0	.175: 1	icmp_se	1=11	ttl=25	4 time=5	8.9	ms	
64	bytes	from	10.2.0	.175: 1	cmp_se	1=12	ttl=25	4 time=5	8.8	ms	
54	bytes	from	10.2.0	.175: 1	cmp_se	q=13	ttl=25	4 time=5	8.9	ms	
^C											
	10.2	.0.17	5 ping :	statist	tics	100					
13	packe	ts tra	ansmitte	ed, 13	receiv	⊵d,	0% pack	et loss,	tir	ne 21ms	
rtt	min/	avg/m	ax/mdev	= 58.7	155/58.1	391/	59.471/	0.334 ms			
lec	2-use	r@1p-	10-1-0-2	246 -]	6 clear						
fec	2-1150	rain.	10.1.0.	246 ~14							
Lec	2-1150	r@in-	10-1-0-1	246 ~14							
Lec	2-450	i GTh.	10-1-0-1	140 14							

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.techwe ekeurope.co.uk/cloud/cloudmanagement/amazon-web-services-publiccloud-185687 [2]."Amazon Web Services(AWS)."https://AWS.amazon.com/ma **rketplace** [3]. L. Wang, G. Laszewski, M. Kunze and J.Tao, —Cloud computing: a perspective study^I, J New Generation Computing, 2010,pp 1-11. [4].https://en.wikipedia.org/wiki/Amazon_We **b** 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 Cloud Benefits of Computing ||, http://cloudsecurity.org/blog/200 8/07/21/assessing-the-security-benefits-ofcloud-computing.html [10]. Getting Started with Amazon Redshift -

by Stefan Bauer.

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