**VIRTUAL PRIVATE NETWORK (VPN)**

**STEPS**

1. CREATE VPC-1 – NAME – AWS SITE (IP: 10.1.0.0/16)
2. CREATE VPC-2- NAME- OFFICE SITE (IP: 10.2.0.0/16)
3. CREATE SUBNET -1 (IP: 10.1.1.0/24)
4. CREATE SUBNET -2 (IP: 10.2.2.0/24)
5. CREATE INTERNET GATEWAY = ATTACHED VPC-1-AWS SITE
6. GOING TO ROUTE TABALE – ATTACHED INTERNET GATWAY –VPC1-AWS SITE
7. LAUNCH INSTANCE –VPC-1-PUB-WITH-ICMP ALL -(OFFICE SITE IP: 10.1.0.0/16)
8. LAUNCH INSTANCE –VPC-2-PVT-WITH-ICMP ALL -(AWS SITE IP: 10.2.0.0/16)
9. LAUNCH INSTANCE-WITH-LINUX-2-AMI – AWS-PUB
10. LAUNCH INSTANCE- WITH-LINUX-2-AMI-OFFICE-PVT
11. GOING TO VPN -> CREATE CUSTOMER GATEWAY -> PUT AWS SITE INSTANCE PUBLIC IP -> AND CREATE
12. GOING TO VIRTUAL PRIVATE GATWAY -> CREATE VIRTUAL PRIVATE GATWAY -> OFFICE SITE VPC
13. CREATE VPN CONNECTION -> ATTACHED VPN -> Virtual private gateway-> Customer gateway ID🡪Routing options---> STATIC IP AWS SITE (IP: 10.1.0.0/16)
14. GOING TO VPN -> SELECTE OPTION DOWNLOAD CONFIGURE -> SEARCH OPENSWAN AND DOWNLOAD
15. GOING TO PUBLIC INSTANCE -> YUM UPDATE –Y -> SUDO YUM INSTALL OPENSWAN –Y
16. sudo vim /etc/sysctl.conf -> paste 3 line
17. net.ipv4.ip\_forward = 1
18. net.ipv4.conf.default.rp\_filter = 0
19. net.ipv4.conf.default.accept\_source\_route = 0 -> SAVE CHANGES
20. sudo sysctl –p
21. sudo systemctl restart network
22. sudo vim /etc/ipsec.conf -> open and uncomment last line
23. create new file sudo vim /etc/ipsec.d/aws.conf -> paste com tunnel 1 block and delete auth-esp option
24. create new file sudo vim /etc/ipsec.d/aws.secrets and paste configur line number -5 -> save
25. sudo systemctl restart ipsec.service
26. sudo systemctl restart network
27. going to aws -> route table -> select office route table -> route propagation -> enable -> save
28. sudo chmod 600 key-name
29. ssh –i key-name ec2-user@private-ip
30. ping ---- private ip