Networking in AWS - Part 2

Advanced Networking

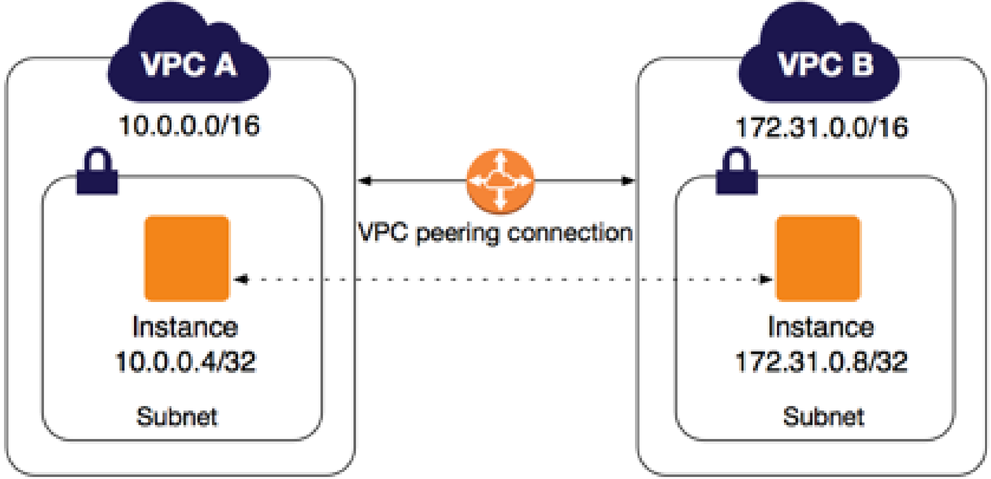
By Chetan Agrawal

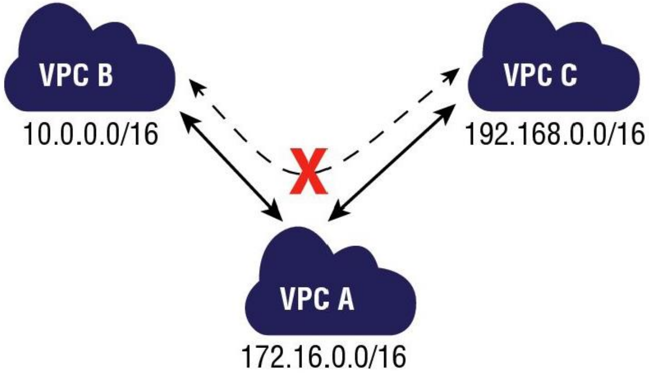
Inter VPC communication - VPC Peering

- Enables private communication between 2 VPCs
- Can connect single VPC to multiple VPCs

Limitations:

- CIDR should be Non-overlapping
- Only one peering between given 2 VPCs
- Peering connection is **not transitive**





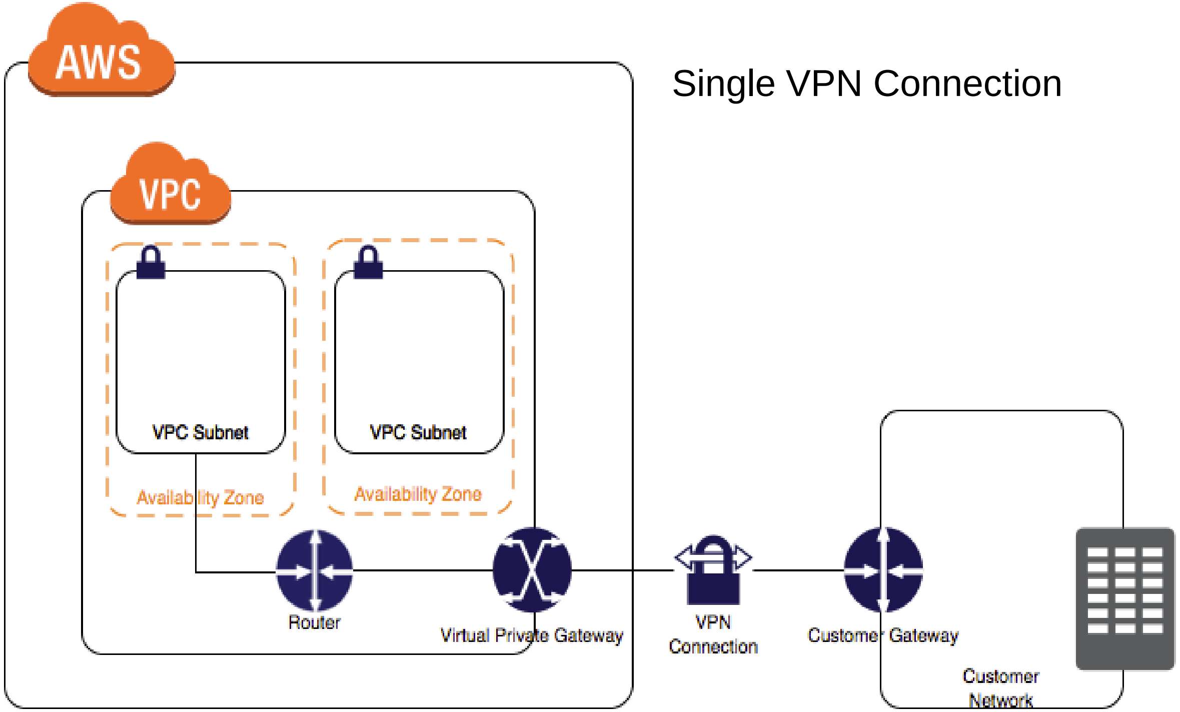
Setup VPC Peering

1. Create VPC B in same region or another region
2. Create Private subnet and private route table in VPC B
3. Launch EC2 instance in private subnet. Security group to all connection from VPC A CIDR (10.100.0.0/16)
4. In Mumbai region -> VPC -> Peering Connection -> Request a new peering connection from VPC A to VPC B in N. Virginia region
5. In N.Virginia region -> VPC -> Peering Connection -> Accept the request
6. For VPC B private route table, add route for VPC A (10.100.0.0/16) and target should be VPC peering connection
7. For VPC A public route table, add route for VPC B (172.31.0.0/16) and target should be VPC peering connection
8. Try to connect to EC2 in VPC-B) from EC2 in VPC-A (You need ssh key for ssh connection)

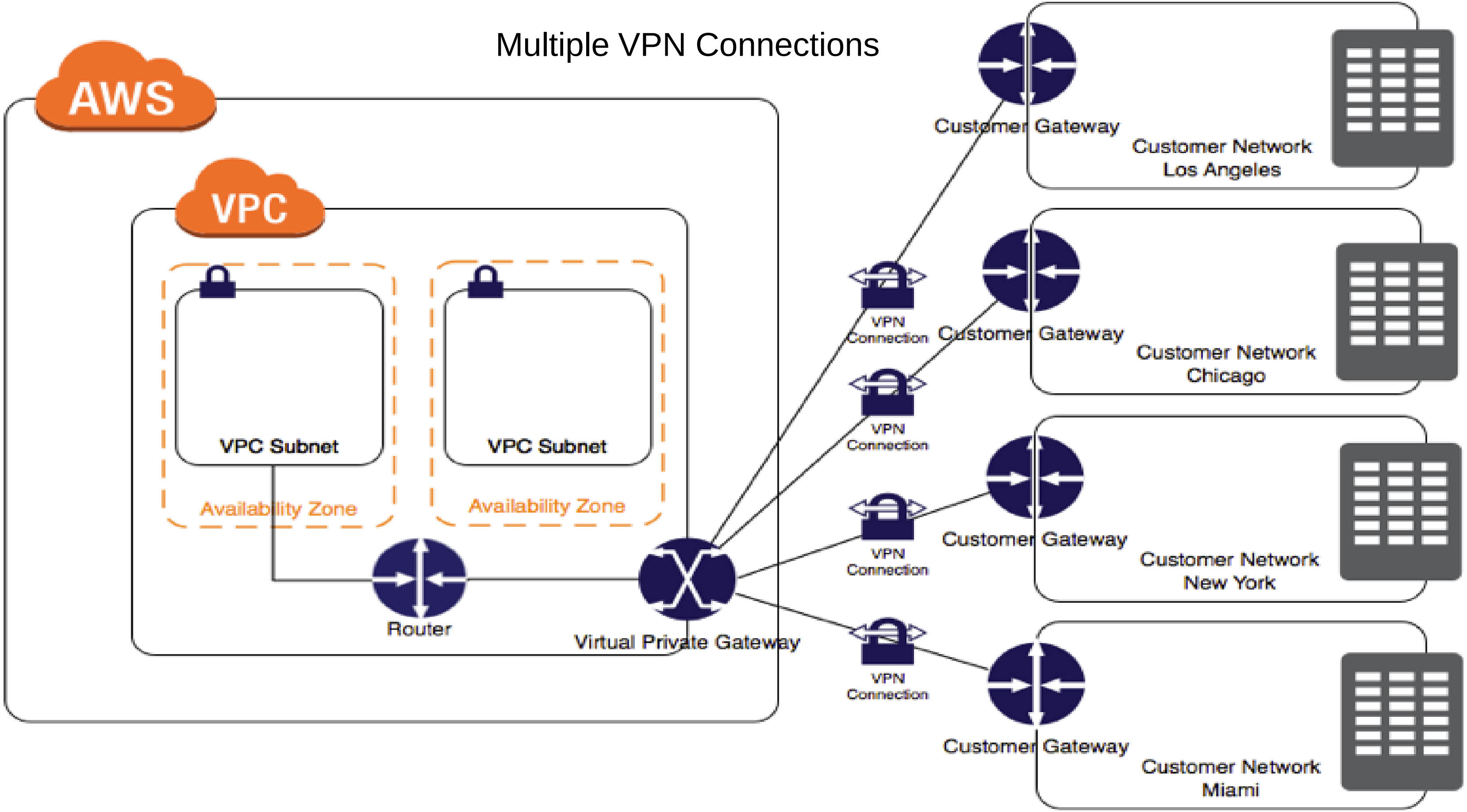
AWS VPN Connections

- AWS Virtual Private Gateways (VGW)
- Customer Gateways
- VPN Tunnels

Single VPN Connection

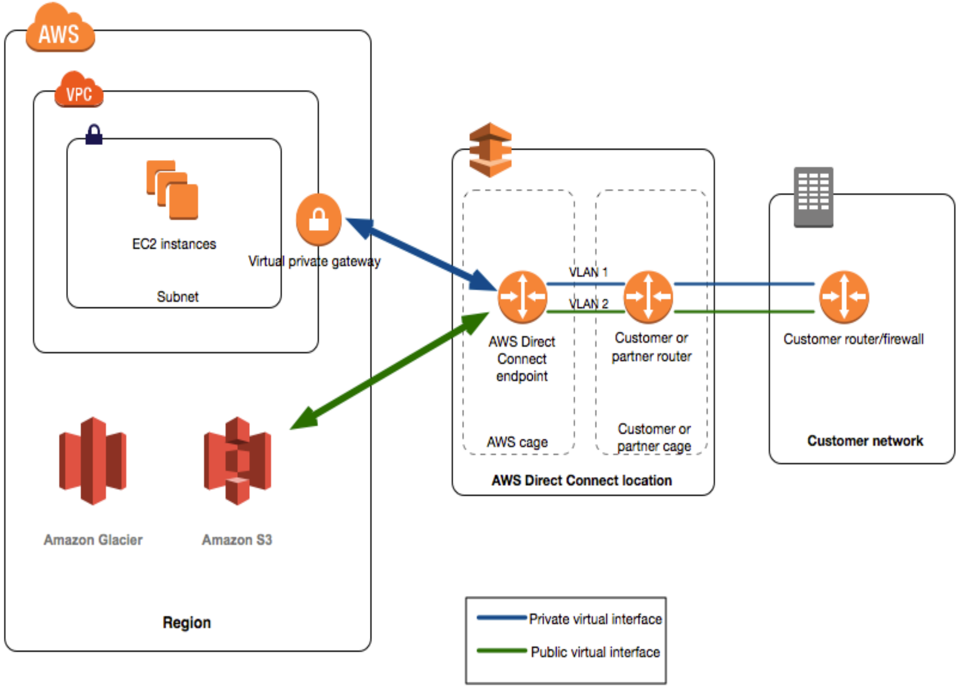


AWS VPN Connections



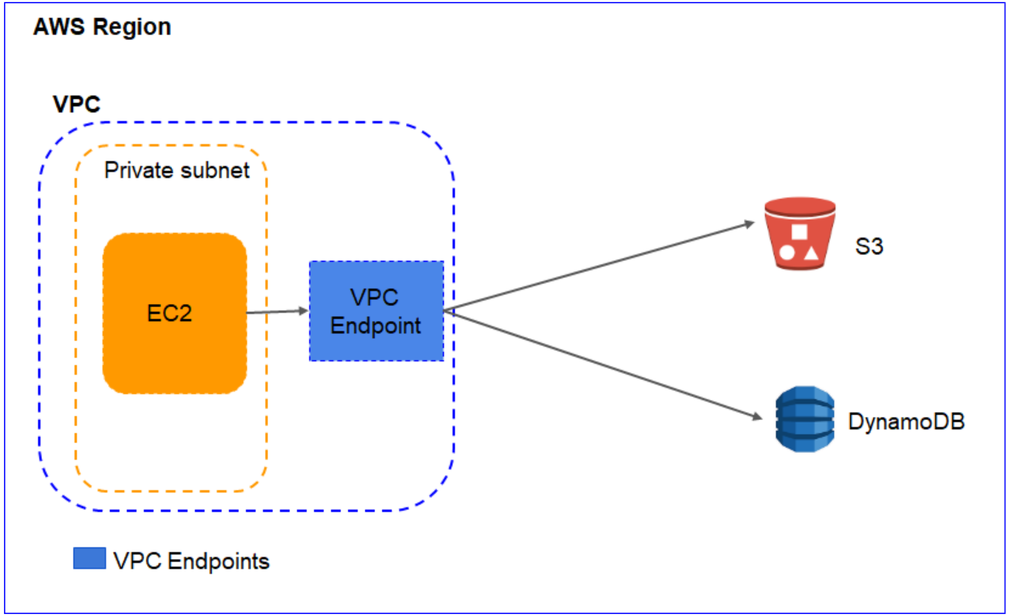
AWS Direct Connect

- Dedicated network connection from on-prem data center to AWS
- Consistent network bandwidth and throughput
- Available in 1 Gig or 10 Gig bandwidth from AWS
- Sub-1 Gbps service from Direct connect partners
- Where Direct connection location is not available, can choose partner network
- 802.1Q VLAN, 1500B MTU
- eBGP



VPC Endpoint

- Private connection between VPC and AWS services
- Currently supports AWS S3 and DynamoDB connection in same AWS region
- Should add corresponding route in Subnet route table



Benefits:

1. NAT not required.
2. Very low cost.
3. Scales automatically

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1dd132211
pl-1a2b3c4d	**vpce-11bb22cc**

VPC Flow logs

- Captures IP traffic information going in/out of network interfaces inside VPC
- We can enable Accept, Reject or All traffic to be captured by flow logs
- Flow logs data can be published to S3 or Cloudwatch Logs
- Flow logs can be created for VPC, a subnet, or a network interface
- Flow log record format:

<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action> <log-status>

Exam Tips

1. VPC is isolated logical network space in AWS
2. VPC contains Subnets, Route tables, SGs, NACL, VGW, Peering, Endpoint
3. Single subnet = Single Availability Zone
4. By default subnet gets associated with VPC main route table and default network ACL which allows all inbound and outbound traffic
5. Custom Network ACL denies all inbound and outbound traffic
6. Security group vs Network ACL (state, level)
7. No transitive VPC peering
8. NAT instance enables internet access to instances in private subnets
9. For NAT instance, you must disable Source/Destination Check
10. NAT traffic depends on underlying instance type. Scale vertically.
11. NAT gateways are managed by AWS. Scales upto 10 gbps

Review Questions

Review Questions

1. What is the minimum size subnet that you can have in an Amazon VPC?

A. /32
B. /24
C. /16
[✓ D. /28]

Review Questions

2. You are a solutions architect working for a large travel company that is migrating its existing server estate to AWS. You have recommended that they use a custom Amazon VPC, and they have agreed to proceed. They will need a public subnet for their web servers and a private subnet in which to place their databases. They also require that the web servers and database servers be highly available and that there be a minimum of two web servers and two database servers each. How many subnets should you have to maintain high availability?

A. 3
B. 1
C. 2
[✓ D. 4]

Review Questions

3. Which of the following is an security control that can be applied at the subnet layer of a VPC?

A. [✓ Network ACL]
B. Security Group
C. Firewall
D. Web application firewall
E. VPC flow logs

Review Questions

4. You create a new subnet and then add a route to your route table that routes traffic out from that subnet to the Internet using an IGW. What type of subnet have you created?

A. An external
B. Internal
[✓ C. Public]
D. Private
E. Outgoing

Review Questions

5. You create a new VPC in US-East-1 and provision three subnets inside this Amazon VPC. Which of the following statements is true?

A. By default, these subnets will not be able to communicate with each other; you will need to create routes

B. All subnets are public by default

⇨ C. All subnets will be able to communicate with each other by default

D. Each subnet will have identical CIDR blocks

E. All subnets with same CIDR will be able to communicate with each other

Review Questions

6. What aspect of an Amazon VPC is stateful?

A. Network ACL

[✓ B. Security Group]

C. VPC flow logs

D. Route Table

Review Questions

7. You have created a custom Amazon VPC with both private and public subnets. You have created a NAT instance and deployed this instance to a public subnet. You have attached an EIP address and added your NAT to the route table. Unfortunately, instances in your private subnet still cannot access the Internet. What may be the cause of this?

A. Your NAT is in a public subnet, but it needs to be in a private subnet

B. Your NAT should be behind an Elastic Load Balancer

C. You did not open security group inbound rule for internet traffic

⇨ D. You should disable source/destination checks on the NAT

Review Questions

8. How many VPC Peering connections are required for four VPCs located within the same AWS region to be able to send traffic to each of the others?

A. 2
B. 4
[✓ C. 6]
D. 8

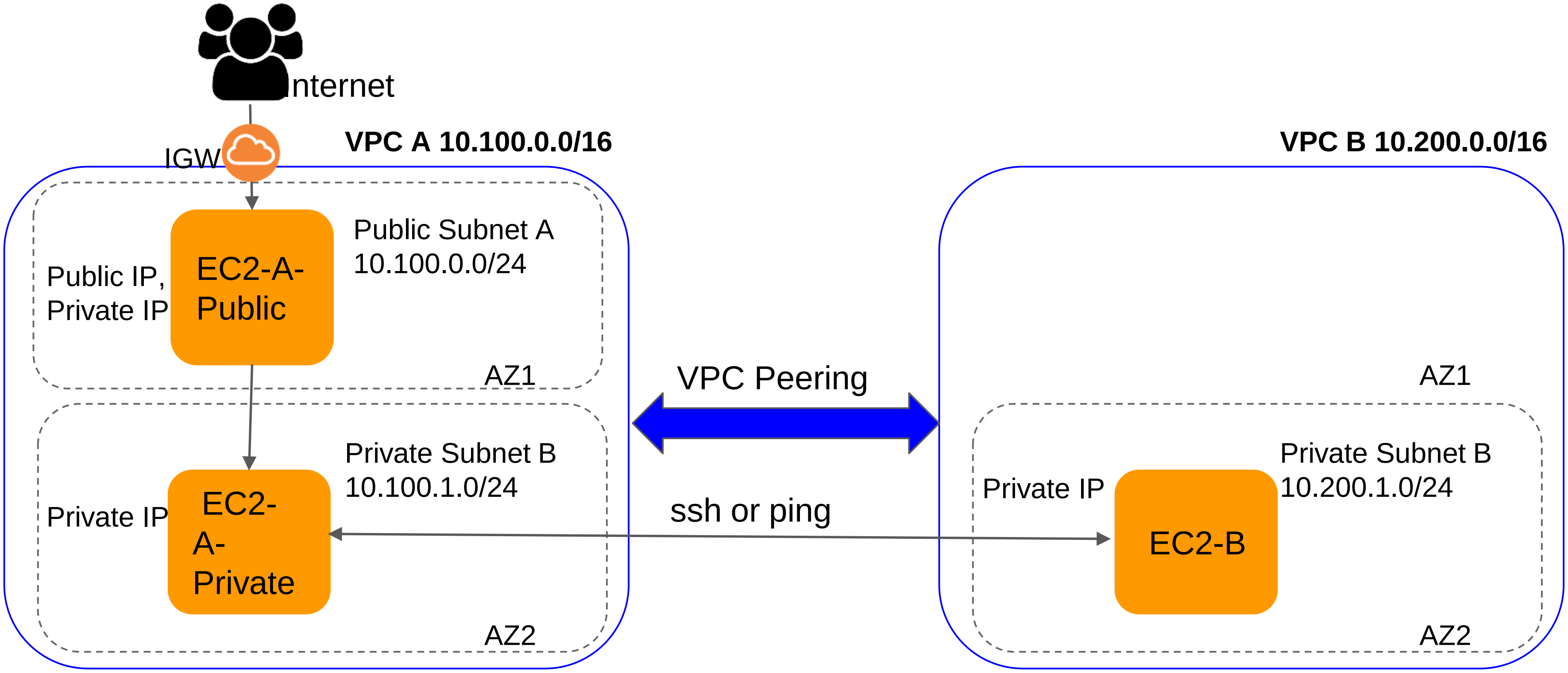
Review Questions

9. You are responsible for your company’s AWS resources, and you notice a significant amount of traffic from an IP address in a foreign country in which your company does not have customers. Further investigation of the traffic indicates the source of the traffic is scanning for open ports on your instances. Which one of the following resources can deny the traffic from reaching the instances?

A. Security group
B. NAT instance
[✓ C. Network ACL]
D. Amazon VPC endpoint

Assignments

Assignment 4 - VPC Peering

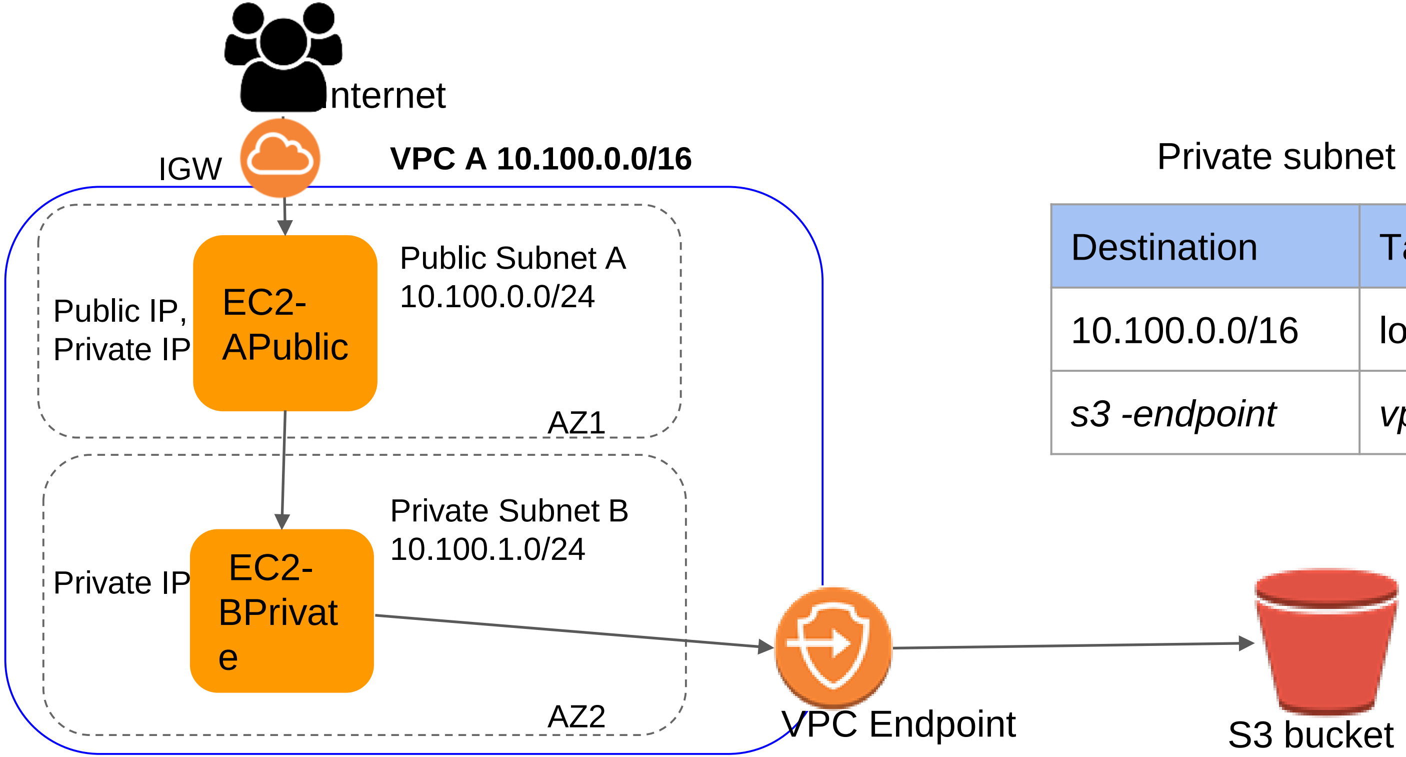


Assignment 4 - VPC Peering

1. Create 2 VPCs - VPC-A and VPC-B with non-overlapping CIDR range
2. Create 1 public, 1 private subnets in each VPC-A
3. Create 1 private subnet in VPC-B
4. Create 1 instance in each VPC in subnets created above.
5. For VPC-A Public EC2 instance open security group 22 for your Public IP (Myip)
6. For VPC-A Private EC2 instance open security group 22 for VPC-A public subnet CIDR
7. For VPC-B EC2, open security group to allow port 22 and ICMP from other VPC-A private subnet CIDR
8. Login (ssh) to VPC-A Public EC2 instance. From there connect to VPC-A Private instance.You should be able to connect. (You need to have ssh key)
9. From VPC-A Private EC2, try to connect to VPC-B EC2 over Private IP. Does not connect.
10. Now create VPC peering between VPC-A and VPC-B.
11. Accept peering request from requested VPC-B
12. Modify route tables for both the subnets and add corresponding routes. i.e in VPC-A Subnet route table add route for destination as VPC-B CIDR and vice-a-versa.
13. Now try again to connect or ping from VPC-A EC2 to VPC-B EC2 using **Private IP**. You should be able to connect/ping.

Watch Video

Assignment 5 - VPC Endpoint



Private subnet route table

Destination	Target
10.100.0.0/16	local
s3 -endpoint	*vpce-id*

Assignment 5 - VPC Endpoint

Watch Video

1. Create VPC in **Mumbai (ap-south-1)** region (as we will be accessing s3 bucket in same region)
2. Create 1 public, 1 private subnets in each VPC
3. Create 1 instance in each subnets created above. Say EC2-A is public EC2 created in public subnet and EC2-B is private EC2 created in private subnet.
4. For EC2-A instance open security group 22 for your Public IP (Myip)
5. For EC2-B instance open security group 22 for public subnet CIDR
6. Login (ssh) to EC2-A instance. From there connect to Private instance EC2-B.You should be able to connect. (You need to have ssh key created locally on EC2-A)
7. From EC2-B, try to download some contents from public s3 bucket (see command below). Does not connect/download.
8. Now create VPC endpoint for s3 endpoint into your VPC. (VPC -> Endpoints)
9. Modify route tables for **Private subnet** and add corresponding routes to route s3 traffic through VPC endpoint.
10. Now try again to download contents from public s3 bucket. You should be able to download.

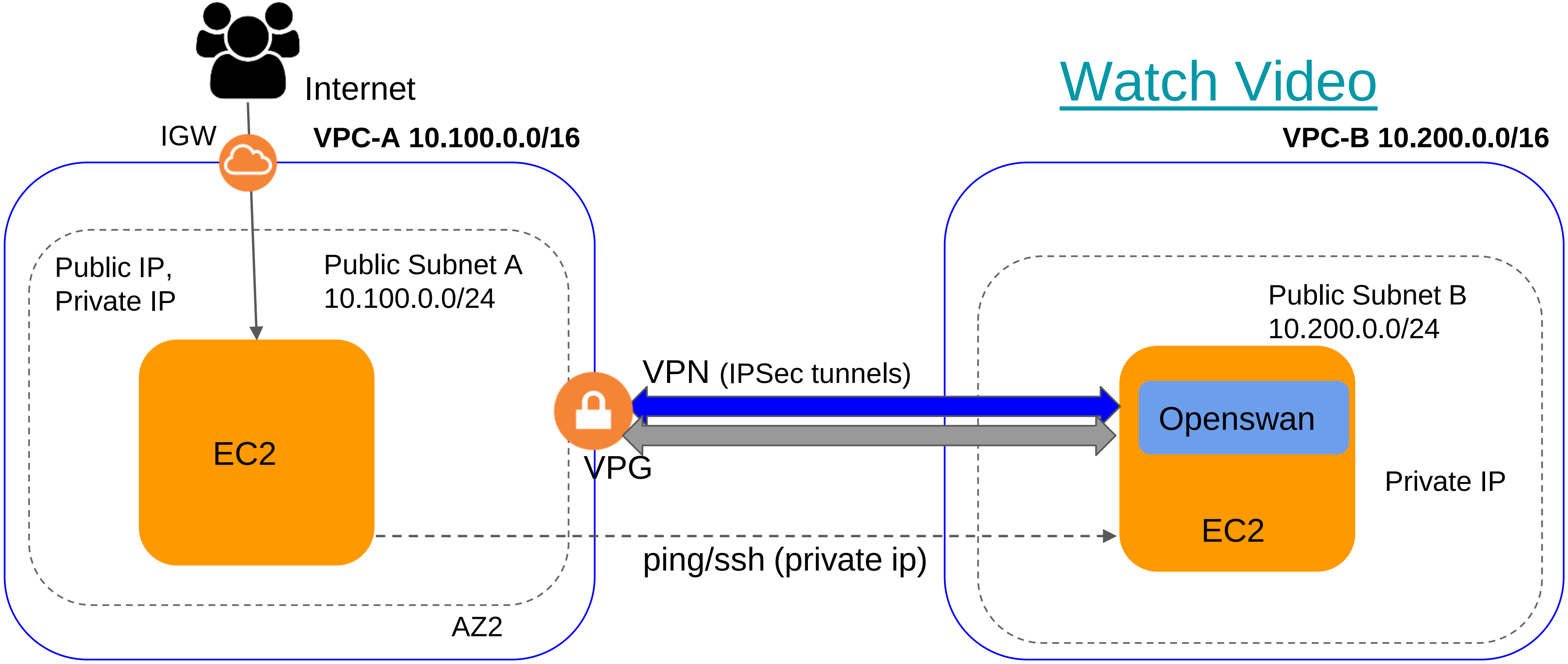
Command to download s3 content:

```
$ wget https://s3.ap-south-1.amazonaws.com/kvriksh.com/index.html
```

Assignment 6 - VPN Connection (going extra mile)

kvriksh

Watch Video



Mumbai Region

N. Virginia Region

Follow this document to implement the VPN connectivity: How to setup VPN connection

Assignment 7 - Going extra mile

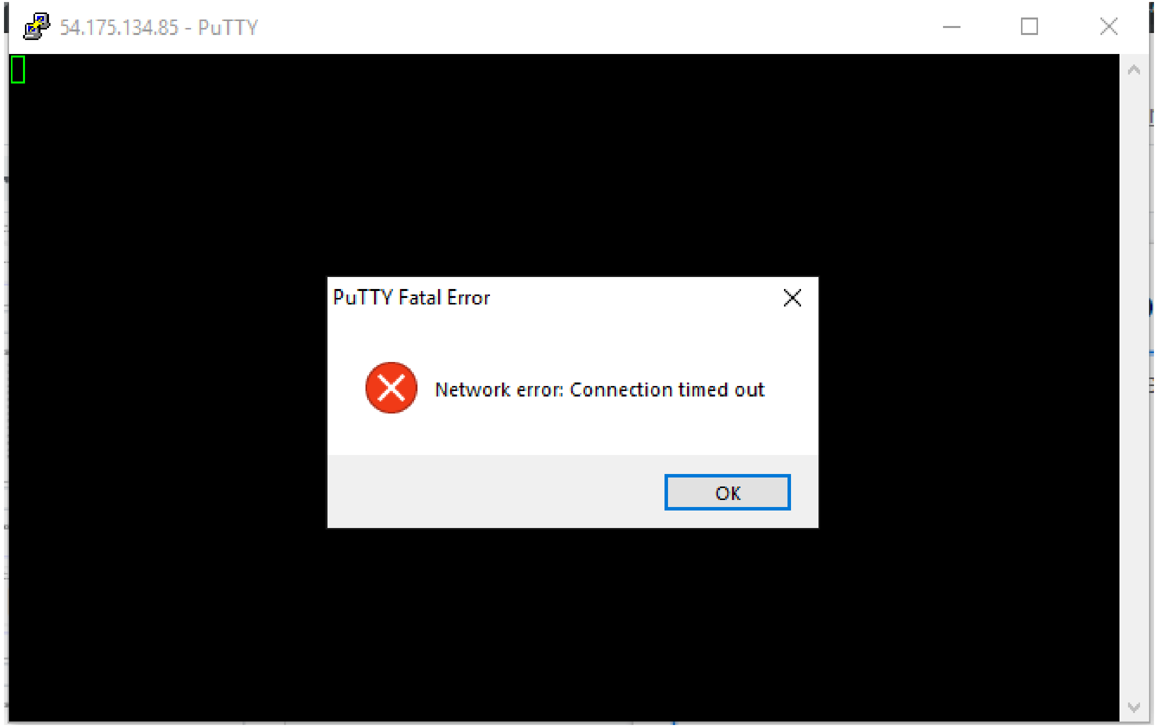
1. Read through this document to understand about NACL rules and Ephemeral ports: https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_NACLs.html

1. Understanding VPC Peering, use cases, limits and invalid scenarios https://docs.google.com/presentation/d/1yNFkt6NB7DCIQ7ZuCoETbXshX0_Qh1cbZMDw4X8W580/edit?usp=sharing

   Watch Video

Appendix: Troubleshooting Tips

1. “Connection Timed out” error while connecting to EC2 instance using PuTTy

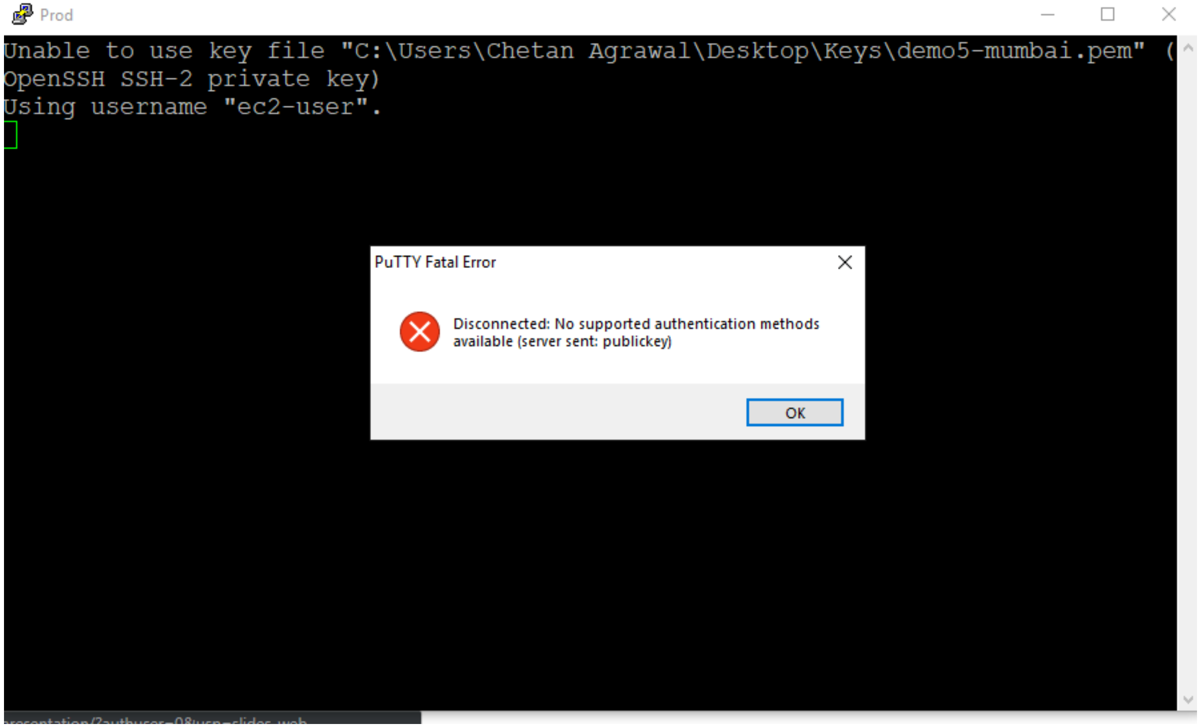


Network error: Connection timed out

Solution

1. Check that you are using EC2 Public IP (not Private IP)
2. Check Security group for EC2 instance and verify that Port 22 (SSH) is open for MyIP or 0.0.0.0/0
3. Check that EC2 instance is launched in Public Subnet
   a. Get the Subnet ID from EC2 -> Descriptions
   b. Go to VPC -> Subnets -> Filter the subnet by Id
   c. Check the Route Table -> You should see the Route for 0.0.0.0/0 through IGW
4. If you don’t see correct route in subnet, you might have missed associating public route table with your subnet. Go to correct route table and associate with your public subnet
5. All above settings are correct but still not able to connect
   a. Go to corresponding public Route table and click on IGW
   b. See if IGW exists. If not -> create new IGW -> Attach with your VPC -> Modify Route table -> Delete existing entry for internet and recreate new with new IGW

2. “No supported Authentication Methods available” error while connecting to EC2 instance using PuTTy



```
Unable to use key file "C:\Users\Chetan Agrawal\Desktop\Keys\demo5-mumbai.pem" (
OpenSSH SSH-2 private key)
Using username "ec2-user".
```

Disconnected: No supported authentication methods available (server sent: publickey)

Solution

1. This is most probably due to wrong SSH key you are using
2. Verify that you are using .ppk key and not .pem key file
3. Verify that you are using correct ppk file with which you had launched EC2 instance
    a. Go to EC2 console -> Select your Instance -> Description
    b. Verify the SSH Key name (It’s possible that you stored SSH key with different name locally. Name does not matter but it should be corresponding private key)
4. If you have lost your SSH key
    a. Terminate current EC2 instance
    b. Go to EC2 console -> SSH keys -> Generate new key pair
    c. Download .pem file and convert it to .ppk on local machine
    d. Launch new EC2 instance with new SSH key

3. “UNPROTECTED PRIVATE KEY FILE” error while connecting EC2 B from EC2 A over SSH

Error Message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@
Permissions 0664 for 'key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key.pem": bad permissions
Permission denied (publickey).
```

Solution

1. The reason for error is that Your SSH key file permissions are too open.
2. You should change permissions to either 600 or 400.
3. Run command:

```
$ chmod 600 key.pem
```

4. “Enter Passphrase” error while connecting EC2 B from EC2 A over SSH

Error Message:

```
[ec2-user@ip-10-0-0-91 ~]$ ssh -i key.pem ec2-user@10.0.0.91
Enter passphrase for key 'key.pem':
```

Solution

1. The reason for error is that your SSH key is not correct
2. Verify that contents of your SSH key that you created on EC2-A instance
3. Make sure SSH key is .pem and not .ppk as we are connecting from Linux to Linux
4. To recreate the key, do the following
    a. On EC2-A instance: rm key.pem
    b. On local machine: Open .pem using notepad and copy the content (CTRL+C)
    c. On EC2-A instance: vim key.pem -> press i -> paste the content by right click -> esc -> :wq -> enter
    d. On EC2-A: chmod 600 key.pem
5. Retry SSH from EC2-A to EC2-B