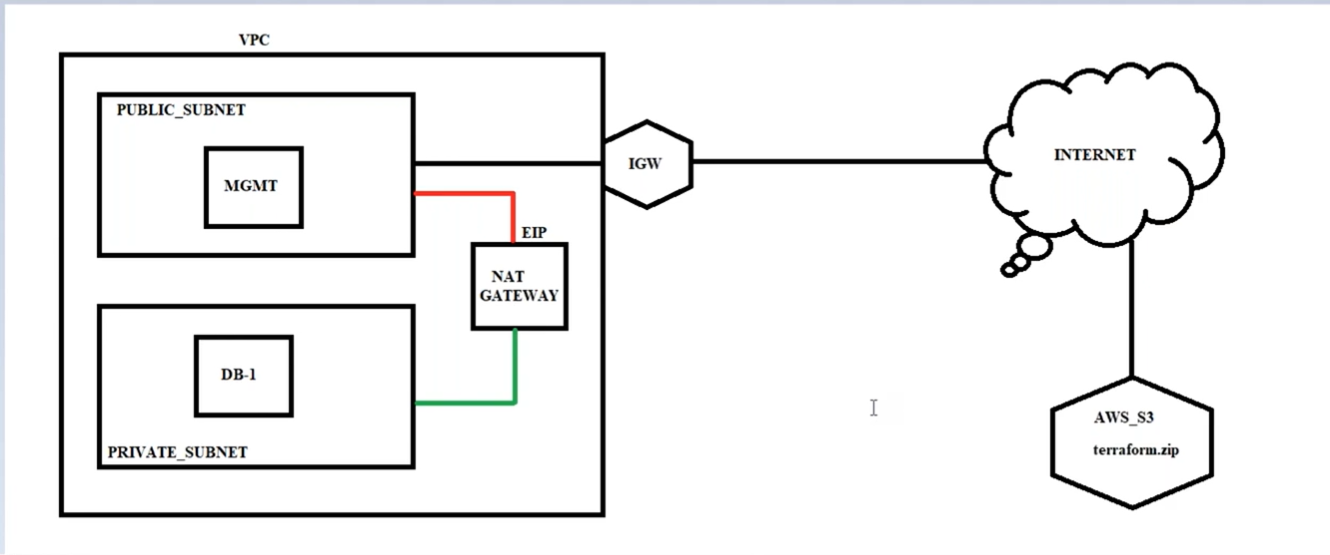
Class 8:

**Endpoints**



After Nat gateway

S3 (is like google drive to store the files)

|

Create bucket

|

Download a file (from terraform.io as a sample file to test) to upload in s3 bucket

|

Click on “create bucket” upload sample file then RightClick on file “make public” URL will display

|

Create MGMT instance public subnet1

|

Create NAT GW to public subnet1 and add in private routing table

|

Open MGMT server in putty then

**Commands**: to move to DB server

Ssh [ec2-user@10.0.10.70](mailto:ec2-user@10.0.10.70) (10.0.10.70 is DB server ip)

|

It fails to move, because we must give key to enter, copy key in .pem file

|

Nano awskey.pem (past in this file, this key should match with DB instance key when created)

|

Chmod 400 (for key permission security, read only option)

|

Ssh -i awskey.pem [ec2-user@10.0.10.70](mailto:ec2-user@10.0.10.70) (10.0.10.70 is DB server ip)

Now goes to DB server, and also ping to internet because private subnet is connected through NAT through private routing table

|

Now **remove NAT GW** connection in Private routing table

|

Try to download file from s3, copy URL of bucket in DB instance

|

Cmd: wget URL (copy s3 bucket url)

Wget <https://awsb26vpcs3bucketendpoint.s3.amazonaws.com/terraform_0.13.4_windows_amd64.zip>

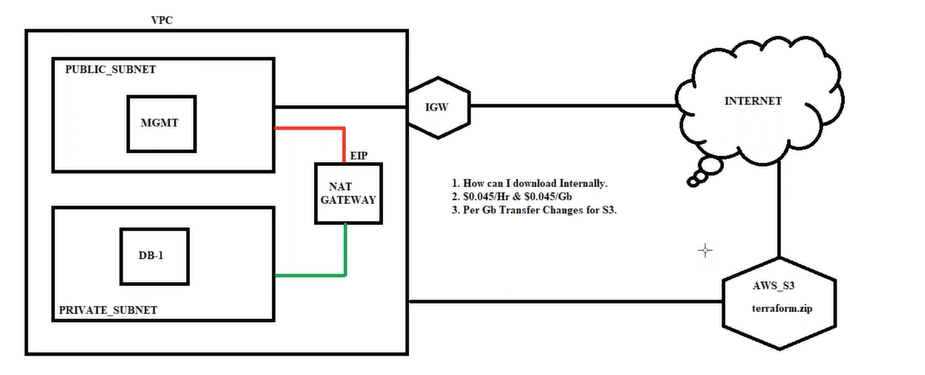
|

It shows connecting but doesn’t as follow

Connecting to awsb26vpcs3bucketendpoint.s3.amazonaws.com (awsb26vpcs3bucketendpo int.s3.amazonaws.com)|52.216.21.99|:443...

|

Now again connect **NAT GW** connection in Private routing table (it says connected)

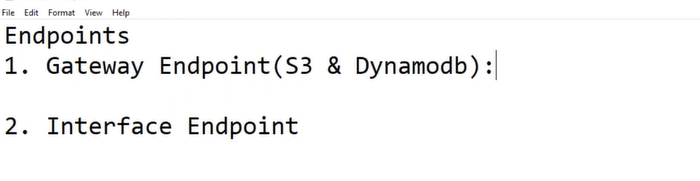


**NOW The problem with above scenario is exposing my DB server to internet through NAT GW, and cost to NAT GW usage**

So, we use End points to download file from S3 to DB instance

First delete file of “terraform.io” to do again using Endpoints, remove NATGW connection

* **Endpoints**

11

1, **Gateway Endpoints:**

**Under VPC navigation**

|

Endpoint

|

Create endpoints

|

|  |  |  |
| --- | --- | --- |
| com.amazonaws.us-east-1.s3 | amazon | Gateway |

|

Select vpc

|

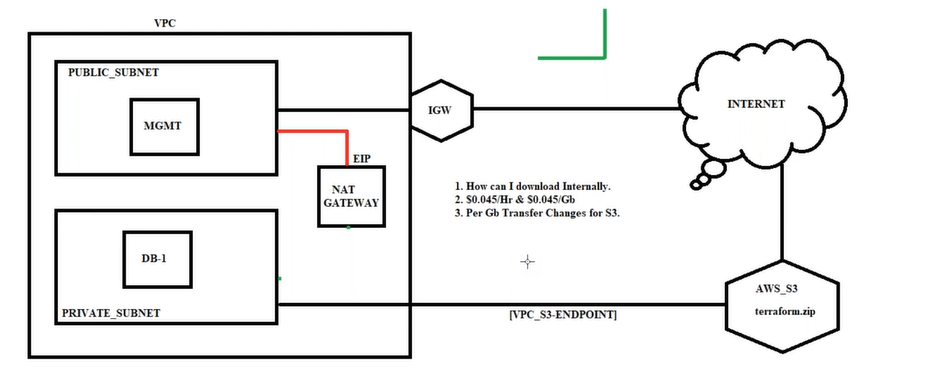
Select private route table and create (now connection b/w s3 & private route table is created)

In private route table is s3 connection is added in routs

|

Now we can download file with “wget url” command

**By using Endpoints, the Traffic will not go through internet and no charges for data transfer and get extra layer of security.**



2, **Interface Endpoints**:

1. Under “services”

* Management & Governance
* Systems manager
* Session manager
* Start session

This Session manager takes to **CLI** (command line interface) in **URL** like putty CLI.

(but it doesn’t show now, because we have to add IAM roles to ec2 instances(web instance & DB))

1. Under “services”

* Security, Identity, & Compliance
* IAM (Identity and Access Management)
* Roles
* Create a role
* AWS Service
* Ec2
* Next permissions
* Select

 [AmazonSSMFullAccess](https://console.aws.amazon.com/iam/home?region=us-east-1" \l "/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMFullAccess" \t "'_blank')  
 [AmazonSSMManagedInstanceCore](https://console.aws.amazon.com/iam/home?region=us-east-1" \l "/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMManagedInstanceCore" \t "'_blank')

* Role name: AWSB26\_ssm\_Role
* Createrole

Now IAM role is created, then assign this role to public instant & private instance (MGMT&DB servers)

1. Now goto

* Ec2 Navigation console
* MGMT instance -> Rc -> Instance Settings -> Modify IAM role
* DB instance -> Rc -> Instance Settings -> Modify IAM role

1. Again, we come to system manager to check our CLI is coming or not

Under “services”

* Management & Governance
* Systems manager
* Session manager
* Start session

MGMT (public subnet server) comes, open and type cmd “bash”

But DB (private subnet server) doesn’t come

**For getting DB server CLI also we use 3 Interface ENDPOINTS**

1. Interface Endpoints

**Endpoint-1**

Under VPC navigation console

* Create Endpoints
* Select

|  |  |  |
| --- | --- | --- |
| com.amazonaws.us-east-1.ec2messages | amazon | Interface |

* Select VPC (AWSB26)
* Private subnet1 (DB server)
* Security group (VPC’s)

**Endpoint-2**

Under VPC navigation console

* Create Endpoints
* Select

|  |  |  |
| --- | --- | --- |
| com.amazonaws.us-east-1.ssm | amazon | Interface |

* Select VPC (AWSB26)
* Private subnet1 (DB server)
* Security group (VPC’s)

**Endpoint-3**

Under VPC navigation console

* Create Endpoints
* Select

|  |  |  |
| --- | --- | --- |
| com.amazonaws.us-east-1.ssmmessages | amazon | Interface |

* Select VPC (AWSB26)
* Private subnet1 (DB server)
* Security group (VPC’s)

1. If we go to

* Ec2 navigation console
* Network Interfaces

In description we should see 3 Interface endpoints & 1 gateway endpoints

1. Again, we come to system manager to check our CLI is coming or not

Under “services”

* Management & Governance
* Systems manager
* Session manager
* Start session

MGMT (public subnet server) comes

DB (private subnet server) comes, open and type cmd “bash”

**Finally**

**1, Gateway Endpoints**:

Is used to download file from s3 to private server

S3 -> Endpoints -> private routing table

**2, Interface Endpoints**:

Is used to get URL CLI for DB private server

IAM -> Assign to Ec2 Public & Private servers -> Endpoints -> Network interface -> session manager