**AMAZON VPC PART 1 – VPC with a Single Public Subnet**

In this post, I will try to give information about Amazon VPC concept.

1. First, I will explain different scenarios like **public vpn, private vpn** and then
2. setup a Site-to-site Vpn with a juniper firewall ( optional ).
3. Also explain and give an example of new **VPC feature, VPC peering.**

VPC is a separated network for your infrastructure in aws cloud.

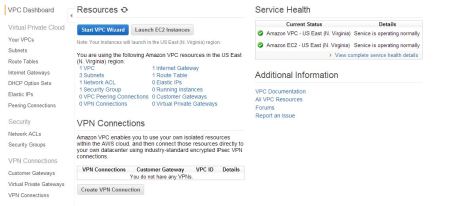
* It gives you the flexibility to configure your own network in a secure manner.
* **In my current company we use VPC to connect aws network with our private clouds so we can easily communicate with our servers.**
* Also VPC gives us the flexibility of security and access control ( by using security groups, NACL ).

The **public VPC** is basically a VPC , isolated your own network that can be reached from internet.

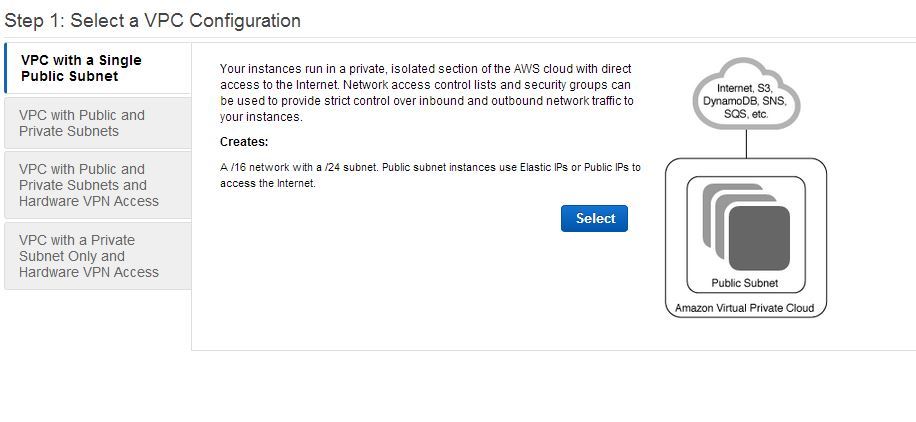
**private subnet** is an isolated your own network that can’t be reached from internet.

In our dashboard we can see our VPC connection status, peering status, and also vpn connections status.

We can use wizard to create VPC and also we can do it manually.

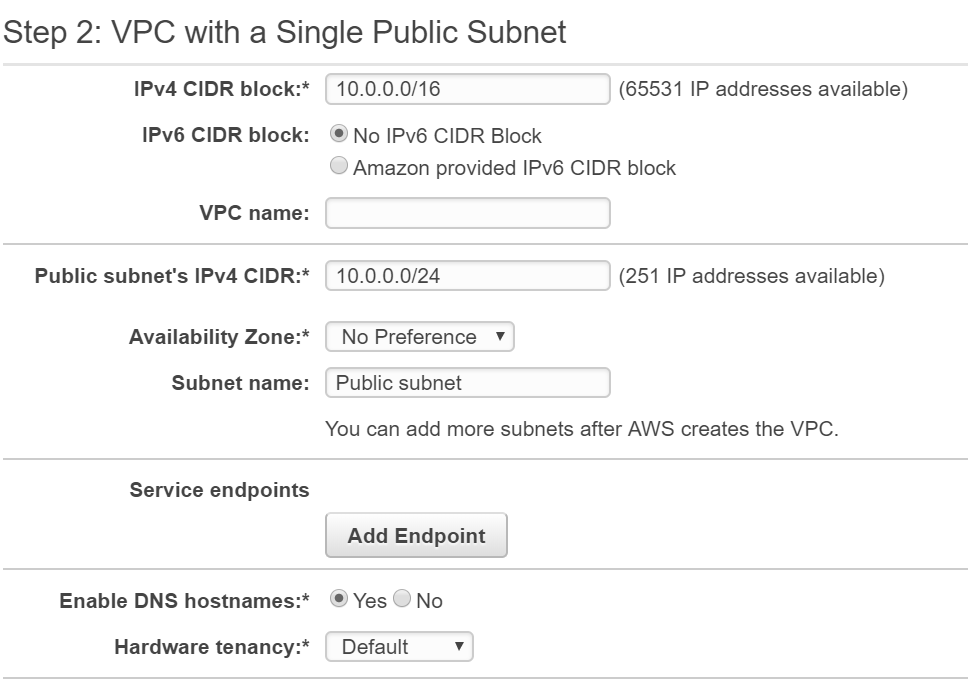
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/dashboard.jpg)

When we click the “start VPC wizard”, it asks me which scenario we want to use. There are four options here.

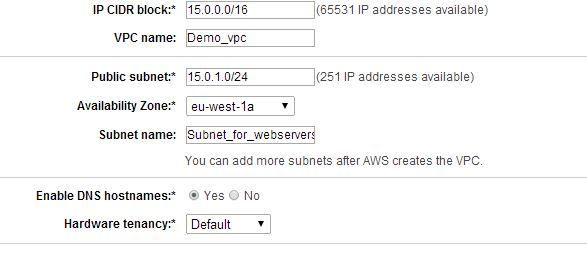
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/vpc_wizard.jpg)

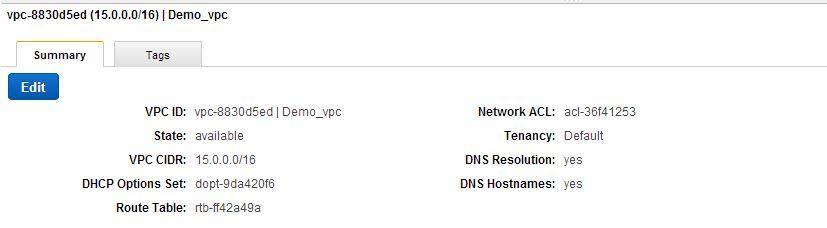
– **VPC with a single public subnet:** It is an isolated network that is reachable from internet.  
– **VPC with public and private subnets:** It is an isolated network that the public subnet is reachable from internet but the private subnet is not. Private subnet can create outbound connections via NAT server.  
– **VPC with public and private subnets and hardware VPN access:** This is like “VPC with public and private subnets” option but it also configures an IPSEC site-to-site VPN with your own corporate network  
– **VPC with a private subnet only and hardware vpn access:** It is an isolated network from internet and can only be accessed with your own corporate network via IPSEC VPN connection.

**Single Public Subnet.**

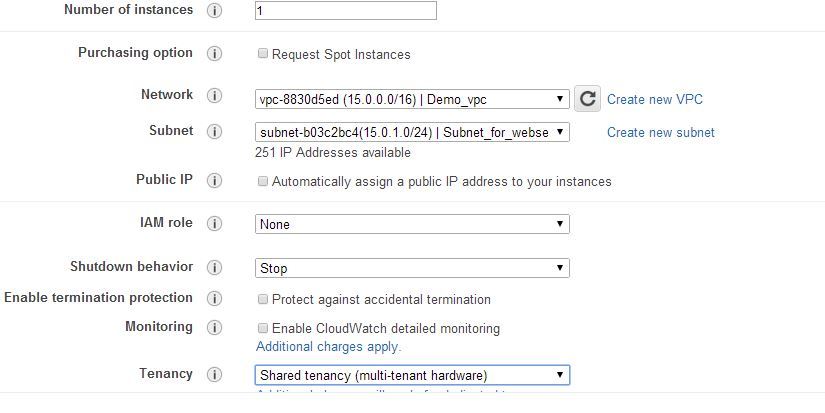


1. In “IP CIDR block” section we will enter the range of IPs that we will use in our VPC**. It must be between /16 and /28 netmasks.** By default it gives us **10.0.0.0/16 that 65531 ip addresses are available for us to use.**
2. Then we give a name to our VPC in “VPC name” section.
3. In “Public subnet” section we will configure the range of our network.
4. It is important to plan which availability zone/zones to be used. B**ecause after we create our VPC and want to create new instances it will be created in that subnet created in that specific AZ ( if only we have one ) .**
5. **For high availability we can create two subnets in different AZs (AFTER AWS CREATES VPC) and** create our instances in that different subnets separately.
6. After that we give a name to our subnet ( After creation VPC it allows us to create additional subnets ) . In “Enable DNS hostnames” section it allows us to enable or disable that created instances in that VPC are provided with hostnames or not. Finally we can choose if our instances created in that VPC are dedicated tenancy instances ( by default they are not ) .

[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/single_public_conf.jpg)

After we hit the create VPC and it is ready to use.[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/demo_vpc.jpg)

Now let’s create a new instance in our demo\_vpc. In our configuration we selected our VPC and it automatically selected our subnet **( subnet\_for\_webservers , 15.0.0.0/24 ).**

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/instance_in_vpc.jpg)

And our instance is ready.

[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/instance_ready.jpg)

**If we want to connect our instance unfortunately it will fail.**

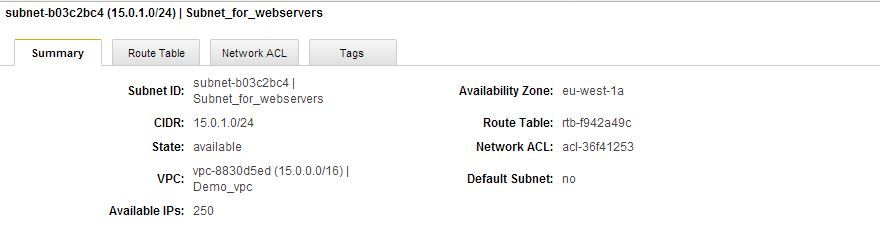
**The reason is it has no public ip address. If we want our instance in public subnet vpc to be reachable, there are some important rules we have to take care.**

– First we have to give a public ip address to our instance either by assigning public ip ( temporary ) or elastic ip ( static )  
– The security group rules for that instance should allow necessary inbound and outbound ports opened. ( for outbound connections by default all traffic is enabled. destination –> 0.0.0.0/0 ).

**Remember that security group rules are instance based and stateful.** That means, you don’t have to open any outbound ports.

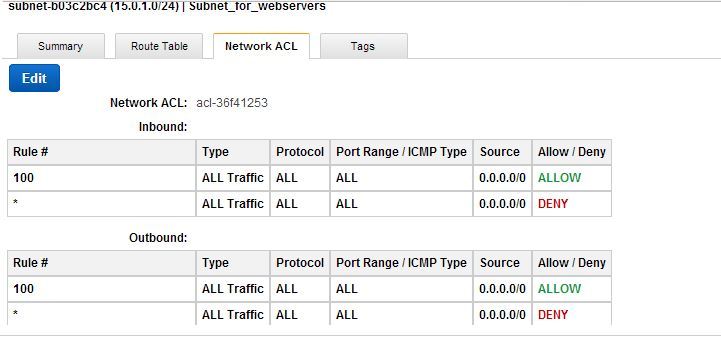
For example if we opened inbound ssh port and deleted default outbound rule in our security group, we are still able to connect our instance over ssh.

– An internet gateway (if we don’t use wizard we have to configure it manually)  
– A route table (if we don’t use wizard we have to configure it manually)

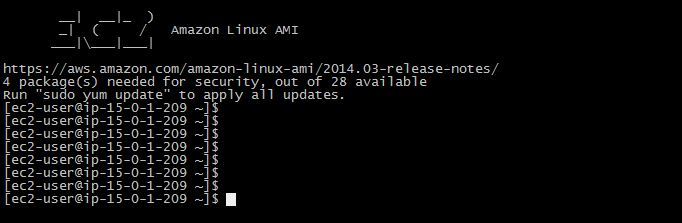
Our Subnet:  
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/subnet.jpg)

Internet gateway:  
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/internet_gateway.jpg)

Route table:  
[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/route_table.jpg)

NACL:  
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/NACL.jpg)

**Now let’s assign an elastic ip address to our instance and check it’s connectivity.**

[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/connectivity_up.jpg)

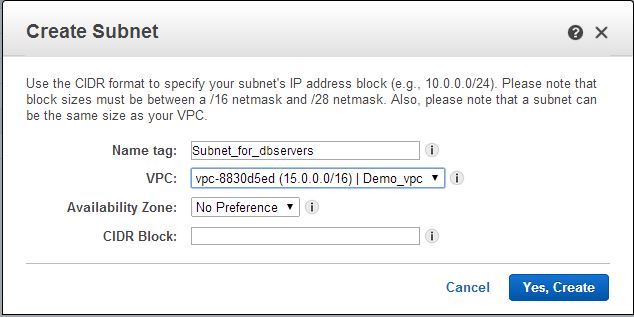
In my next post we will configure VPC with public and private subnets. If you have any questions please feel free to ask/comment.

**AMAZON VPC PART 2 – VPC with a Single Private Subnet**

**In this post, we will add a private subnet to our VPC and configure a NAT server manually.** After adding our subnet and enable our instances to reach the internet , next step will be adding a hardware vpn.  In my last blog I had created a VPC with 15.0.0.0/16 block and a subnet 15.0.1.0/24 (Subnet\_for\_webservers). Now let’s create our second subnet.

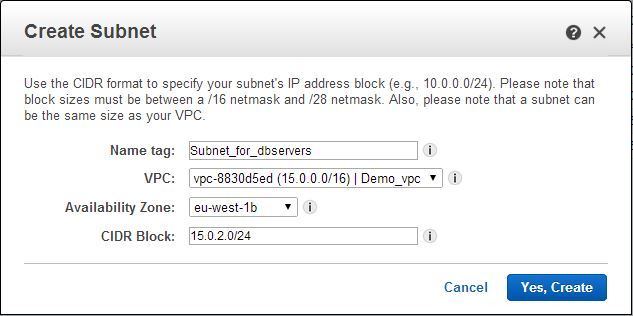
When we click the “Create Subnet” button , as you see,

1. it asks for a name of the subnet, the name of the VPC we will **create a subnet in, the availability zone (remember that it is important to choose a different AZ for HA solutions) and the range.**

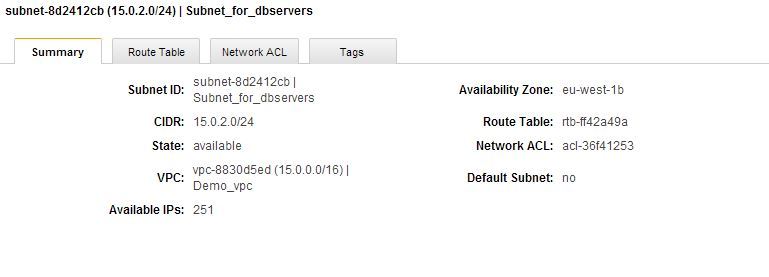
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/create_subnet.jpg)

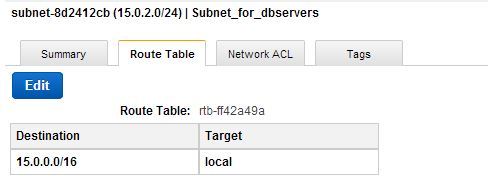
We will use the settings below.

Name tag: Subnet\_for\_dbservers  
VPC: Demo\_vpc  
AZ: eu-west-1b  
CIDR block: 15.0.2.0/24

[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/created_subnet.jpg)

Now we’ve created our subnet and we have to check the status and the route table .

As you see below, it uses our default route table and the route table says that only the instances in that subnet can communicate with each other (There is no route for outbound and inbound).  
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/subnet_db.jpg)

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/route_db.jpg)

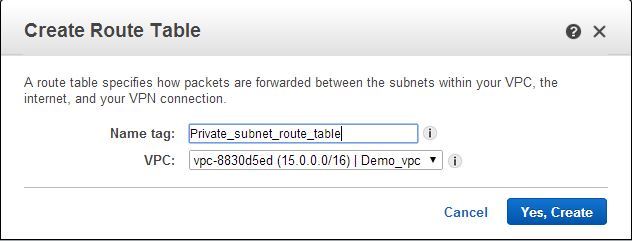
**Remember that if we add a default route to our subnet it will change to a public subnet (the difference between subnet and private is there is a 0.0.0.0/0 route and the target is  
igw-89dfcdeb , our internet gateway).**

You can imagine that if we create a NAT server and create a route for 0.0.0.0/0 and configure our target as NAT server, instances in our private subnet will be able to reach the internet. So our next step is create a NAT server. If you configured your VPC by using wizard, it will automatically create your NAT server. In our case we have to create it manually. On our VPC dashboard, you can launch an instance and use search to find a NAT server. I will use amzn-ami-vpc-nat-pv-2013.09.0.x86\_64-ebs – ami-f3e30084 as a NAT server.

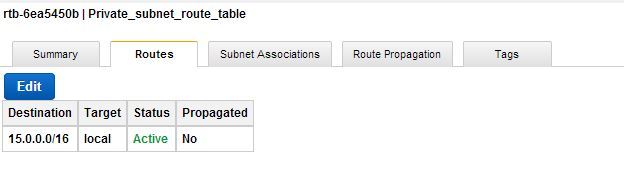
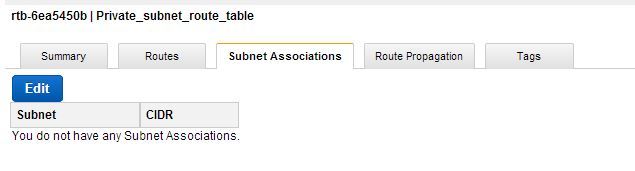
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/NATami.jpg)

When we launch our NAT instance ,there are some steps we have to be careful:  
1- We have to choose our correct VPC (in our case it is demo\_vpc)  
2- Second we have to choose our public subnet(subnet\_for\_webservers)  
3- We have to assign a public ip address. Wizard lets us to choose. Also we can use an EIP later  
4- We should **disable “source/destination check”** on our NAT instance  
5- Configure security group for your NAT server (Allow only what you need)

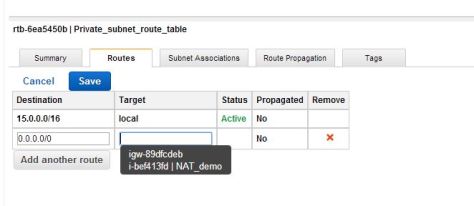
After you launched your instance, you can connect to it and if it is ok, you can add a route for our private subnet (If you have trouble to connect to your NAT instance , you can check your security group). Now we will add a new route table for our subnet and configure it that all internet traffic (0.0.0.0/0) will go to our NAT instance.

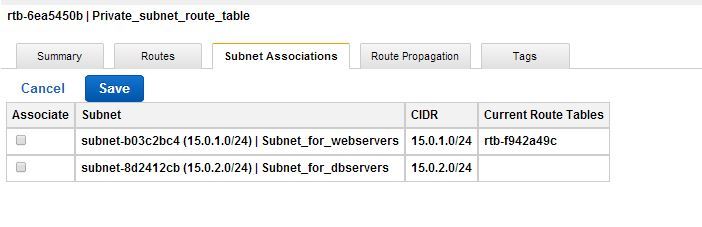
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/private_route.jpg)

As you see it is only routed in locally and the subnet association is empty. We will add a route and associate the table with our db\_server subnet.

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/private_route_table.jpg)  
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/private_route_subnet.jpg)

When we edit the route table our NAT server can be added as a target. And in subnet association, we can choose our db\_server subnet.

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/route_nat.jpg)

[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/private_route_subnet_added.jpg)

Last step is to configure a security group for your instance. For example if these instances in our db\_server subnet runs mysql you should create seperate security groups for your NAT and db\_servers subnet. You can check the necessary configuration in [aws example](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html" \t "_blank).

**AMAZON VPC PART 3 – Hardware VPN Access**

on: April 15, 2014In: [Amazon aws](http://www.awsomeblog.com/category/amazon-aws/), [vpc](http://www.awsomeblog.com/category/amazon-aws/vpc/)[4 Comments](http://www.awsomeblog.com/amazon-vpc-part-3-hardware-vpn-access/#comments)

This is my third post about Amazon aws vpc. In this post I will explain how to configure a hardware vpn access. By configuring hardware vpn access, you can extend your own datacenter to amazon cloud. Amazon aws supports multiple vendor devices to create site to site vpn access. We will use juniper ssg series firewall device but you can easily configure your device if it is different. In order to configure Hardware Vpn, there are 3 steps we have to complete:

1- Create a customer gateway  
2- Create a virtual gateway  
3- Create a VPN connection

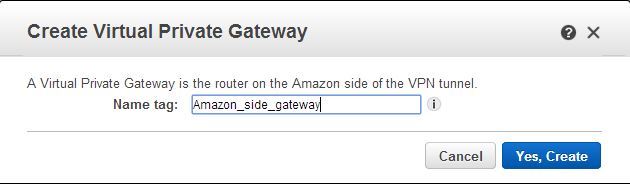
Let’s start with configuring customer gateway. In “Create Customer Gateway” screen we have to give a name tag to our device. we have 2 different routing options. If you want to use BGP and have an ASN you can choose “Dynamic routing” or you can use static routing. I will continue with static routing. After we enter our device public ip address we can create our customer gateway.

[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/customer-gateway.jpg)

Now customer gateway which is the endpoint in our side is ready.

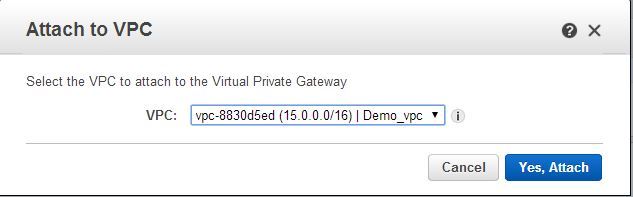
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/customer-gateway_conf.jpg)

Next step is creating a virtual private gateway, the router on the Amazon side.

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/aws_gateway.jpg)

As you see it is in “detached” state. We have to aatach to a VPC that we want to create a site to site vpn. I will attach it to my demo\_vpc.

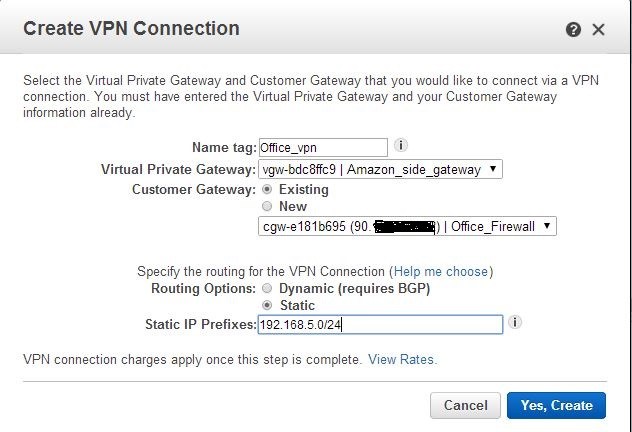
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/aws_gateway_detached.jpg)

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/attach_to_vpc.jpg)

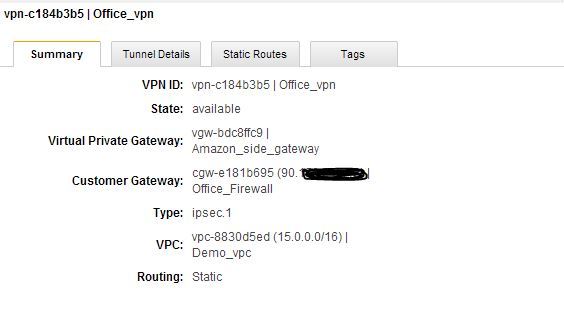
Now it is in “attaching” state. After a few minutes it will be in “attached” state.

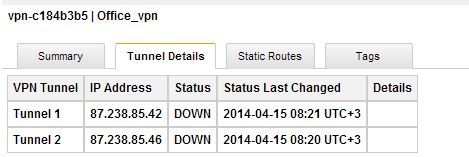
[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/aws_gateway_attached.jpg)

And last step is creating a VPN connection. In this screen we have to give a name tag to our connection. I have only one virtual private gateway ( Amazon\_side\_gateway). I will choose my existing customer gateway or I can create a new one. If you preferred to use BGP, select dynamic routing , otherwise you have to enter static IP prefixes. I will use 192.168.5.0/24 block that is my ip range in our customer side.

[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/create_vpn1.jpg)

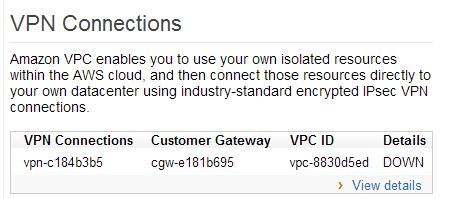
Again we have to wait a few minutes to aws creates our VPN connection. After it finishes you can see it is in available state.

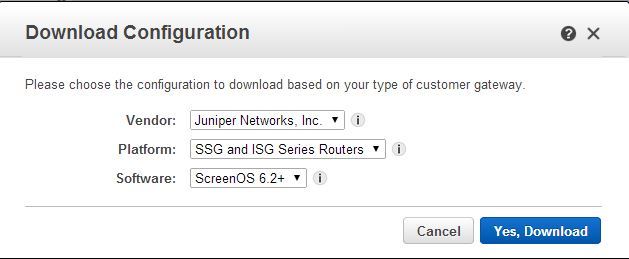
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/vpn_summary.jpg)

Aws creates two tunnels and we will also create to tunnels on our side.  
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/vpn_tunnel.jpg)

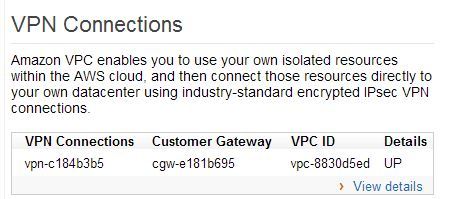
Route for ip range in our side.  
[](https://i2.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/vpn_routes.jpg)

After we download our vpn configuration and merge it to existing juniper configuration, our VPN connection will be up. Dashboard screen shows the status of our vpn connection and it is down now.

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/vpn_down.jpg)

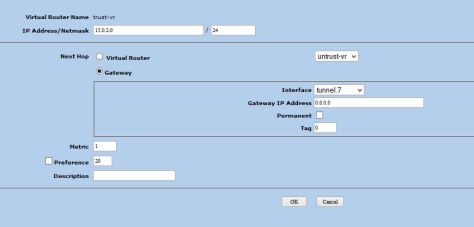
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/download_config.jpg)

I merged it with the previous one and now our VPN connection is UP.

[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/vpn_up.jpg)

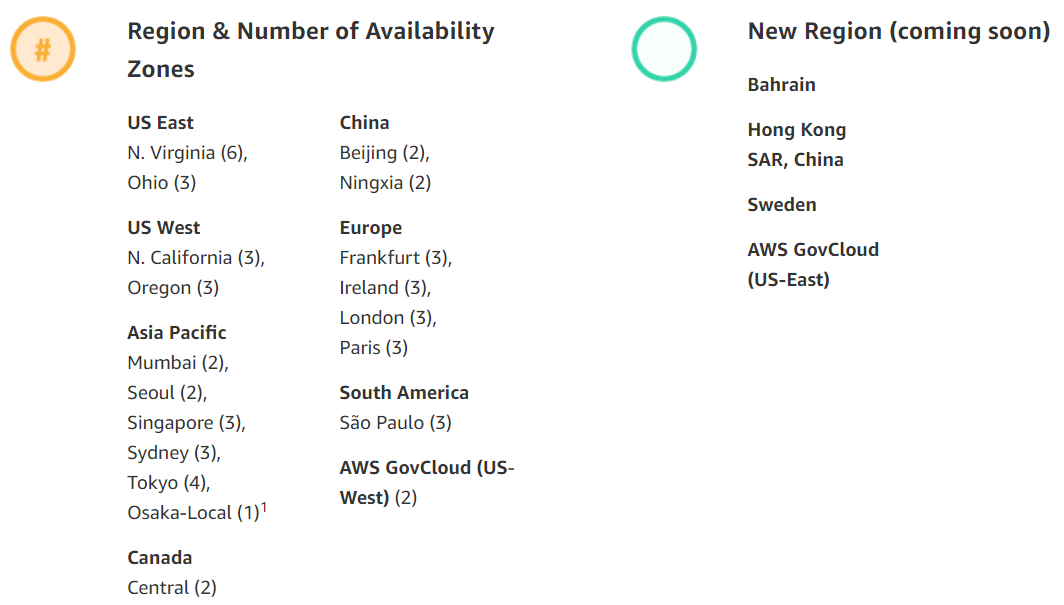
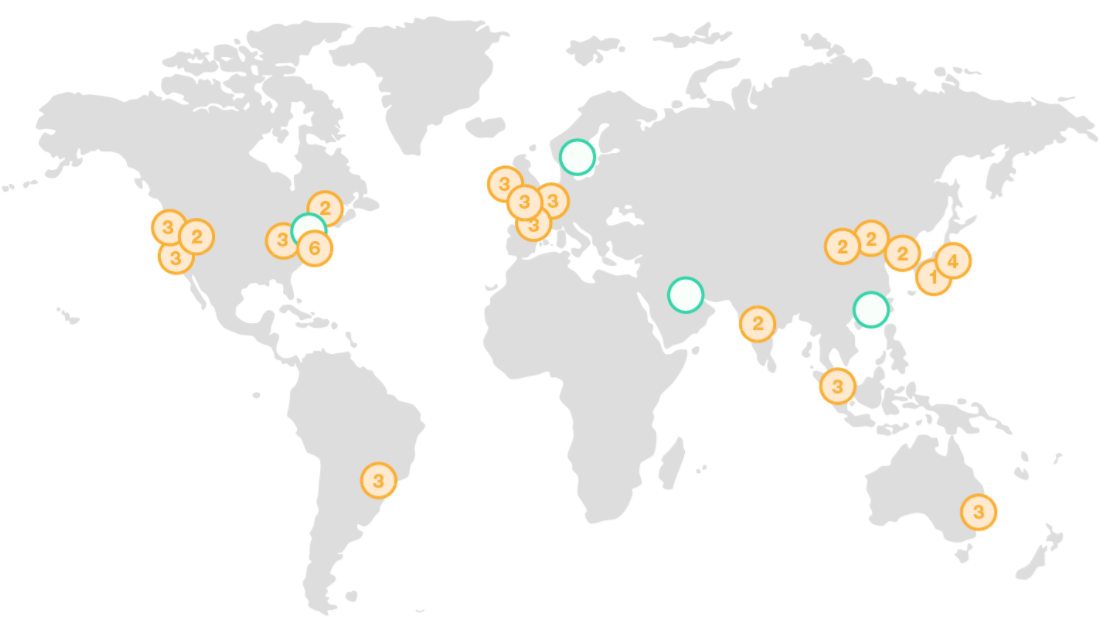
I have to add routes for both AWS side and my side.

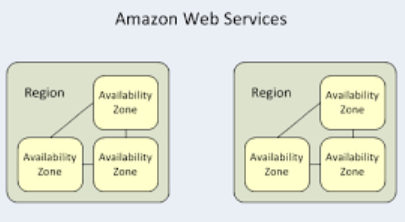
In AWS I have to add a route for 192.168.5.0/24 in Private\_subnet\_route\_table.  
[](https://i1.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/vpn_route_add.jpg)

I also have to add a route for 15.0.2.0/24 in Juniper configuration  
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/juniper_route.jpg)

And my security group was allowing to make ssh connection , and it works.  
[](https://i0.wp.com/www.awsomeblog.com/wp-content/uploads/2014/04/connection_up.jpg)

If you have any question or comment please feel free to write.



Every Region have Minimum of 2 Data centers. If 1 DC fails, other will be used. 

AZ will be connected.