Module 8 – Site-Site VPN

Site-Site VPN.

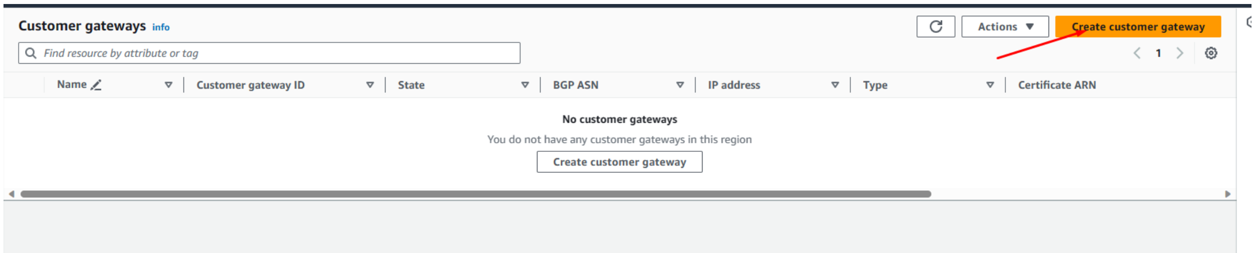
Site-Site VPN – Suppose our all on-premises servers are running on Data Centre and we have some applications running on AWS, but how applications running on AWS can communicate with On-Prem servers. So here comes Site-Site VPN where we have a tunnel between AWS and on-premises. We will have Customer Gateway configured between AWS and On-Prem and all the data transfer will be highly secured.

So, in this example we will use two different AWS regions, one is US-EAST-1 and another one is Mumbai region which will behave like ON-Prem DC Both will have VPC 172.31.0.0/16 and Mumbai will have 192.168.0.0/16. Also, we will Launch EC2 instance in both the region.

Setup – Mumbai Region. - VPC will be 192.168.0.0/24

- It will have two Public and two Private Subnet. We will Launch 1 EC2 instance in each subnet.
- For OpenSwan – we need to launch Amazon 2

- Now let switch back to us-east-1 and first we create Customer GW
- Click on create customer gateway.

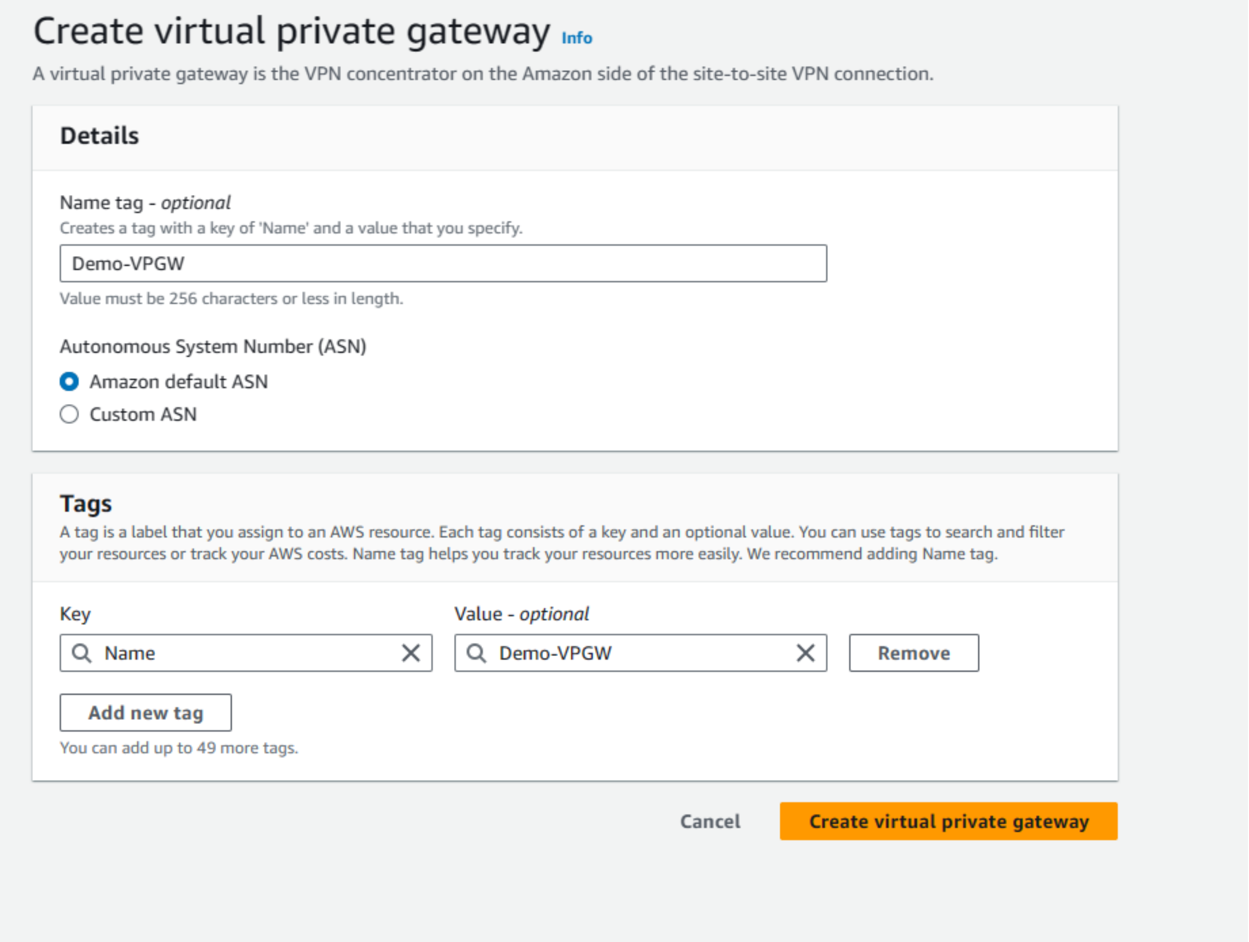


Name	Customer gateway ID	State	BGP ASN	IP address	Type	Certificate ARN

No customer gateways

You do not have any customer gateways in this region

- Fill in the details and put the Public IP address from EC2 instance Mumbai Region.
- Click on Create customer gateway.
- Now let's create the Virtual Private Gateway.



Create virtual private gateway Info

A virtual private gateway is the VPN concentrator on the Amazon side of the site-to-site VPN connection.

Details

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
Demo-VPGW
Value must be 256 characters or less in length.

Autonomous System Number (ASN)
● Amazon default ASN
○ Custom ASN

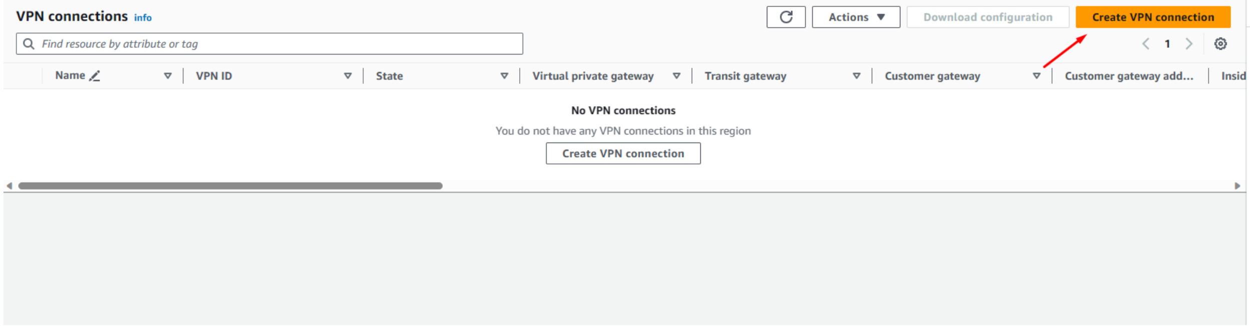
Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key	Value - *optional*
Name	Demo-VPGW

You can add up to 49 more tags.

- Now once the Virtual Private gateway is created, we have to attach this with VPC.
- Next step is to configure Site-Site VPN. So, click on.
- Click on Create VPN connection.



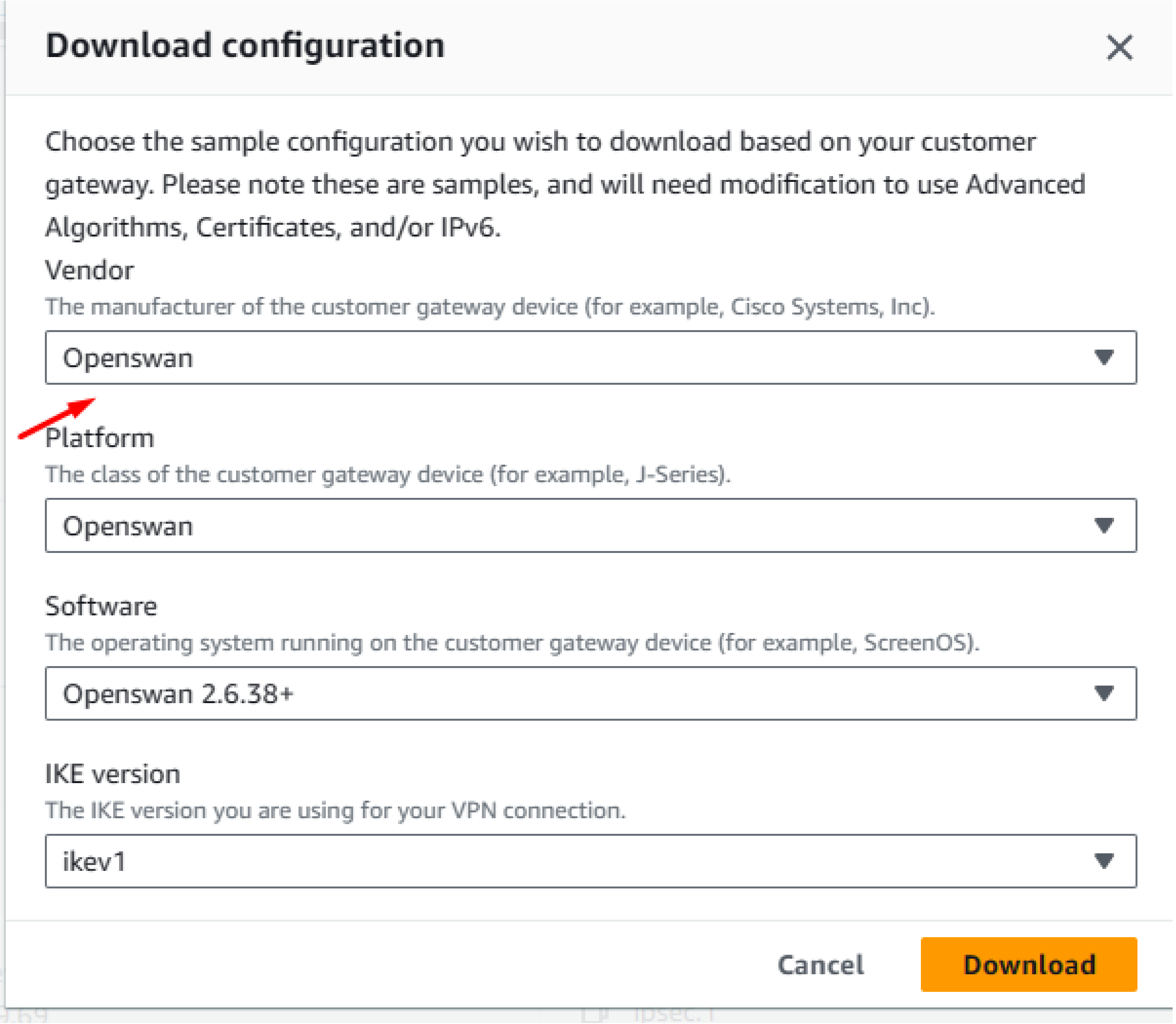
VPN connections info

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Customer gateway add...	Insid

No VPN connections
You do not have any VPN connections in this region

- Select the Target gateway type as Virtual Private Gateway and put the Customer gateway ID which we have created just now.
- Next part is the Static IP, so put the VPC CIDR block for both the regions.
- Keep the other parameter as default.
- Let’s now install the OpenSwan VPN on the EC2 instance of Mumbai region.
- Command to install Openswan.

- yum install openswan -y
- Now let's download the VPN configuration and then start configuring the Openswan.
- Select the VPN and click on Download configuration.
- We need to select Vendor as Openswan.



Download configuration

Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

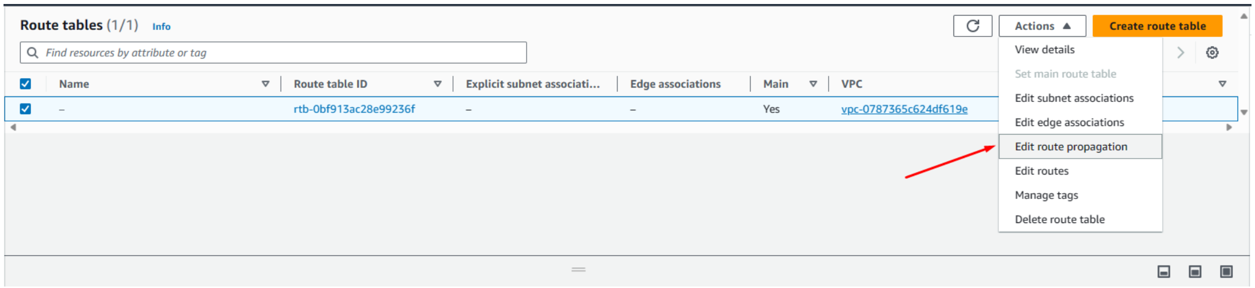
Vendor
The manufacturer of the customer gateway device (for example, Cisco Systems, Inc).
Openswan

Platform
The class of the customer gateway device (for example, J-Series).
Openswan

Software
The operating system running on the customer gateway device (for example, ScreenOS).
Openswan 2.6.38+

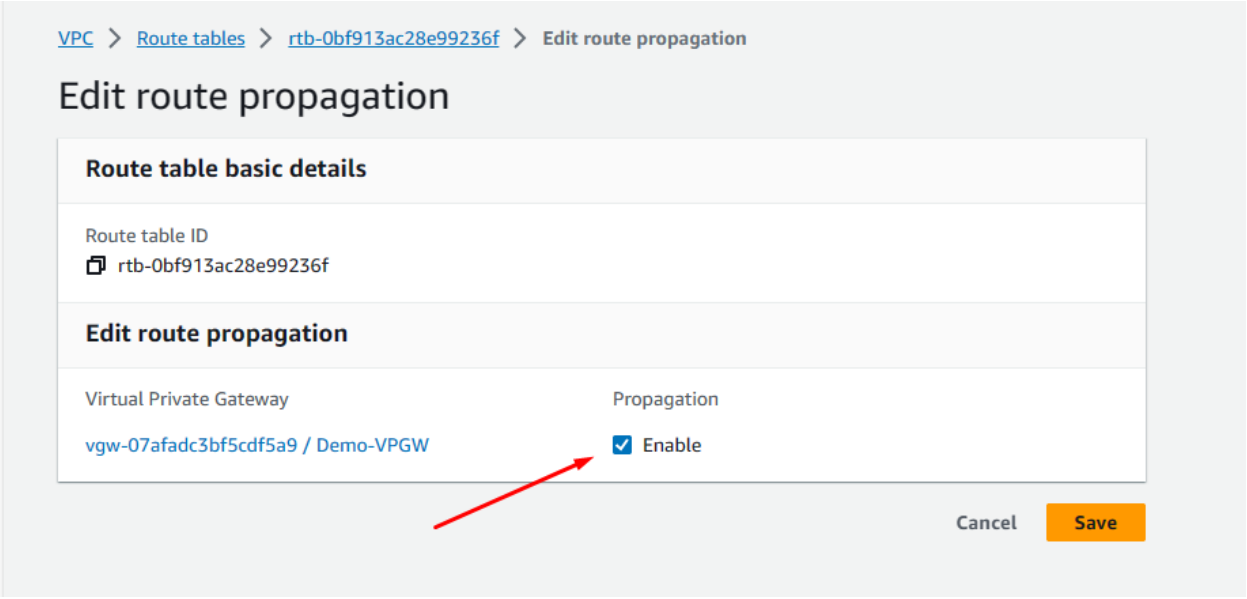
IKE version
The IKE version you are using for your VPN connection.
ikev1

- Open this file and now make the configuration changes in EC2 instance as per the document.
- Vim /etc/sysctl.conf – add the parameters as per the VPN file.
- sysctl -p
- vim /etc/ipsec.conf – make sure to remove **auth=esp** also update the leftsubnet and rightsubnet. Note – leftsubnet will be always where we are installing the Openswan. So put the VPC CIDR in the leftsubnet and US-EAST-1 on the right subnet.
- Now in the US-EAST-1 we need to update the route table entries.
- So go to route table select Action → Edit route propagation and make Virtual Private GW enable and save it.



Route tables (1/1) Info

☑	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
☑	–	rtb-0bf913ac28e99236f	–	–	Yes	vpc-0787365c624df619e



VPC > Route tables > rtb-0bf913ac28e99236f > Edit route propagation

Edit route propagation

Route table basic details

Route table ID
rtb-0bf913ac28e99236f

Edit route propagation

Virtual Private Gateway	Propagation
vgw-07afadc3bf5cdf5a9 / Demo-VPGW	☑ Enable

- Now go Back to Mumbai region, edit public route table, and add the route. (172.31.0.0/16 with target as instance.)
- Go to the EC2 instance Mumbai region and make the below changes.
- Select EC2 – Action → Networking → Change source/des check and make it stop
- Vim /etc/ipsec.d/aws.secrets and the data as per the VPN configuration file.
- Now let start the ipsec service
- systemctl start ipsec.service
- Now we can see tunnel 1 is UP.
- Let try to ping both the instances.