AWS VPC to SU EPV-RTR VPN Creation and Configuration

The document’s sole purpose is to be a guide in the creation of an IPsec site-to-site VPN tunnel between a customer AWS VPC to Stanford University’s EPV-RTR (External Provider/Partner VPN router). For any terms and terminologies used that sounds unclear, please refer to the following documentation from AWS:

https://docs.aws.amazon.com/general/latest/gr/glos-chap.html
https://aws.amazon.com/documentation/vpc/

What is a VPC?

VPC – virtual private cloud, it is a virtual network that closely resembles a traditional network that you’d operate in your own data center, with the benefits of using the scalable infrastructure of Amazon Web Services (AWS). It can be thought of as a branch/DC LAN that connects back via an IPsec VPN.

How does a AWS VPC connect back to the SU campus?

UIT Communication and Network Services is providing IPsec VPN connectivity to cloud providers and university partners back to the campus. A pair of VPN routers are racked at two ECHs on campus to provide high availability. They are setup in active and standby mode, if the active goes down the standby becomes active and establishes the VPN tunnels to the providers and partner VPN endpoints in a matter of seconds. We call these routers as External Provider/Partner VPN RTRs (EPV-RTRs).

In order for us to establish connectivity between the users’ AWS VPC and SU campus via IPsec VPN. The user should have access to their AWS account console and put in a request on Service Now. Please follow the green arrow throughout the guide.

The following are what the network engineers have to provide to users wanting to connect their VPCs to SU campus via VPN:

1. Customer Gateway Address (SU Public IP address) = 171.67.198.185
2. BGP Autonomous System Number (ASN) = 32
3. VPC network record to be carved out of unassigned-10-AWS-Nets, depending how large the network needed.
4. Tunnel interface networks – aws-epv-tun-int-nets, provision two /30 network space for two tunnel interfaces to be configured on the EPV-RTRs.
In this example we are going to use 10.96.9.0/26 as a subnet that will be assigned to a AWS VPC:

1. The user needs to log into their AWS account and look for the Networking & Content and beneath it click on the VPC service:
1. The **VPC** service page presents you the status of VPC resource you are using. There is a default VPC provide by AWS but we are not going to use that instead we will create a new one carved out of the unassigned-10-AWS-nets on NetDB by the networking team.
2. Hit Your VPCs on the left and you will be presented with the page below:

![Create VPC page](image)

3. Hit the Create VPC button to start creating a VPC and fill in the details of the VPC:

![Create VPC dialog](image)
4. Fill in the information with the following procedures:

   a. **Name tag** = aws-"project name"-vpc
   b. **IPv4 CIDR block**, will be the carved-out subnet from the unassigned-10-AWS-nets given to you by a backbone network engineer. In these example 10.96.0/26. The CIDR block can be as big as the subnet provide or bigger depending on the requirements are.
   c. **IPv6 CIDR block**, leave as it is since we are not using IPv6, otherwise if required user can opt for an Amazon provided IPv6 CIDR block.
   d. **Tenancy** leave as Default, otherwise Dedicated if required by the user’s setup.
   e. Hit **Yes, Create** after filling every information
5. We can now verify the created VPC afterward on the Your VPCs page, the details on the table and below:

![Image of AWS console showing VPC details]

6. Create Subnet, though the subnet is the same or as big as the CIDR we created, it really depends on the requirements. In this case we have a subnet as big as the CIDR. Now we need to create a subnet to associate with our VPC. Hit Create Subnet to start.

![Image of AWS console showing subnet creation]
Fill in the following:

- **Name tag**, this will be the subnet name as named in NetDB,
  i. ex. `aws-backbone-vpc-net`
- **VPC**, select the VPC you created earlier, in this case `aws-backbone-vpc`
- **Availability Zone**, select **No Preference** unless users required to be set to a certain zone given by AWS. Please verify your options first before selecting.
- **IPv4 CIDR block**, can be the equal to the subnet or the subset range of the subnet of the VPC. In our example we enter the subnet itself.
- **Hit Yes, Create** if you are ready to create the subnet
7. **Create Customer Gateway**, here we define the epv-rtr VPN router at the SU campus where we will establish the BGP peering with:

   a. On the left side you see **VPN Connections** underneath it is **Customer Gateways** hit that and we will be presented with the page below:

   b. Once you hit **Create Customer Gateway**, you will be ask to fill out the following:
      i. **Name** of the customer gateway, `epv-rtr.stanford.edu`
      ii. **Routing** options are Dynamic or Static, in our case we select **Dynamic**.
      iii. **BGP ASN**, `65000` by the default, we’ll use `32`.
      iv. **IP Address** of the customer gateway to where we are going to terminate the VPN, in our case it is `171.67.198.185`. 
Fill up the information as shown on the diagram then hit Create Customer Gateway:
8. Create Virtual Private Gateway, now we will create a virtual private gateway that we will need to initiate a VPN connection to the epv-rtr, which is our customer gateway. Hit the Virtual Private Gateways underneath VPN Connections:
Hit Create Virtual Private Gateway and you will be asked to fill in:

a. Name tag for the virtual private gateway, in our case we tag it as **aws-su-bb-vpg**

b. ASN, hit Custom ASN and specify **7224**:

Hit **Create Virtual Private Gateway** button to create it after filling in info then hit the **Close** button:
If you noticed the state of the VPC, it indicates that it is “detached” meaning that it is not attached to any VPC that will originate traffic from. Next step is to attach it to a VPC.

9. Still on the Virtual Private Gateways page, we attach the VPC to the Virtual Private Gateway that we created so we can establish the VPN and let traffic flow from the VPC and SU campus.

   a. Hit the Actions button above select Attach to VPC
b. Select the VPC that we created, **aws-backbone-vpc**, then hit **Yes, Attach.**

c.

10. **Create VPN Connection**, this would be the last option underneath **VPN Connections** Section on the left side. Hit the **Create VPN Connection** button to start creating the VPN:
The Create VPN Connection requests the following information:

a. **Name tag**, name that we will assign to the VPN connection, `aws-to-su-bb-vpn`
b. **Virtual Private Gateway** that we will use,
c. **Customer Gateway**, 
d. **Routing Options**, **Dynamic** or **Static**, we will opt for **Dynamic** since we are going to use BGP to route between the AWS VPC to SU Campus

e. **Tunnel Options**:
   i. **Inside IP CIDR for Tunnel 1** – this tunnel will be the primary tunnel that will be used. This will be provided together with the request and will be carved out from NetDB by Network team.
   ii. **Pre-shared Key for Tunnel 1** - you can opt for this to be generated by Amazon.
   iii. **Inside IP CIDR for Tunnel 2** – this tunnel will be a backup tunnel in case Tunnel 1 on this VPC does not work, only Tunnel 1 will be configured on the epv-rtr.
   iv. **Pre-shared key for Tunnel 2** - you can opt for this to be generated by Amazon.
**Virtual Private Gateway**, Select the VPG that was created

![Virtual Private Gateway screenshot]

**Customer Gateway ID**, select the epv-rtr:

![Customer Gateway ID screenshot]

**Routing Options** should be Dynamic, because we are going to use BGP
Tunnel Interfaces and the Pre-shared keys, they can be randomly generated thru AWS however for the tunnel interfaces this will be provided by Networking:

Below is the completed information, please check out all the options pointed by the green arrows:
Hit **Create VPN Connection** button at the bottom right corner to proceed:

Hit the **Close** button:

To get the view of the VPN status that was created hit **VPN Connections**:
Tunnel 1 is still down because Networking needs to configure the other end which is on the epv-rtr at the SU campus:

In order to configure the other end, we need to download the generated configuration for a Cisco IOS router from AWS. This configuration can be downloaded when you hit the Download Configuration button above:
Please select the following:

a. **Vendor** = Cisco Systems, Inc.
b. **Platform** = ISR Series Routers
c. **Software** = IOS 12.4+

Once everything is filled up you may hit the **Download** button. Please provide the download Cisco router configuration file to the network engineer who is working on the request and he will apply the configurations on the EPV-RTRs.

Once everything is done correctly on the EPV-RTRs we should have the result below that the we have established connectivity between AWS VPC and SU campus:
As of now, we only need a single tunnel to be working. High availability is provisioned at the EPV-RTRs. These are two routers setup in HA, racked in two separate ECH located on campus, Press and Northwest. If the active goes down the standby goes active and negotiates the VPN tunnels in a matter of seconds.

Troubleshooting SU to AWS VPC connectivity:

1. Check Network ACLs on the Security section to verify if Inbound and Outbound rules.
2. Routing issues check the Routable if the route is propagated. If not, update it to be propagated.
3. For issues for regarding Instances on EC2 unreachable check if your Security Group Inbound and Outbound rules if they permit or deny incoming traffic from SUNET addresses.
4. You might want to filter out the hosts that would need to access your AWS instances thru the VPN, here is a link that you may use to filter out the networks that has access to them [https://uit.stanford.edu/guide/lna/network-numbers](https://uit.stanford.edu/guide/lna/network-numbers).