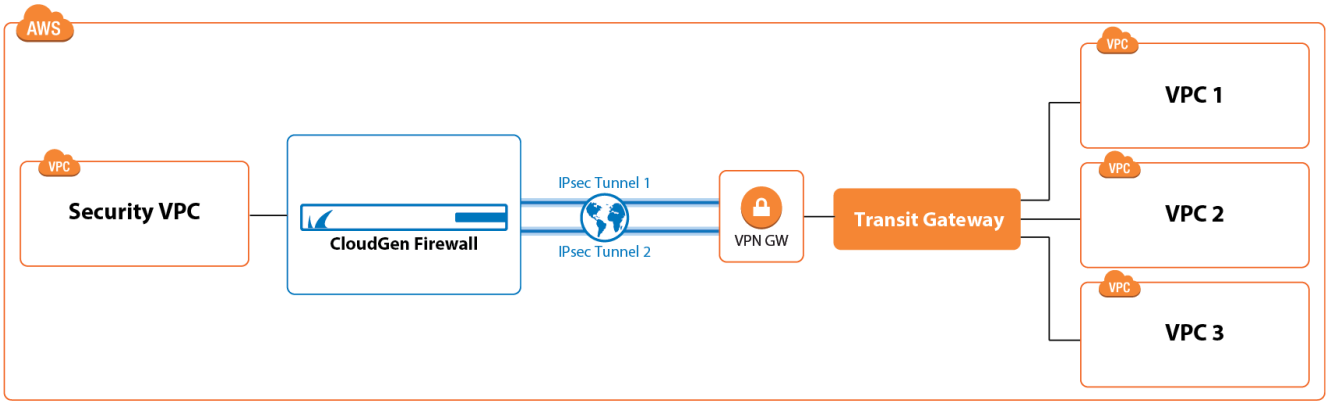
AWS Reference Architecture - Transit Gateway with Attached VPN Gateway using CloudGen Firewall

https://campus.barracuda.com/doc/91980623/

Connecting multiple VPCs to multiple locations, such as your data center or customer offices, can cause significant configuration overhead, especially if VPCs are frequently added and removed. For example, adding a new VPC requires configuration changes to each on-premises location. A second weak point is the communication between the VPCs. To share common resources, VPCs must be peered if they are in the same region; otherwise, the traffic must be routed through your data center.

To reduce the number of VPN connections required by each device participating in the network, use a central Transit Gateway, with all your cloud resources (VPCs and VPN Gateway) attached to it, and a Barracuda CloudGen Firewall connecting to the VPN Gateway through IPSec. In this setting, you will have a hub and spoke topology where the Transit Gateway acts as the hub and routes the traffic between all attached resources. The default configuration of the Transit Gateway is any-to-any communication, which allows all attached devices to reach all other attached devices. The VPCs and VPN Gateway attached to the Transit Gateway are propagated via BGP.

For more information on AWS Transit Gateway, see https://aws.amazon.com/transit-gateway/.



Before You Begin

The security VPC and remote (VPC) subnets must not overlap. E.g, if your security VPC network is 10.0.1.0/24, do not use 10.0.0.0/16 for your other VPCs.

Step 1. Create a Firewall in a High Availability Cluster in AWS

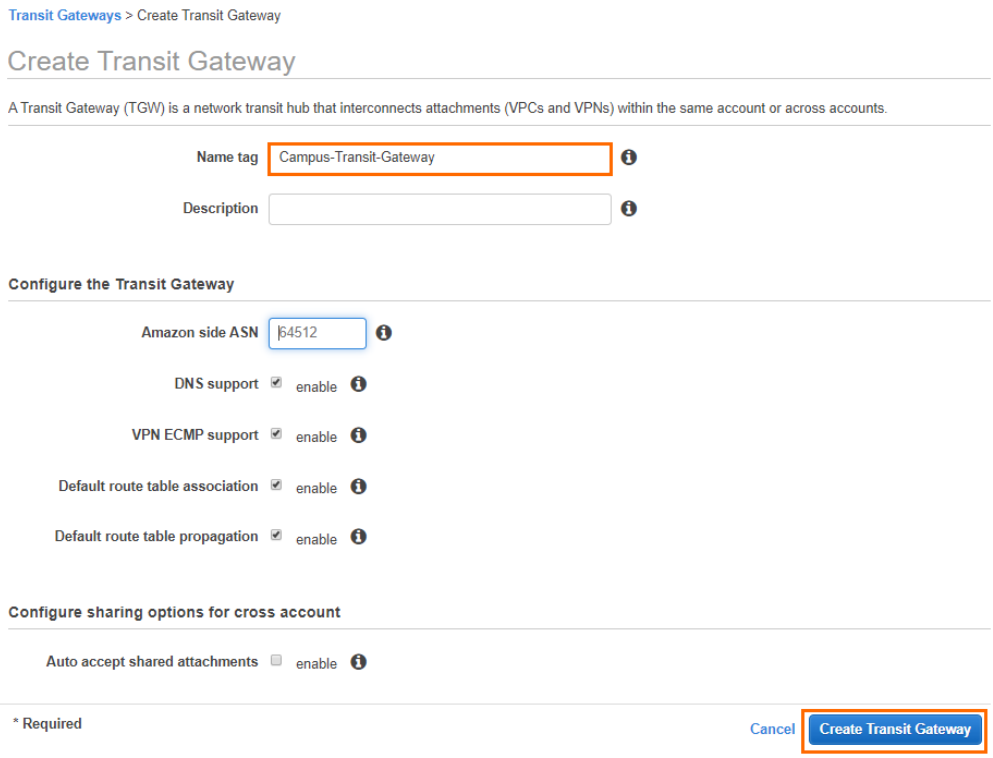
This firewall will later connect to your Transit Gateway using a VPN IKEv1 or IKEv2 IPsec tunnel to an Amazon VPN Gateway attached to your Amazon Transit Gateway.

1. Deploy a firewall in a high availability cluster in Amazon. For more information, see High Availability in AWS and AWS Reference Architecture - CloudGen Firewall HA Cluster with Route Shifting.
2. Configure source-based routing for the network the firewall is attached to (usually the public subnet). For more information, see How to Configure Source-Based Routes.
3. Disable the **Source/Destination Check** for the network interface. For more information, see Step 7 in How to Deploy a CloudGen Firewall in AWS via AWS Console.

Step 2. Create an Amazon Transit Gateway

Create an Amazon Transit Gateway that will later connect all your VPCs and the Amazon VPN Gateway.

1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. In the **Transit Gateways** section, click **Transit Gateways**.
4. Enter a name for your Transit Gateway and keep the default values.

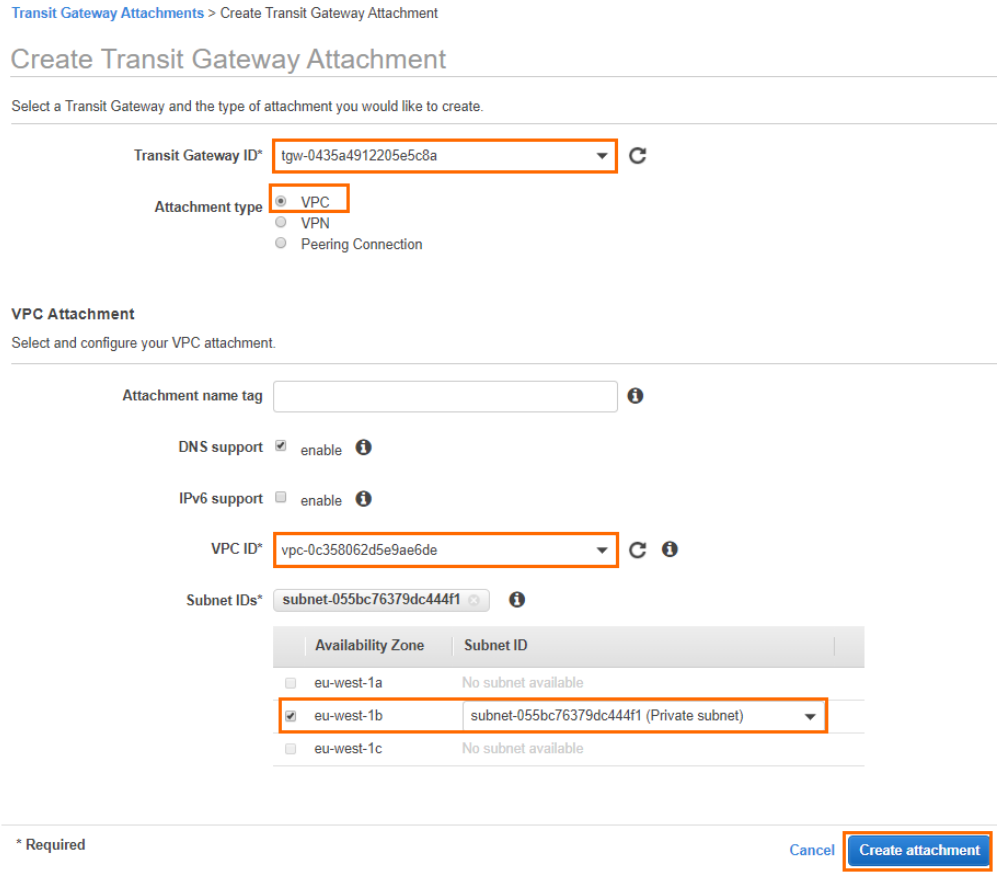


5. Click **Create Transit Gateway**.
6. Click **Services** and select **VPC**.
7. In the **Transit Gateways** section, click **Transit Gateways**.
8. Click on the **Transit Gateway** just created and write down the ASN number next to **Amazon ASN**.

Step 3. Attach Your VPCs to the Transit Gateway

Attach the VPCs you want to be reachable through the Transit Gateway.

1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. In the **Transit Gateways** section, click **Transit Gateway Attachments**.
4. Click **Create Transit Gateway Attachment** and specify values for the following:
   - **Transit Gateway ID** - Select the Transit Gateway created in Step 2.
   - **Attachment type** - Select **VPC**.
   - **VPC ID** - Select the VPC you want to attach to the Transit Gateway.
   - **Subnet ID** - Select the subnet you want to attach to the Transit Gateway.

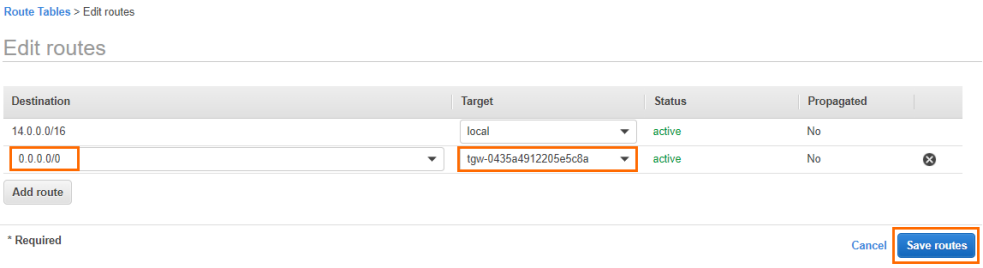


5. Click **Create attachment**.
6. Repeat Step 3 with all VPCs you want to attach to the Transit Gateway.

Step 4. Specify the Transit Gateway as the Default Route of the Attached VPCs.

Configure the route table of the VPCs attached to the Transit Gateway in Step 3 to use the Transit Gateway as default route.

1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. Click **Route Tables**.
4. Search for the name of your VPC attached to the Transit Gateway in Step 3.
5. Select the route table of your VPC and click **Actions > Edit routes**. The **Edit routes** window opens.
6. Click **Add route** and specify values for the following:
   - **Destination** - Enter `0.0.0.0/0.`
   - **Target** - Select **Transit Gateway** from the drop-down list and select the Transit Gateway created in Step 2.

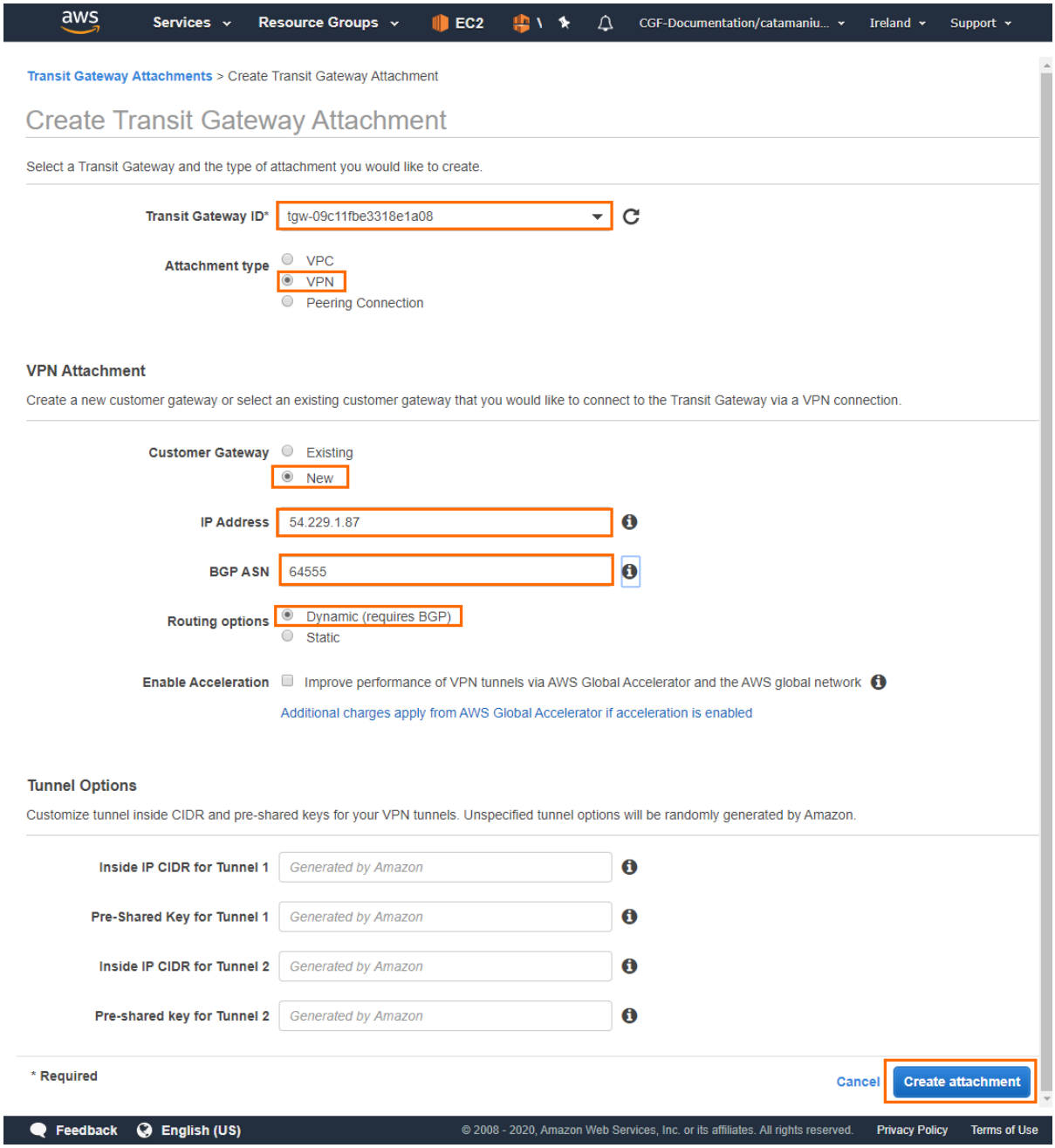


7. Click **Save routes**.
8. Repeat Step 4 with all route tables of all VPCs attached to the Transit Gateway in Step 3.

Step 5. Attach the Amazon VPN Gateway to Your Transit Gateway

Attach the VPN Gateway to your Transit Gateway to allow traffic between all VPCs attached to the Transit Gateway and the VPN Gateway.

1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. In the **Transit Gateways** section, click **Transit Gateway Attachments**.
4. Click **Create Transit Gateway Attachment** and specify values for the following:
   - **Transit Gateway ID** - Select the Transit Gateway created in Step 2.
   - **Attachment type** - Select **VPN**.
   - **Customer Gateway** - Select **New**.
   - **IP Address** – Enter your external **IP Address**, assigned to your firewall in Step1.
   - **BGP ASN** – Enter your BGP ASN number.
   - **Routing options** - Select **Dynamic (requires BGP)**.



5. Click **Create attachment**.

The VPN Gateway is attached to the Transit Gateway and a site-to-site VPN connection is created automatically.

Step 6. Configure an IKEv1 or IKEv2 IPsec VPN to the AWS VPN Gateway Attached to Your Transit Gateway

Step 6.1 Download the Configuration File

Download the configuration file of the site-to-site VPN connection automatically created in Step 5.

1. Log into the AWS console.
2. Click **Services** and select **VPC**.
3. Click **Site-to-Site VPN Connections**.
4. Select the VPN site where the Transit Gateway created in Step 2 is attached to.
5. Click **Download Configuration**.
6. Select generic vendor and platform settings for the configuration file:
   - **Vendor** – Select **Generic**.
   - **Platform** – Select **Generic**.
   - **Software** – Select **Vendor Agnostic**.
7. Click **Download** , and save the `vpn-<YOUR-S2S-ID>.txt` file. The configuration file contains all required information to configure each VPN tunnel and the respective BGP routing options on your CloudGen Firewall.

Step 6.2 Configure an IKEv1 or IKEv2 IPsec Tunnel to the AWS VPN Gateway.

Create an Amazon VPN Gateway and connect your firewall with an IKEv1 or IKEv2 IPsec VPN tunnel with BGP routing enabled. The Amazon virtual private gateway uses two parallel tunnels to ensure constant connectivity.

1. Use the IP addresses provided in the Amazon generic VPN configuration file you downloaded at the end of Step 6.1.
2. Use the ASN number you wrote down before.
3. To connect your firewall, follow the respective guide. Start with Step 2 since the AWS VPN Gateway has already been created :
   - For more information on using an IKEv1 tunnel, see How to Configure an IKEv1 IPsec VPN to an AWS VPN Gateway with BGP
   - For more information on using an IKEv2 tunnel, see How to Configure an IKEv2 IPsec VPN to an AWS VPN Gateway with BGP .
4. Verify that the network your firewall is attached to is advertised via BGP. For more information see Step 3.1 from the guide linked above.
5. Verify that the network your firewall is attached to is allowed by the host firewall rule to access all the VPCs in AWS. For more information see Step 4 from the guide linked above.

Next Steps

- (optional) The default configuration of the Transit Gateway is any-to-any communication, which allows all attached devices to reach all other attached devices. Edit the routing table of your Transit Gateway and the attached VPCs to match your requirements and create host firewall rules accordingly.
- (optional) Connect an on-premise CloudGen Firewall with a TINA tunnel. For more information,

see TINA VPN Tunnels.

Figures

1. ipsec_vpc_aws.png
2. create_tgw.png
3. create_attach2.png
4. edit_routes.png
5. tgw_vpn_attach042020.png