AWS VPC VPN – CloudHub Connections

# VPC VPN Connections

* VPC VPN connections are used to extend on-premise data centers to AWS
* **VPC VPN connections provide secure IPSec connections from on-premise computers/services to AWS**
* **AWS hardware VPN**
  + Connectivity can be established by creating an IPSec, hardware VPN connection between the VPC and the remote network.
  + On the AWS side of the VPN connection, a Virtual Private Gateway (VGW) provides two VPN endpoints for automatic failover.
  + On customer side a customer gateway (CGW) needs to be configured, which is the physical device or software application on the remote side of the VPN connection
* **AWS Direct Connect**
  + **AWS Direct Connect provides a dedicated private connection from a remote network to your VPC.**
  + **Direct Connect can be combined with an AWS hardware VPN connection to create an IPsec-encrypted connection**
* AWS VPN CloudHub
  + For more than one remote network for e.g. multiple branch offices, multiple AWS hardware VPN connections can be created via the VPC to enable communication between these networks
* **Software VPN (AWS Client VPN)**
  + VPN connection can be setup by running a software VPN like OpenVPN appliance on an EC2 instance in the VPC
  + AWS does not provide or maintain software VPN appliances; however, there are range of products provided by partners and open source communities

## Client VPN endpoint (AWS Client VPN)

## Graphical user interface Description automatically generated

**Lab Steps:**

* + 1. Download OpenVPN software package.
    2. Install OpenVPN software on a windows machine.
    3. Follow instructions to generate client & server certificate to upload in AWS certificate manager.
    4. Using windows machine IP range & uploaded ACM certs, Create new Client VPN endpoint “My-OpenVPN-Connection”
    5. Associate a VPC & subnet as destination with “My-OpenVPN-Connection” for windows machine to connect.
    6. Once association finishes, down client configuration file.
    7. Import client configuration file in OpenVPN software on windows machine.
    8. Try to establish a connection & verify if it works.

## Hardware VPN Connection (Site to Site VPN)

### A screenshot of a computer Description automatically generated with medium confidence

### VPN Components

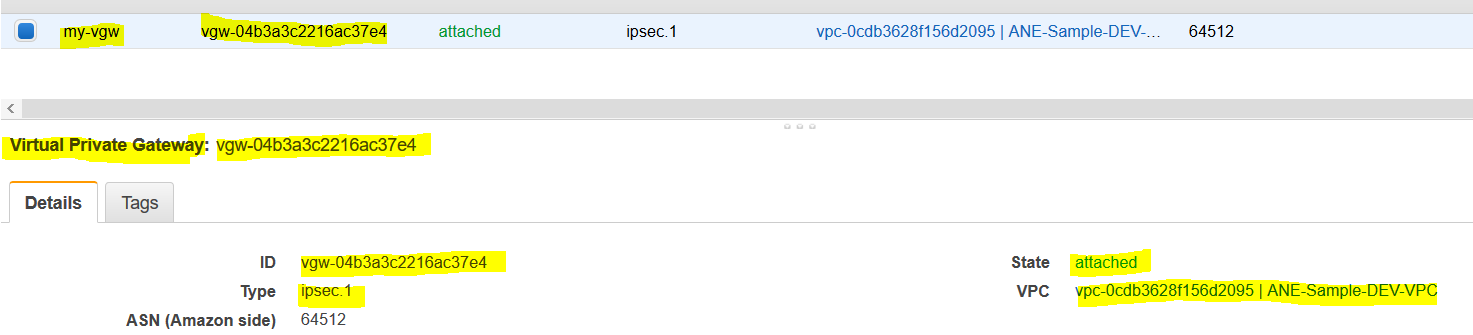
* **Virtual Private Gateway – VGW**
  + A virtual private gateway is the VPN concentrator on the AWS side of the VPN connection
* **Customer Gateway – CGW**
  + A customer gateway is a physical device or software application on customer side of the VPN connection.
  + **When a VPN connection is created, the VPN tunnel comes up when traffic is generated from the remote side(OnPrem DataCenter) of the VPN connection**.
  + **VGW is not the initiator**; **CGW must initiate the tunnels**
  + **If the VPN connection experiences a period of idle time, usually 10  seconds, depending on the configuration, the tunnel may go down. To prevent this, a network monitoring tool to generate keepalive pings; for e.g. by using IP SLA.**

### A screenshot of a computer Description automatically generated with medium confidence

### VPN Configuration

* VPC has an attached virtual private gateway, and the remote network includes a customer gateway, which must be configured to enable the  
  VPN connection.

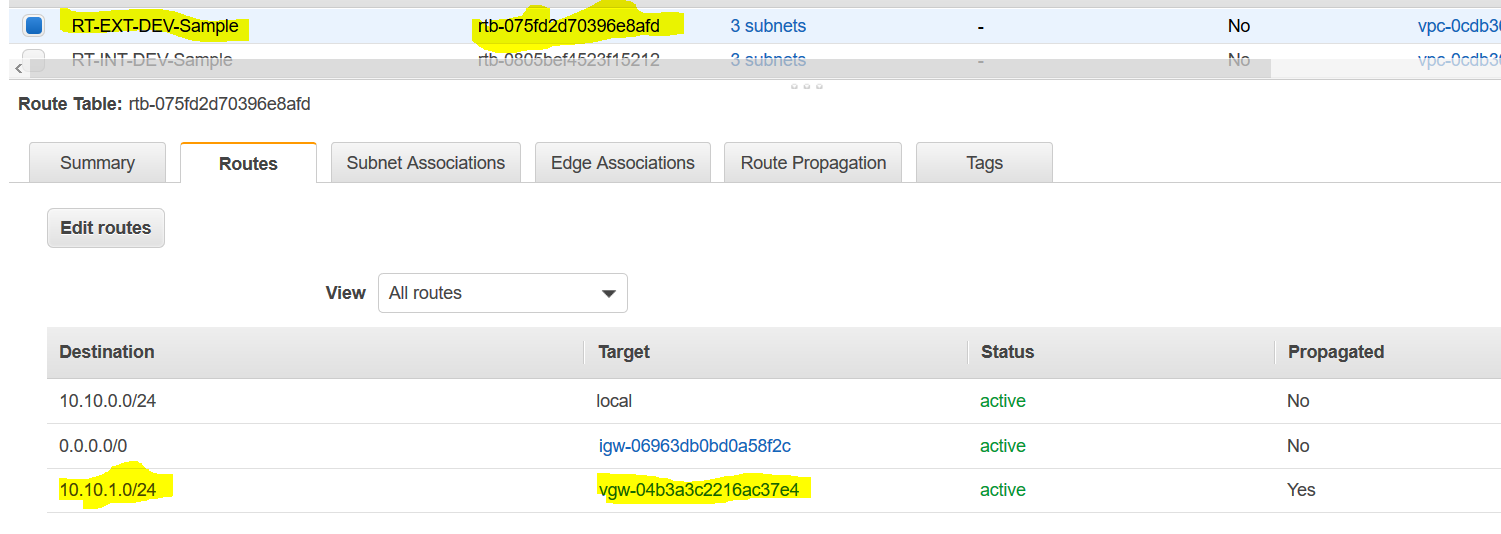
VGW:



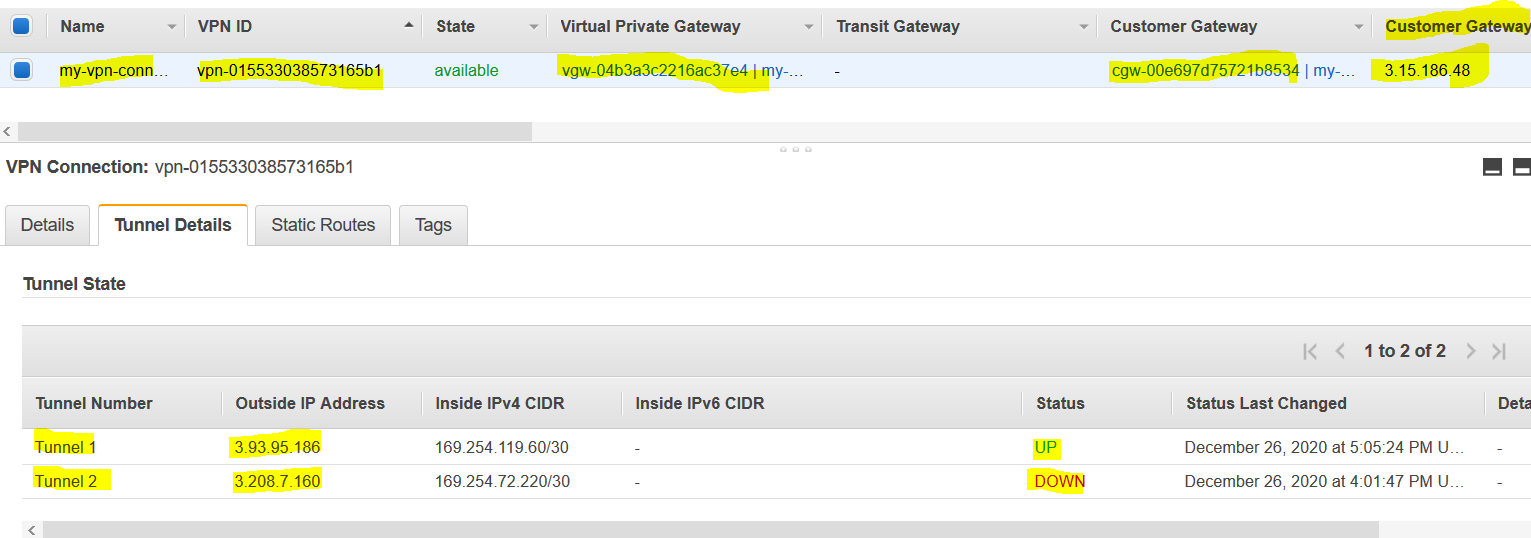
CGW:



* Routing must be setup so that any traffic from the VPC bound for the remote network is routed to the virtual private gateway.



* Each VPN has two tunnels associated with it that can be configured on the customer router, as is not single point of failure.

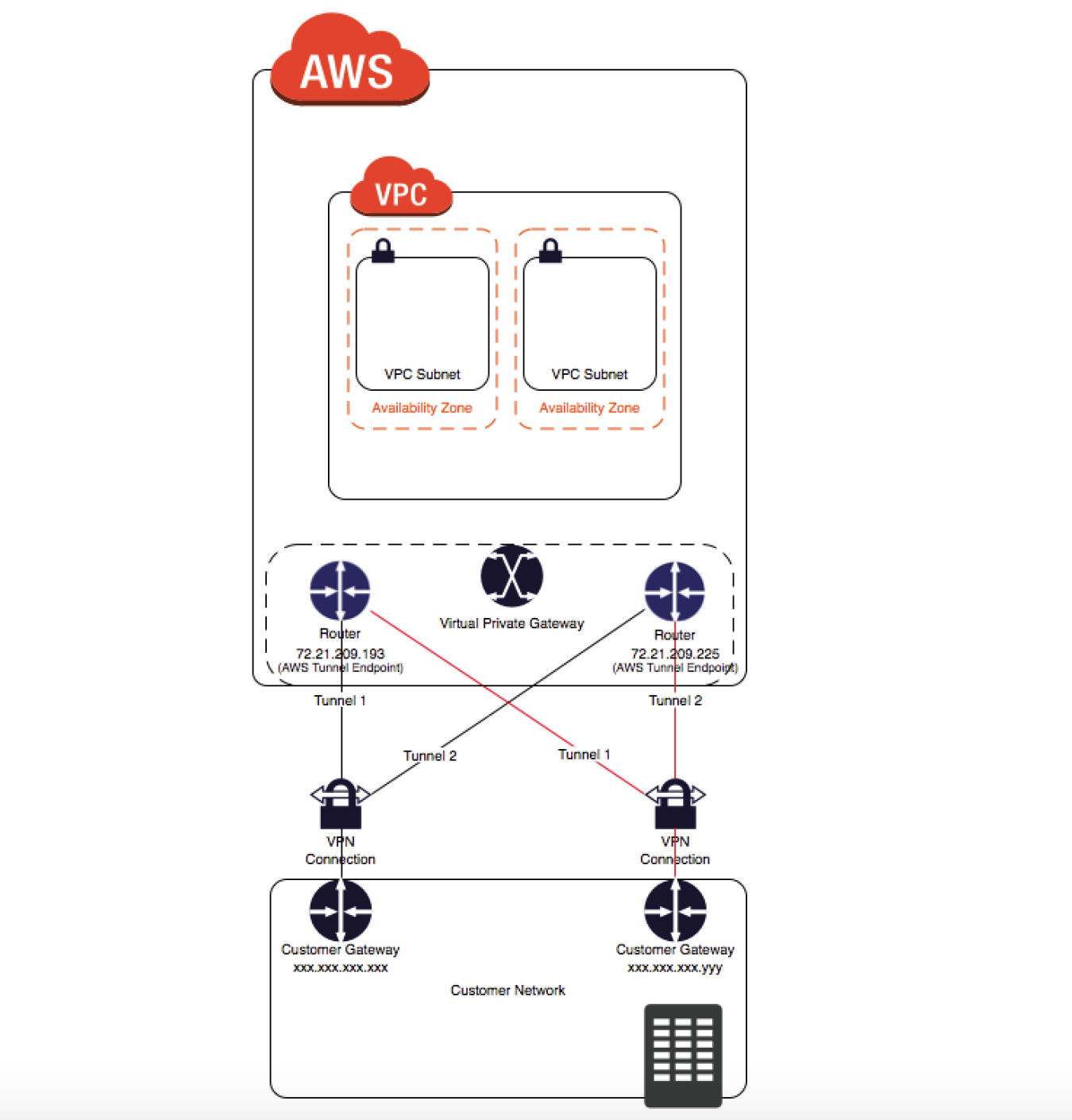


* **Multiple VPN connections to a single VPC can be created, and a second CGW can be configured to create a redundant connection to the same external location or to create VPN connections to multiple geographic locations**.

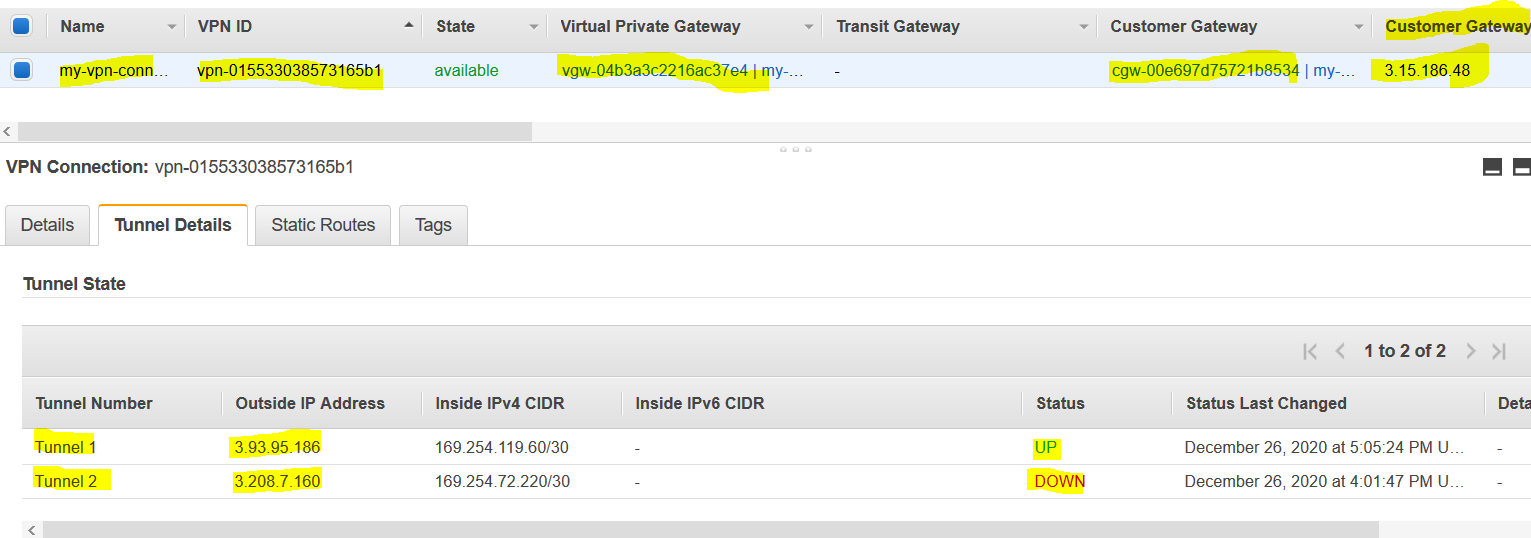
### VPN Routing Options

* For a VPN connection, the route table for the subnets should be updated with the type of routing (static of dynamic) that you plan to use.
* Route tables determine where network traffic is directed. Traffic destined for the VPN connections must be routed to the virtual private gateway.
* **Type of routing can depend on the make and model of your VPN devices.**
  + **Static Routing**
    - **If your device does not support BGP, specify static routing.**
    - **Using static routing, the routes (IP prefixes) can be specified that should be communicated to the virtual private gateway.**
    - Devices that don’t support BGP may also perform health checks to assist failover to the second tunnel when needed.
  + **BGP dynamic routing**
    - If the VPN device supports Border Gateway Protocol (BGP), specify dynamic routing with the VPN connection.
    - **When using a BGP device, static routes need not be specified to the VPN connection because the device uses BGP for auto discovery and to advertise its routes to the virtual private gateway.**
    - **BGP-capable devices are recommended as the BGP protocol offers robust liveness detection checks that can assist failover to the second VPN tunnel if the first tunnel goes down**.
* Only IP prefixes known to the virtual private gateway, either through BGP advertisement or static route entry, can receive traffic from your VPC.
* Virtual private gateway does not route any other traffic destined outside of the advertised BGP, static route entries, or its attached VPC CIDR.

#### **VPN Connection Redundancy**



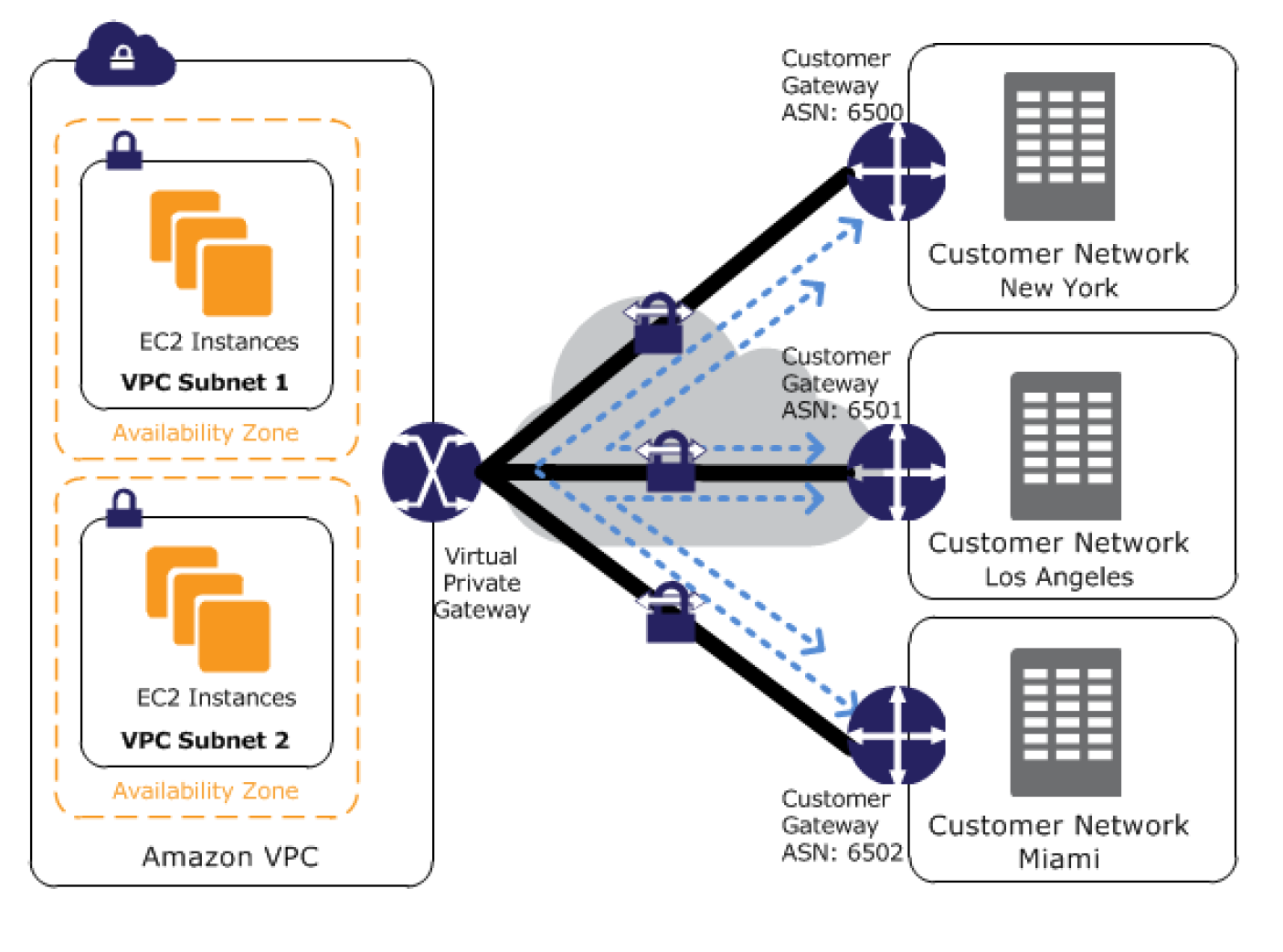
* A VPN connection is used to connect the customer network to a VPC.
* Each VPN connection has two tunnels to help ensure connectivity in case one of the VPN connections becomes unavailable, with each tunnel using a unique virtual private gateway public IP address.



* Both tunnels should be configured for redundancy.
* When one tunnel becomes unavailable, for e.g. down for maintenance, network traffic is automatically routed to the available tunnel for that specific VPN connection.
* **To protect against a loss of connectivity in case the customer gateway becomes unavailable, a second VPN connection can be setup to the VPC and virtual private gateway by using a second customer gateway**.
* **Customer gateway IP address for the second VPN connection must be publicly accessible.**
* By using redundant VPN connections and CGWs, maintenance on one of the customer gateways can be performed while traffic continues to flow over the second customer gateway’s VPN connection.
* **Dynamically routed VPN connections using the Border Gateway Protocol (BGP) are recommended, if available, to exchange routing information between the customer gateways and the virtual private gateways.**
* Statically routed VPN connections require static routes for the network to be entered on the customer gateway side.
* BGP-advertised and statically entered route information allow gateways on both sides to determine which tunnels are available and reroute traffic if a failure occurs.

## VPN CloudHub

* VPN CloudHub can be used to provide secure communication between sites, if you have multiple VPN connections
* VPN CloudHub operates on a simple hub-and-spoke model that can be used with or without a VPC.
* Design is suitable for customers with multiple branch offices and existing Internet connections who’d like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices



A picture containing timeline

Description automatically generated

* VPN CloudHub architecture with blue dashed lines indicates network traffic between remote sites being routed over their VPN connections.
* AWS VPN CloudHub requires a virtual private gateway with multiple customer gateways.
* Each customer gateway must use a unique Border Gateway Protocol (BGP) Autonomous System Number (ASN)
* Customer gateways advertise the appropriate routes (BGP prefixes) over their VPN connections.
* Routing advertisements are received and re-advertised to each BGP peer, enabling each site to send data to and receive data from the other sites.
* Routes for each spoke must have unique ASNs and the sites must not have overlapping IP ranges.
* Each site can also send and receive data from the VPC as if they were using a standard VPN connection.
* Sites that use AWS Direct Connect connections to the virtual private gateway can also be part of the AWS VPN CloudHub.
* To configure the AWS VPN CloudHub,
  + multiple customer gateways can be created, each with the unique public IP address of the gateway and the ASN.
  + a VPN connection can be created from each customer gateway to a common virtual private gateway.
  + each VPN connection must advertise its specific BGP routes. This is done using the network statements in the VPN configuration files for the VPN connection.

## AWS Certification Exam Practice Questions

1. You have in total 5 offices, and the entire employee related information is stored under AWS VPC instances. Now all the offices want to connect the instances in VPC using VPN. Which of the below help you to implement this?
   1. you can have redundant customer gateways between your data center and your VPC
   2. you can have multiple locations connected to the AWS VPN CloudHub
   3. You have to define 5 different static IP addresses in route table.
   4. **1 and 2**
   5. 1,2 and 3
2. You have in total 15 offices, and the entire employee related information is stored under AWS VPC instances. Now all the offices want to connect the instances in VPC using VPN. What problem do you see in this scenario?
   1. You can not create more than 1 VPN connections with single VPC (Can be created)
   2. You can not create more than 10 VPN connections with single VPC (soft limit can be extended)
   3. When you create multiple VPN connections, the virtual private gateway can not sends network traffic to the appropriate VPN connection using statically assigned routes. (Can route the traffic to correct connection)
   4. Statically assigned routes cannot be configured in case of more than 1 VPN with virtual private gateway. (can be configured)
   5. **None of above**
3. You have been asked to virtually extend two existing data centers into AWS to support a highly available application that depends on existing, on-premises resources located in multiple data centers and static content that is served from an Amazon Simple Storage Service (S3) bucket. Your design currently includes a dual-tunnel VPN connection between your CGW and VGW. Which component of your architecture represents a potential single point of failure that you should consider changing to make the solution more highly available?
   1. Add another VGW in a different Availability Zone and create another dual-tunnel VPN connection.
   2. **Add another CGW in a different data center and create another dual-tunnel VPN connection.**(Refer [link](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html))
   3. Add a second VGW in a different Availability Zone, and a CGW in a different data center, and create another dual-tunnel.
   4. No changes are necessary: the network architecture is currently highly available.
4. You are designing network connectivity for your fat client application. The application is designed for business travelers who must be able to connect to it from their hotel rooms, cafes, public Wi-Fi hotspots, and elsewhere on the Internet. You do not want to publish the application on the Internet. Which network design meets the above requirements while minimizing deployment and operational costs? **[PROFESSIONAL]**
   1. Implement AWS Direct Connect, and create a private interface to your VPC. Create a public subnet and place your application servers in it. (High Cost and does not minimize deployment)
   2. Implement Elastic Load Balancing with an SSL listener that terminates the back-end connection to the application. (Needs to be published to internet)
   3. Configure an IPsec VPN connection, and provide the users with the configuration details. Create a public subnet in your VPC, and place your application servers in it. (Instances still in public subnet are internet accessible)
   4. **Configure an SSL VPN solution in a public subnet of your VPC, then install and configure SSL VPN client software on all user computers. Create a private subnet in your VPC and place your application servers in it.**(Cost effective and can be in private subnet as well)
5. You are designing a connectivity solution between on-premises infrastructure and Amazon VPC Your server’s on-premises will De communicating with your VPC instances You will De establishing IPSec tunnels over the internet You will be using VPN gateways and terminating the IPsec tunnels on AWS-supported customer gateways. Which of the following objectives would you achieve by implementing an IPSec tunnel as outlined above? (Choose 4 answers) **[PROFESSIONAL]**
   1. End-to-end protection of data in transit
   2. End-to-end Identity authentication
   3. **Data encryption across the Internet**
   4. **Protection of data in transit over the Internet**
   5. **Peer identity authentication between VPN gateway and customer gateway**
   6. **Data integrity protection across the Internet**
6. A development team that is currently doing a nightly six-hour build which is lengthening over time on-premises with a large and mostly under utilized server would like to transition to a continuous integration model of development on AWS with multiple builds triggered within the same day. However, they are concerned about cost, security and how to integrate with existing on-premises applications such as their LDAP and email servers, which cannot move off-premises. The development environment needs a source code repository; a project management system with a MySQL database resources for performing the builds and a storage location for QA to pick up builds from. What AWS services combination would you recommend to meet the development team’s requirements? **[PROFESSIONAL]**
   1. A Bastion host Amazon EC2 instance running a VPN server for access from on-premises, Amazon EC2 for the source code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIP for the source code repository and project management system, Amazon SQL for a build queue, An Amazon Auto Scaling group of Amazon EC2 instances for performing builds and Amazon Simple Email Service for sending the build output. (Bastion is not for VPN connectivity also SES should not be used)
   2. An AWS Storage Gateway for connecting on-premises software applications with cloud-based storage securely, Amazon EC2 for the resource code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, Amazon Simple Notification Service for a notification initiated build, An Auto Scaling group of Amazon EC2 instances for performing builds and Amazon S3 for the build output. (Storage Gateway does provide secure connectivity but still needs VPN. SNS alone cannot handle builds)
   3. An AWS Storage Gateway for connecting on-premises software applications with cloud-based storage securely, Amazon EC2 for the resource code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, Amazon SQS for a build queue, An Amazon Elastic Map Reduce (EMR) cluster of Amazon EC2 instances for performing builds and Amazon CloudFront for the build output. (Storage Gateway does not provide secure connectivity, still needs VPN. EMR is not ideal for performing builds as it needs normal EC2 instances)
   4. **A VPC with a VPN Gateway back to their on-premises servers, Amazon EC2 for the source-code repository with attached Amazon EBS volumes, Amazon EC2 and Amazon RDS MySQL for the project management system, EIPs for the source code repository and project management system, SQS for a build queue, An Auto Scaling group of EC2 instances for performing builds and S3 for the build output.**(VPN gateway is required for secure connectivity. SQS for build queue and EC2 for builds)