Advanced VPC Concepts: Virtual Private Networks (VPNs)

Andru Estes
Principal Author
andru-estes

Protecting VPC Networking with VPNs

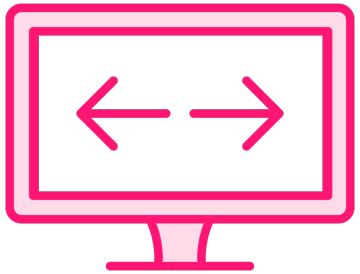
Virtual Private Network (VPN)

A VPN is meant to establish encrypted connections between computer devices over the public Internet. A secure method to mimic the privacy of an internal/private network connection.

There are 4 primary VPN methods to connect to your AWS VPC.

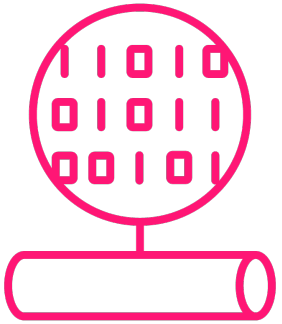
VPN Methods

Site-to-Site VPN



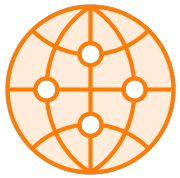
AWS Client VPN

AWS VPN CloudHub



Third-party VPN

Important AWS VPN Components - VGW



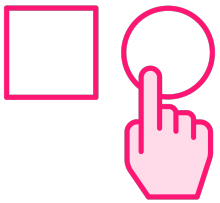
A Virtual Private Gateway (VGW) is the VPN concentrator that is deployed on the AWS side of a VPN connection

You create a VGW and then you attach it to the VPC that you wish to create your Site-to-Site VPN connection with

You have the ability to customize the Autonomous System Number (ASN) if you desire

Important AWS VPN Components - CGW

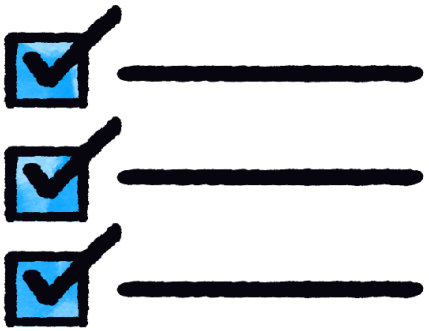
A Customer Gateway (CGW) is the software appliance or physical networking device on the customer side of the VPN connection



You are required to fully configure the device to work with the Site-to-Site VPN, and not all devices are supported

The AWS CGW resource essentially provides the required information to AWS about your device or software application

VPN Use Cases



- Securing hybrid cloud network architectures
- Implementing Disaster Recovery (DR) networking connections
- Interconnecting VPCs
- Establishing Transit VPCs
- Connecting to third-party vendors

Site-to-Site (S2S) VPNs

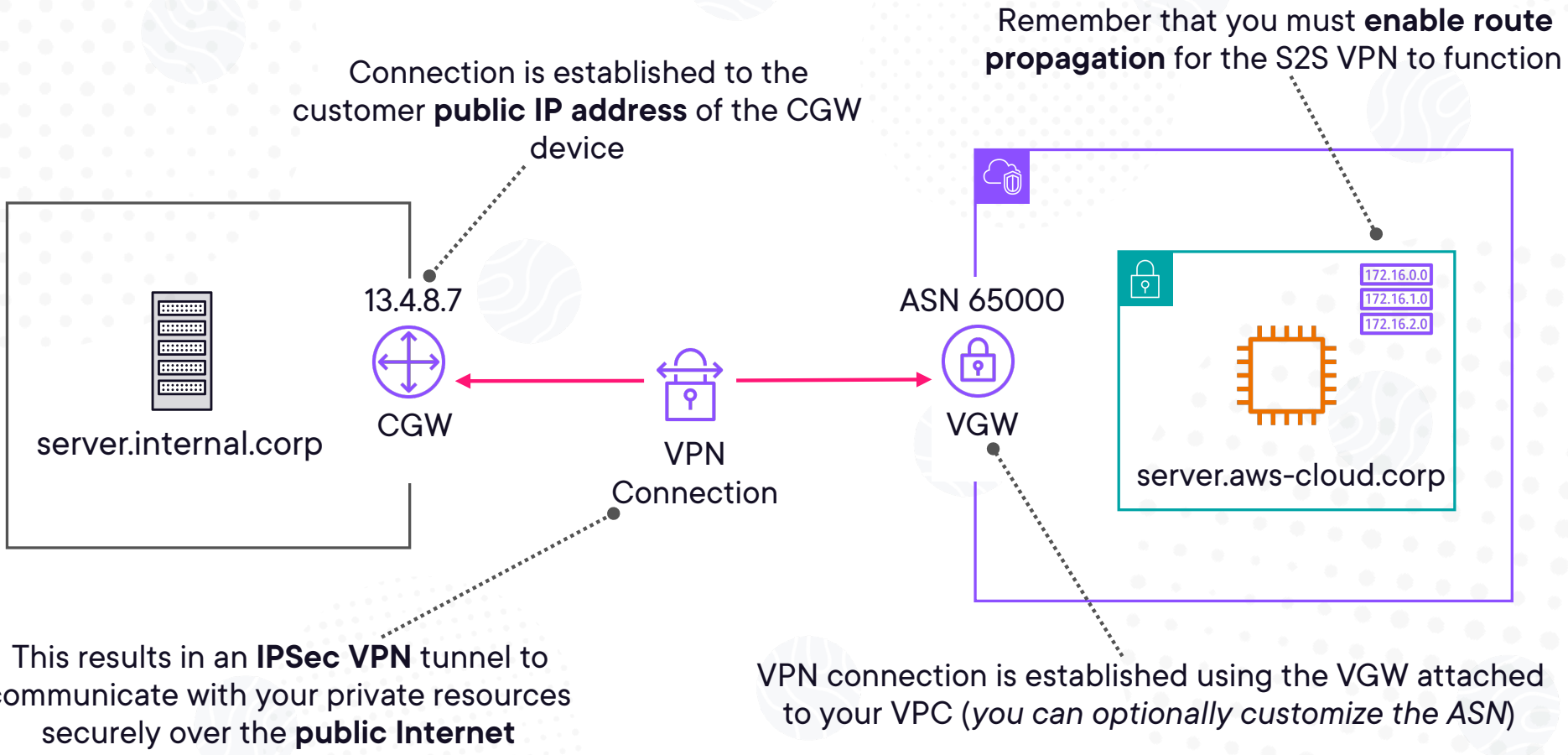
Requirements for the CGW

You must use a publicly resolvable IP address on your side of the VPN connection

If you have NAT-T (*NAT Traversal*) in place, then you use the public IP of the NAT device that fronts your CGW

You must enable route propagation within your VPC route tables for this to work

Site-to-Site VPN Diagram



Exam Pro Tip: If you need an IPSec VPN solution, you likely want to consider a Site-to-Site VPN.

AWS Client VPN

AWS Client VPN

Managed client-based VPN service that enables you to securely access your AWS resources and resources in your on-premises network

AWS Client VPN Concepts

AWS-managed version of well-known OpenVPN

You can use any OpenVPN compatible software to connect

Allows you to connect from anywhere in the world

Leverages TLS connections for the VPN

Automatically scales to support the number of users

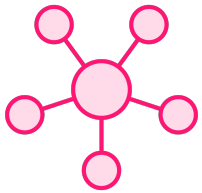
Exam Pro Tip: Use this to access your resources from any location using an OpenVPN-based VPN client.

AWS VPN CloudHub

AWS VPN CloudHub

Allows you to securely communicate from one site to another via Site-to-Site VPNs

AWS VPN CloudHub Concepts

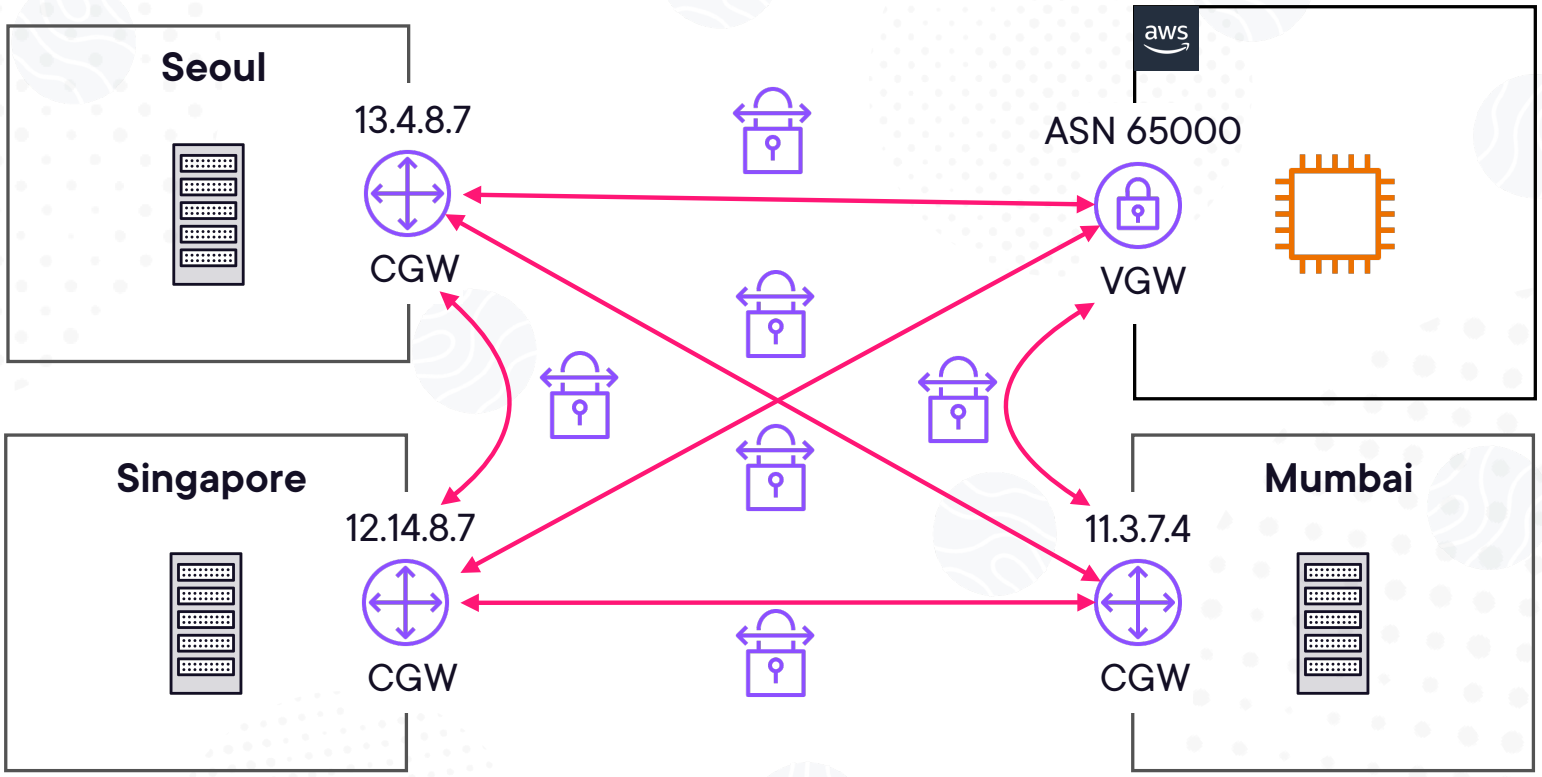


Allows you to set up and operate a simple hub-and-spoke VPN model for multiple Site-to-Site VPN (S2S VPN)

You can use with or without a VPC in place!

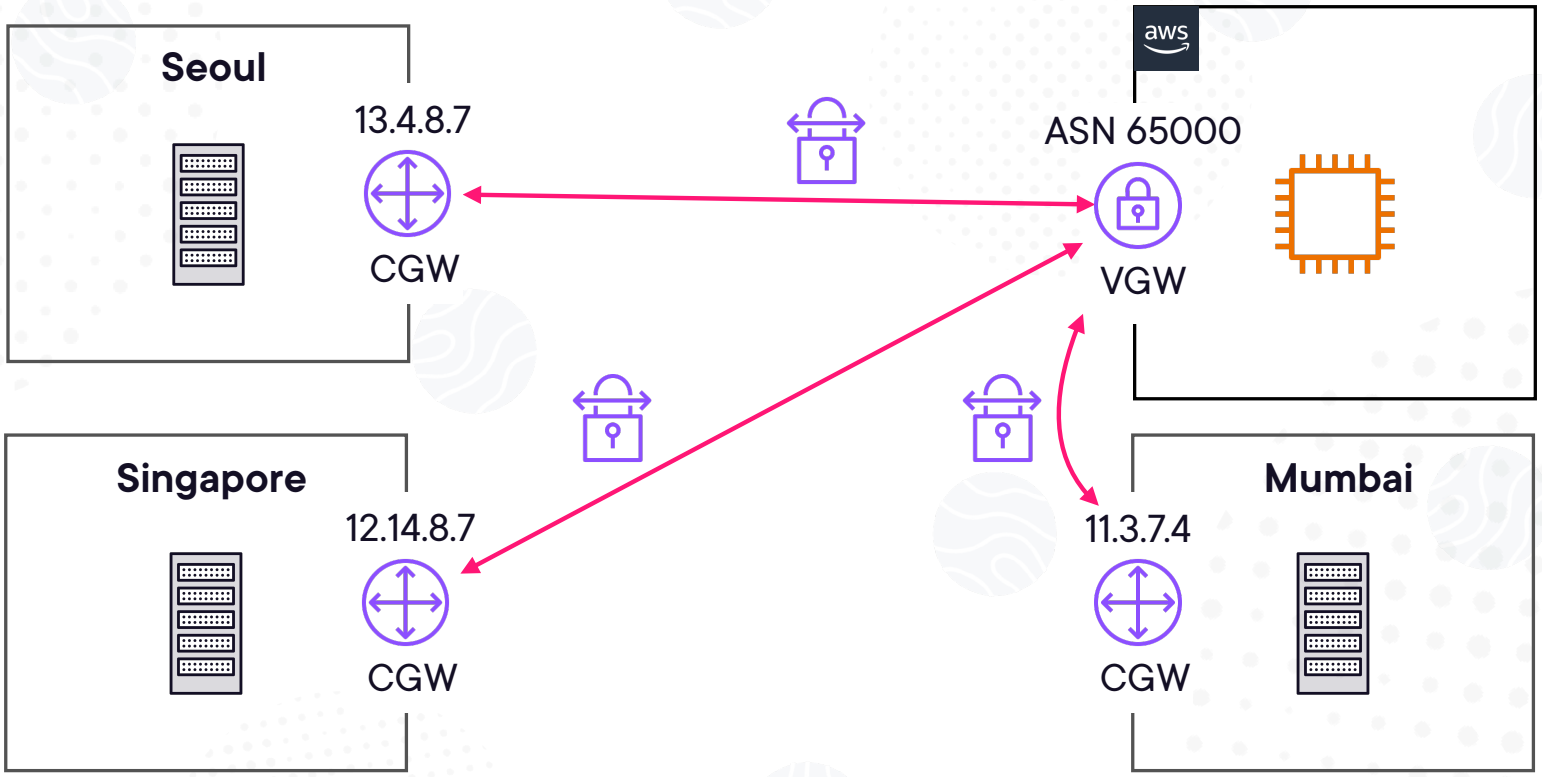
Perfect for multiple data centers where you need convenient, low-cost hub-and-spoke VPN connectivity

AWS VPN CloudHub Diagram - Without CloudHub



To communicate between datacenters, you need a separate VPN Connection between each one, as well as a connection from each datacenter to the VPC.
Adds complexity and overhead!

AWS VPN CloudHub Diagram - With CloudHub



VPN CloudHub allows all spoke datacenters (*Site-to-Site VPN*) to communicate with one another and, optionally, VPCs.
More efficient and less overhead!

Exam Pro Tip: Use AWS VPN CloudHub to simplify S2S VPN connection management!

Implementing a Third-party VPN

Using Third-party VPNs

These are typically obtained from the AWS Marketplace and they will run on EC2 instances

Scenarios when you might use a third-party VPN:

- Need to enable transitive routing on the AWS side of things
- Desire to enable special capabilities not native to AWS-managed VPNs
- Bandwidth considerations

Things You Need to Know

Disable source/ destination check on the EC2 instance

Automating failover recovery is your responsibility

Need to plan your EC2 instance sizing carefully

Vertically scaling is common with this type of VPN

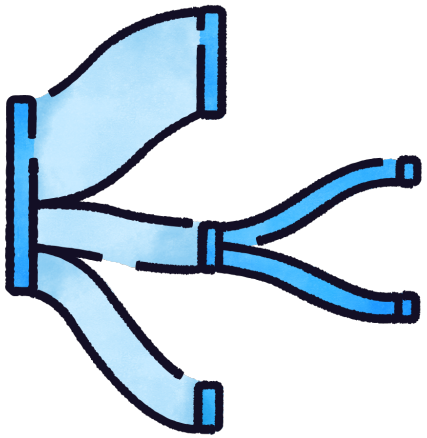
Generally not recommended for exam scenarios

Exam Pro Tip: Exam scenarios rarely want you to select this type of VPN solution.

Module Summary and Exam Tips

Remember that VPNs are put into place to offer encrypted, protected networking channels.

VGWs and CGWs



Virtual Private Gateways

VPN concentrator that is deployed on the AWS side of a VPN connection and is attached to VPCs

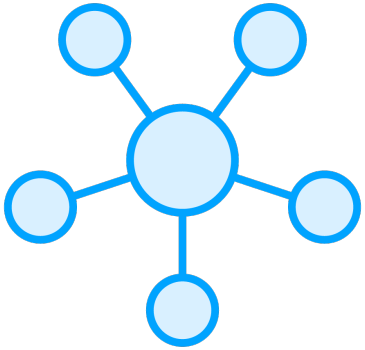
Customer Gateways

The software appliance or physical networking device on the customer side of the VPN connection

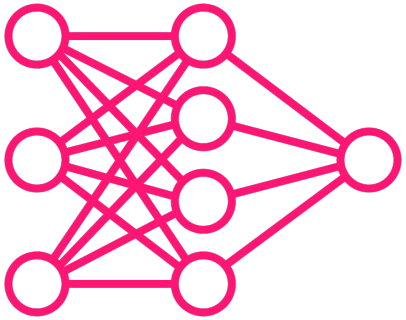
Which VPN to Choose?

Site-to-Site
Most secure due to IPSec connections

AWS Client VPN
TLS connections using OpenVPN clients



VPN CloudHub
Hub-and-spoke VPN model for S2S VPNs



Third-party
Whenever you need very specific customizations