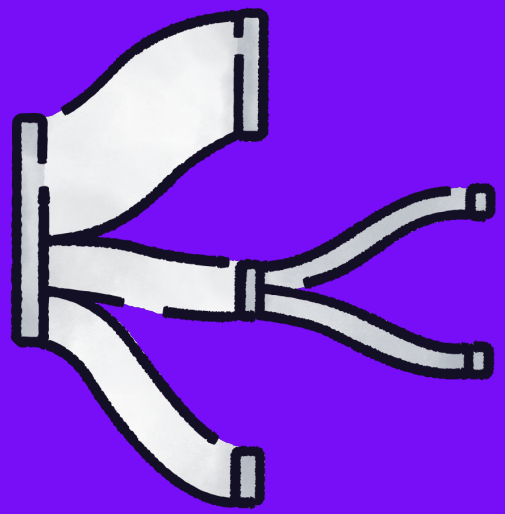
# Advanced VPC Concepts: Direct Connections, Direct Connect Gateways, and Transit Gateways

**Andru Estes**
Principal Author
andru-estes

# Exploring Direct Connections



# AWS Direct Connect (DX)

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS

# Private Connectivity

Using AWS DX, you can establish private connectivity between AWS and your datacenter or office

You can actually reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than using internet-based connections

These have to be set up between your datacenters and a DX location

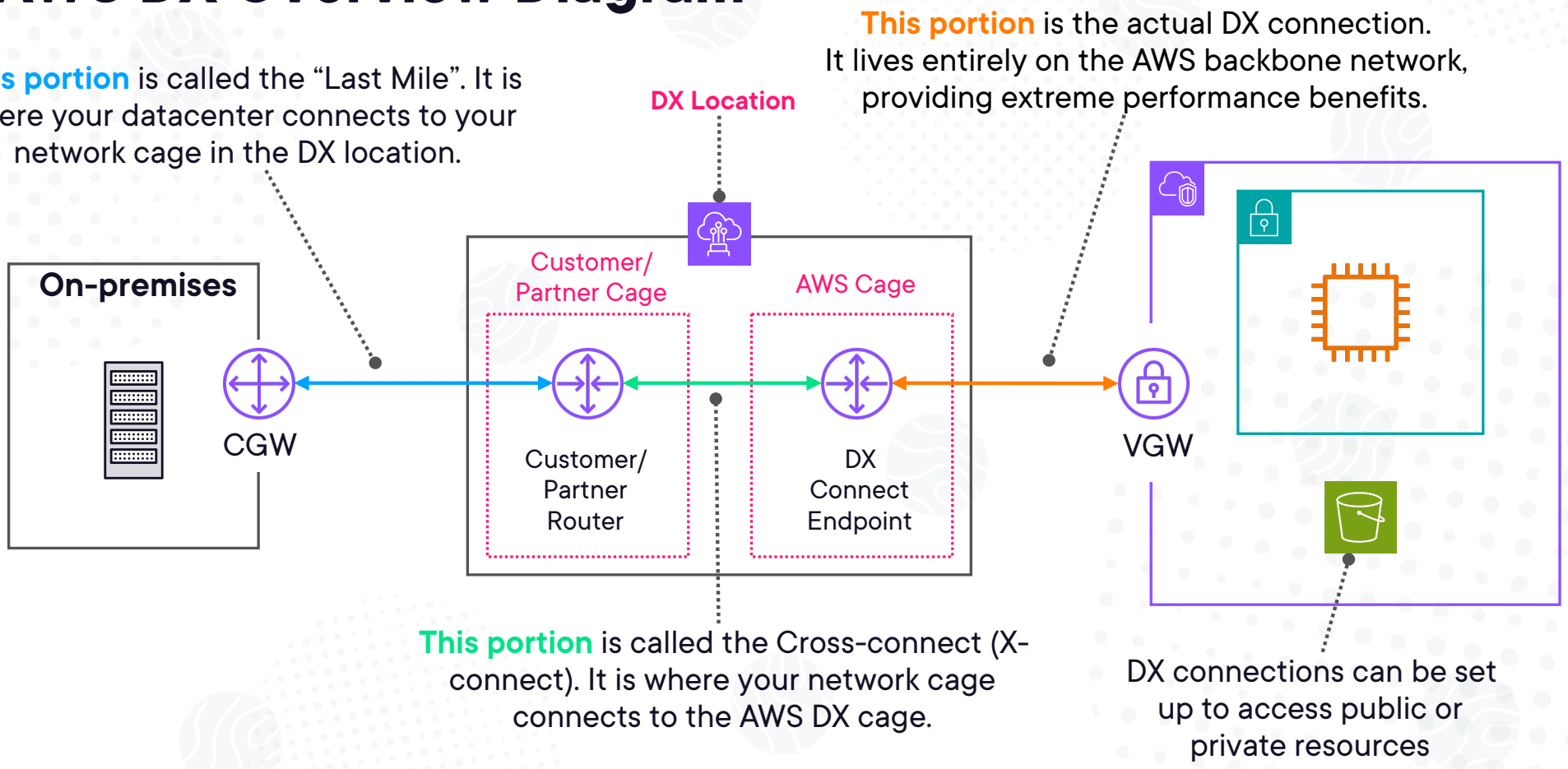
To use a DX, you must create a VGW and attach it to your VPC

They offer private access to both public and private resources (*discussed later on*)

DX connections support both IPv4 and IPv6

*Image Source: http://unsplash.com*

# AWS DX Overview Diagram

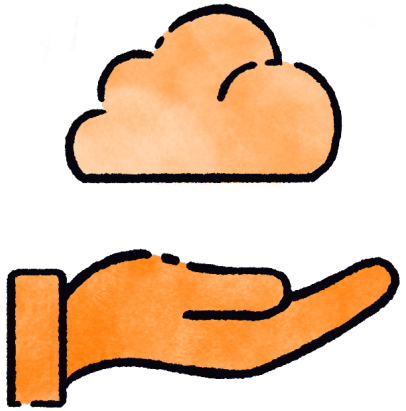


# Choosing the Correct Direct Connect Type

# The Different DX Connection Types

**Dedicated**

A physical Ethernet connection associated with a single customer

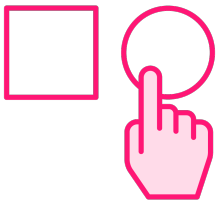


**Hosted**

A physical Ethernet connection that an AWS DX Partner provisions on behalf of a customer

# Dedicated Connection Types

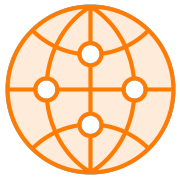
Customers can request one through the AWS DX console, the CLI, or the API. Request is made to AWS, and then completed by a DX partner.



Available capacity: 1 Gbps, 10 Gbps, 100 Gbps, and 400 Gbps

Usually the best option if you need maximum DX performance and you need full privacy of the connection, but far less flexibility in choices.

# Hosted Connection Types



You request these by contacting a partner in the AWS DX Partner Program, and you can add or remove capacity as required.

Available capacity: 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps*, 2 Gbps*, 5 Gbps*, 10 Gbps*, and 25 Gbps*

These provide the most flexibility, but only specific AWS DX partners can create connections with speeds marked with the asterisks (*).

**Keep in mind that DX connections are not immediately available to use!**

# Virtual Interfaces

**You leverage DX connections by attaching the DX Virtual Interfaces (VIF) to your VGW that is attached to your VPCs**

**VIFs allow you to connect to AWS services over the private DX connection instead of the public internet**

**They come in two primary categories:**

- Public: S3, DynamoDB, Route 53, SQS
- Private: EC2 instances, RDS, Lambda, VPC endpoints

# Virtual Interfaces Summary

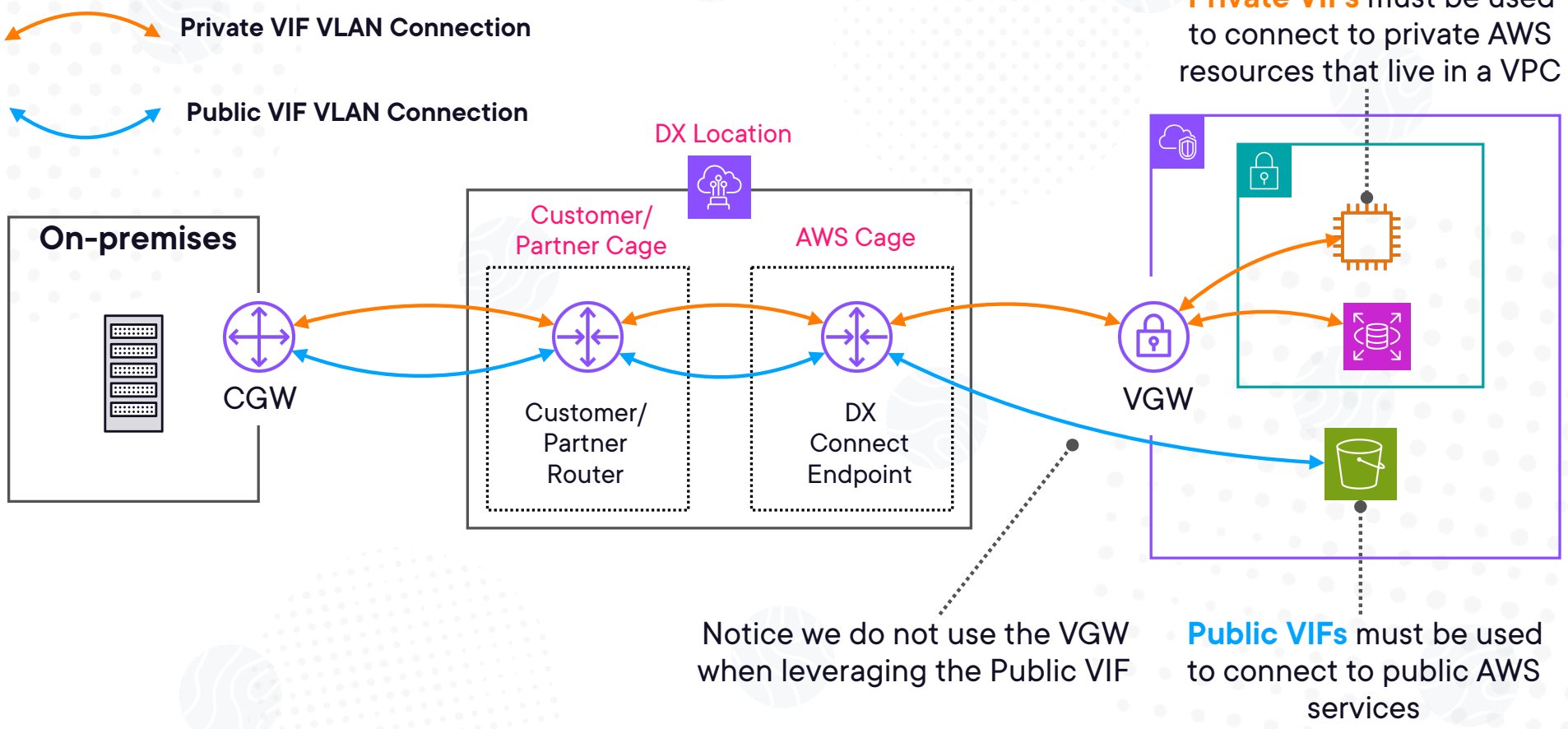
## Public VIF

Access public AWS services

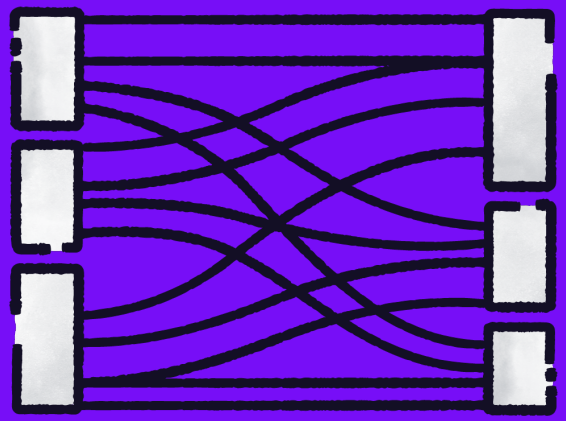
## Private VIF

Access private (VPC) resources

# AWS DX VIF Diagram



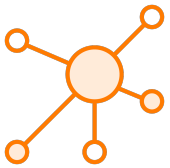
# Centralizing Management with Direct Connect Gateways



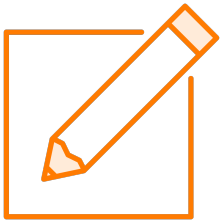
# AWS Direct Connect Gateways

Globally available resource that allows you to connect multiple VPCs across different AWS Regions to your on-premises networks through a single Direct Connect connection

# AWS Direct Connect Gateway Concepts



Direct Connect gateways connect to a Direct Connect location in a Region, which connects to the chosen DX location



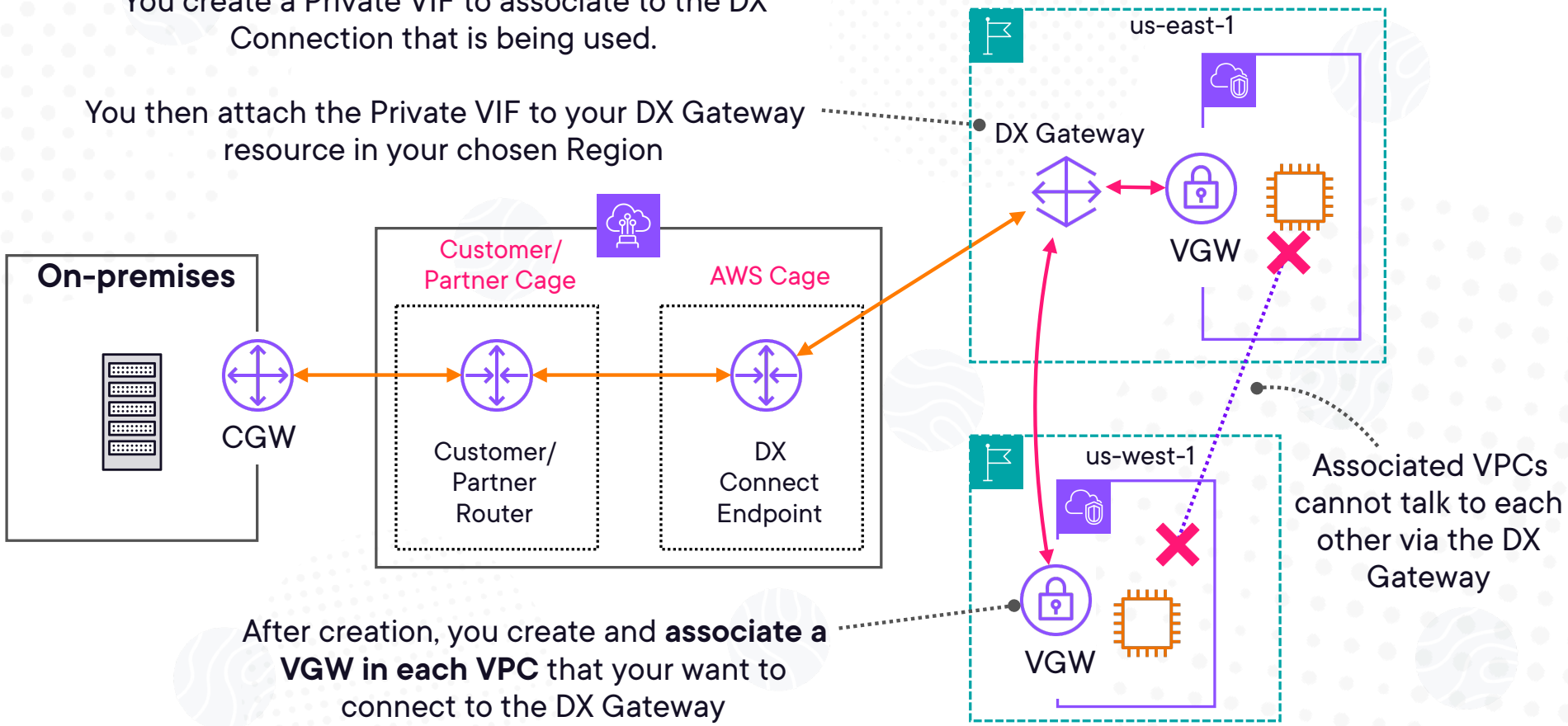
**Important Note**: AWS recently launched multi-account support for this feature, allowing up to 10 VPCs to be associated from different accounts (*must be in the same AWS Organization with a shared Payer account)*

These **do not allow** gateway associations that are on the same Direct Connect gateway to send traffic to each other (*VPC to VPC*)

# AWS DX Gateway Diagram

You create a Private VIF to associate to the DX Connection that is being used.

You then attach the Private VIF to your DX Gateway resource in your chosen Region



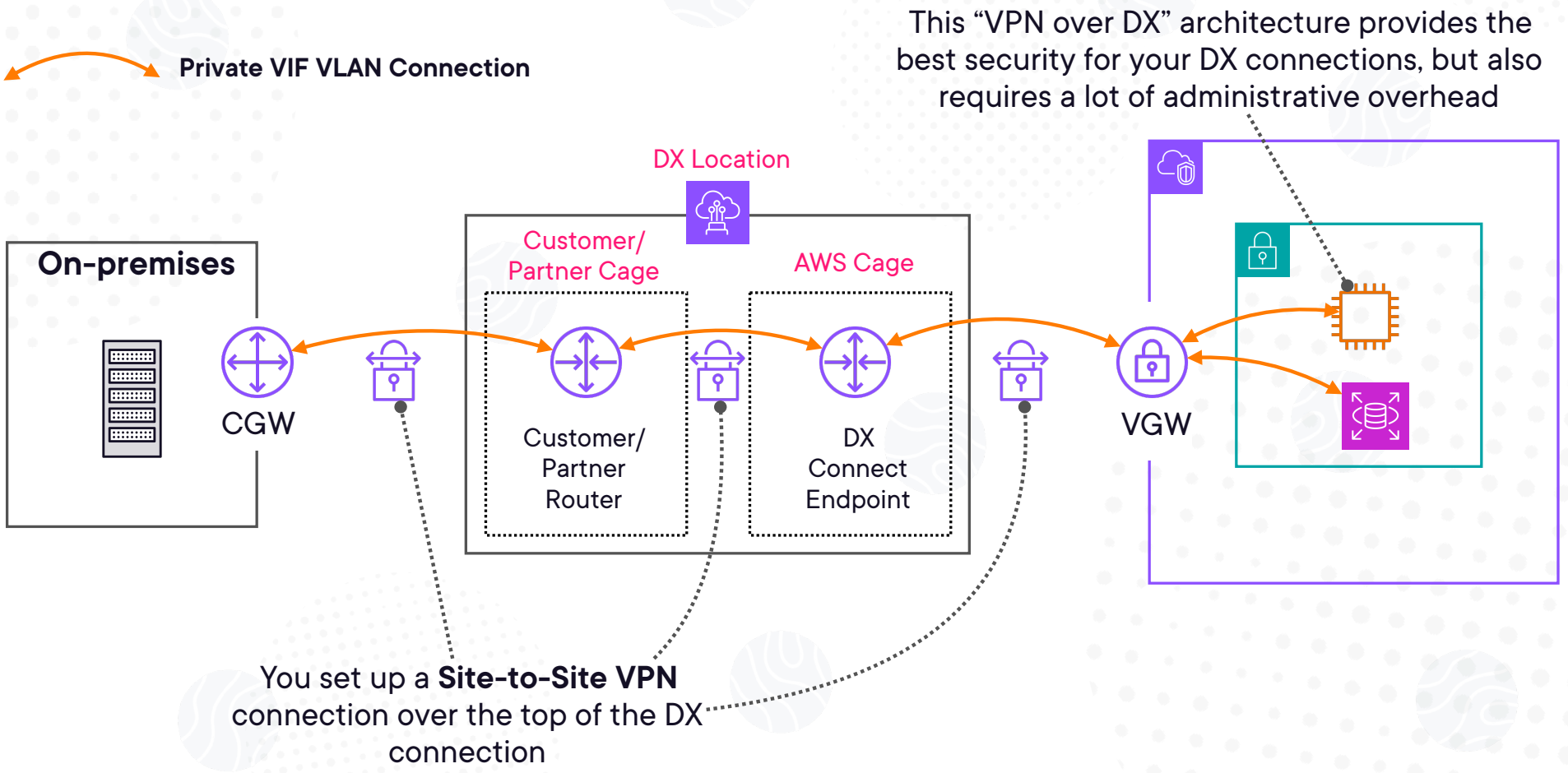

After creation, you create and **associate a VGW in each VPC** that your want to connect to the DX Gateway

**Exam Pro Tip: This resource offers a centralized point for managing connections between your on-premises network and AWS resources via AWS DX.**

# Encrypting Network Traffic with VPN over Direct Connect

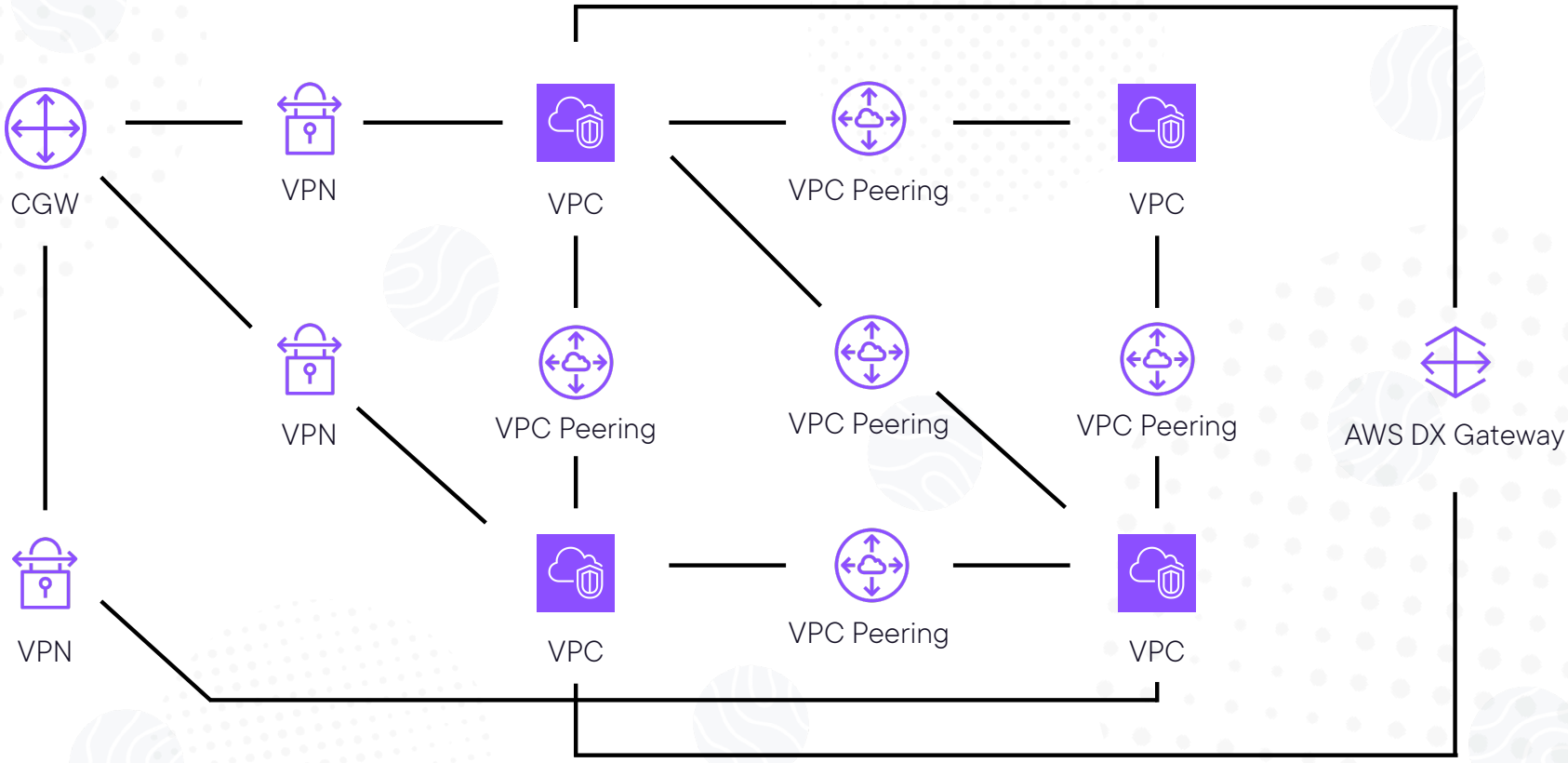
**Traffic traversing a Direct Connect connection is private, but it is NOT encrypted! Know the difference!**

# AWS DX and VPN Diagram

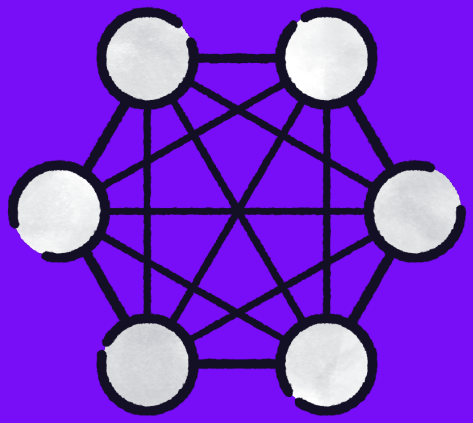


# Centralized Traffic with AWS Transit Gateways

# Common Network Architectures - Before



# Would you say that the previous network architecture is complicated?

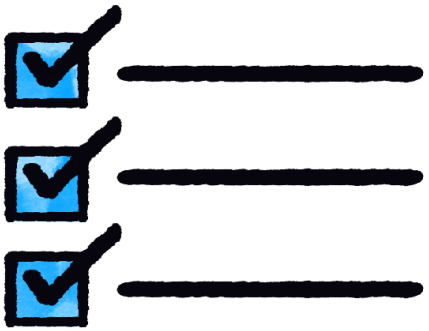


# Transit Gateway (TGW)

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. It simplifies your network and puts an end to complex peering relationships.

A TGW is meant to act as a cloud router — each new connection is only made once.

# Transit Gateway Concepts



Allow you to set up a hub-and-spoke network topology

Connect thousands of VPCs and on-prem networks in a simple manner

You deploy this to a Region, but they can work Cross-Region

Control what traffic can go where by using TGW Route Tables that are configured for attachments on VPCs

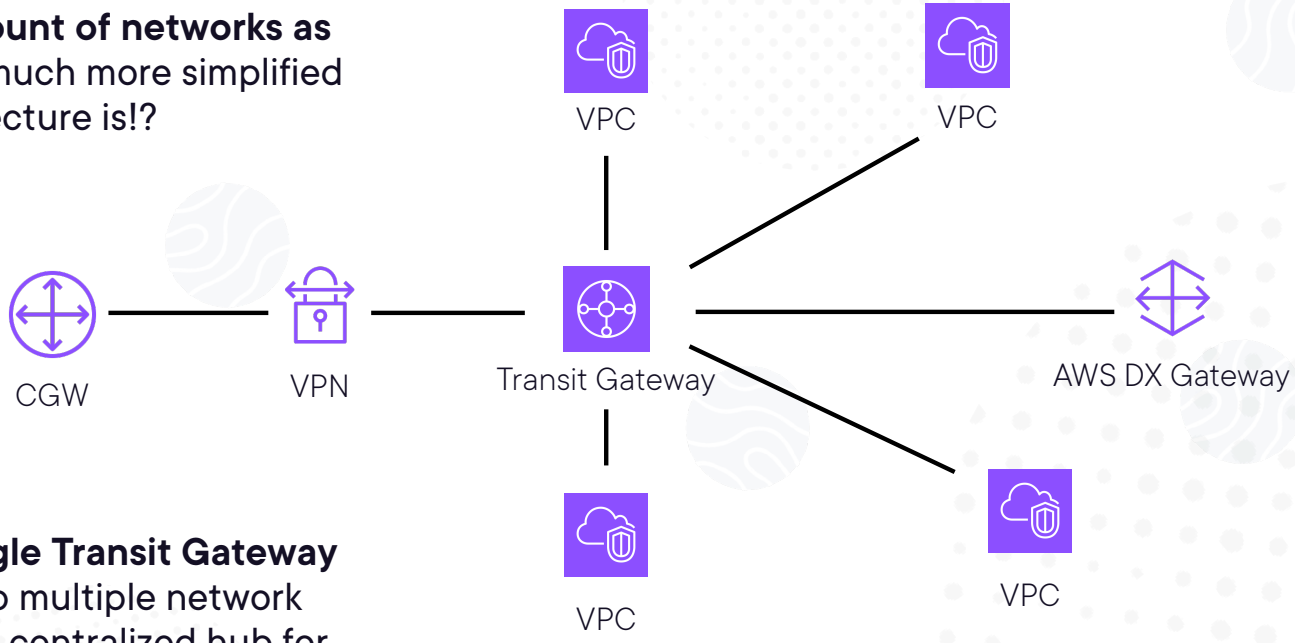
Integrates with DX connections, DX Gateway, and even VPN connections

You can share theses between accounts in an Organization using AWS Resource Access Manager (*AWS RAM*)

**Exam Pro Tip: TGW supports IP multicast, which is not supported by any other AWS networking service.**

# Common Network Architectures - After

This is the **same amount of networks as before**, but see how much more simplified the architecture is!?



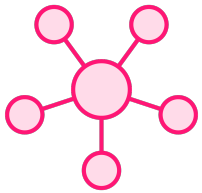

Now, we have a **single Transit Gateway** that is attached to multiple network resources to offer a centralized hub for controlling network communications

# Attaching Transit Gateways

A TGW enables you to attach VPCs and VPN connections and route traffic between them.

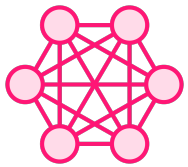
You can also peer TGWs, which allows you to connect Transit Gateways across different AWS Regions or within the same Region.

# Exploring the Common TGW Attachments



**VPC Attachments**: Attaches a VPC to a transit gateway by picking one subnet from each AZ to be used by the transit gateway to route traffic. This enables traffic to reach resources in every subnet in that AZ.


**VPN Attachments**: TGW feature that allows you to connect your on-premises network via VPN to multiple Amazon VPCs over the TGW.



**Peering Attachments**: Use these to peer both intra-Region and cross-Region transit gateways, and route traffic between them. Peering attachments are not available in TGWs that are shared with you.

# Transit Gateway Route Tables

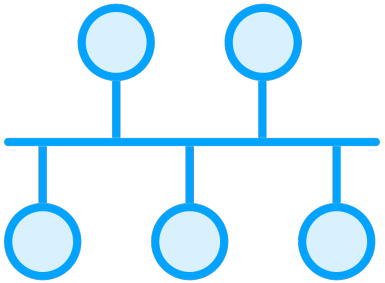
Transit Gateway route tables are an essential component of AWS Transit Gateways

You use these to configure routing for your transit gateway attachments

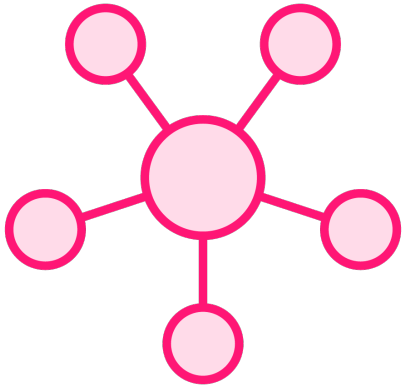
Each attachment for a Transit Gateway is associated with exactly **one transit gateway route table**

A Transit Gateway can have multiple route tables, allowing for complex routing scenarios and control

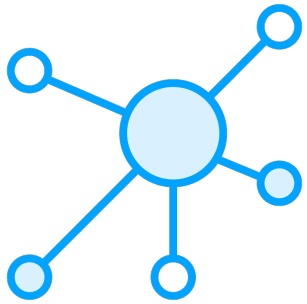
# Transit Gateway Route Table Use Cases



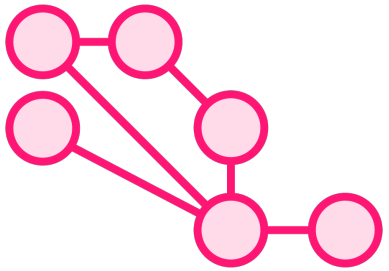
**Network Segmentation**
Create isolated routing domains within a single Transit Gateway



**Hub-and-Spoke**
Centralize routing for multiple VPCs and on-premises networks



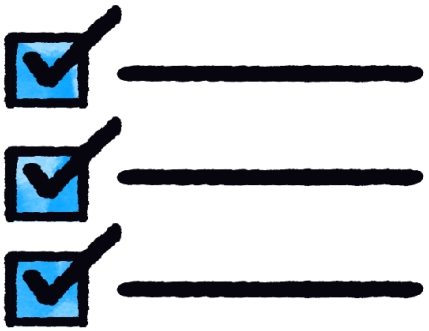
**Shared Services**
Route traffic to a shared service VPC from multiple VPCs



**Complex Routing Scenarios**
Advanced routing patterns

# Module Summary and Exam Tips

# AWS Direct Connection Exam Tips



**Allow you to establish private connectivity between AWS and your datacenter or office**

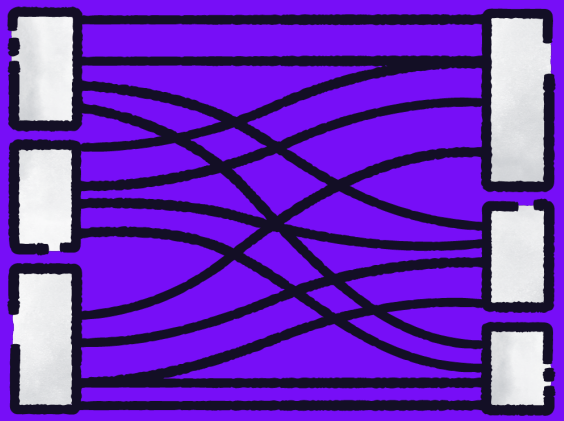
**Use this if you need a stable and reliable connection**

**These are private but they are NOT encrypted! You must run a VPN over the DX if encryption is required.**

**They offer private access to public resources via a public VIF, and private resources via a Private VIF**

**Remember the two connection types and their use cases:**

- Dedicated (*Usually the highest performance*)
- Hosted (*More options for capacity*)



# AWS Direct Connect Gateways

These allow you to connect multiple VPCs, even in multiple Regions, to a single Direct Connect connection.

# Transit Gateway Exam Tips

Allows for transitive peering between VPCs and on-premises data centers

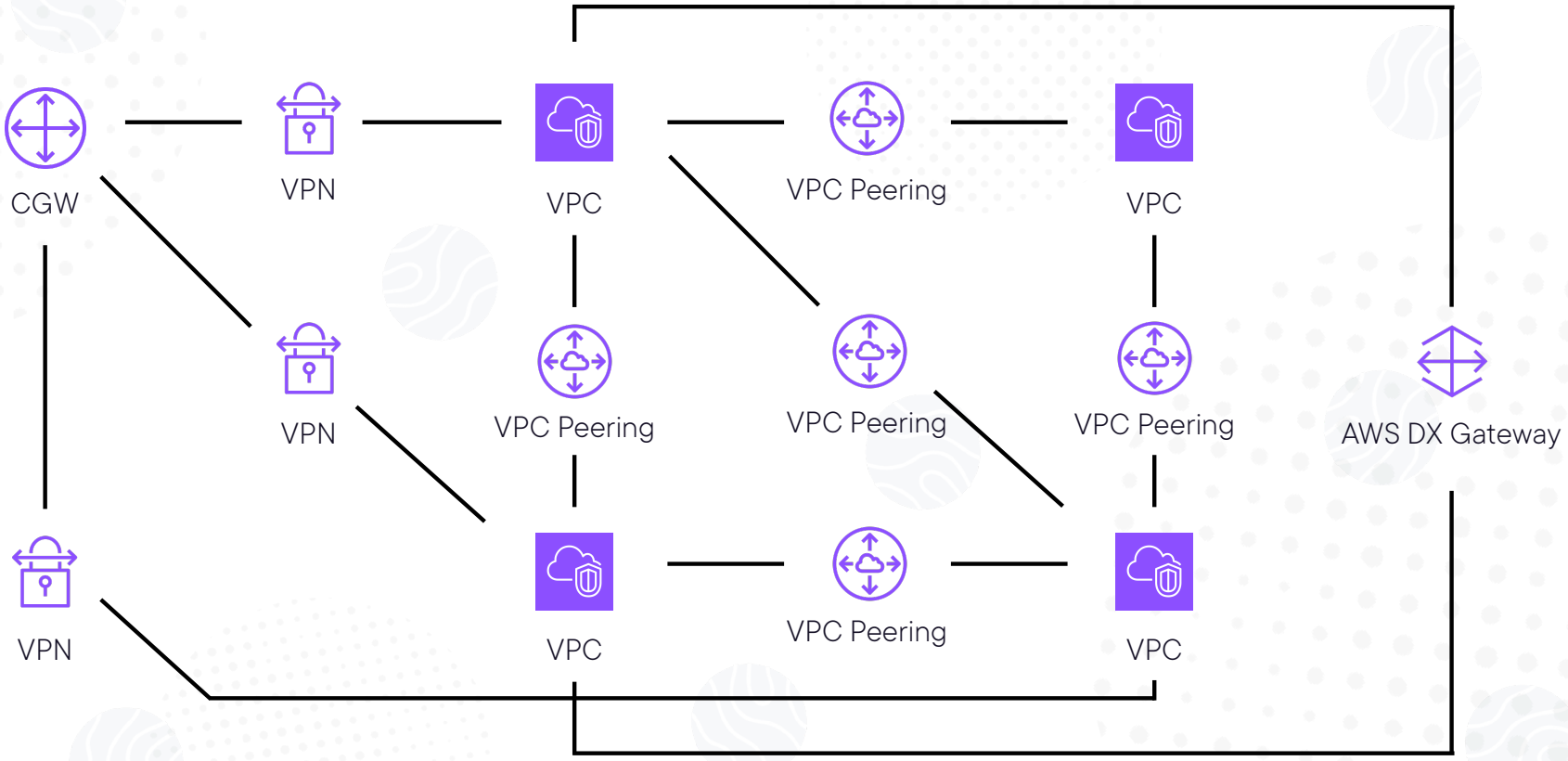
Works on a hub-and-spoke model and can be shared via AWS RAM

Deployed on a Regional basis, but you can have it work across Regions

Remember these attachment types: VPC, VPN, and Peering

Works with DX as well as VPN connections, and supports IP Multicast

# Transit Gateway Exam Tips - Before TGW



# Transit Gateway Exam Tips - After TGW