aws academy

CSCI 5902 Adv. Cloud Architecting
Fall 2023
Instructor: Lu Yang

Module 7 Connecting Networks Environment
(Sections 1 - 6)
Oct 23, 2023

Housekeeping and feedback

1. Start recording

- Questions

Is route table similar to/the same as a load balancer?

AWS Academy Cloud Architecting

Module 7: Connecting Networks

Module overview

Sections

1. Architectural need
2. Connecting to your remote network with AWS Site-to-Site VPN
3. Connecting to your remote network with AWS Direct Connect
4. Connecting VPCs in AWS with VPC peering
5. Scaling your VPC network with AWS Transit Gateway
6. Connecting your VPC to supported AWS services

Module objectives

At the end of this module, you should be able to:

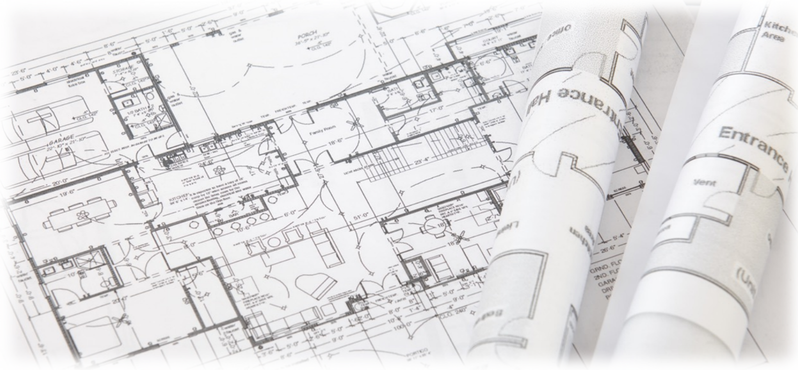
- Describe how to connect an on-premises network to the Amazon Web Services (AWS) Cloud
- Describe how to connect VPCs in the AWS Cloud
- Connect VPCs in the AWS Cloud by using VPC peering
- Describe how to scale VPCs in the AWS Cloud
- Describe how to connect VPCs to supported AWS services

Module 7: Connecting Networks

Section 1: Architectural need

Café business requirement

The workloads for the café are increasing in complexity. The architecture must support connectivity between multiple VPCs, and be highly available and fault tolerant.



Module 7: Connecting Networks

Section 2: Connecting to your remote network with AWS Site-to-Site VPN

AWS Site-to-Site VPN

AWS
Site-to-Site VPN

AWS Site-to-Site is a highly available solution that enables you to securely connect your on-premises network or branch office site to your VPC.

- Uses internet protocol security (IPSec) communications to create encrypted virtual private network (VPN) tunnels
- Provides two encrypted tunnels per VPN connection
- Charged per VPN connection-hour

Static and dynamic routing

Dynamic routing

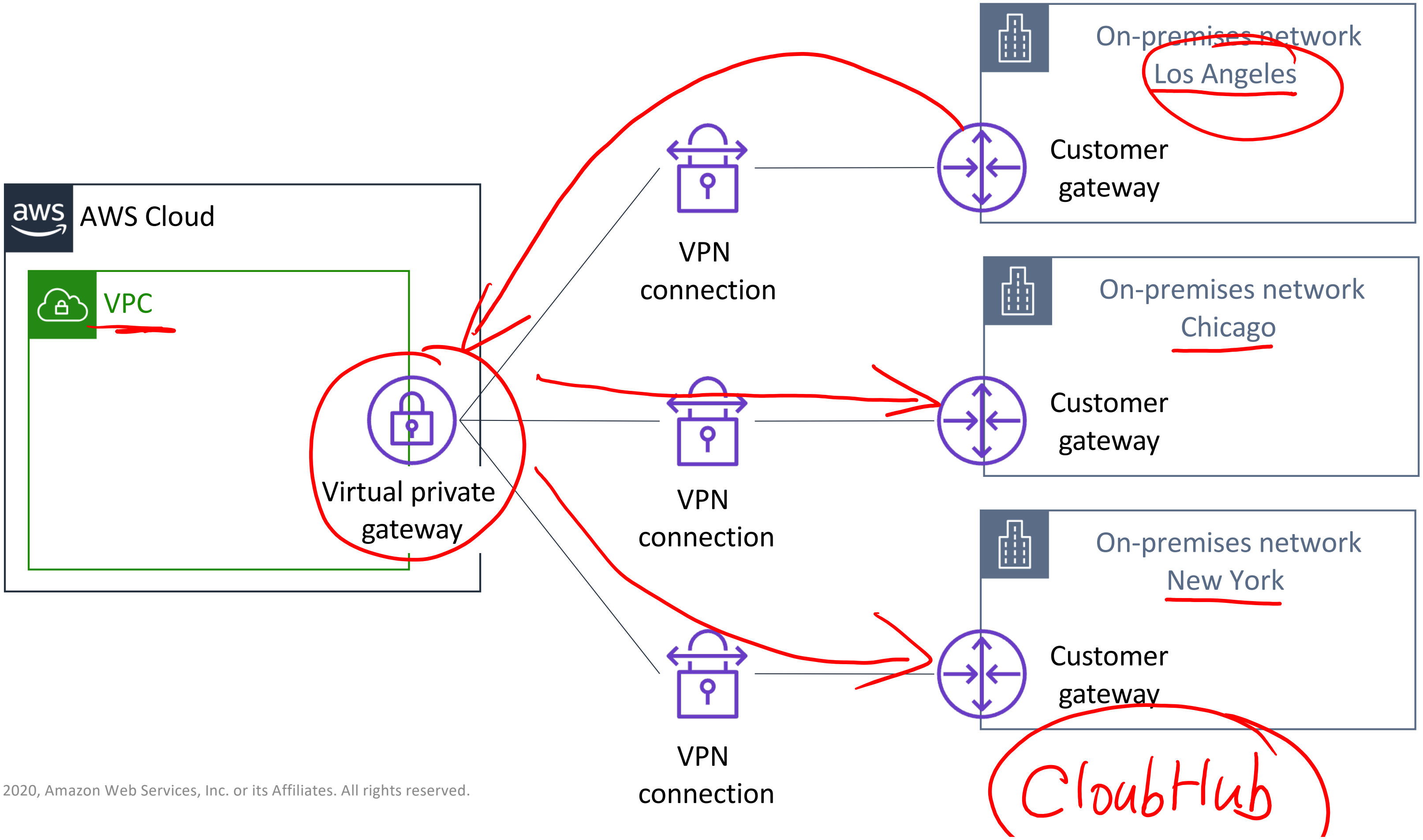
- Uses the Border Gateway Protocol (BGP) to advertise its routes to the virtual private gateway
- Specify *dynamic routing* if your customer gateway device supports BGP*
  - By specifying the ASN (Autonomous System Number) of the CGW and VGW

Static routing

- Requires you to specify all routes (IP prefixes)
- Specify *static routing* if your customer gateway device does not support BGP

*We recommend that you use BGP-capable devices because the BGP protocol offers robust liveness detection checks.

Connecting multiple VPNs



Section 2 key takeaways

- AWS Site-to-Site VPN is a highly available solution that enables you to securely connect your on-premises network or branch office site to your VPC
- AWS Site-to-Site VPN supports both static and dynamic routing
- You can establish multiple VPN connections from multiple customer gateway devices to a single virtual private gateway CGW VGW

Module 7: Connecting Networks

Section 3: Connecting to your remote network with AWS Direct Connect

AWS Direct Connect (DX)

AWS Direct Connect

AWS Direct Connect (which is also known as DX) provides you with a dedicated, private network connection capacity of either 1 Gbps, 10 Gbps, or 100Gbps.

Reduces data transfer costs

Improves application performance with predictable metrics

- More expensive than VPN
- Bypass ISP
- No redundant by default
- Need ~a month to setup

DX use cases

AWS Direct Connect

- Hybrid environments
- Transferring large datasets
- Network performance predictability
- Security and compliance
- **Who use it?**

AWS Direct Connect is most often used by companies with >10000 employees and >1000M dollars in revenue.

Reference: https://enlyft.com/tech/products/aws-direct-connect

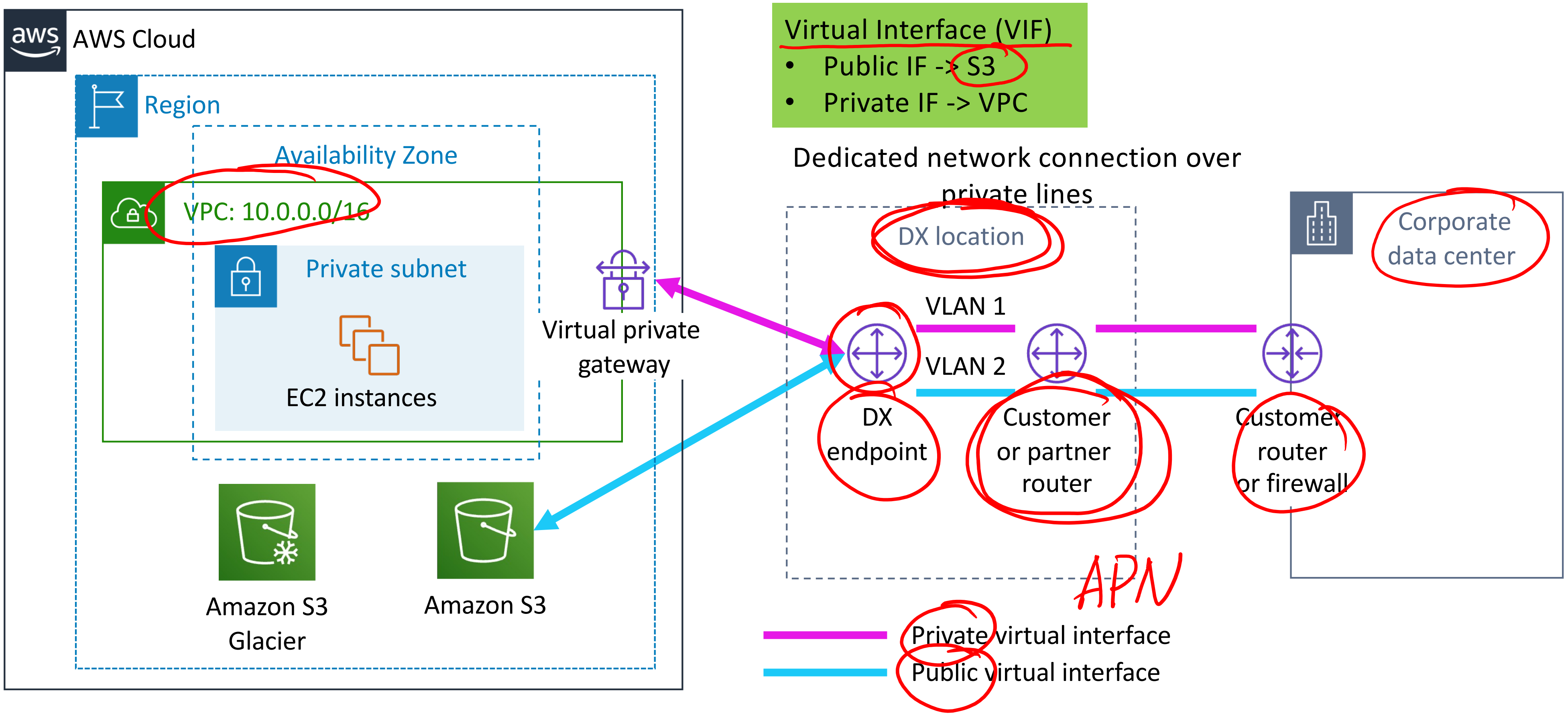
AWS Direct Connect is a dedicated network connection from your datacenter to AWS. Due to its high cost, you should only invest in Direct Connect if you require continuous replication and connectivity between AWS and your datacenter. If you're making a one-time move to AWS, building a Direct Connect is a waste.

Extending on-premises network to AWS using DX

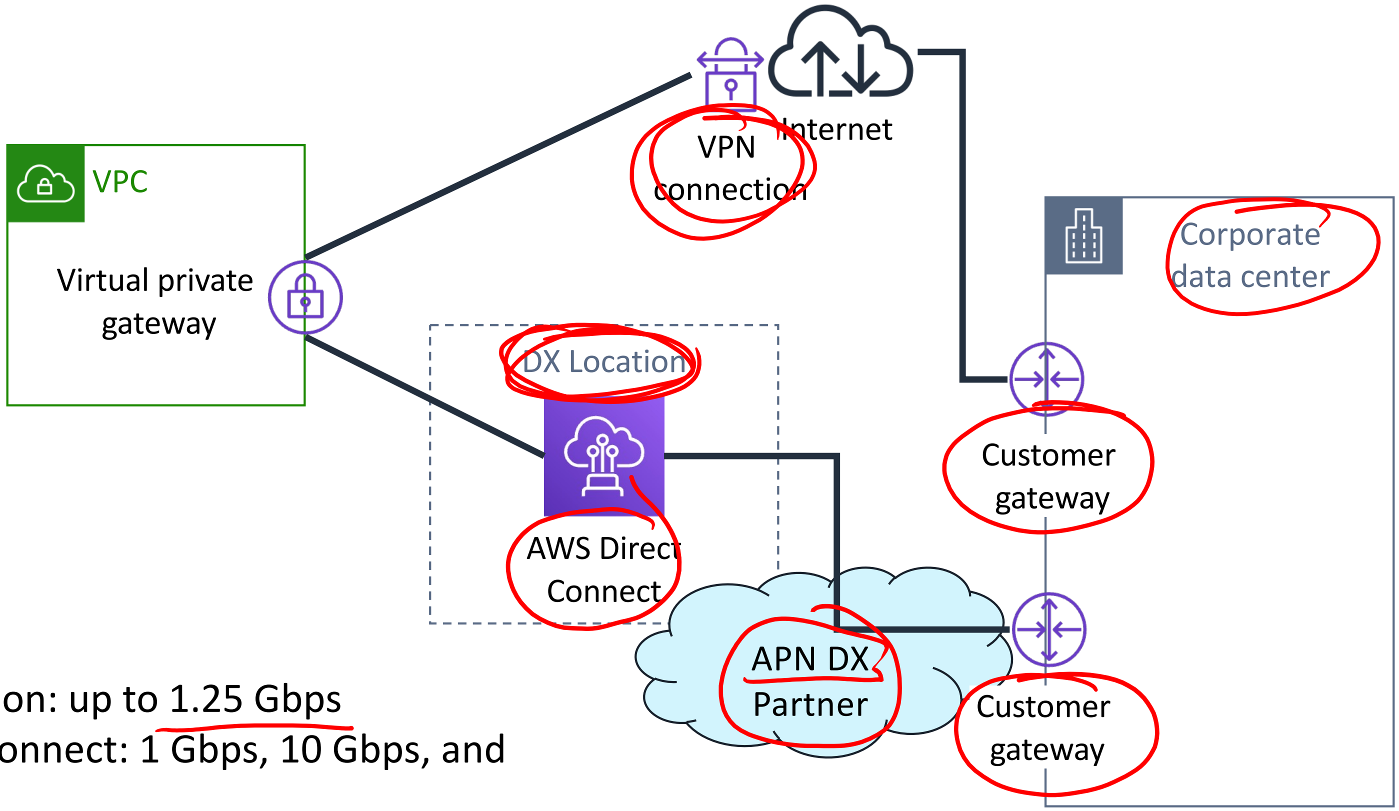
Virtual Interface (VIF)

- Public IF -> S3
- Private IF -> VPC

Dedicated network connection over private lines

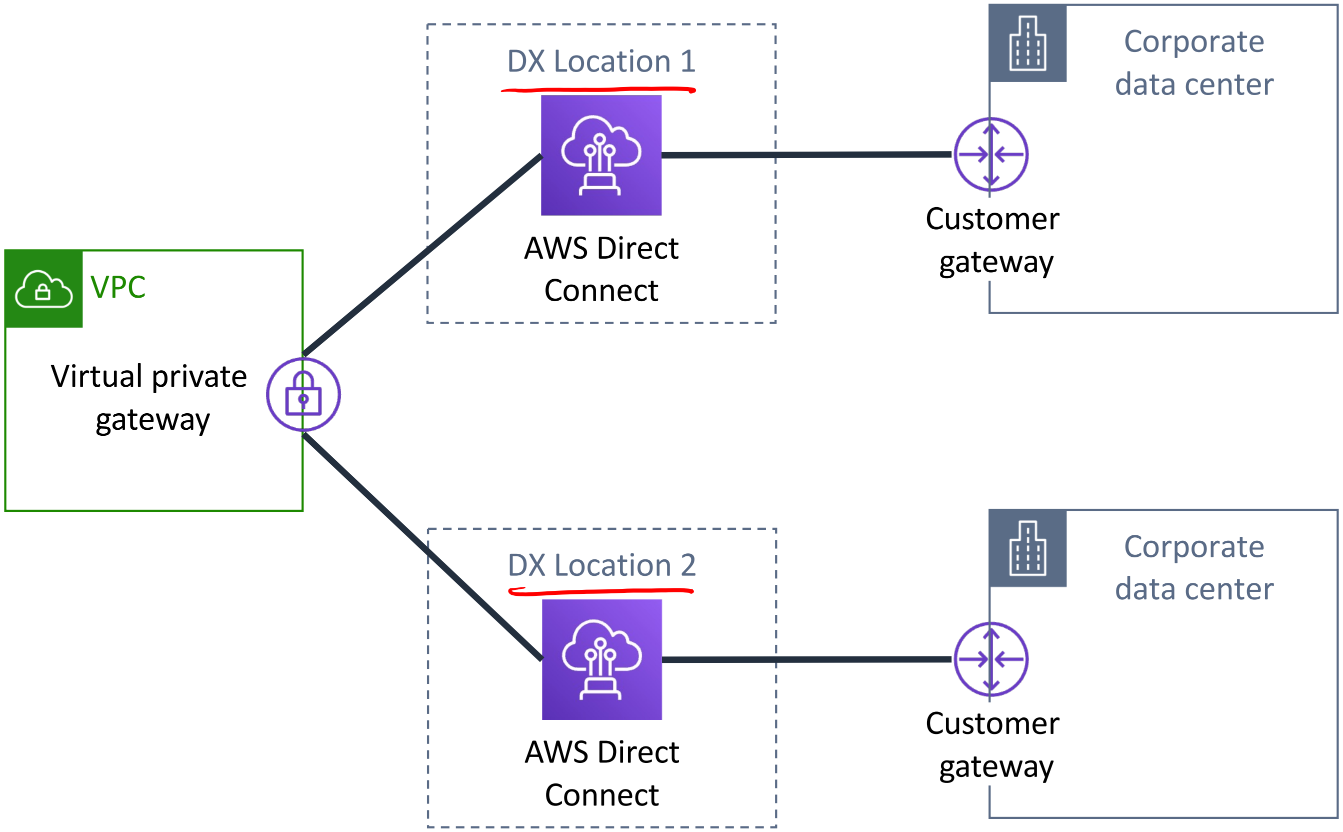


Enabling high availability: DX with backup VPN connection



- VPN connection: up to 1.25 Gbps
- AWS Direct Connect: 1 Gbps, 10 Gbps, and 100Gbps

Enabling high resiliency for critical workloads with DX



Section 3 key takeaways

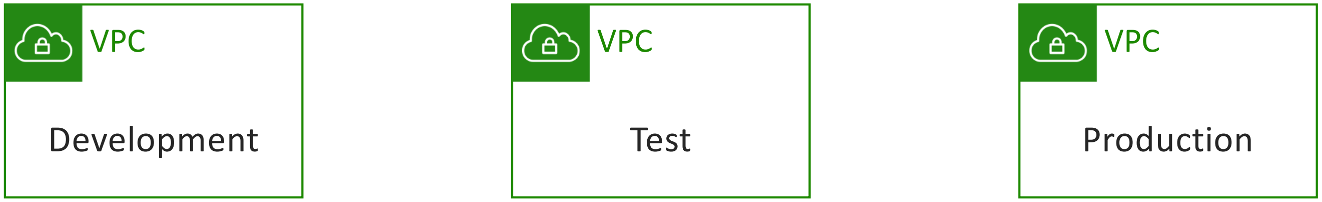
- AWS Direct Connect uses open standard 802.1q VLANs that enable you to establish a dedicated, private network connection from your premises to AWS
- You can access any VPC or public AWS service in any Region from any supported DX location
- You can implement highly available connectivity between your data centers and your VPC by coupling one or more DX connections that you use for primary connectivity with a lower-cost, backup VPN connection
- To implement a highly resilient, fault-tolerant architecture, connect to your AWS network from multiple data centers so you can have physical location redundancy

Module 7: Connecting Networks

Section 4: Connecting VPCs in AWS with VPC peering

Connecting VPCs

- Isolating some of your workloads is generally a good practice
- However, you might need to transfer data between two or more VPCs



VPC

Development

VPC

Test

VPC

Production

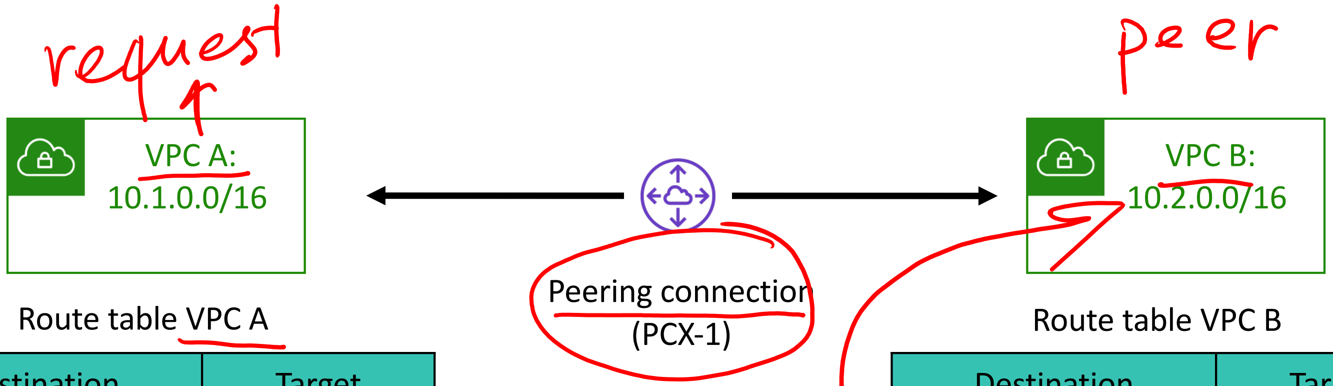
Service

VPC

VPC peering

- One-to-one networking connection between two VPCs
- No gateways, VPN connections, and separate network appliances needed
- Highly available connections
- No single point of failure or bandwidth bottleneck
- Traffic always stays on the global AWS backbone
- Can peer with VPCs inter-region and cross AWS account
- Route tables must be updated to ensure instances can communicate
    - Security Groups may have to be modified as well

Establishing VPC peering



request

VPC A:
10.1.0.0/16

Peering connection
(PCX-1)

peer

VPC B:
10.2.0.0/16

Route table VPC A

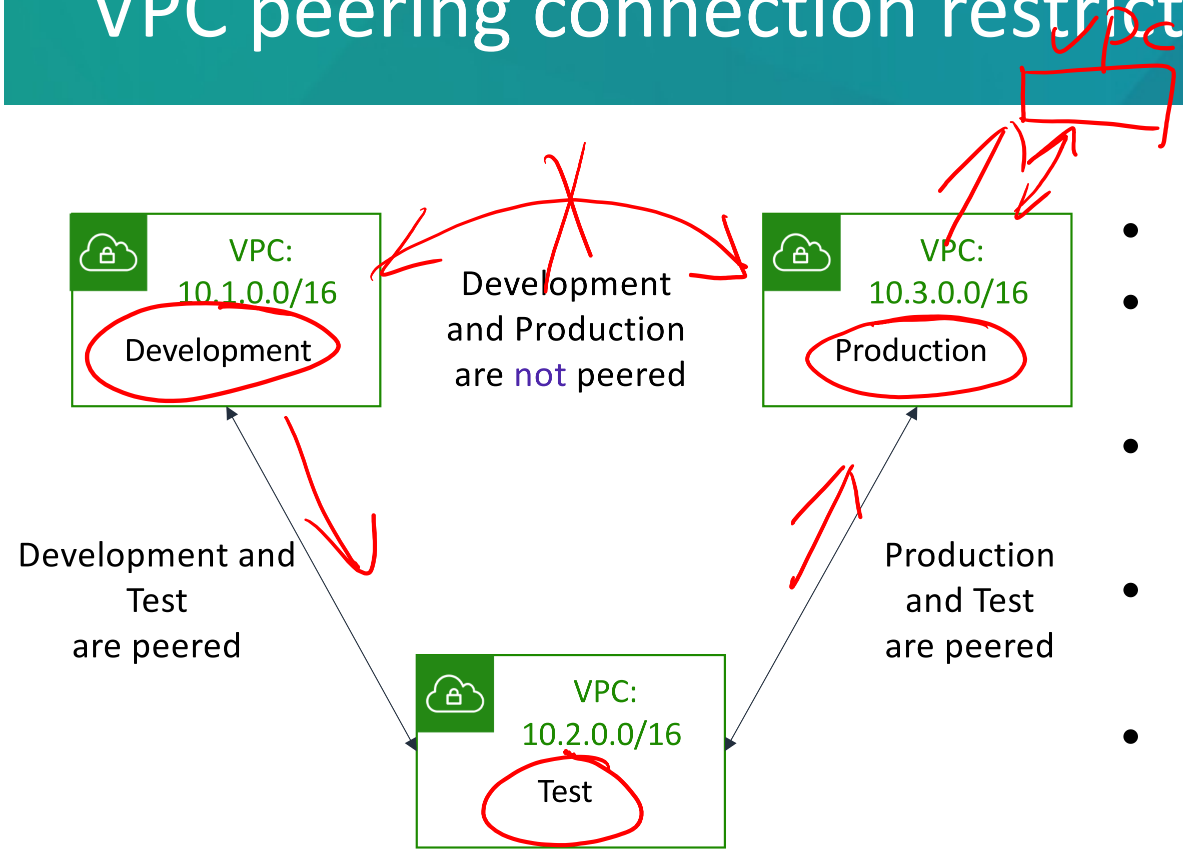
Destination	Target
10.1.0.0/16	local
10.2.0.0/16	PCX-1

Route table VPC B

Destination	Target
10.2.0.0/16	local
10.1.0.0/16	PCX-1

VPC peering connection restrictions

aws academy



VPC: 10.1.0.0/16

Development

Development and Production are not peered

VPC: 10.3.0.0/16

Production

Development and Test are peered

VPC: 10.2.0.0/16

Test

Production and Test are peered

- Use private IP addresses
- Can be established between different AWS accounts
- Cannot have overlapping CIDR blocks
- Can have only one peering resource between any two VPCs
- Do not support transitive peering relationships

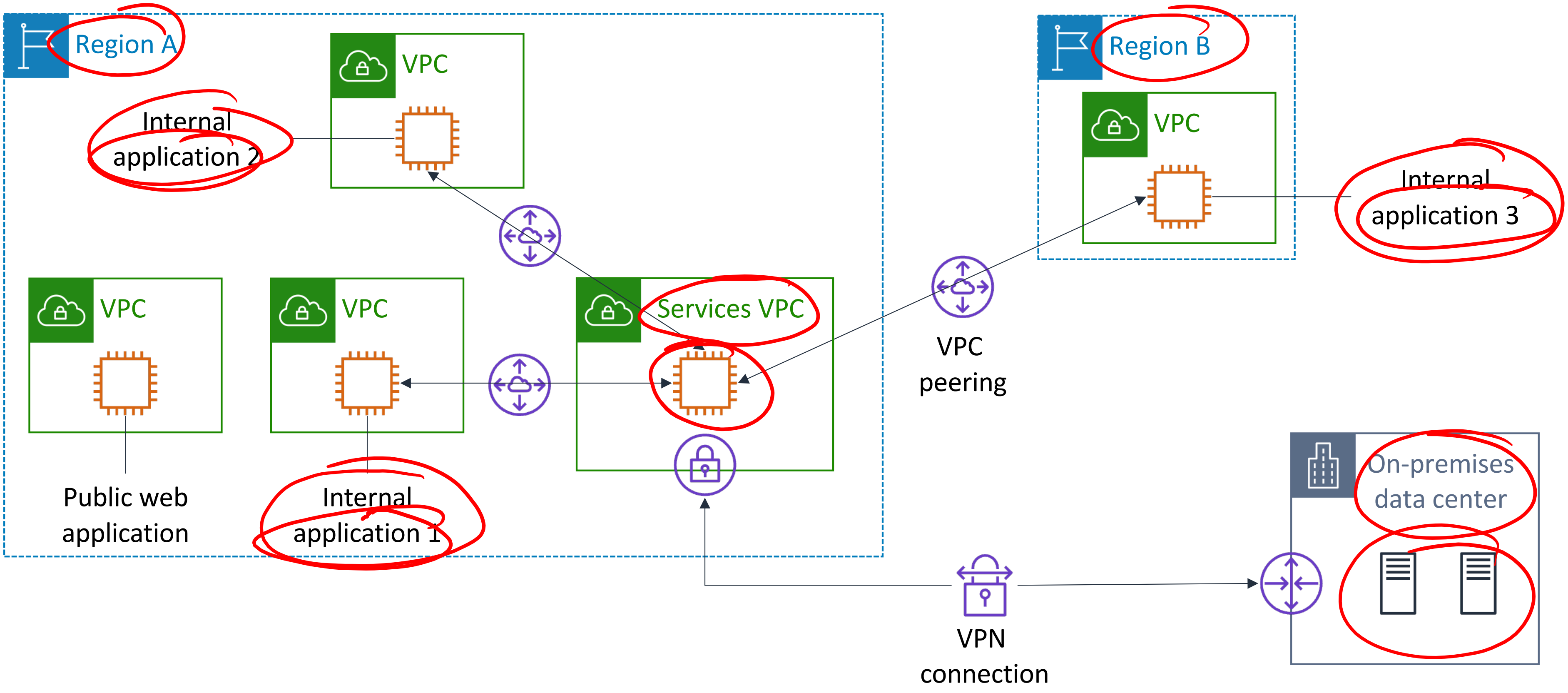
Considerations for peering multiple VPCs

When you connect multiple VPCs, consider these network design principles:

Only connect essential VPCs

Make sure your solution can scale

Example: VPC peering for shared resources



Section 4 key takeaways

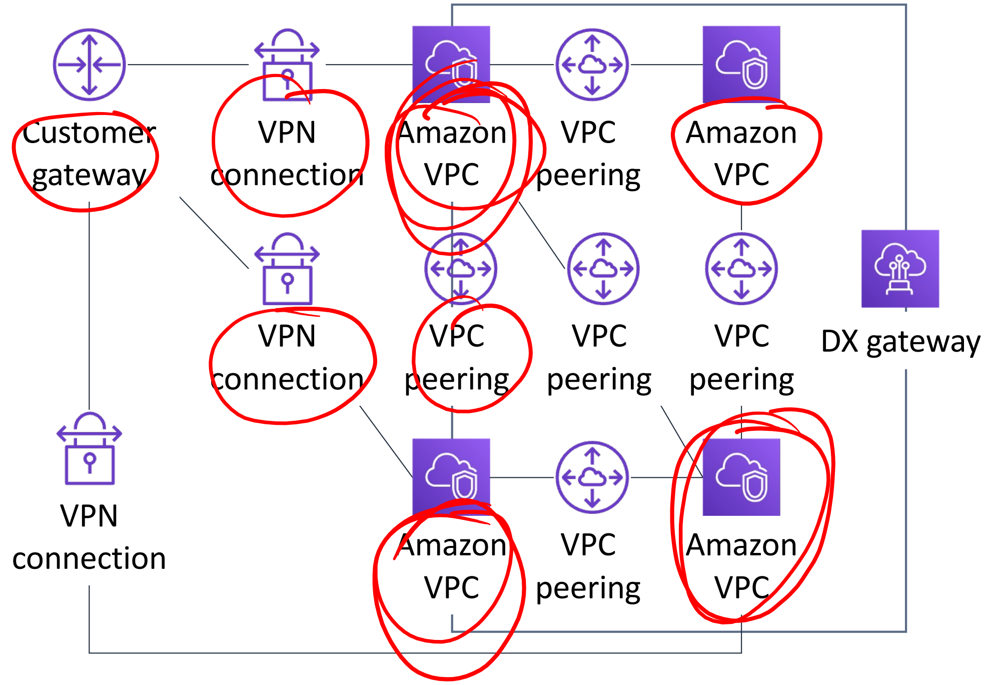
- VPC peering is a one-to-one networking connection between two VPCs that enables you to route traffic between them privately
- You can establish peering relationships between VPCs across different AWS Regions accounts
- VPC peering connections –
  - Use private IP addresses
  - Can be established between different AWS accounts
  - Cannot have overlapping CIDR blocks
  - Can have only one peering resource between any two VPCs
  - Do not support transitive peering relationships

Module 7: Connecting Networks

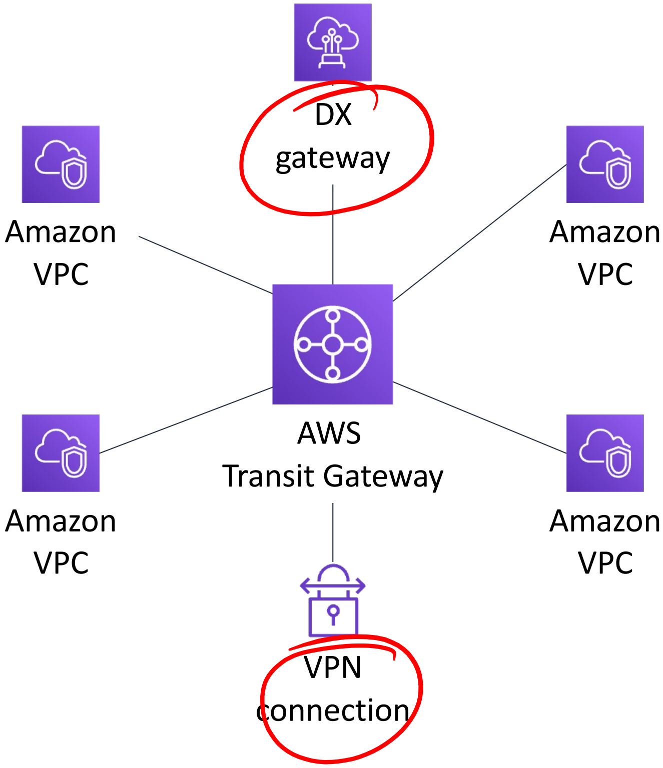
Section 5: Scaling your VPC network with AWS Transit Gateway

Need to scale networks across multiple VPCs

From this…



… to this

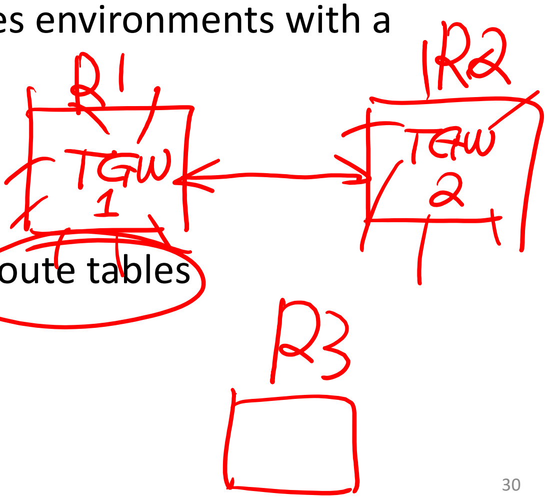


AWS Transit Gateway

AWS Transit Gateway

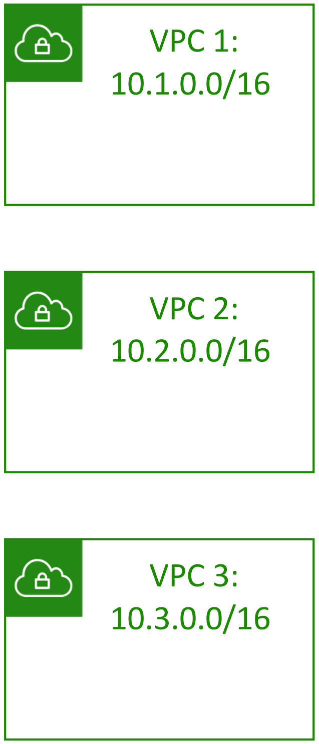
AWS Transit Gateway is a service that enables you to connect your VPCs and on-premises networks to a single gateway.

- Fully managed, highly available, flexible routing service
- Acts as a hub for all traffic to flow through between your networks
- Connects up to 5,000 VPCs and on-premises environments with a single gateway
- Can work cross regions
- Can peer Transit Gateway across regions
- Limit which VPC can talk to which VPC by route tables
- Works with Direct Connect and VPN



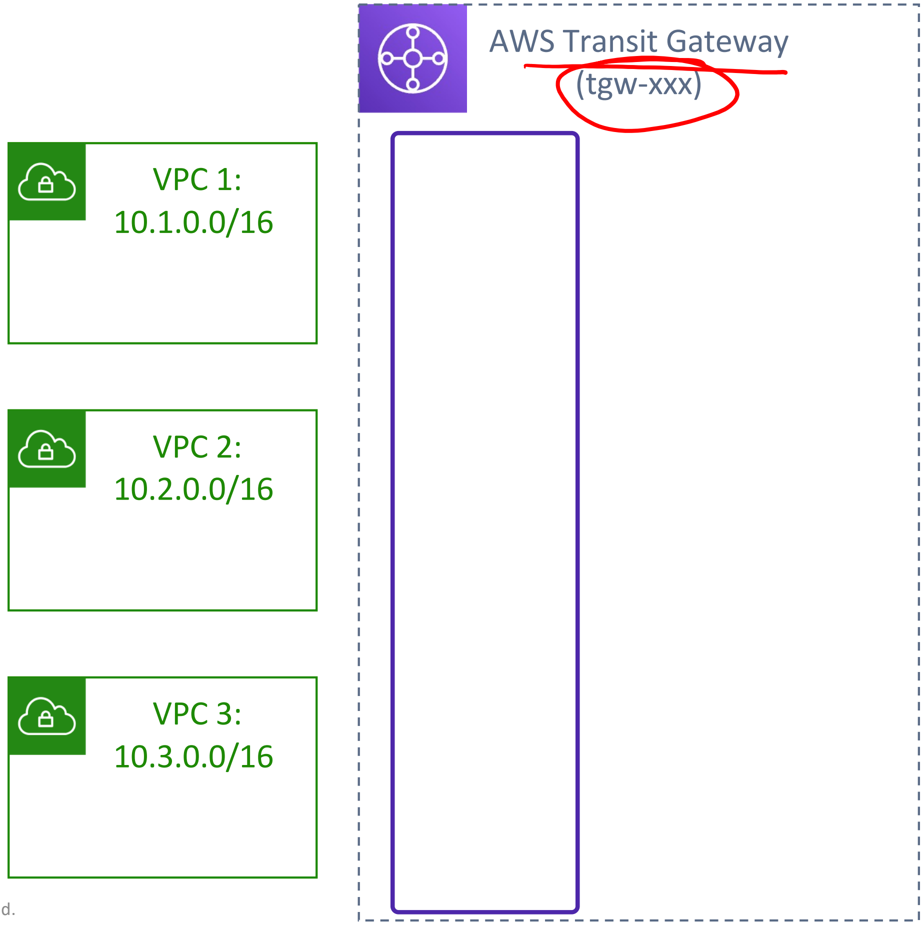
Connecting multiple VPCs

Scenario: We want to fully connect three VPCs.



Step 1: Create a transit gateway

Scenario: We want to fully connect three VPCs.



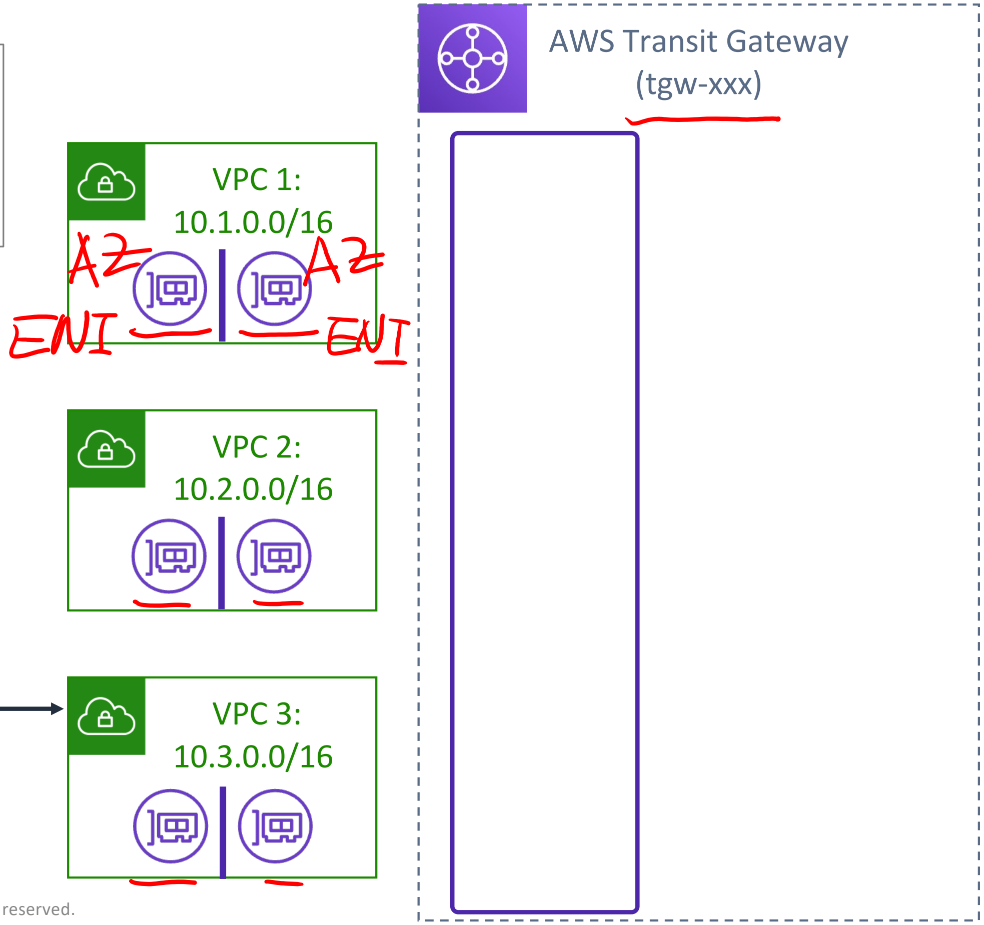
Step 2: Deploy elastic network interfaces

aws academy

Scenario: We want to fully connect three VPCs.

VPC 3 route table

Destination	Target
10.3.0.0/16	local

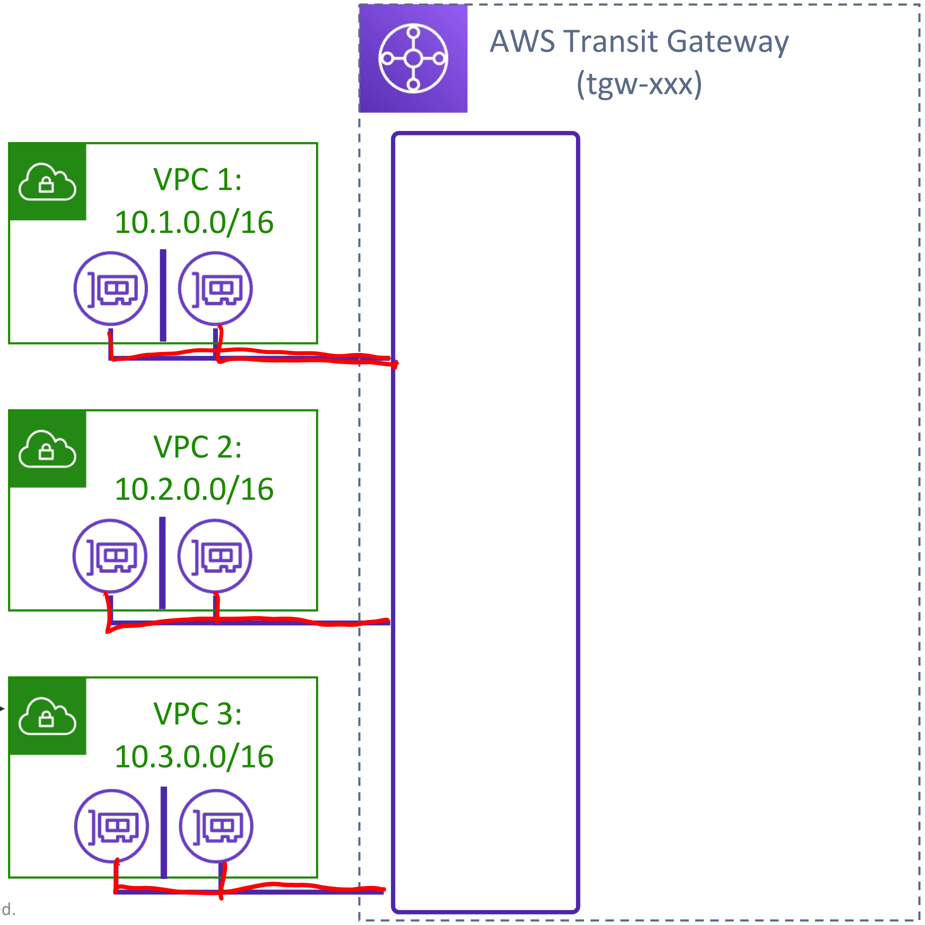


Step 3: Update the VPC route table

Scenario: We want to fully connect three VPCs.

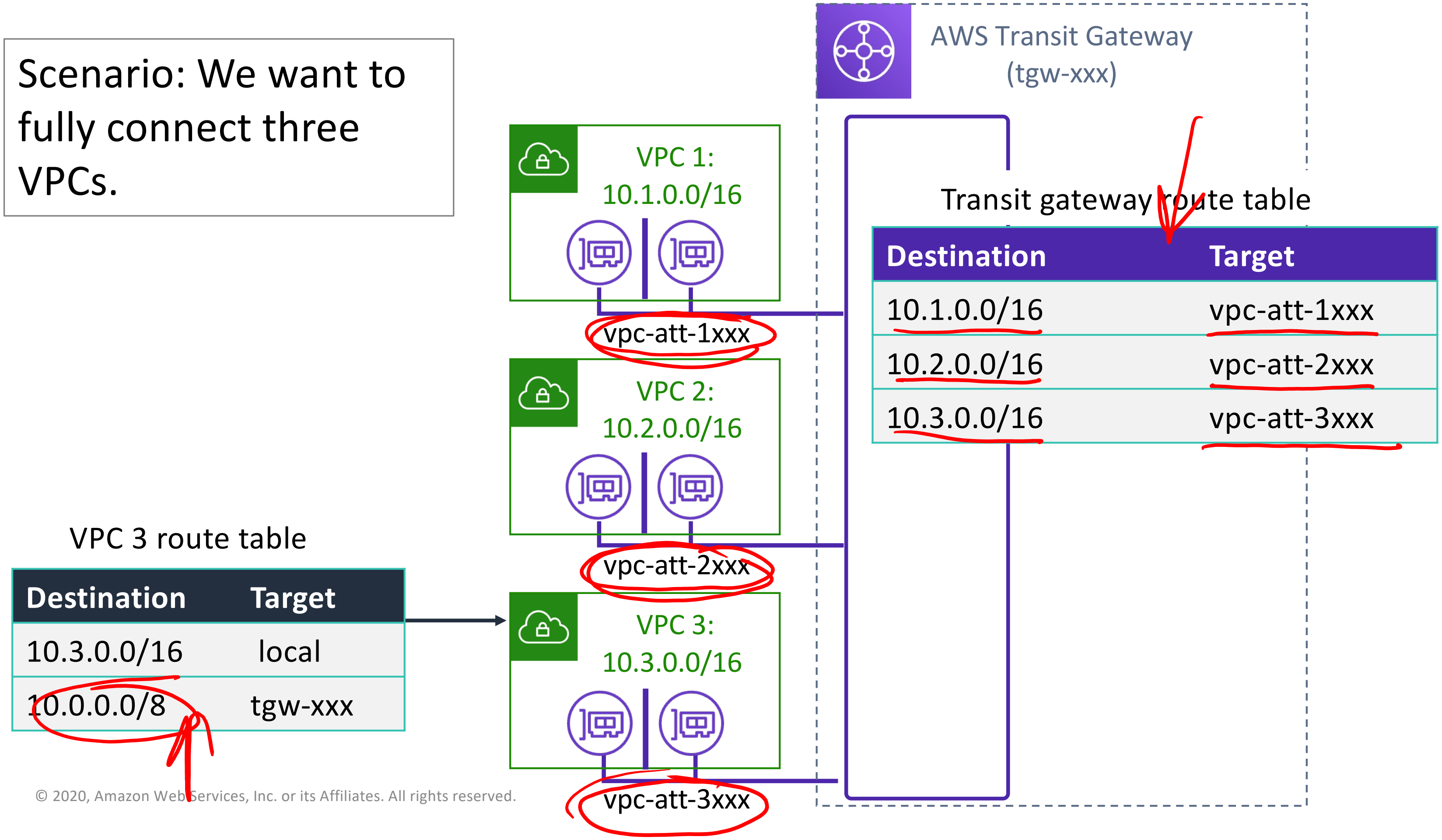
VPC 3 route table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx



Step 4: Update the transit gateway route table

Scenario: We want to fully connect three VPCs.



Transit gateway route table

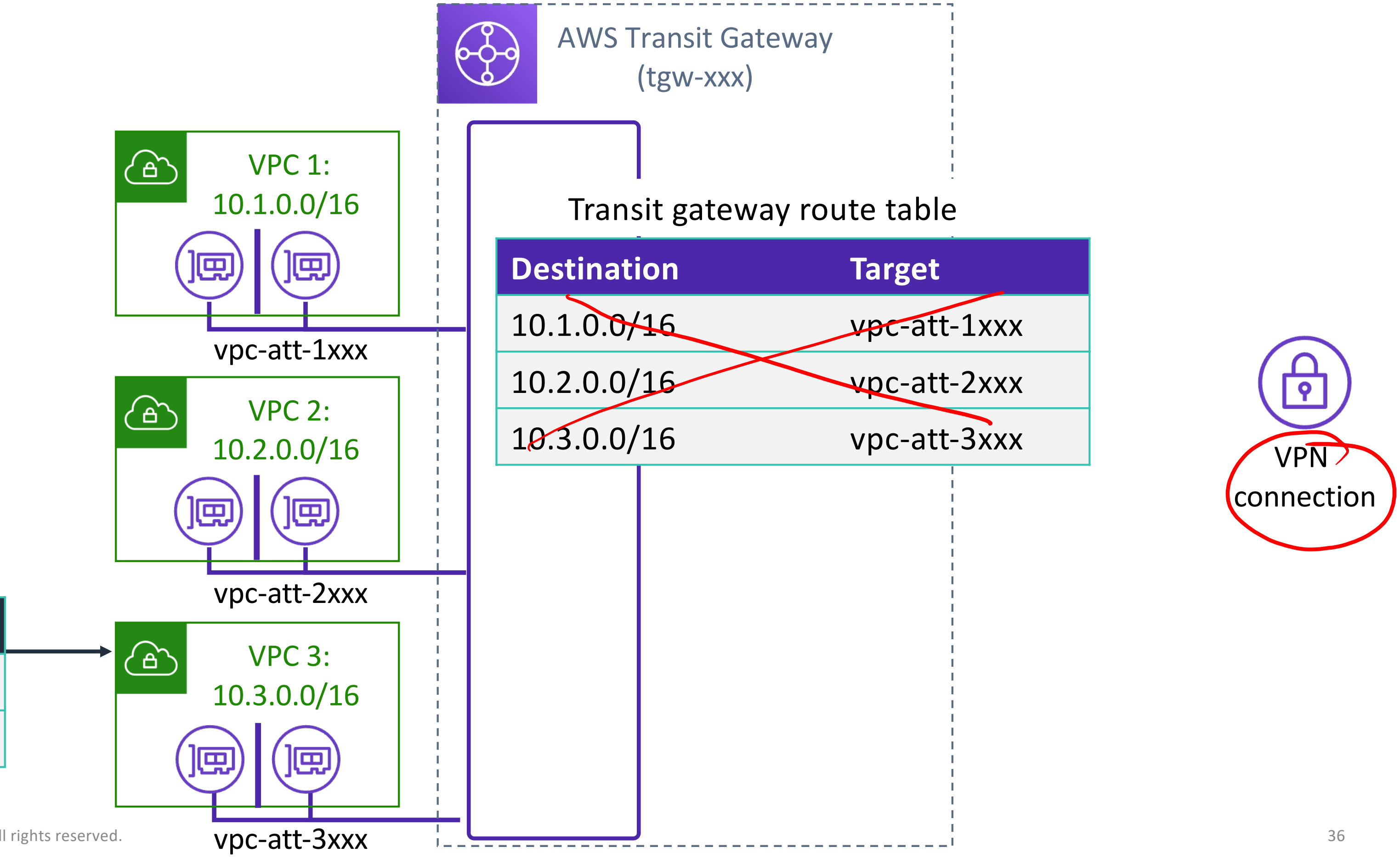
Destination	Target
10.1.0.0/16	vpc-att-1xxx
10.2.0.0/16	vpc-att-2xxx
10.3.0.0/16	vpc-att-3xxx

VPC 3 route table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Using AWS Transit Gateway to achieve VPC isolation (1 of 3)

Scenario: We now want VPN access but isolated VPC connectivity.



Transit gateway route table

Destination	Target
~~10.1.0.0/16~~	~~vpc-att-1xxx~~
~~10.2.0.0/16~~	~~vpc-att-2xxx~~
~~10.3.0.0/16~~	~~vpc-att-3xxx~~

VPC 3 route table

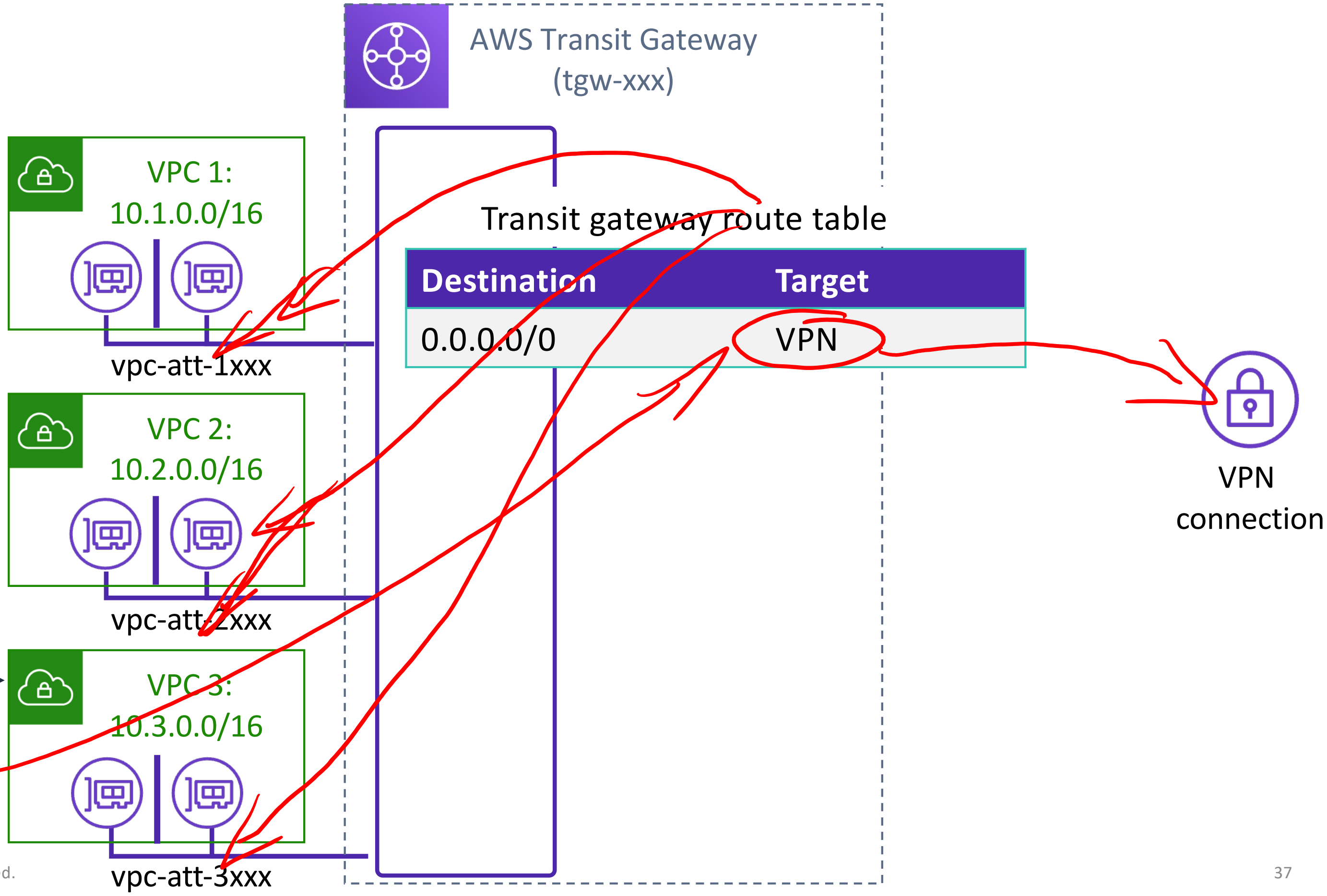
Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Using AWS Transit Gateway to achieve VPC isolation (2 of 3)

Scenario: We now want VPN access but isolated VPC connectivity.

VPC 3 route table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx



Transit gateway route table

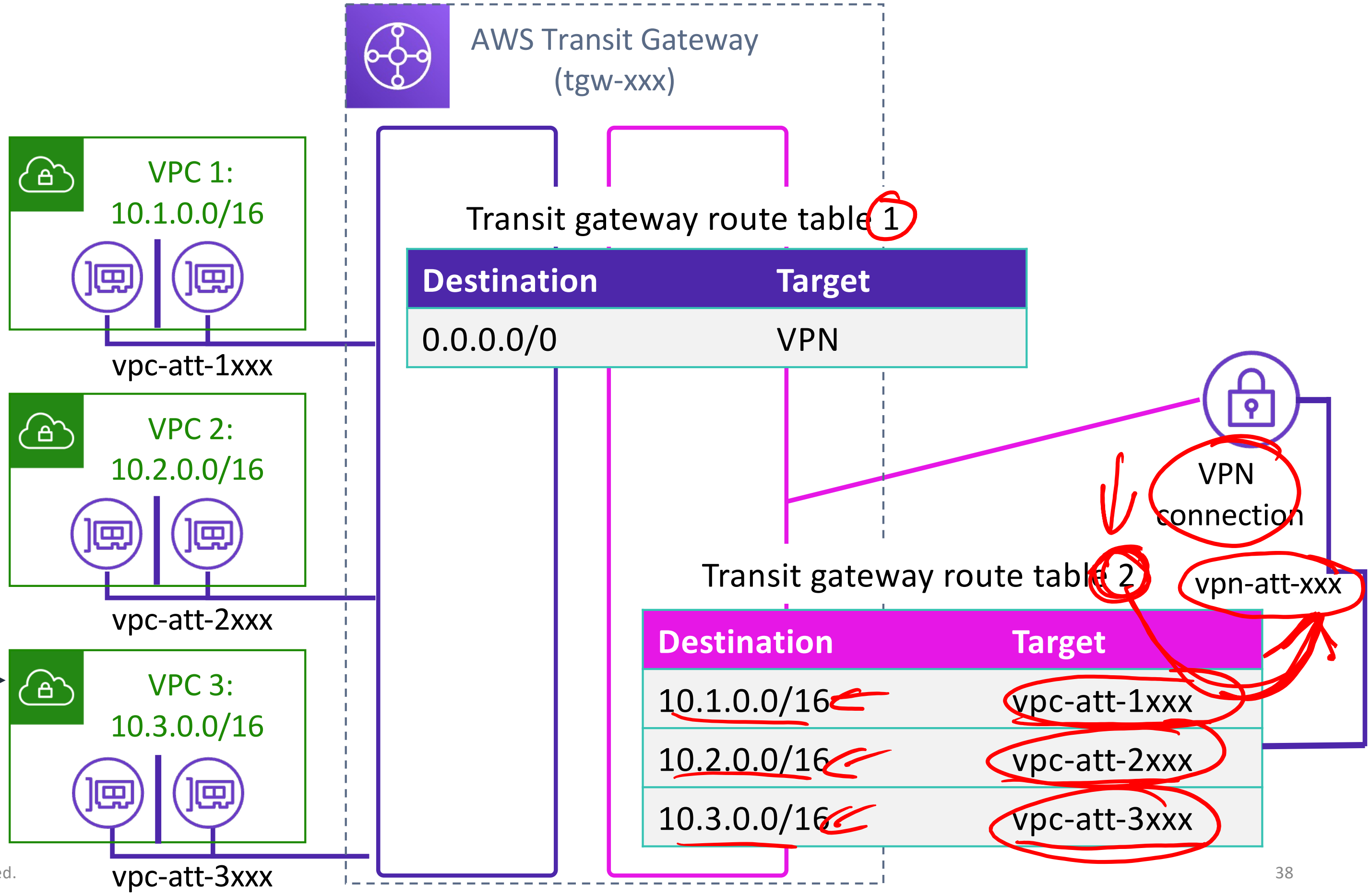
Destination	Target
0.0.0.0/0	VPN

Using AWS Transit Gateway to achieve VPC isolation (3 of 3)

Scenario: We now want VPN access but isolated VPC connectivity.

VPC 3 route table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx



Transit gateway route table 1

Destination	Target
0.0.0.0/0	VPN

Transit gateway route table 2

Destination	Target
10.1.0.0/16	vpc-att-1xxx
10.2.0.0/16	vpc-att-2xxx
10.3.0.0/16	vpc-att-3xxx

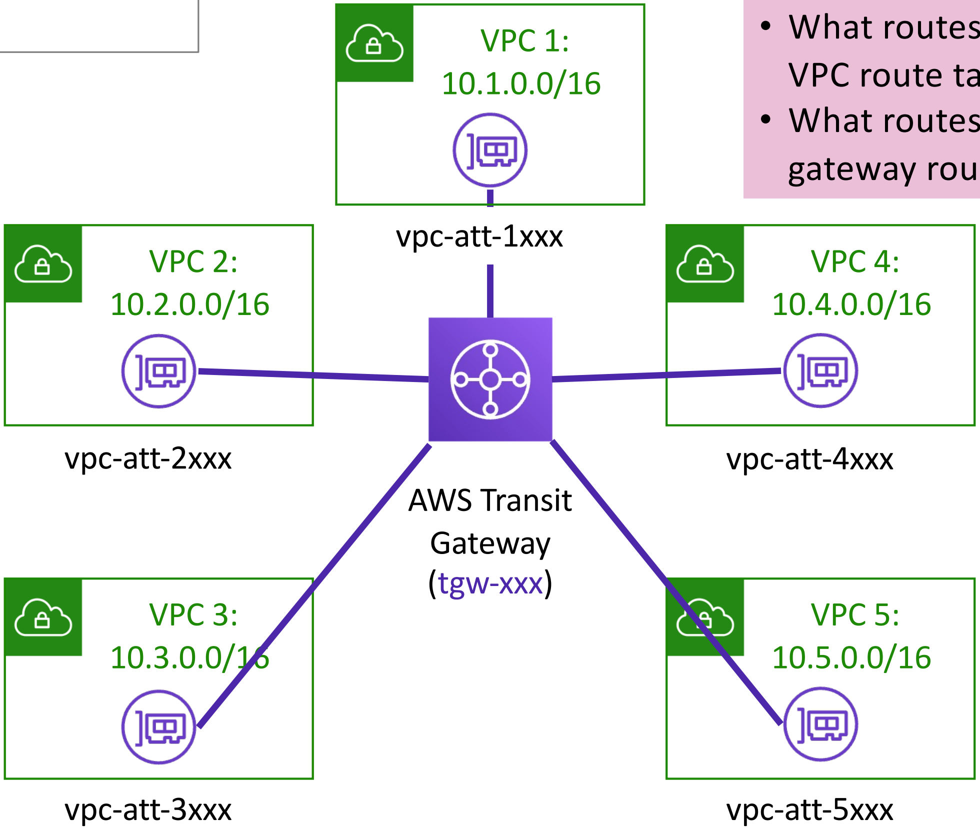
Activity: AWS Transit Gateway

AWS Transit Gateway: Challenge

Scenario: How do you connect these five VPCs?

Answer the following questions:

- What routes are necessary to add to each of the VPC route tables to enable full connectivity?
- What routes are necessary to add to the transit gateway route table to enable full connectivity?



3

VPC # route table

Destination	Target
10.#.0.0/16	local
?	?

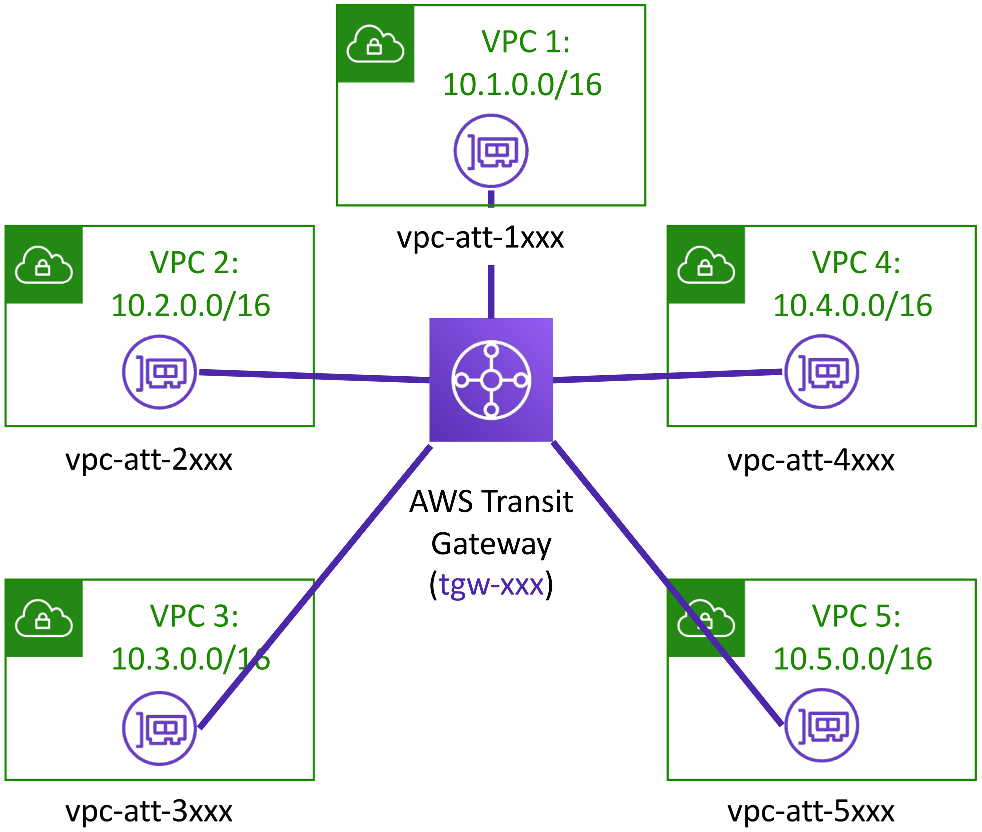
3

Transit gateway route table

Destination	Target
?	?

AWS Transit Gateway activity: Solution

Scenario: How do you connect these five VPCs?



VPC 3 route table

Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

Transit gateway
route table

Destination	Target
10.1.0.0/16	vpc-att-1xxx
10.2.0.0/16	vpc-att-2xxx
10.3.0.0/16	vpc-att-3xxx
10.4.0.0/16	vpc-att-4xxx
10.5.0.0/16	vpc-att-5xxx

Section 5 key takeaways

- AWS Transit Gateway enables you to connect your VPCs and on-premises networks to a single gateway (called a transit gateway)
- AWS Transit Gateway uses a hub-and-spoke model to simplify VPC management and reduce operational costs

Thank you, and Kahoot!

aws academy