AWS Academy Cloud Architecting

Module 7: Connecting Networks

aws academy

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

Activity

- AWS Transit Gateway

Lab

- Guided Lab: Creating a VPC Peering Connection

✓ **Knowledge check**

Module objectives

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

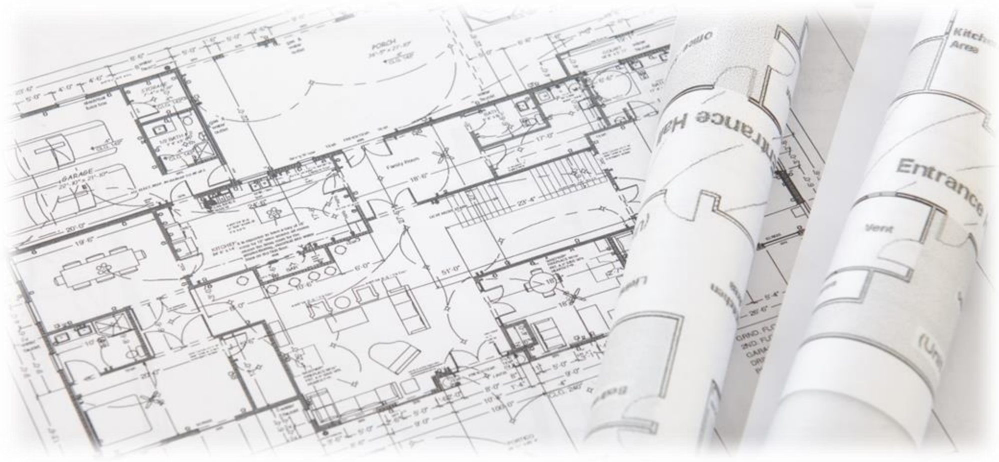
- Describe how to connect an on-premises network to the Amazon Web Services (AWS) Cloud
- Describe how to connect VPCs in the AWS Cloud
- Connect VPCs in the AWS Cloud by using VPC peering
- Describe how to scale VPCs in the AWS Cloud
- Describe how to connect VPCs to supported AWS services

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

Static routing

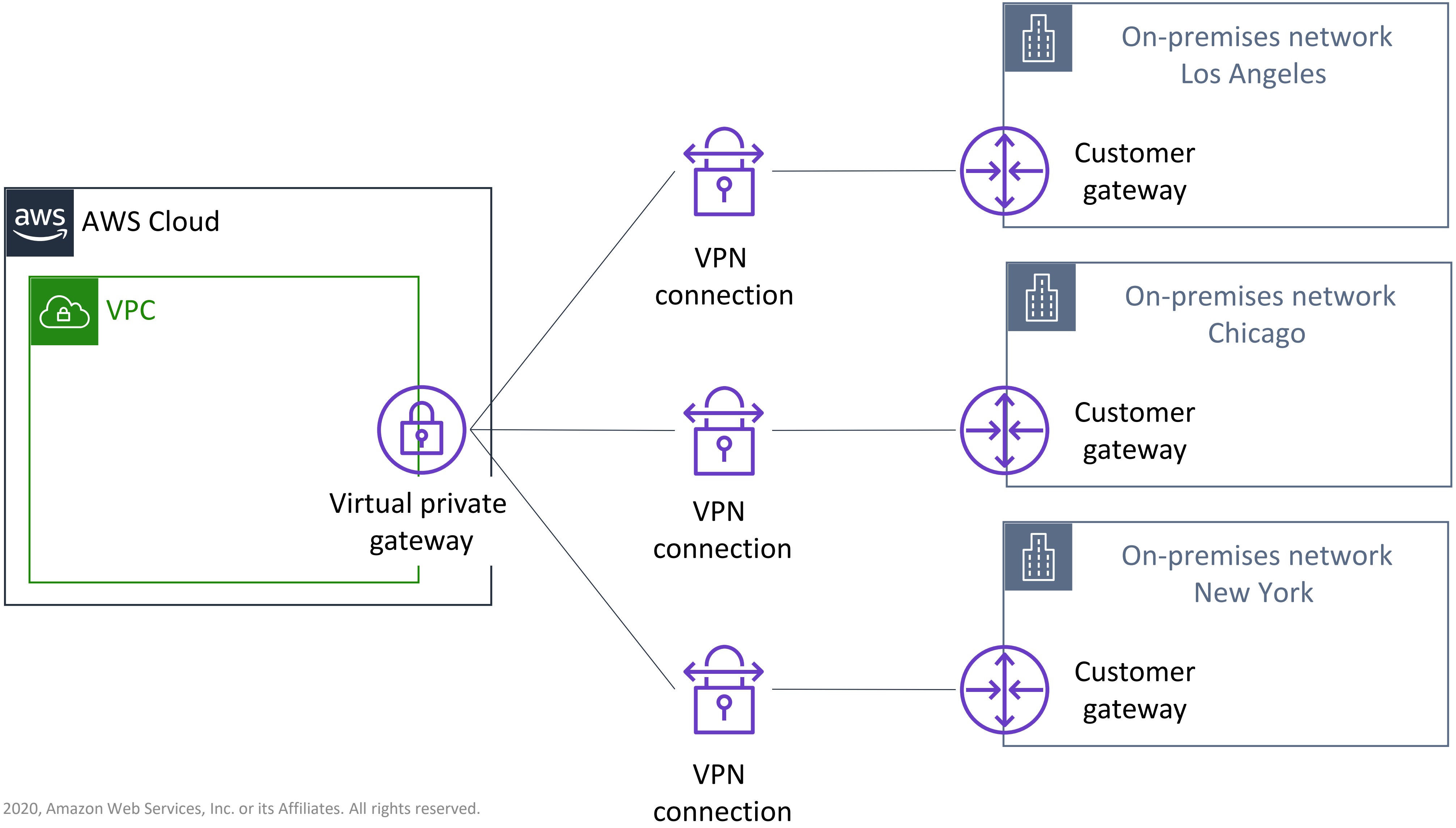
- Requires you to specify all routes (IP prefixes)
- Specify *static routing* if your customer gateway device does not support BGP

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*

*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

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 or 10 Gbps.

Reduces data transfer costs

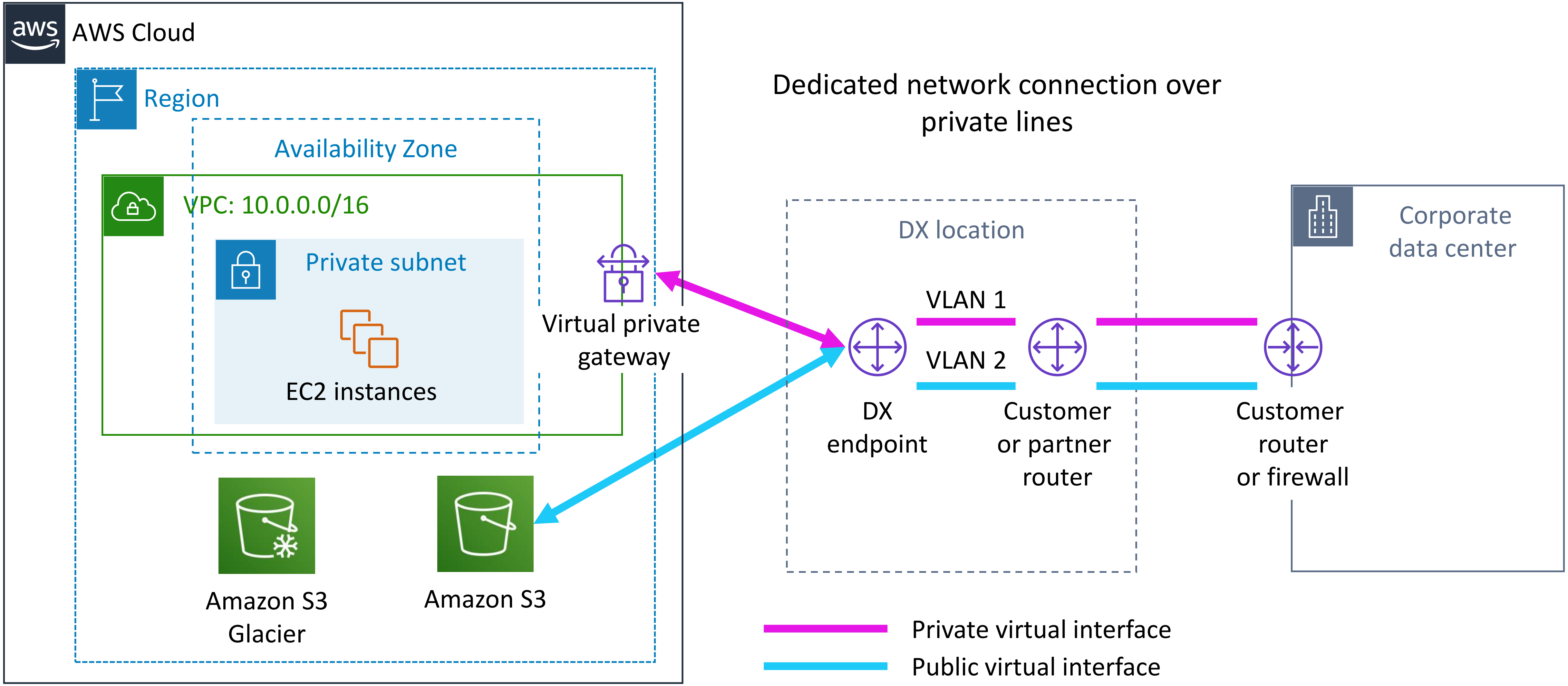
Improves application performance with predictable metrics

DX use cases

AWS Direct Connect

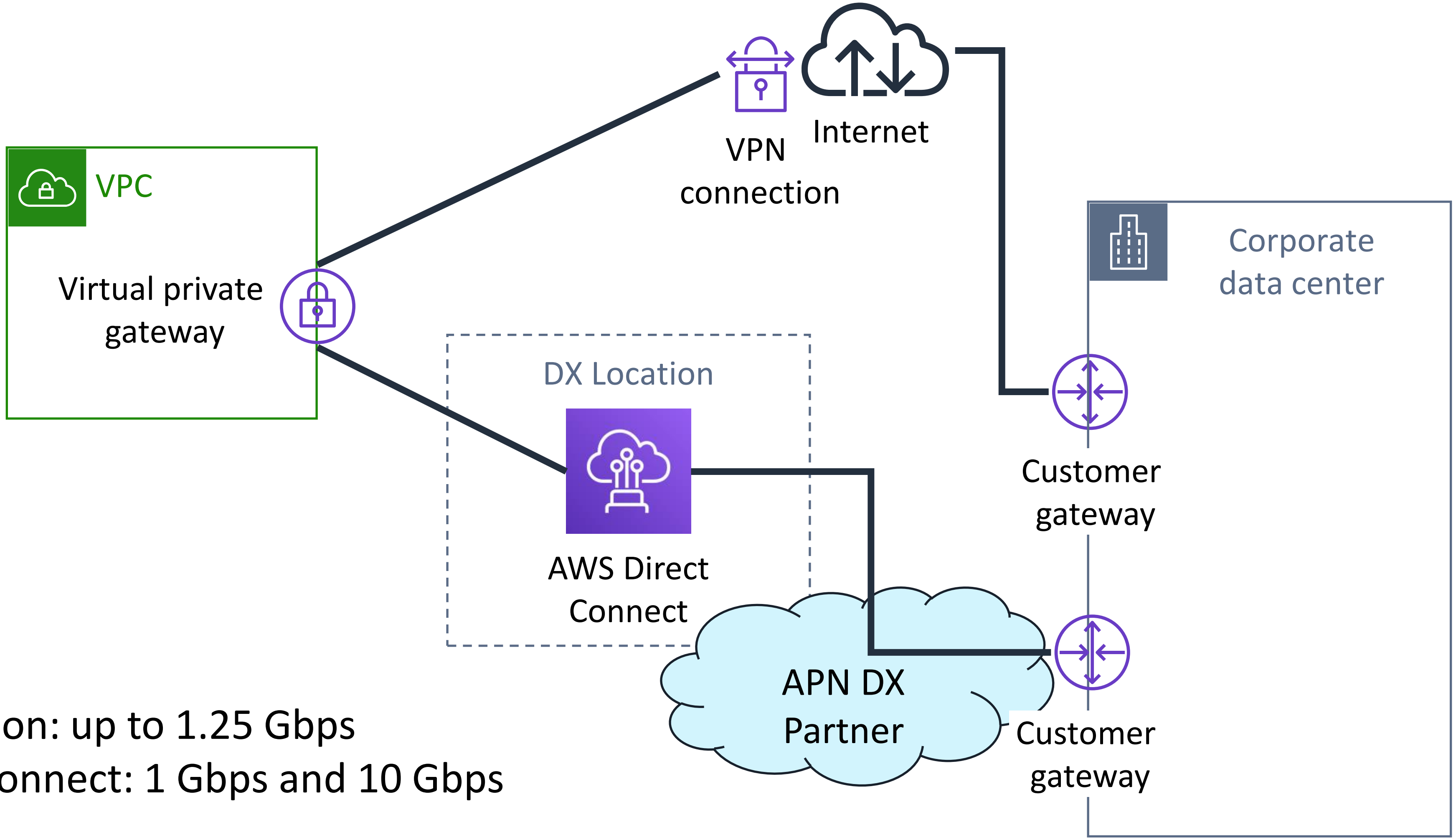
- Hybrid environments
- Transferring large datasets
- Network performance predictability
- Security and compliance

Extending on-premises network to AWS using DX



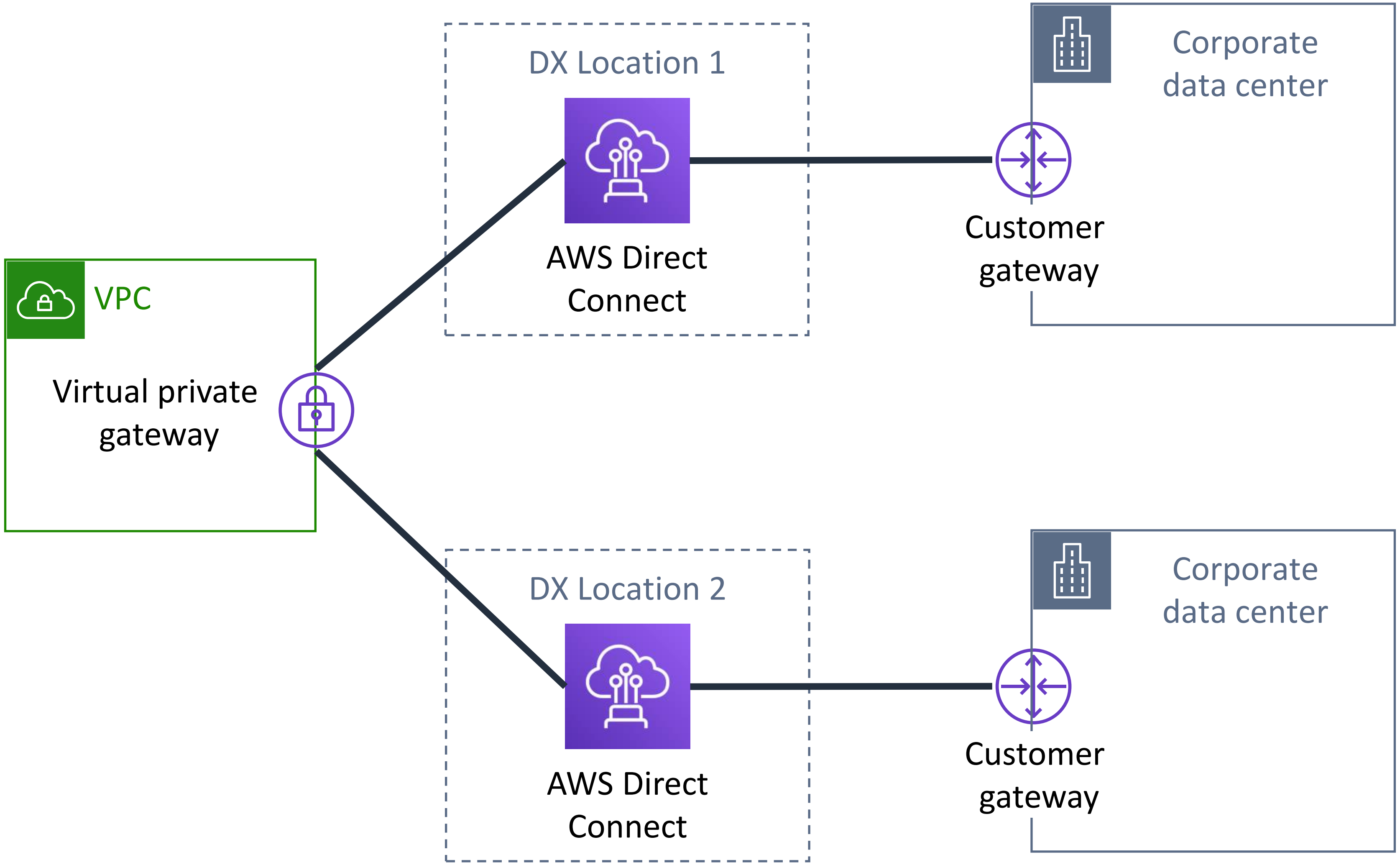
Dedicated network connection over private lines

Enabling high availability: DX with backup VPN connection



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

Enabling high resiliency for critical workloads with DX



Section 3 key takeaways

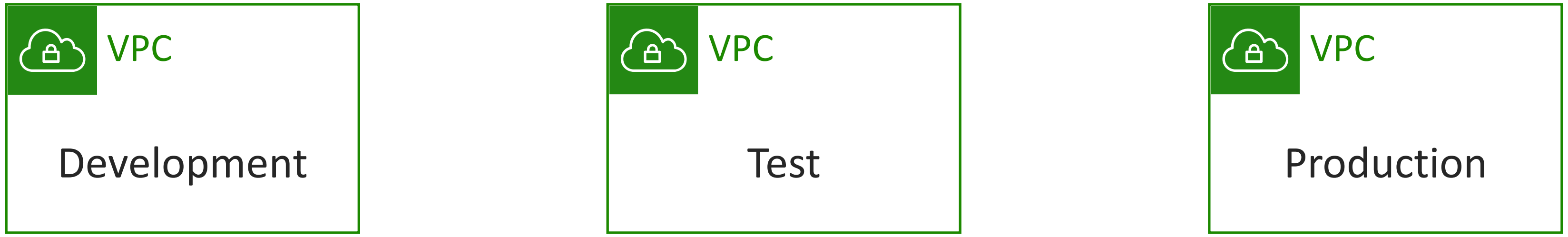
- AWS Direct Connect uses open standard 802.1q VLANs that enable you to establish a dedicated, private network connection from your premises to AWS
- You can access any VPC or public AWS service in any Region (except China) from any supported DX location
- You can implement highly available connectivity 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

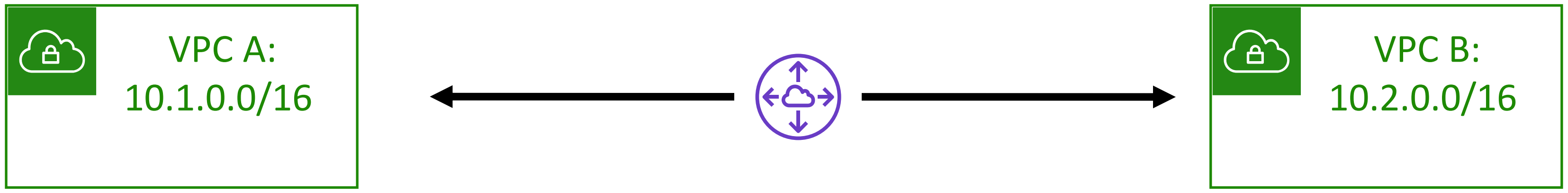
- Isolating some of your workloads is generally a good practice
- However, you might need to transfer data between two or more VPCs



VPC 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

Establishing VPC peering



Peering connection
(PCX-1)

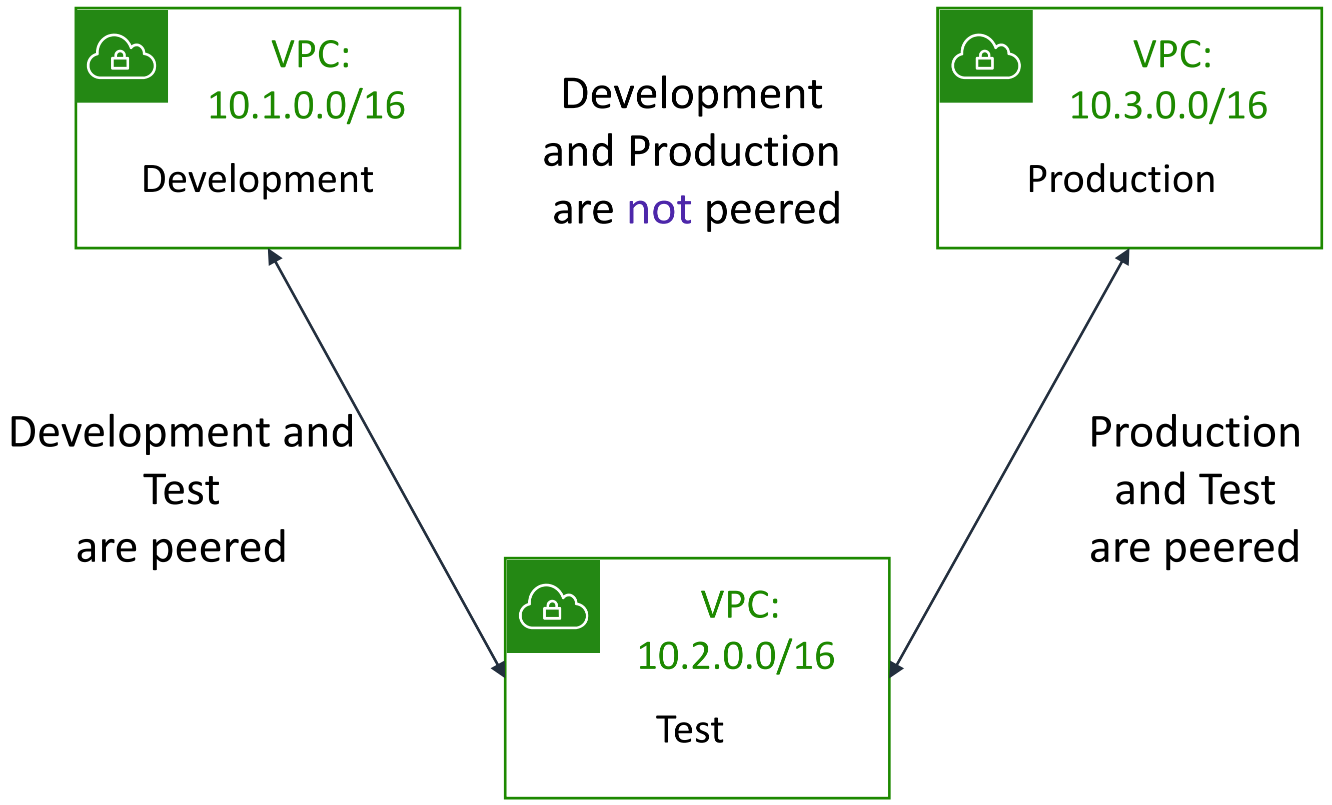
Route table VPC A

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


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
Production and Test are peered
VPC:
10.2.0.0/16
Test

- 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

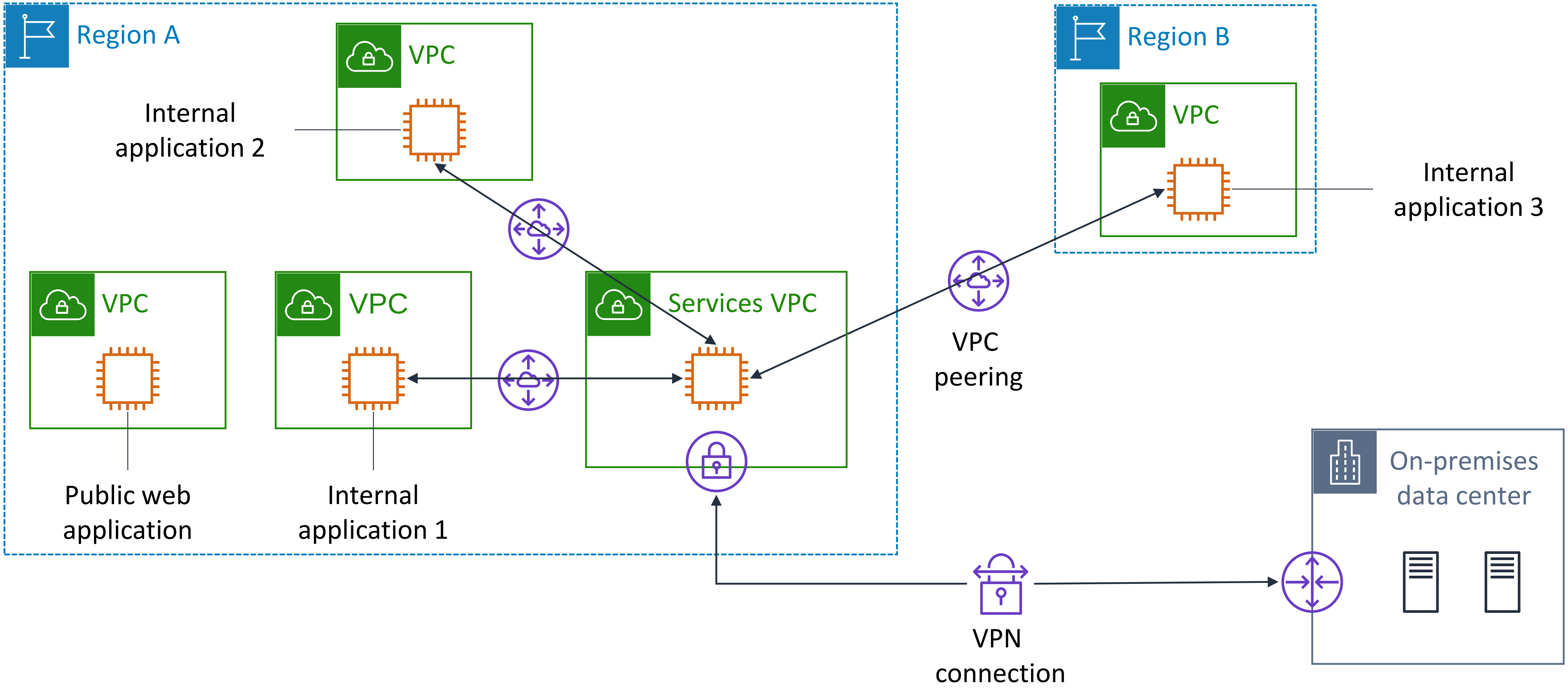
Considerations for peering multiple VPCs

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

Only connect essential VPCs

Make sure your solution can scale

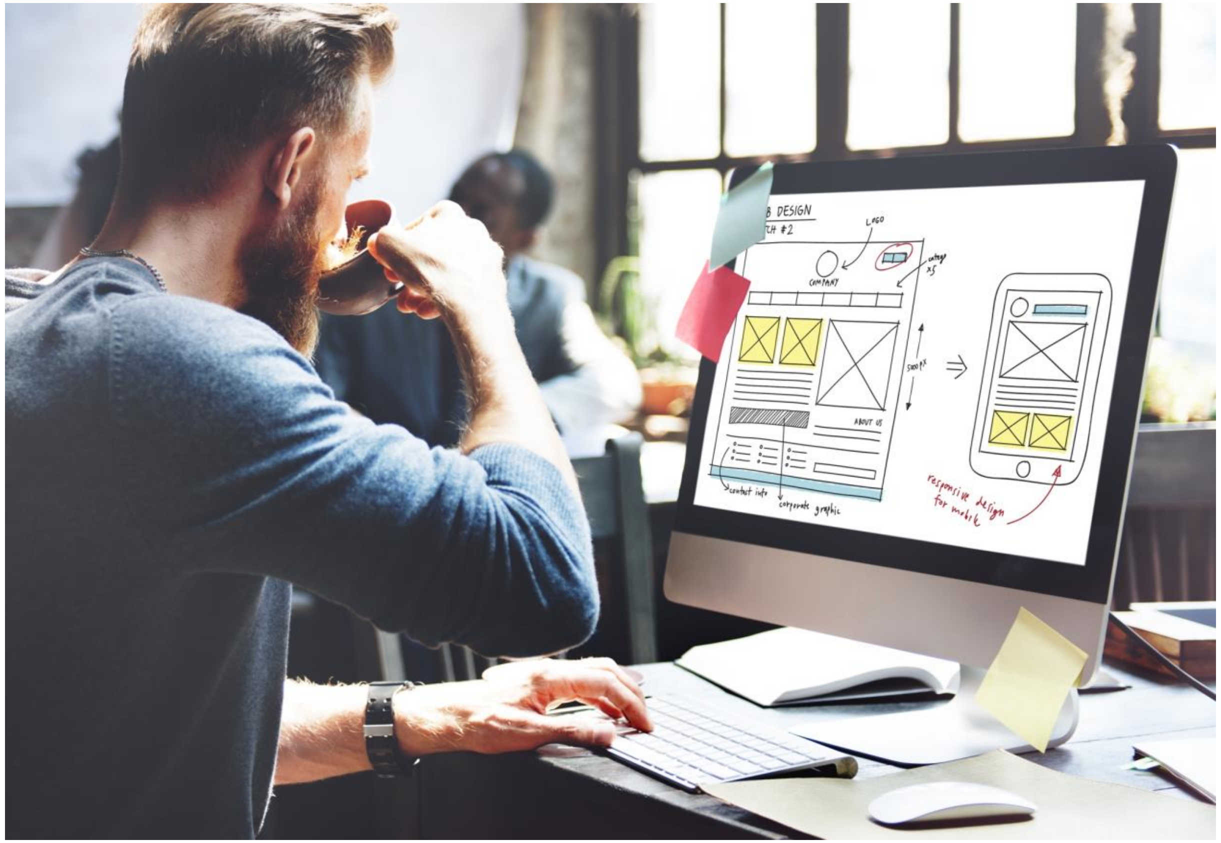
Example: VPC peering for shared resources



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
- 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

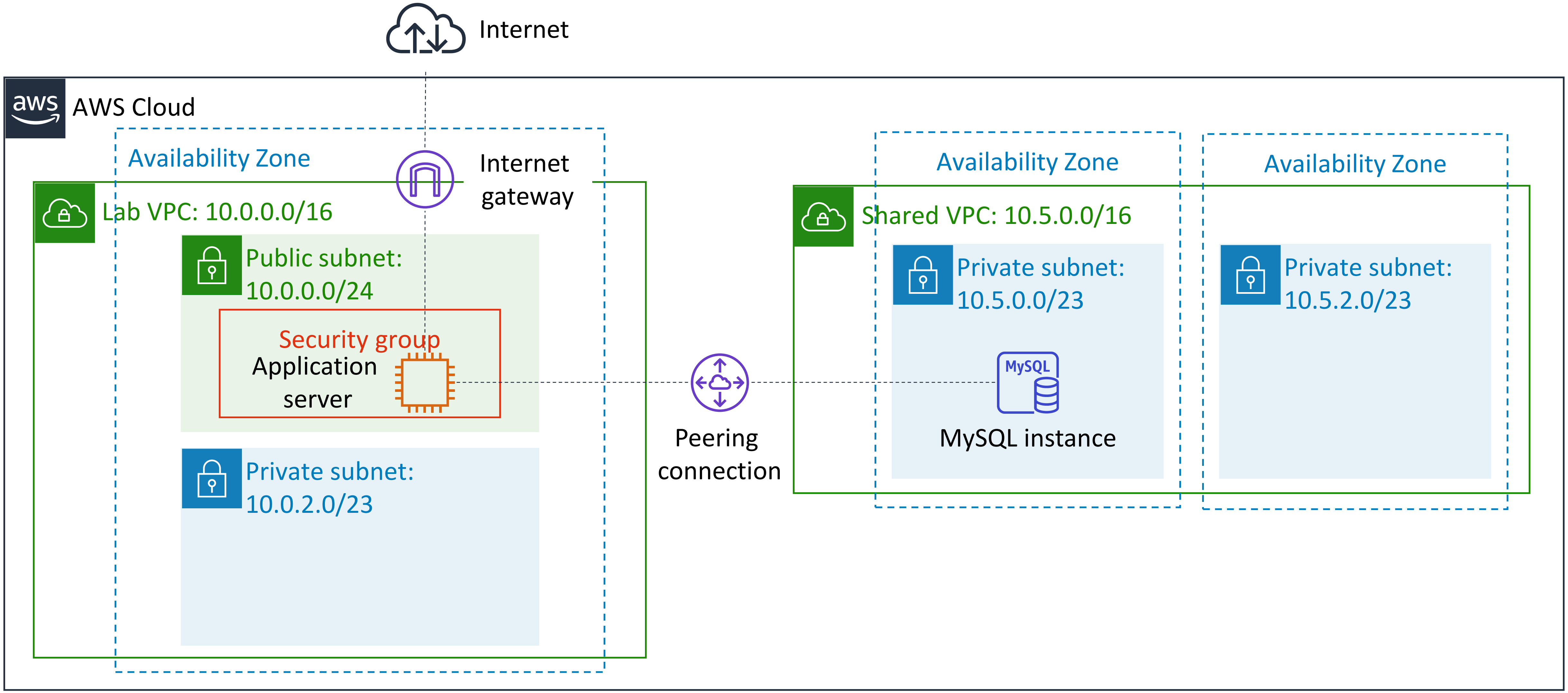
Module 7 – Guided Lab: Creating a VPC Peering Connection



Guided lab: Tasks

1. Create a peering connection between two VPCs
2. Configure route tables to send traffic to the peering connection
3. Test the peering connection

Guided lab: Final product



~ 20 minutes

Begin Module 7 – Guided Lab: Creating a VPC Peering Connection

Guided lab debrief: Key takeaways

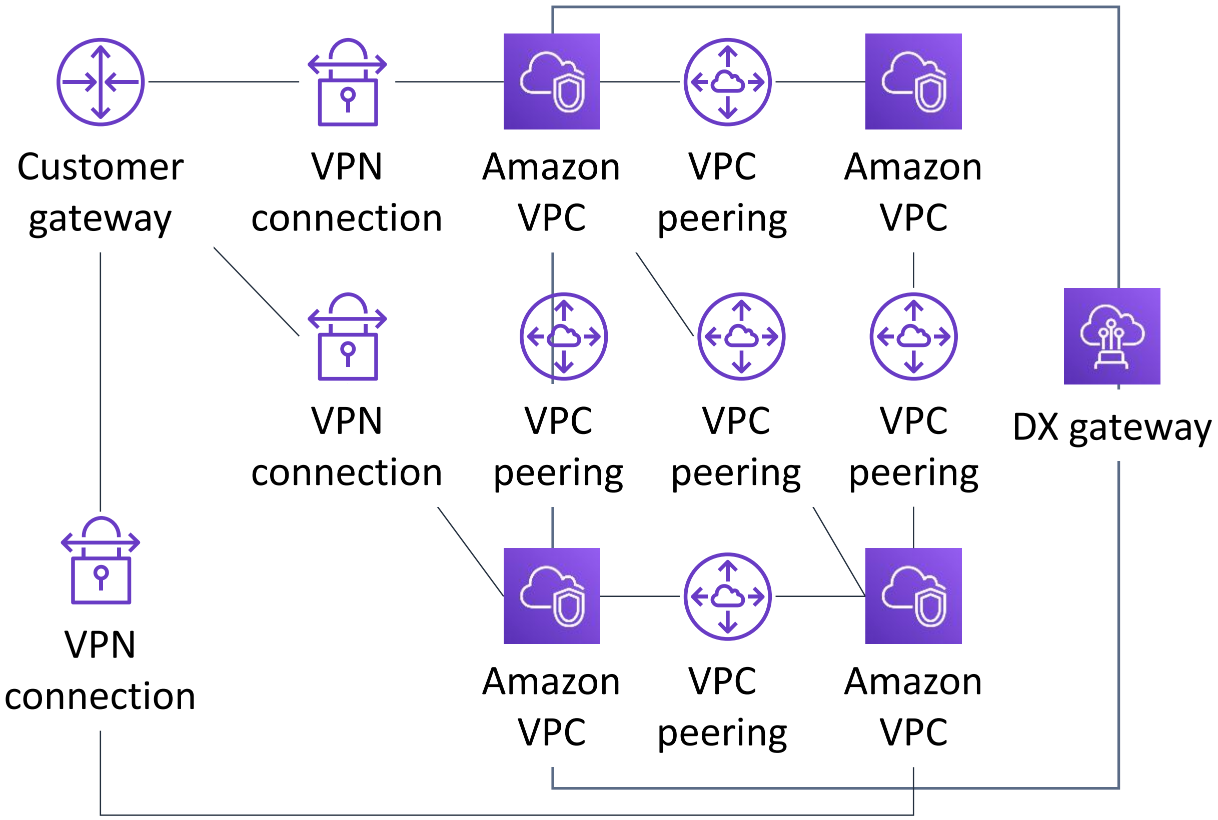
Module 7: Connecting Networks

Section 5: Scaling your VPC network with AWS Transit Gateway

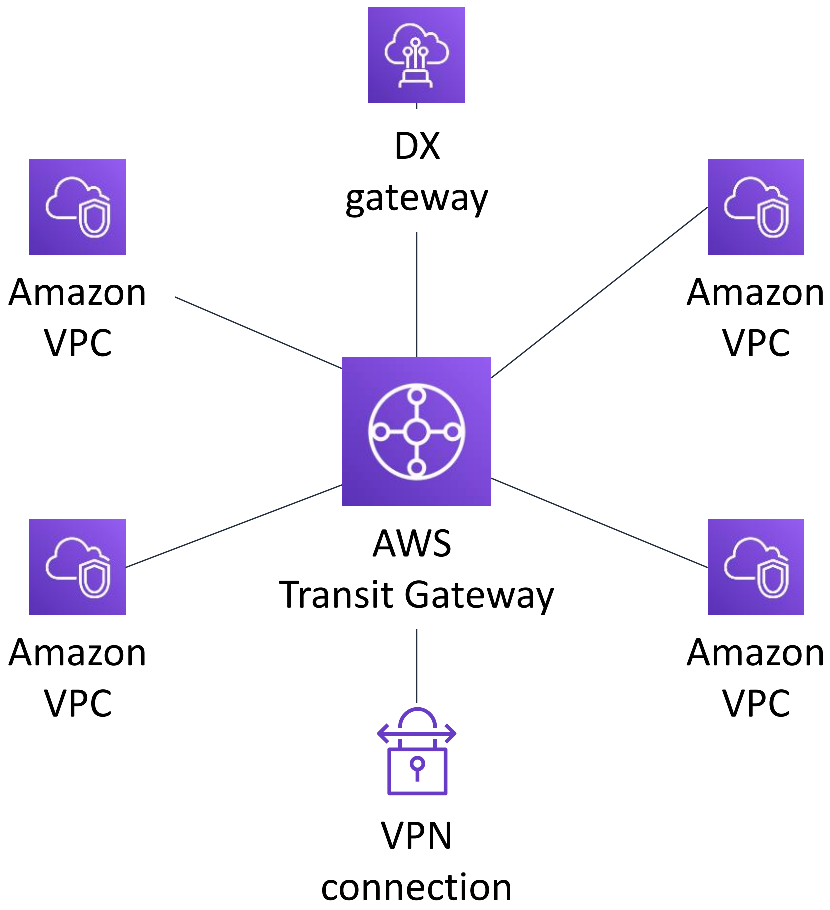
aws academy

Need to scale networks across multiple VPCs

From this...



... to this



AWS Transit Gateway

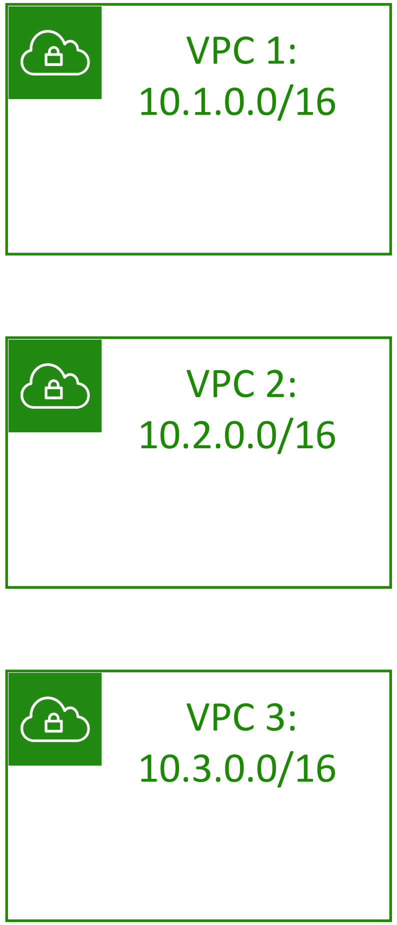
AWS Transit Gateway

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

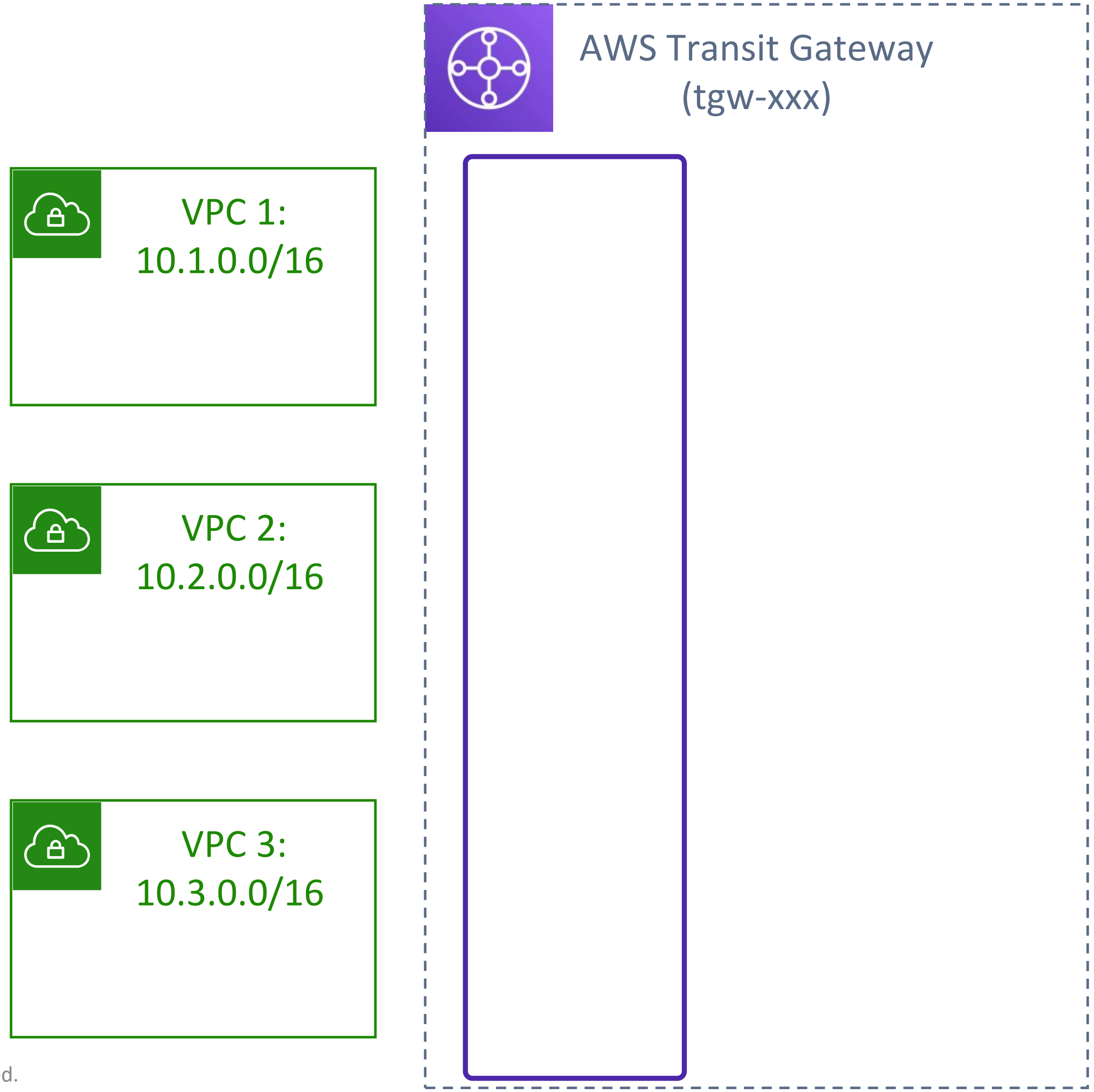
Connecting multiple VPCs

Scenario: We want to fully connect three VPCs.



Step 1: Create a transit gateway

Scenario: We want to fully connect three VPCs.

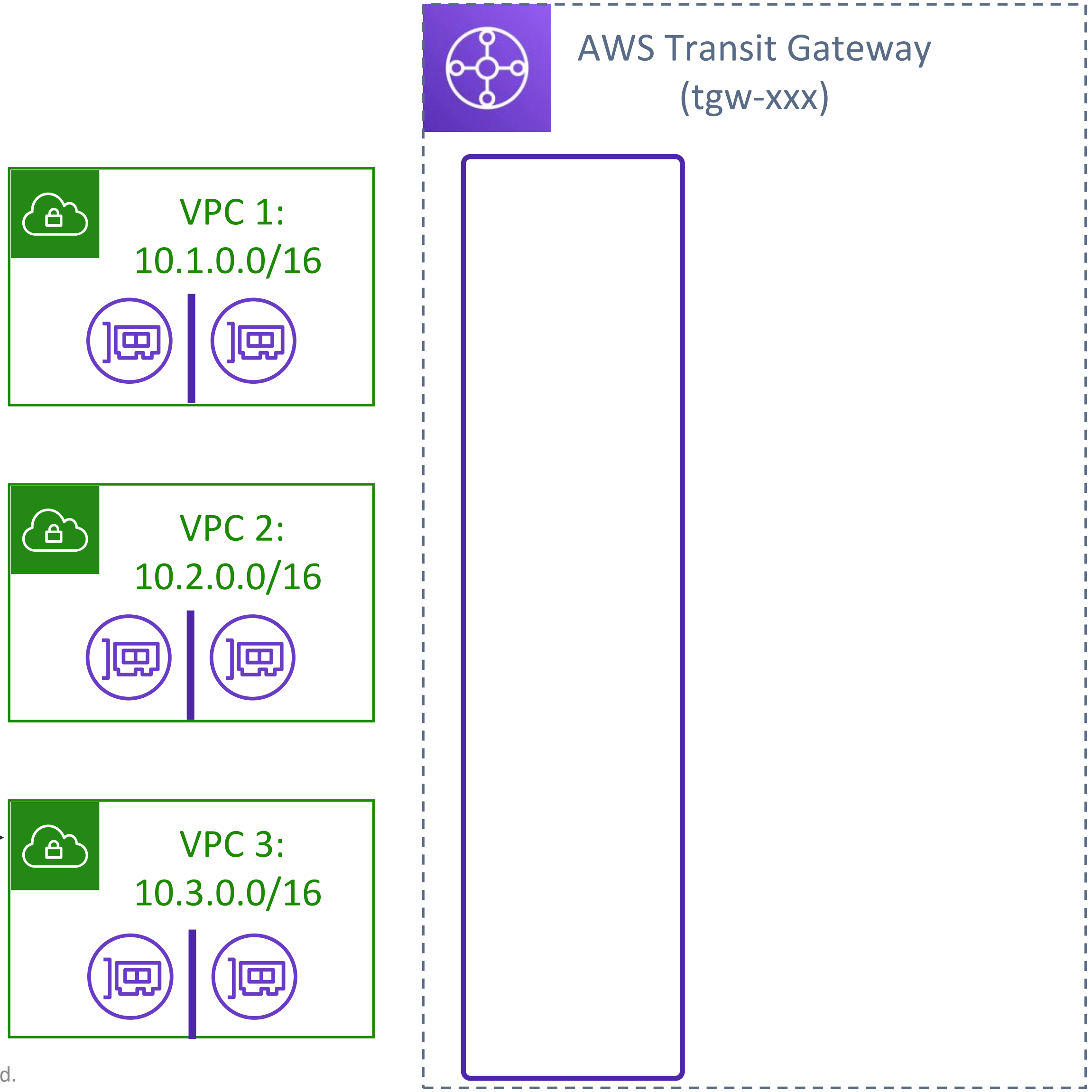


Step 2: Deploy elastic network interfaces

Scenario: We want to fully connect three VPCs.

VPC 3 route table

Destination	Target
10.3.0.0/16	local

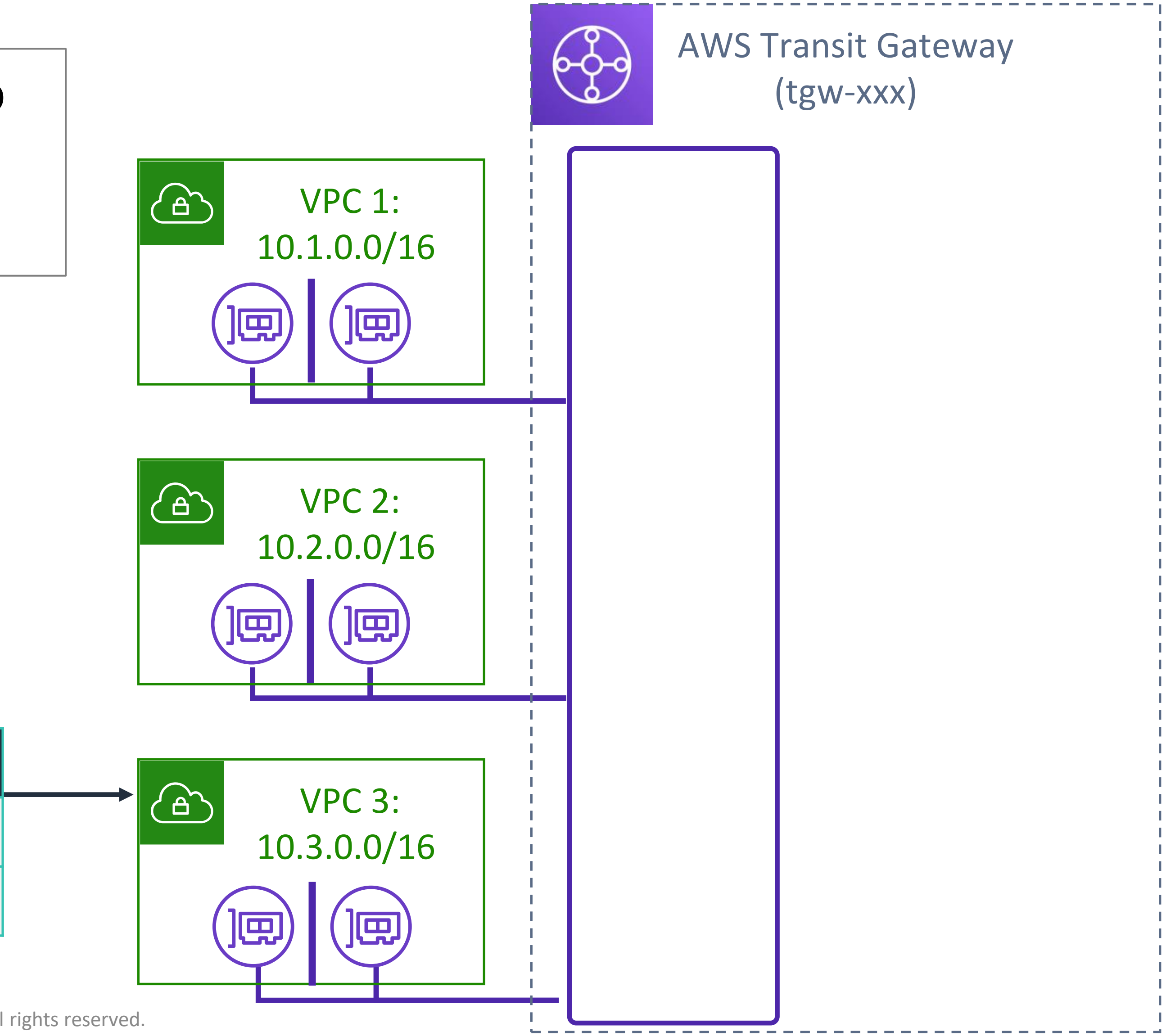


Step 3: Update the VPC route table

Scenario: We want to fully connect three VPCs.

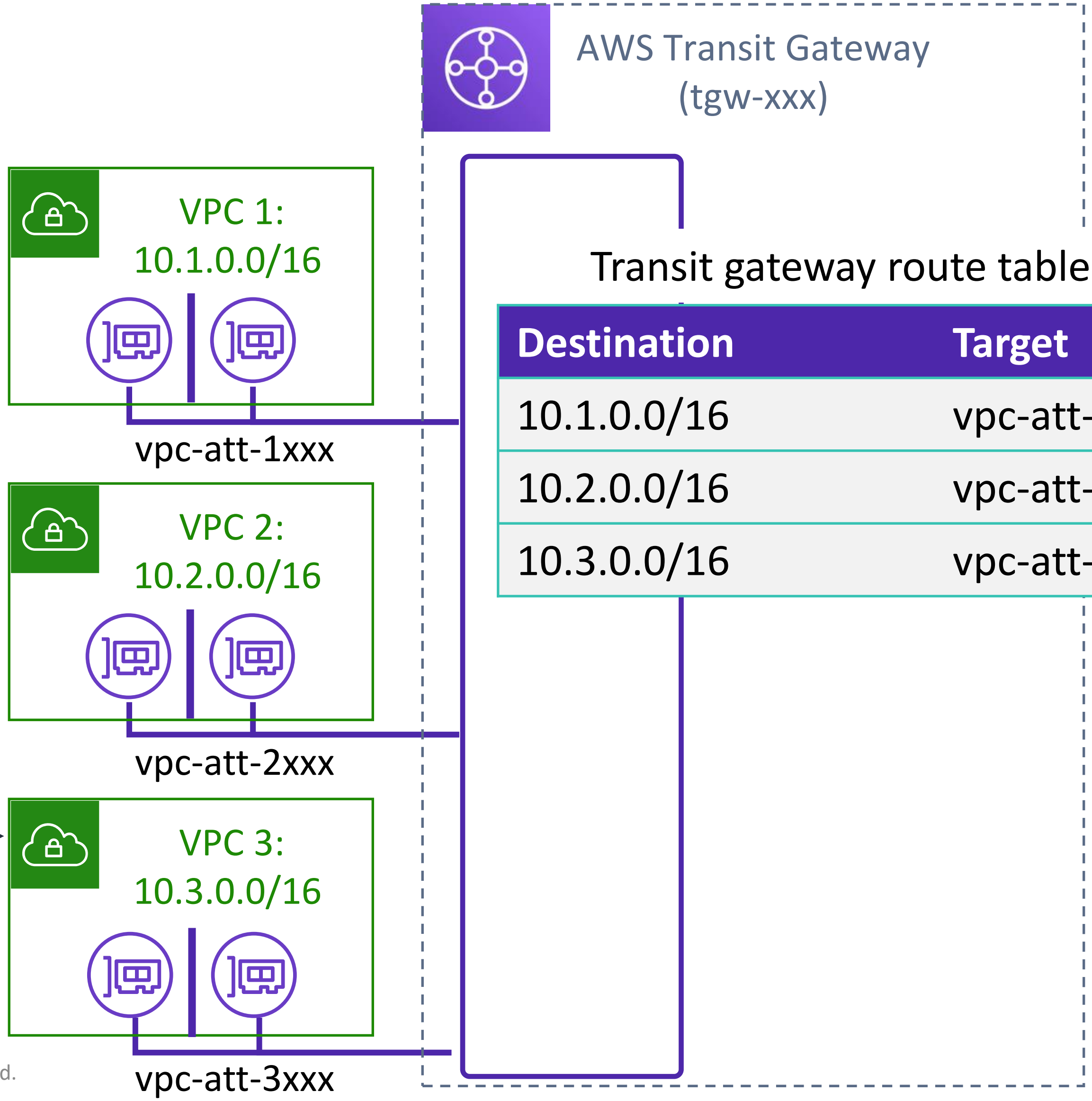
VPC 3 route table

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

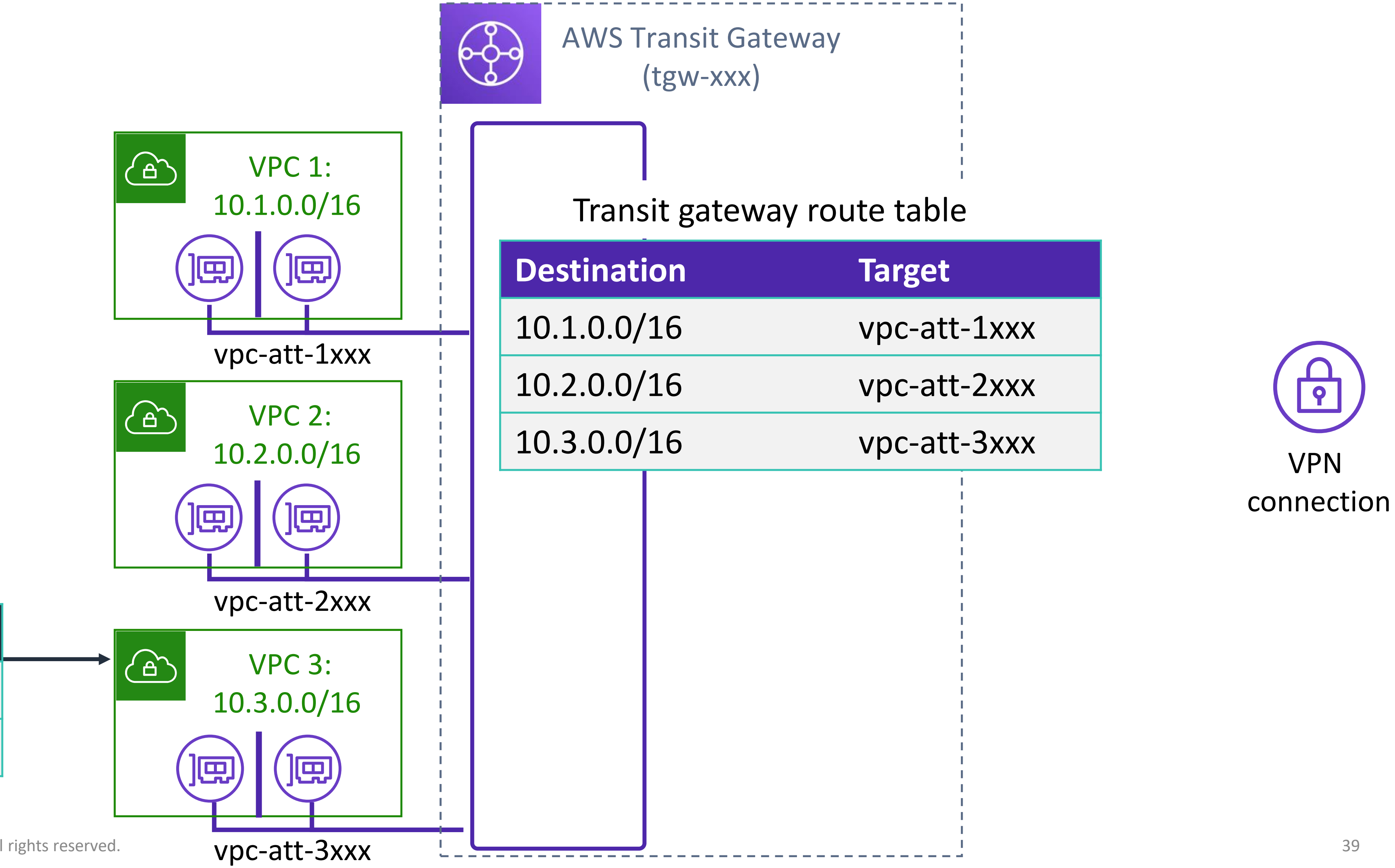
Destination	Target
10.3.0.0/16	local
10.0.0.0/8	tgw-xxx

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

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

VPC 3 route table

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



Transit gateway route table

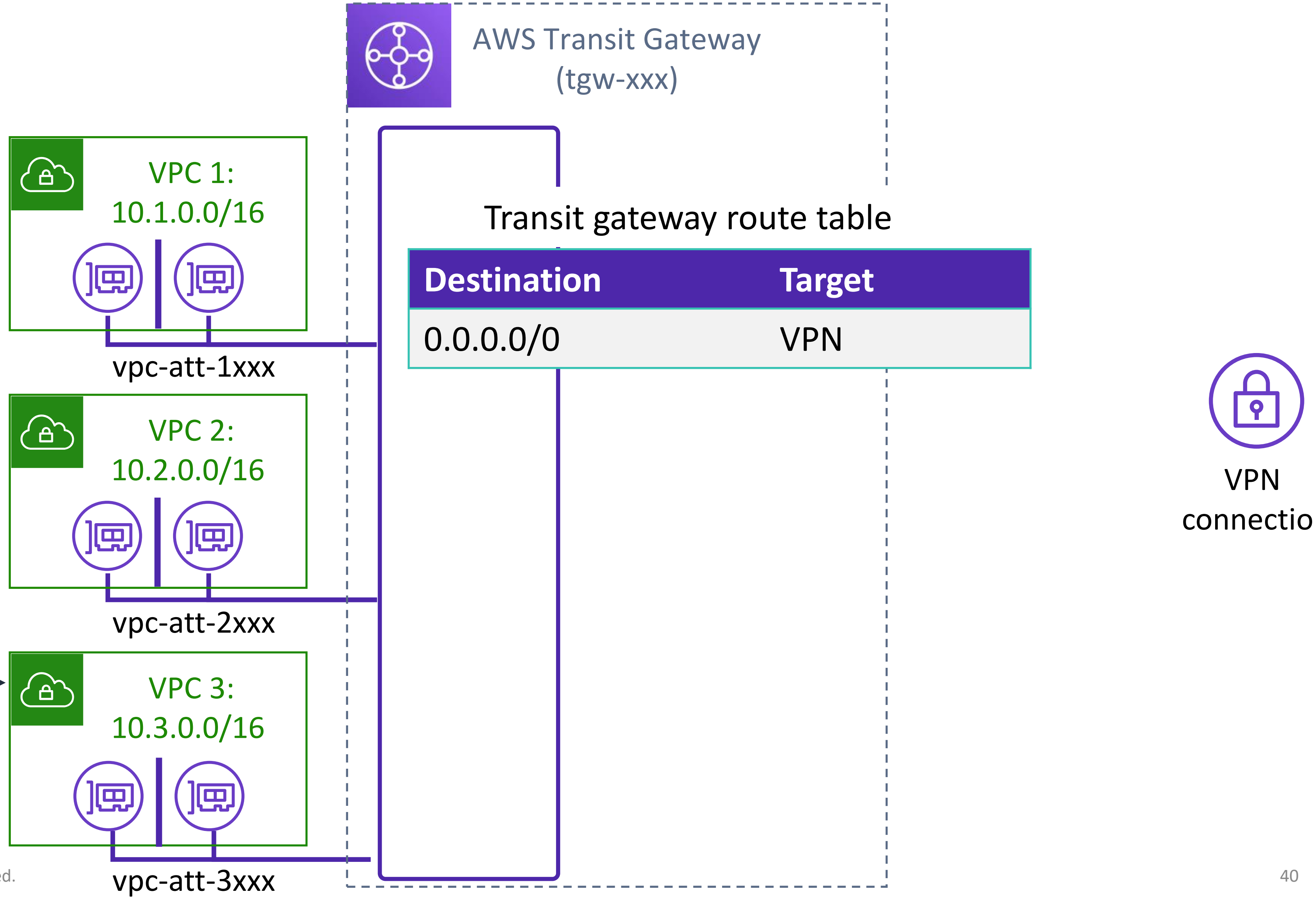
Destination	Target
10.1.0.0/16	vpc-att-1xxx
10.2.0.0/16	vpc-att-2xxx
10.3.0.0/16	vpc-att-3xxx

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

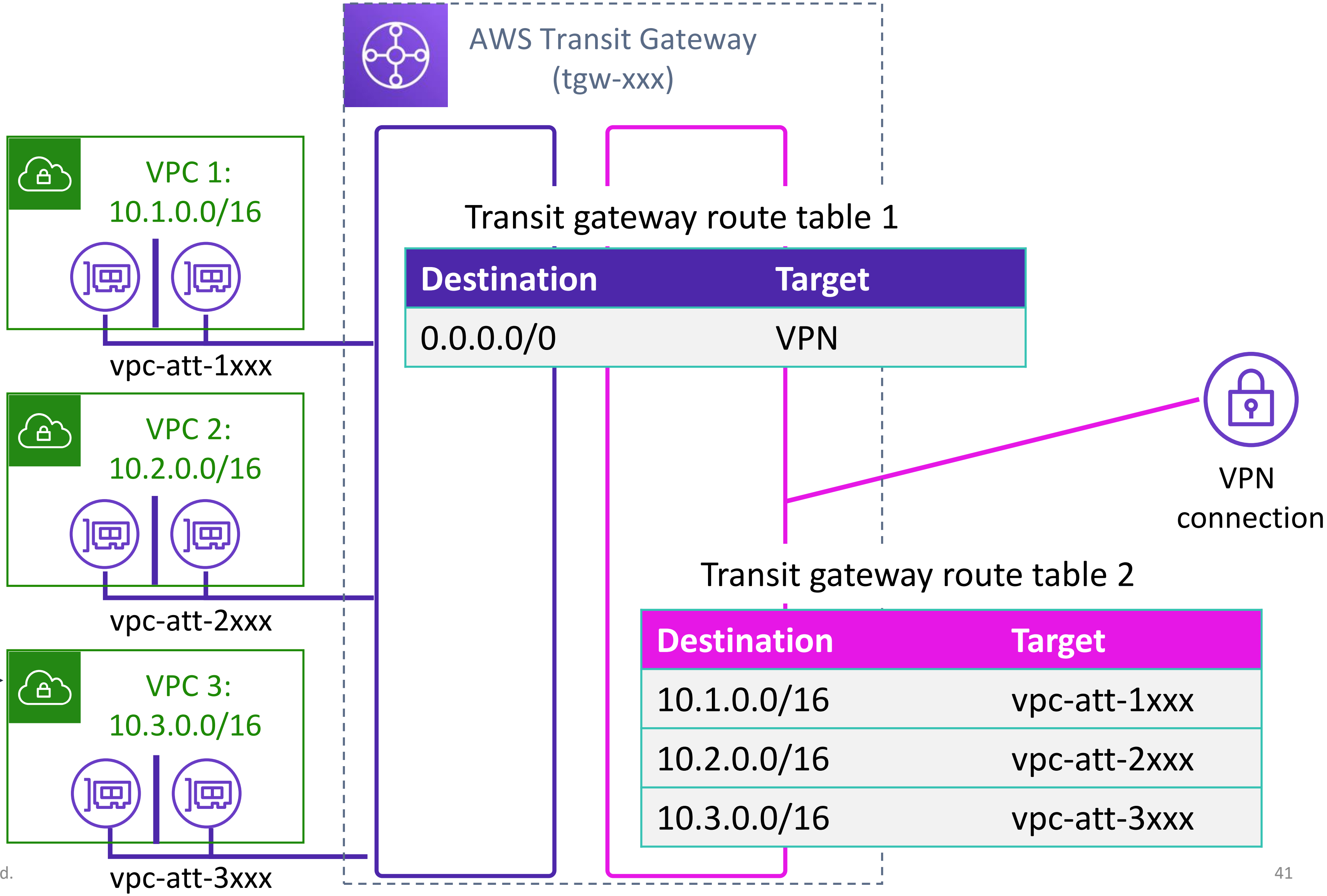
Destination	Target
0.0.0.0/0	VPN

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

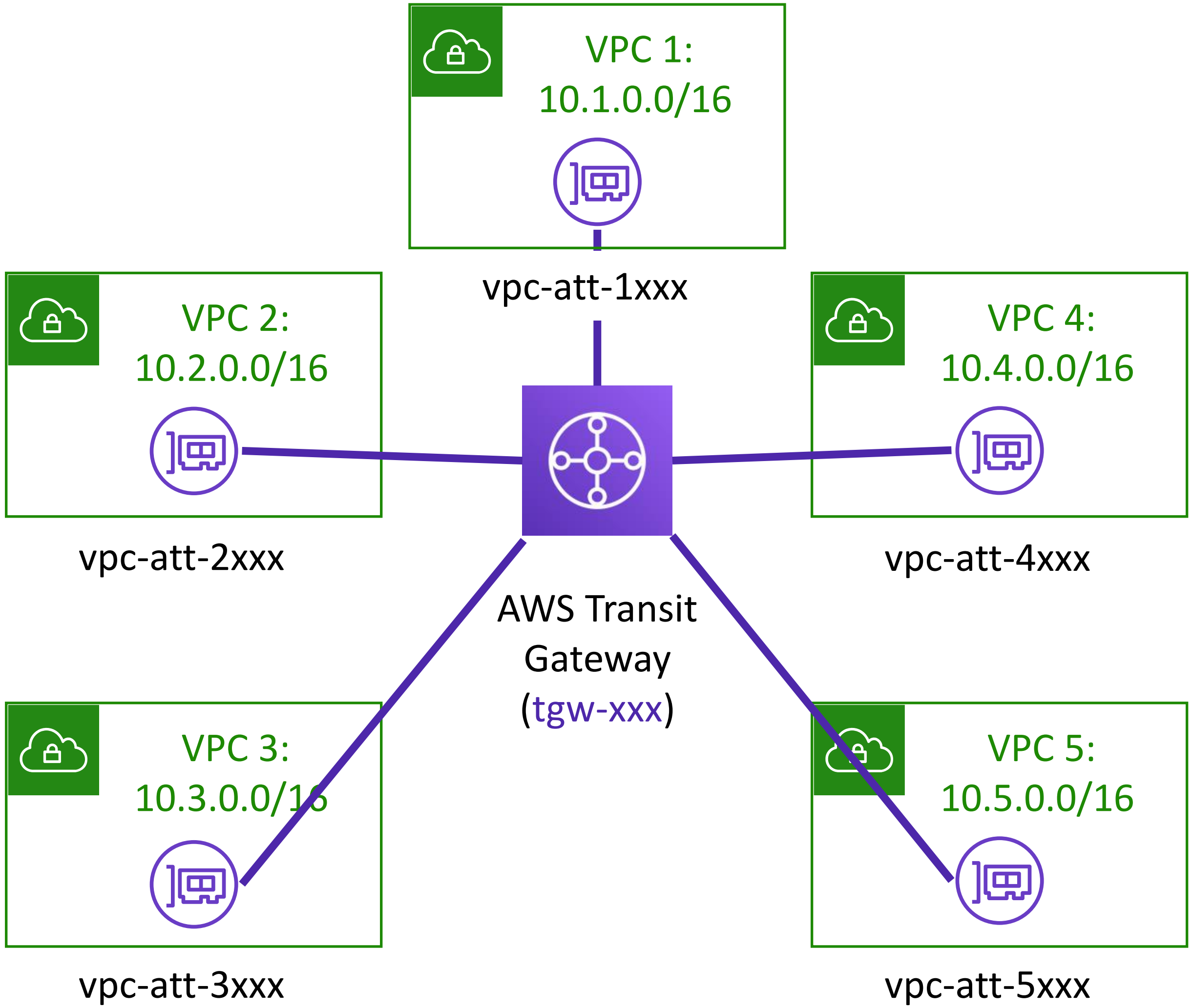
Activity: AWS Transit Gateway

AWS Transit Gateway: Challenge

Scenario: How do you connect these five VPCs?

VPC # route table

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



VPC 1:
10.1.0.0/16

vpc-att-1xxx

VPC 2:
10.2.0.0/16

vpc-att-2xxx

VPC 4:
10.4.0.0/16

vpc-att-4xxx

AWS Transit Gateway
(tgw-xxx)

VPC 3:
10.3.0.0/16

vpc-att-3xxx

VPC 5:
10.5.0.0/16

vpc-att-5xxx

Transit gateway route table

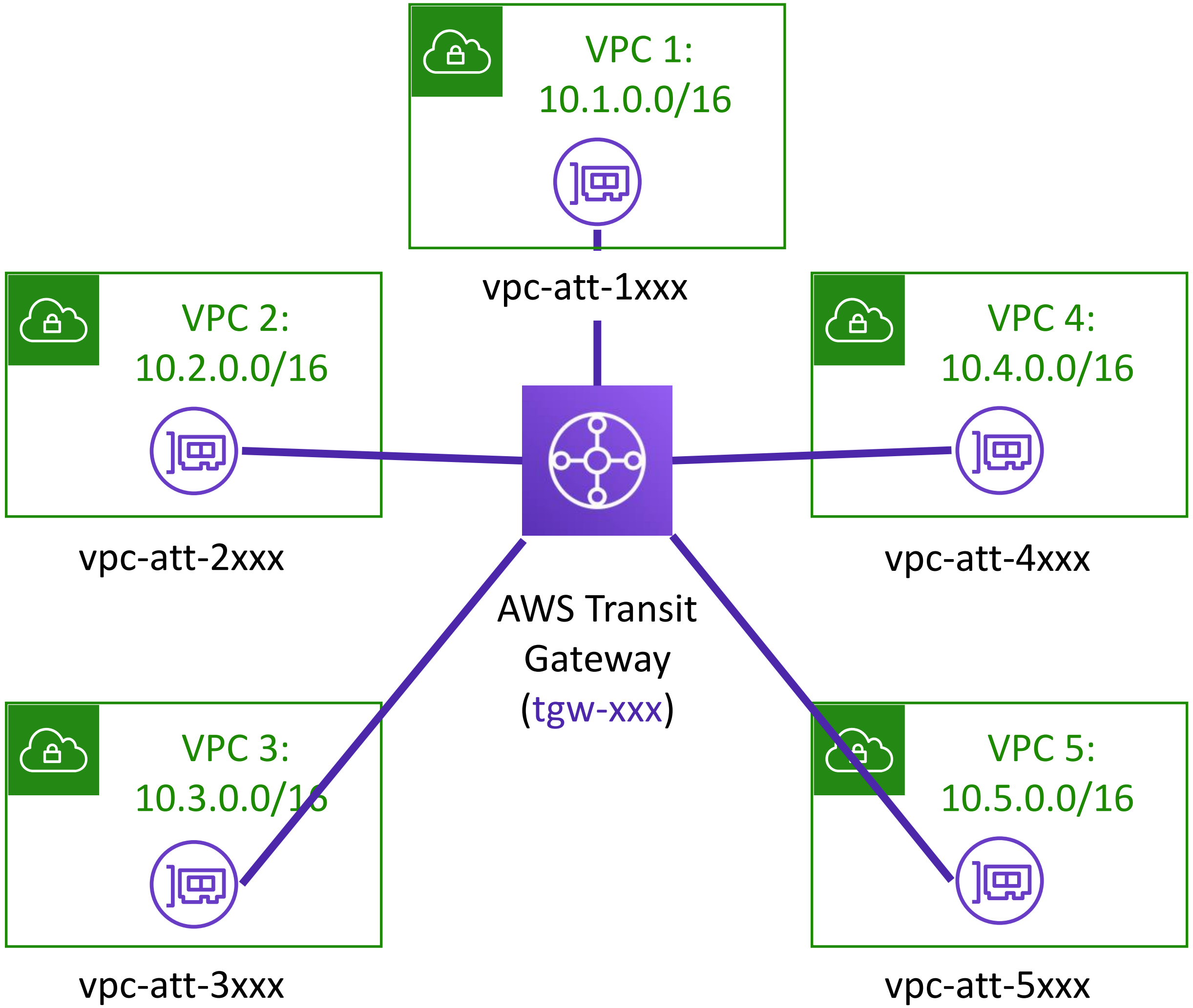
Destination	Target
?	?

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

Module 7: Connecting Networks

Section 6: Connecting your VPC to supported AWS services

VPC endpoints

- Enable you to privately connect your VPC to supported AWS services and to VPC endpoint services that are powered by AWS PrivateLink

- Enable traffic between your VPC and the other service without leaving the Amazon network

- Do not require an internet gateway, VPN, network address translation (NAT) devices, or firewall proxies

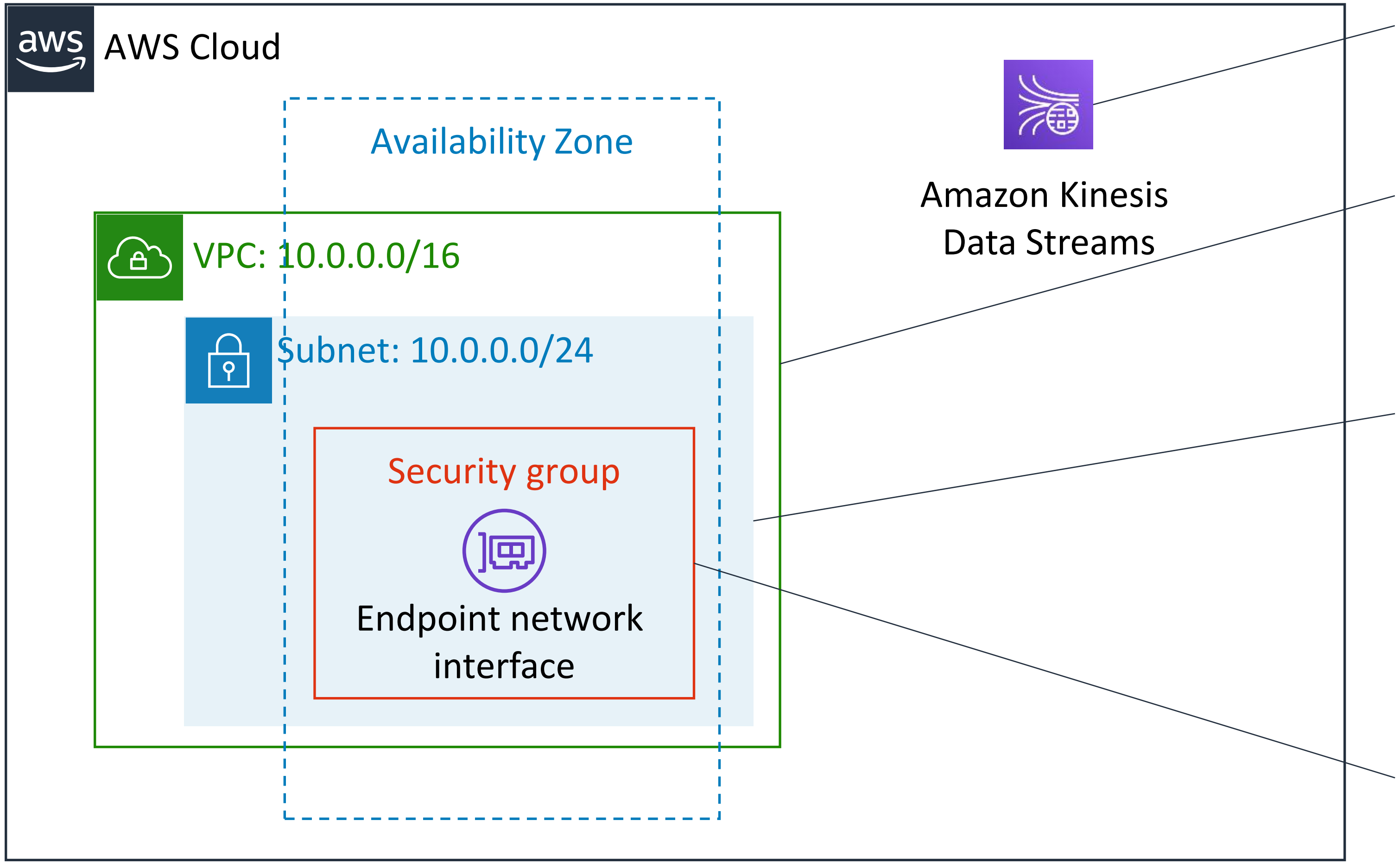
- Are horizontally scaled, redundant, and highly available

Two types of VPC endpoints

- Interface endpoint – An elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service
- Powered by AWS PrivateLink
- Examples –
  - Amazon CloudWatch
  - Amazon EC2 API
  - Elastic Load Balancing

- Gateway endpoint – A gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service
- Supported AWS services –
  - Amazon S3
  - Amazon DynamoDB

How to set up an interface endpoint



1. Specify the AWS service, endpoint service, or AWS Marketplace service you want to connect to.

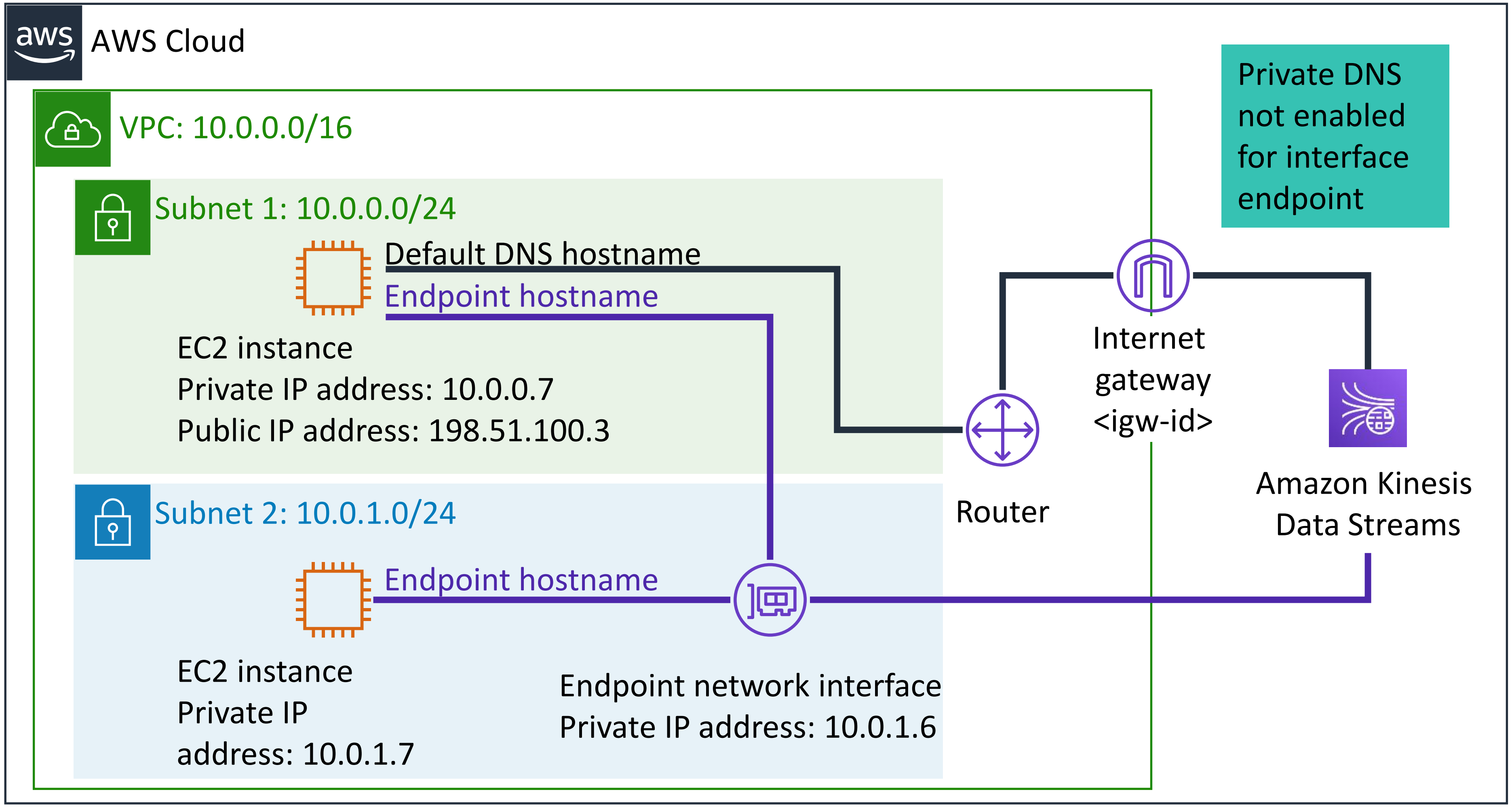
2. Choose the VPC where you want to create the interface endpoint.

3. Choose a subnet in your VPC that will use the interface endpoint. You can specify more than one subnet in different Availability Zones (as supported by the service).

4. (Optional) Enable private Domain Name System (DNS) for the endpoint.

5. Specify the security groups to associate with the network interface.

Example of using VPC endpoints (1 of 2)



Subnet 1 route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

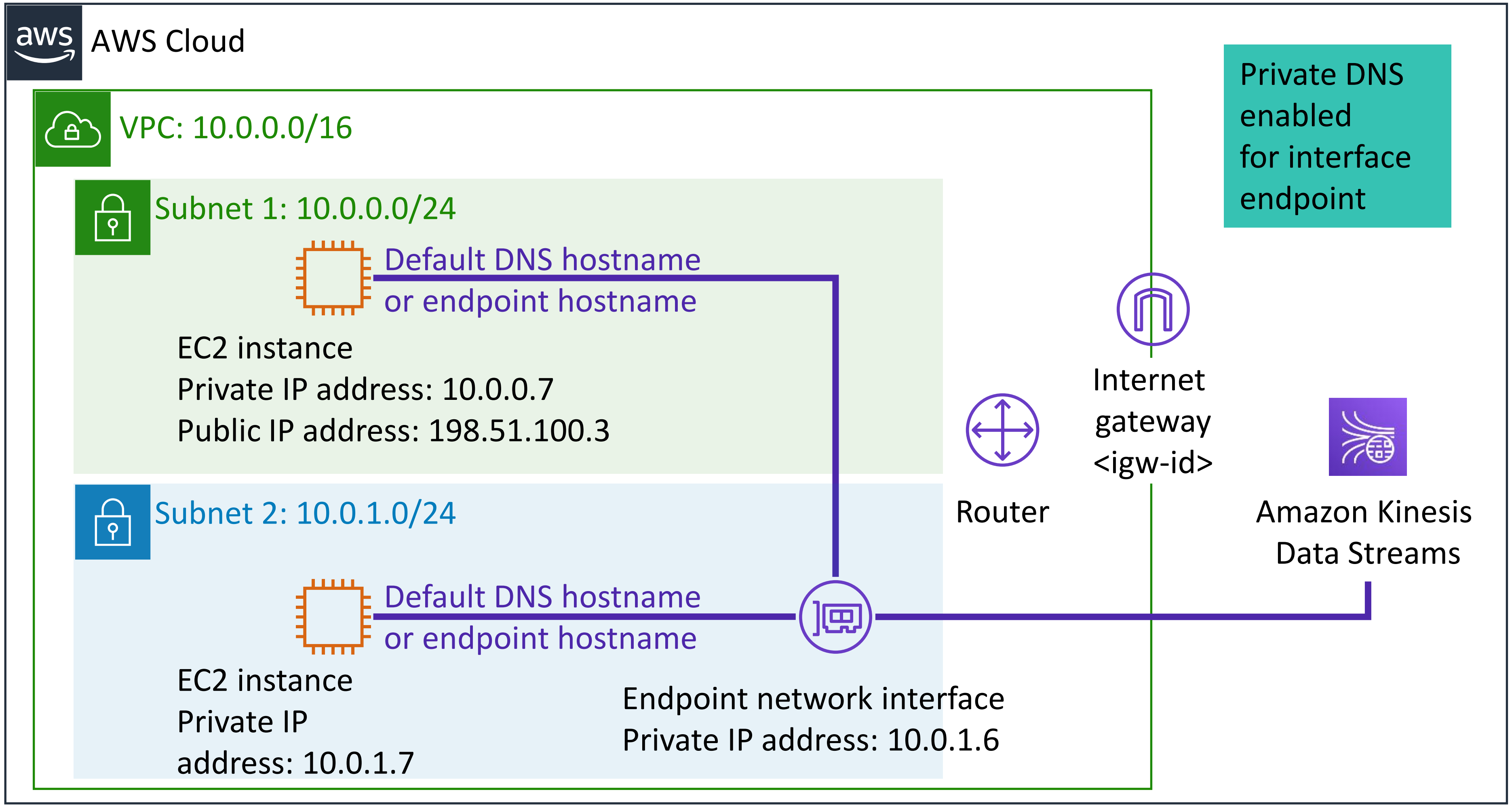
Subnet 2 route table

Destination	Target
10.0.0.0/16	local

Default DNS hostname: kinesis.us-east-1.amazonaws.com

Endpoint-specific DNS hostname: vpce-123-ab-kinesis.us-east-1.vpce.amazonaws.com

Example of using VPC endpoints (2 of 2)



Subnet 1 route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Internet

Subnet 2 route table

Destination	Target
10.0.0.0/16	local

Default DNS hostname: kinesis.us-east-1.amazonaws.com

Endpoint-specific DNS hostname: vpce-123-ab-kinesis.us-east-1.vpce.amazonaws.com

Section 6 key takeaways

- A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink
- VPC endpoints do not require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection
- There are two types of VPC endpoints: interface endpoints and gateway endpoints

Module 7: Connecting Networks

Module wrap-up

Module summary

In summary, in this module, you learned how to:

- Describe how to connect an on-premises network to the 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

Complete the knowledge check

```
<div id="content">
  <header id="topnav">
    <nav>
      <ul>
        <li class="active"><a class="scroll" href=
                                </a></li>
          Home
        <li><a class="scroll" href="#service">
                                </a></li>
          Service
        <li><a class="scroll" href="#product">
                                </a></li>
          Products
        <li><a class="scroll" href="#portfolio">
                                </a></li>
          Portfolio
        <li><a class="scroll" href="#team">
                                </a></li>
          Team
        <li><a class="scroll" href="#contact">
                                </a></li>
          Contact
        <div class="clear"></div>
      </ul>
    </nav>
    <div class="logo">
      <a href="./">
        <img src="web/images/logo3.png" id="logo_l
```

Sample exam question

An application running on Amazon Elastic Compute Cloud (Amazon EC2) instances processes sensitive information stored on Amazon Simple Storage Service (Amazon S3). The information is accessed over the internet. The security team is concerned that the internet connectivity to Amazon S3 is a security risk.

Which solution will resolve the security concern?

A. Access the data through an internet gateway.

B. Access the data through a VPN connection.

C. Access the data through a NAT gateway.

D. Access the data through a VPC endpoint for Amazon S3.

Additional resources

- AWS re:Invent 2018 video: AWS VPN Solutions
- AWS Knowledge Center video: How do I create a VPN with Amazon VPC?
- How do I configure a VPN over AWS Direct Connect?
- AWS re:Invent 2019 video: From one to many: Evolving Amazon VPC design
- Building a Scalable and Secure Multi-VPC AWS Network Infrastructure whitepaper
- AWS Knowledge Center video: What is AWS Peering?
- AWS re:Invent 2019 video: AWS Transit Gateway reference architectures for many VPCs
- AWS Knowledge Center video: What is an Interface VPC Endpoint and How Can I Create Interface Endpoints for my VPC?

Thank you