

AWS
re:Invent

NET412-R

Become an AWS VPN and AWS Direct Connect expert

Madhura Kale

Sr. Product Manager
Amazon EC2
Amazon Web Services

Steve Seymour

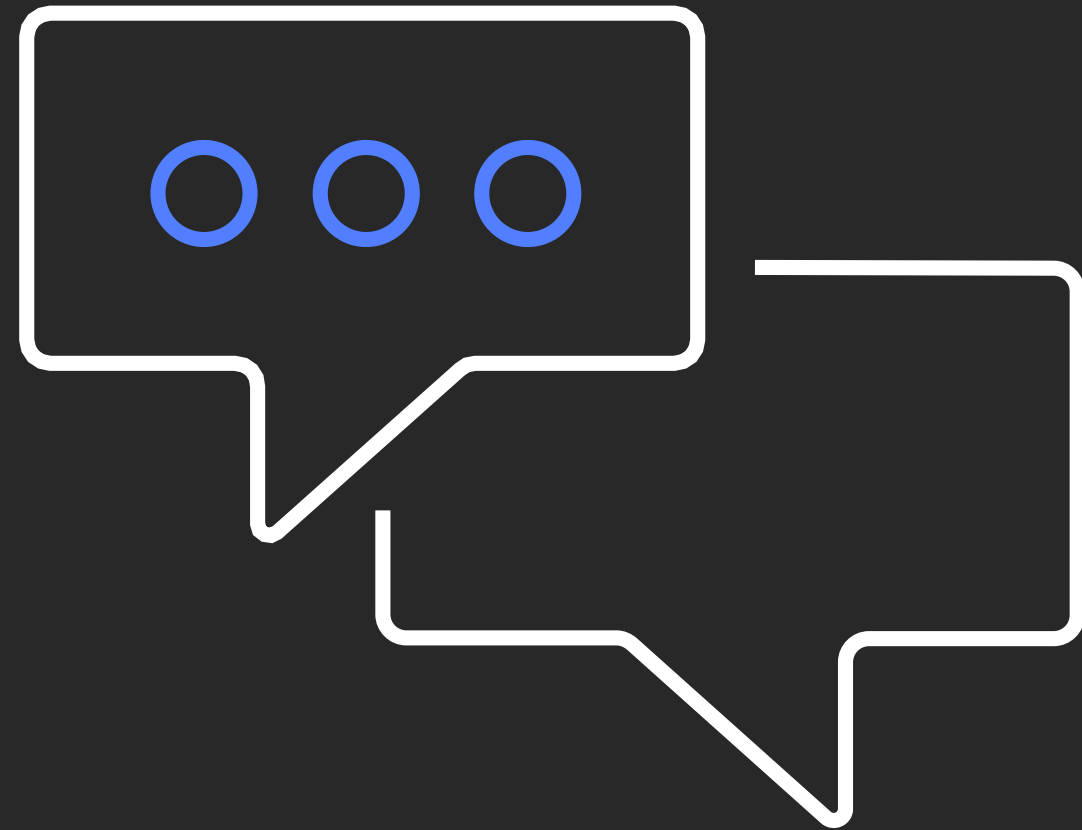
WW Tech Leader, Networking
Solutions Architecture
Amazon Web Services

The plan

An overview of:

- AWS Site-to-Site VPN
- AWS Client VPN
- AWS Direct Connect

Your questions!



AWS Site-to-Site VPN

AWS Site-to-Site VPN setup options

Static

- Policy- or route-based
- Static routing
- Authentication: Pre-shared key or **certificate-based (NEW)**

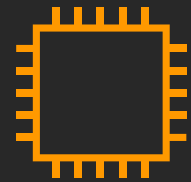
Dynamic

- Route-based only
- Dynamic routing (BGP)
- Authentication: Pre-shared key or **certificate-based (NEW)**

AWS Site-to-Site VPN

Create VPN Connection

I don't

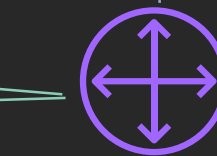
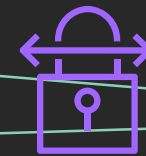


Instance

I know how to get to
172.16.0.0/16



Virtual private
gateway



Customer
gateway



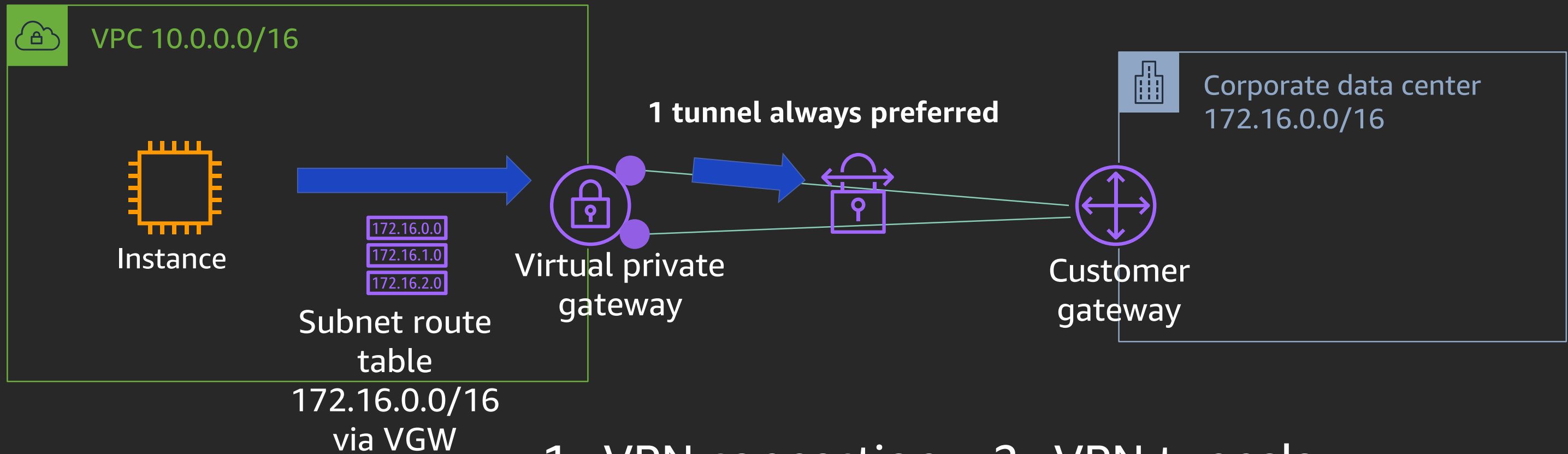
Corporate data center
172.16.0.0/16

1x VPN connection = 2x VPN tunnels

AWS Site-to-Site VPN



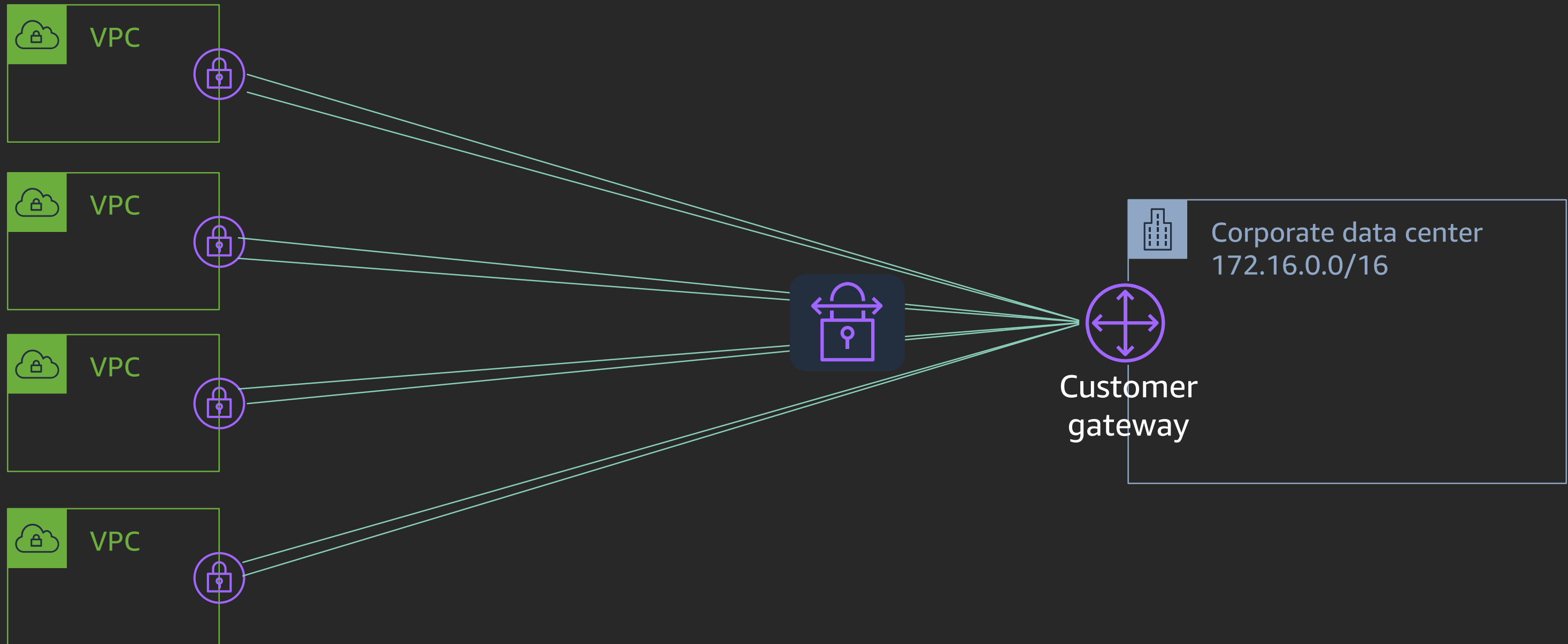
AWS Site-to-Site VPN



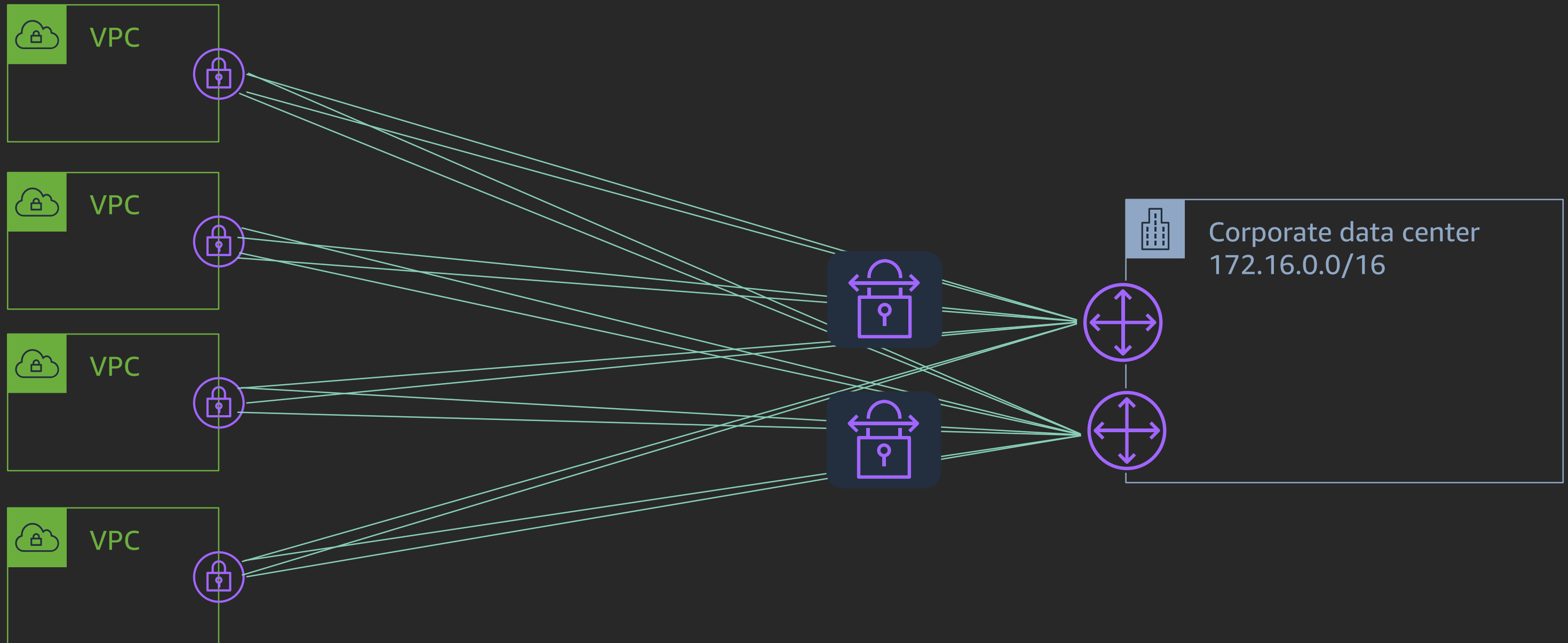
1x VPN connection = 2x VPN tunnels

1x VPN tunnel = 1.25Gbps

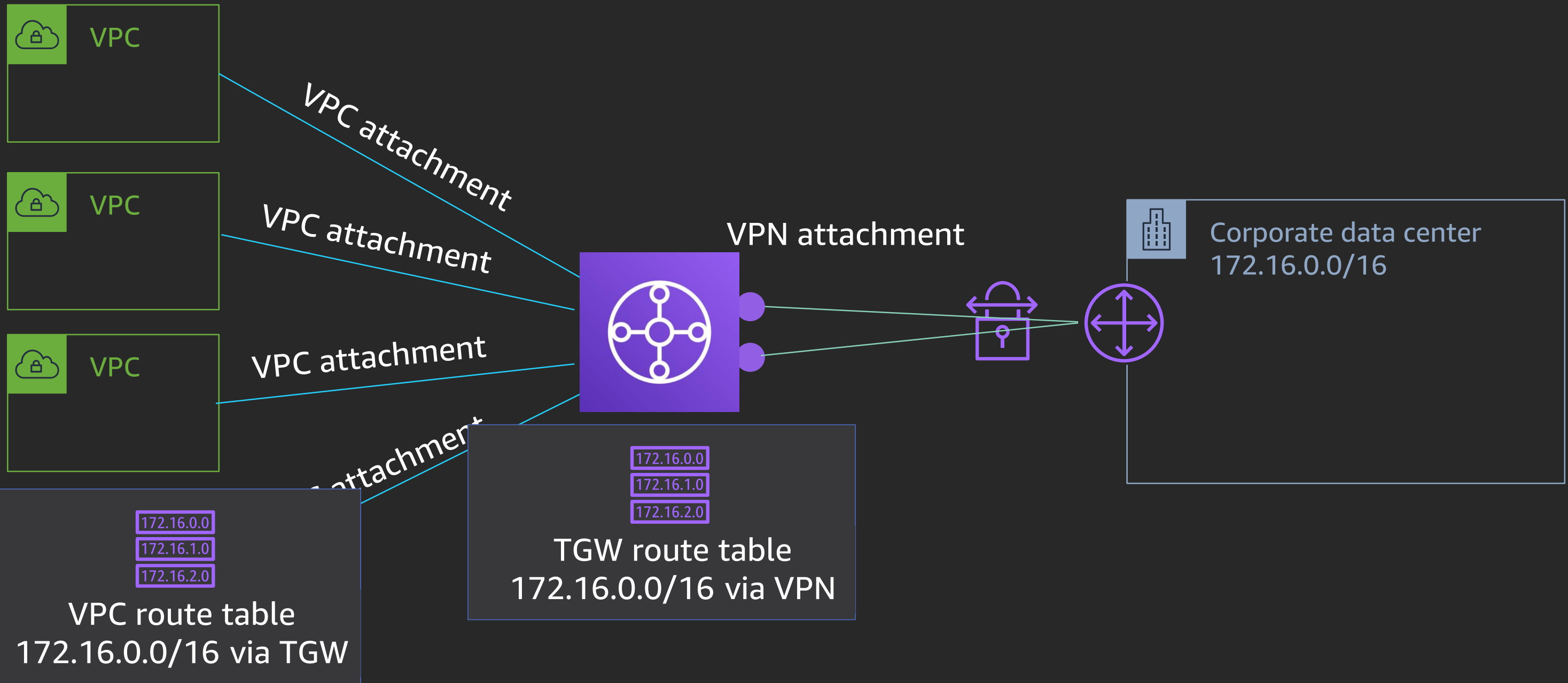
Multiple AWS Site-to-Site VPNs via VGW



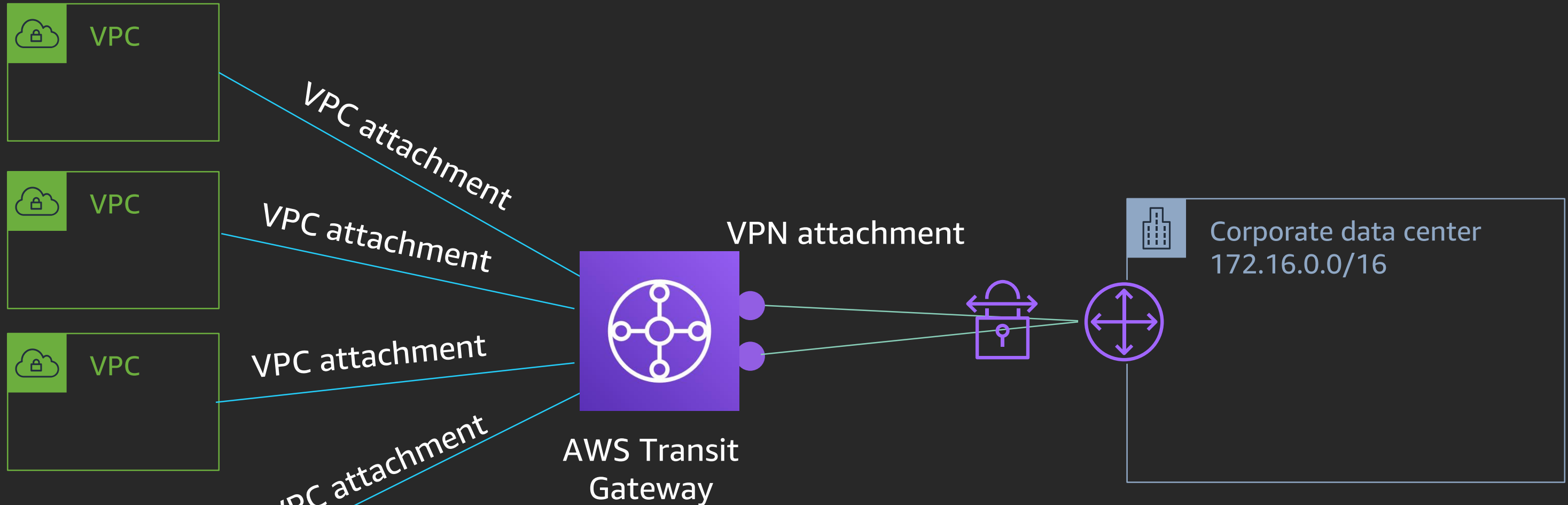
Multiple AWS Site-to-Site VPNs via VGW



Multiple AWS Site-to-Site VPNs via AWS Transit Gateway



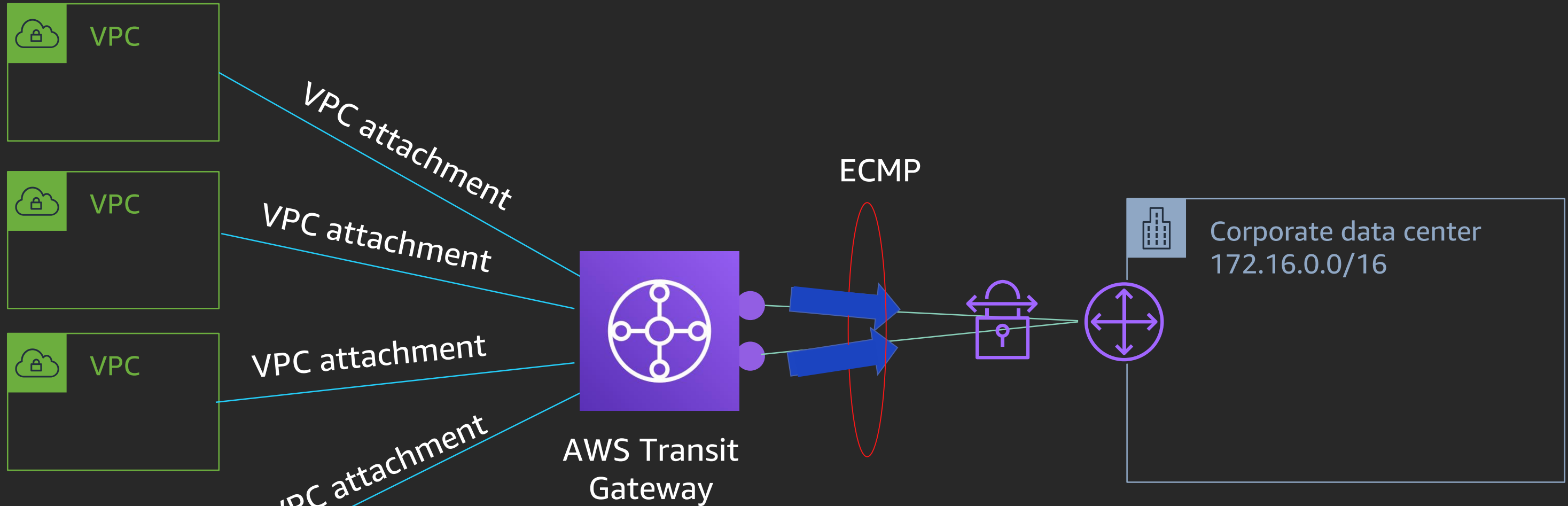
Multiple AWS Site-to-Site VPNs via AWS Transit Gateway



1x VPN connection = 2x VPN tunnels

1x VPN tunnel = 1.25Gbps

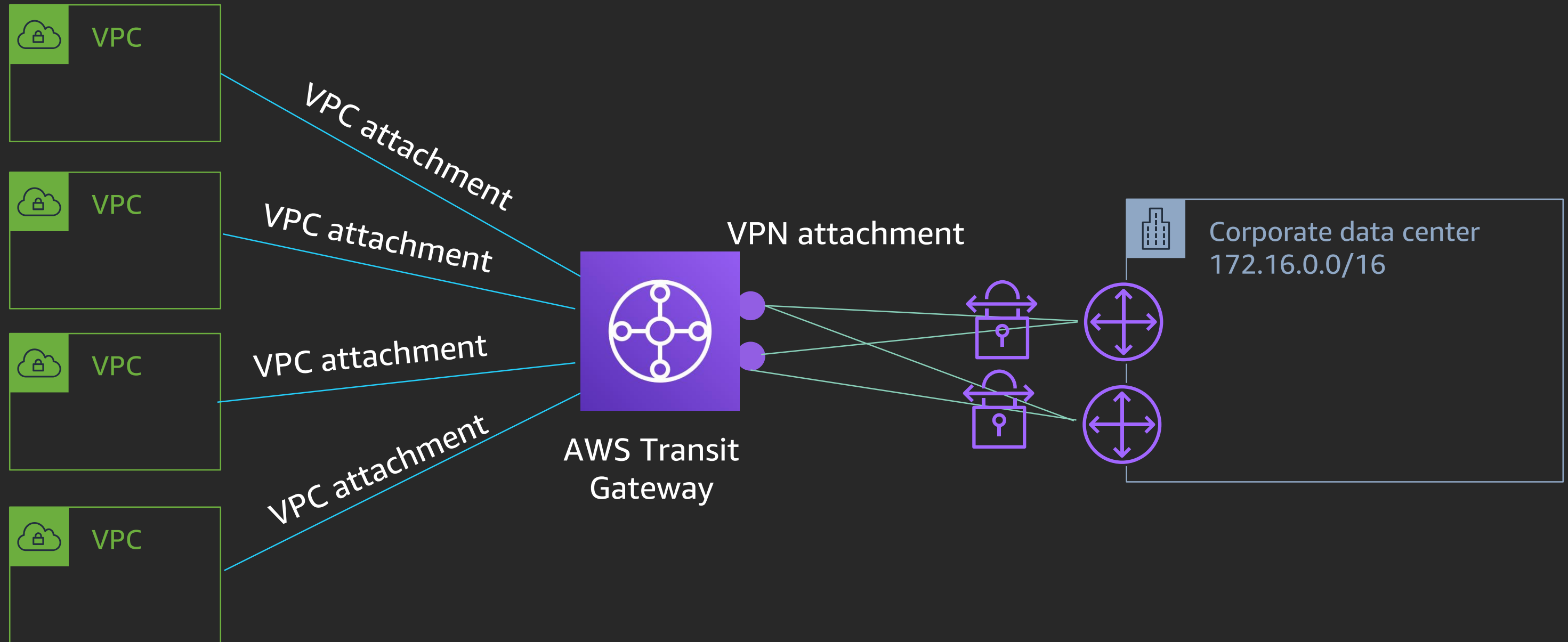
Multiple AWS Site-to-Site VPNs via AWS Transit Gateway



1x VPN connection = 2x VPN tunnels

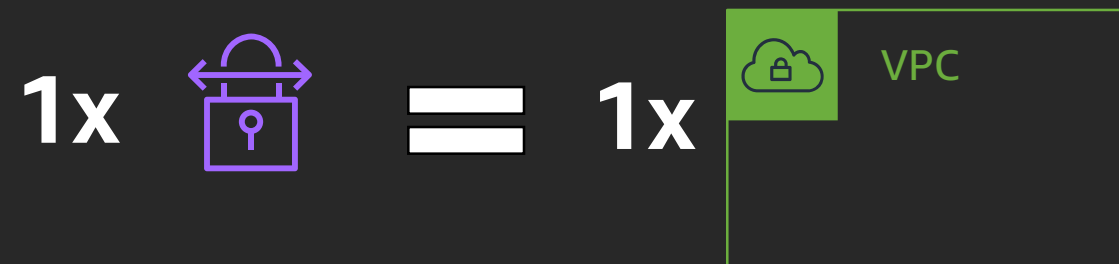
1x VPN tunnel = 1.25Gbps


Multiple AWS Site-to-Site VPNs via AWS Transit Gateway



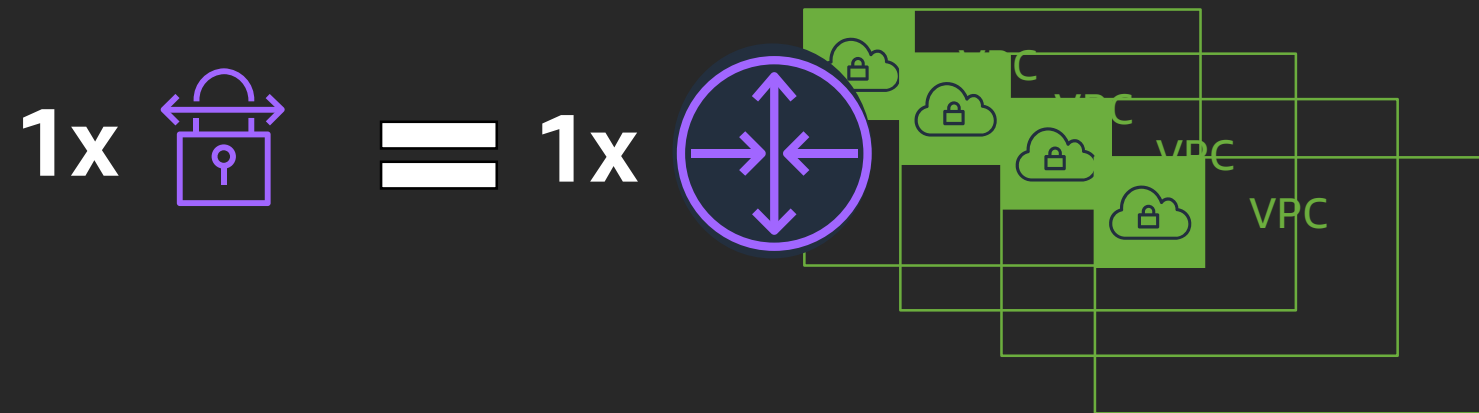
AWS Site-to-Site VPN considerations

VPN to virtual private gateway



1x  = 1.25Gbps

VPN to transit gateway



1x  = 2.5 Gbps (ECMP)

2x  = 5.0 Gbps (ECMP)

3x  = 7.5 Gbps (ECMP)

 - VPN connection (2 tunnels)

+\$\$\$ per GB of TGW processed data

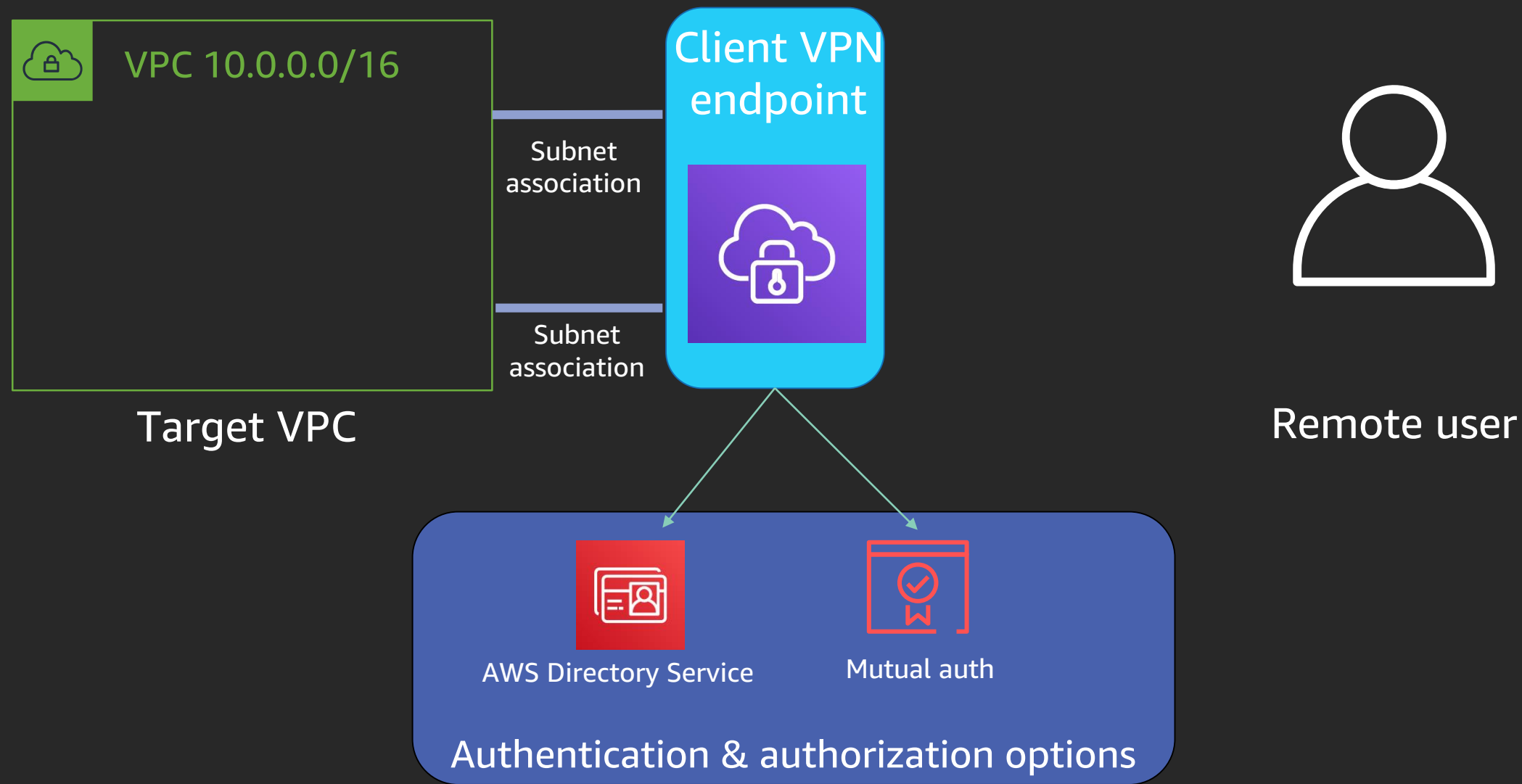
AWS Client VPN

AWS Client VPN

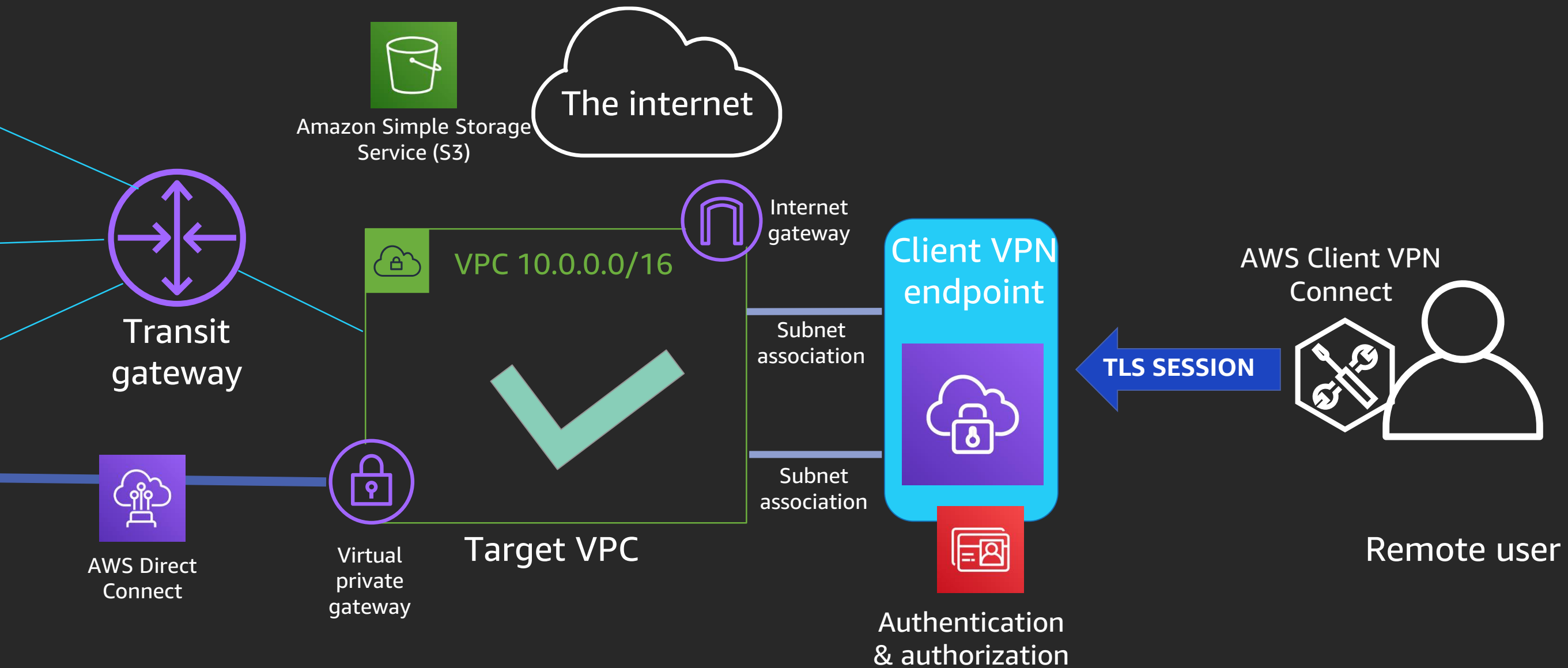


- AWS-managed client-based VPN service that automatically scales to user demand
- Provide secure & granular access to any resource in AWS and on-premises from anywhere using OpenVPN clients
- Seamlessly integrate with existing infrastructure, like Amazon Virtual Private Cloud (VPC), Active Directory

Deploying AWS Client VPN



Connecting to AWS Client VPN

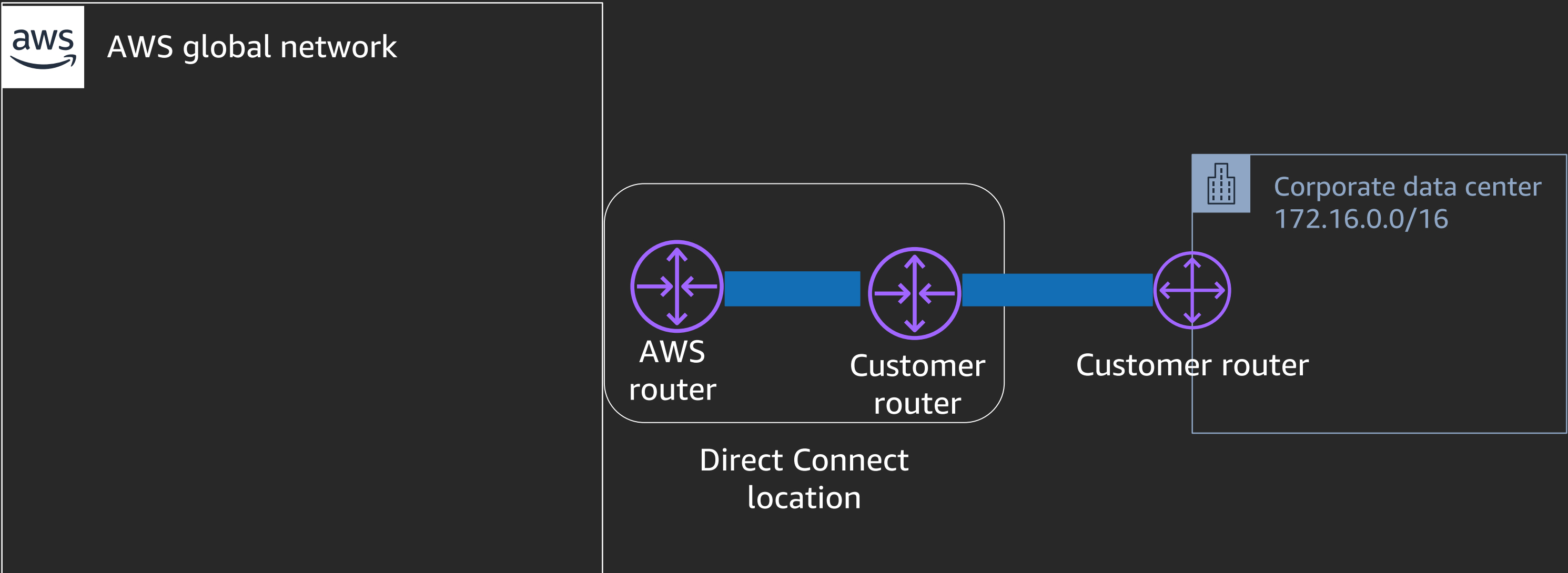


AWS Direct Connect

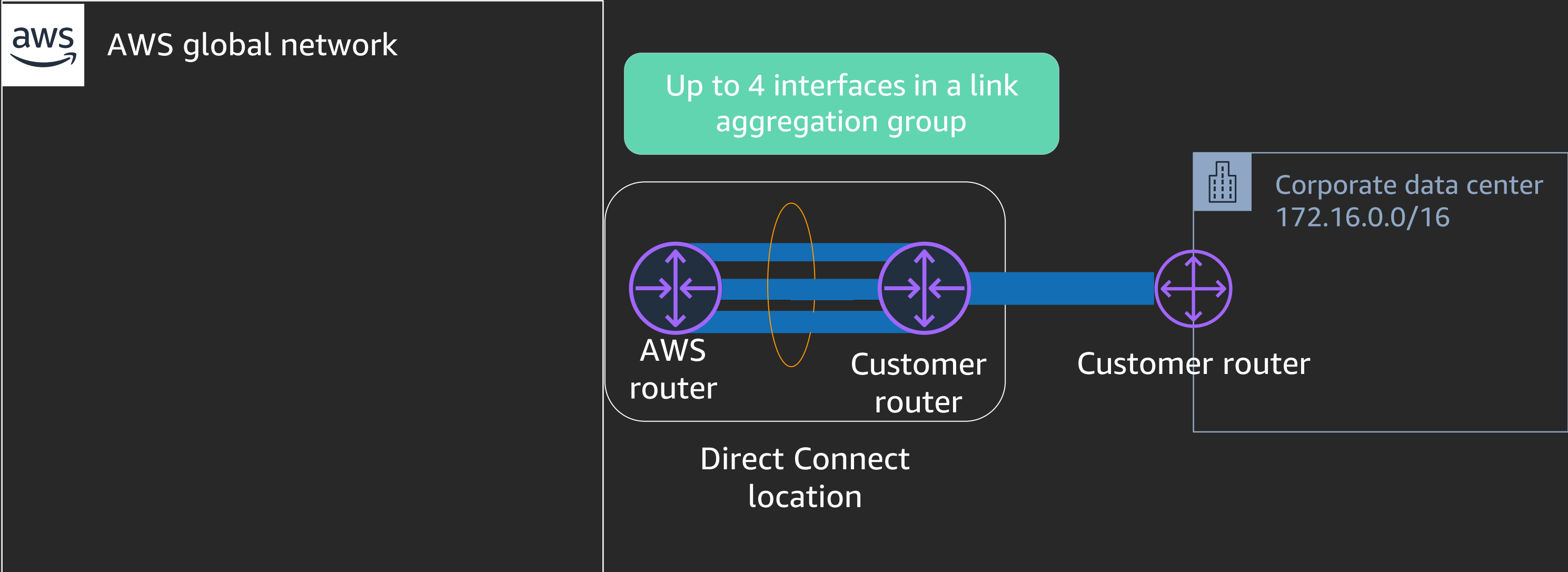
AWS Direct Connect

Dedicated network connection to AWS
providing **consistent** performance and **reduced**
bandwidth costs

AWS Direct Connect – Physical connection



AWS Direct Connect – Link Aggregation



Direct Connect new features – Resiliency toolkit

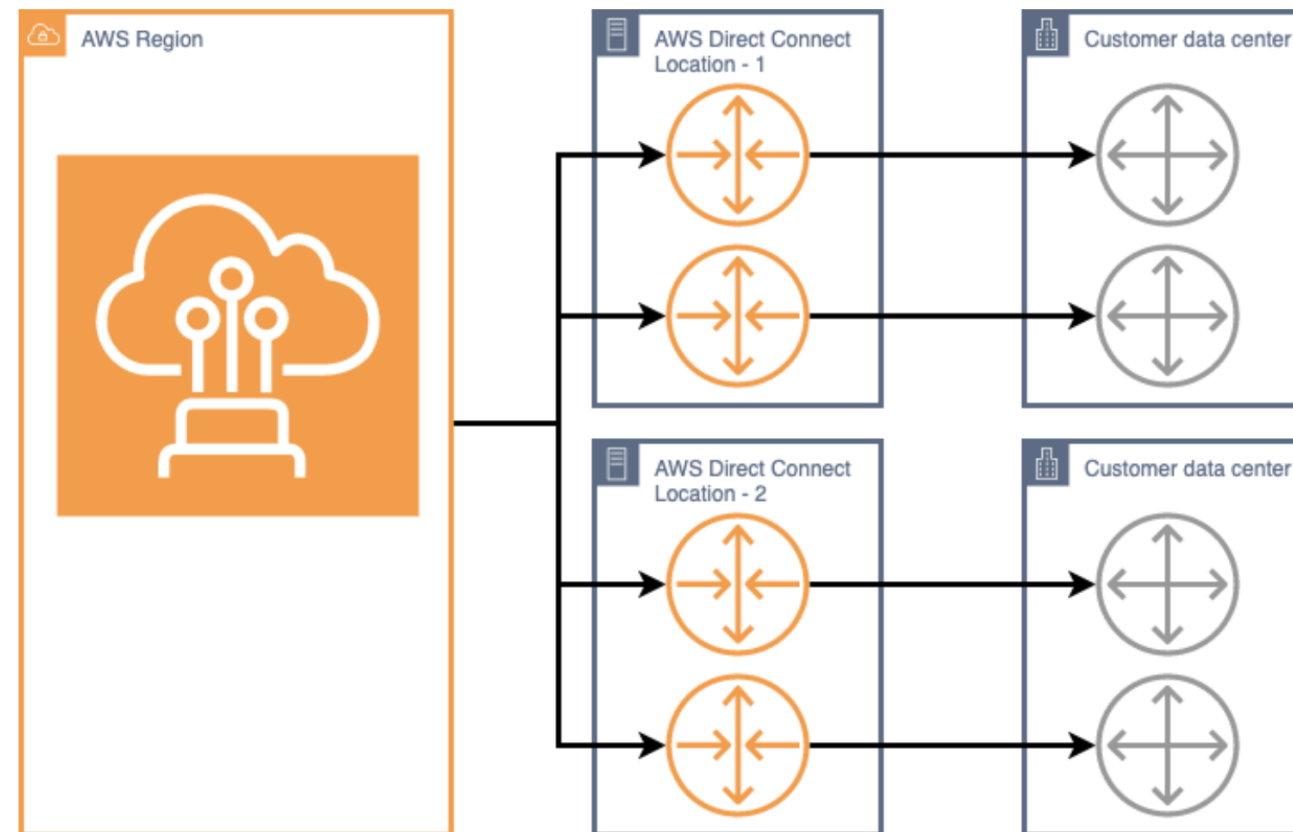
Maximum Resiliency
Maximum Resiliency for Critical Workloads

High Resiliency
High Resiliency for Critical Workloads

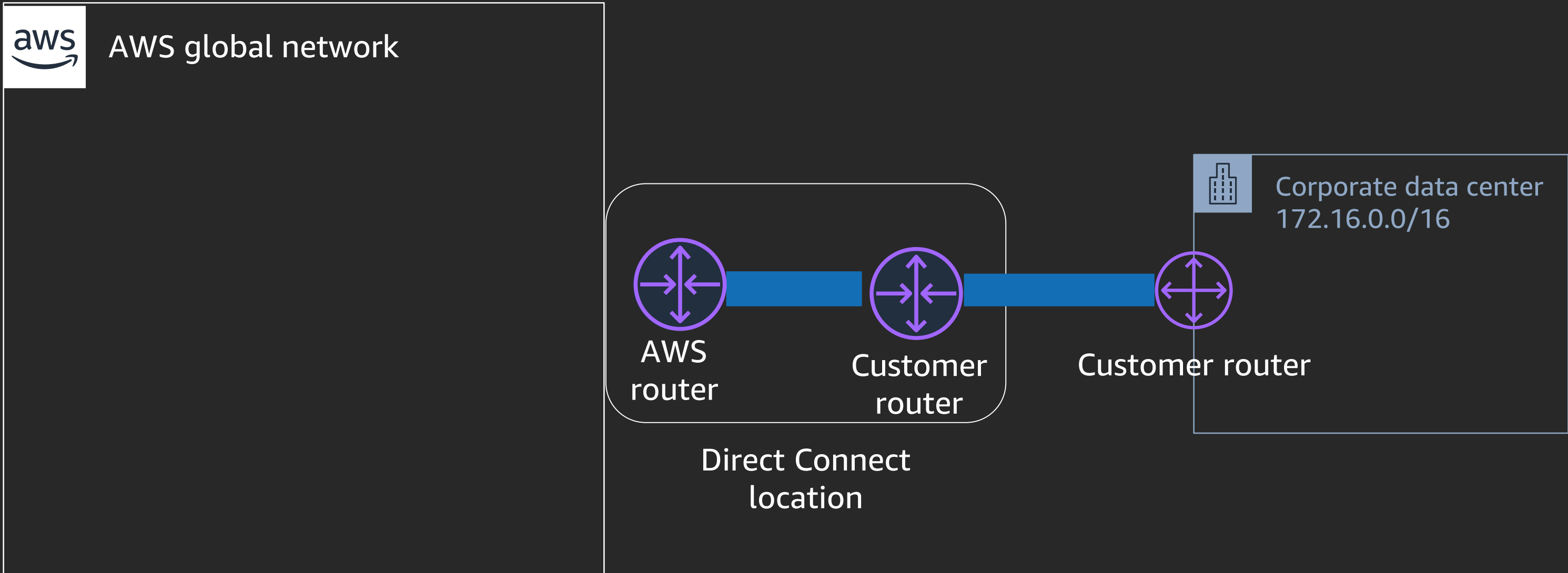
Development and Test
Non Critical Workloads or Development Workloads

Maximum Resiliency

You can achieve maximum resiliency for critical workloads by using separate connections that terminate on separate devices in more than one location (as shown in the figure). This topology provides resiliency against device, connectivity, and complete location failures.



AWS Direct Connect – Physical connection

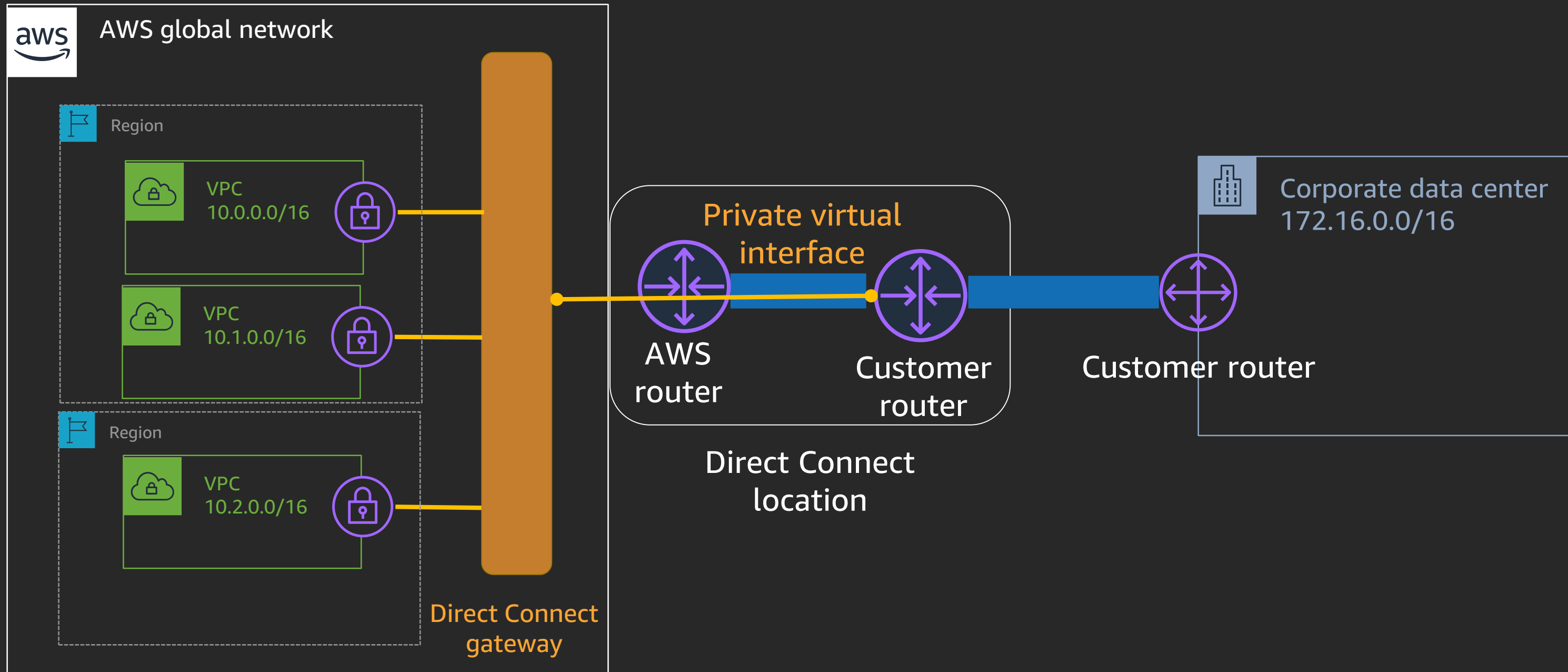


AWS Direct Connect – Interface types

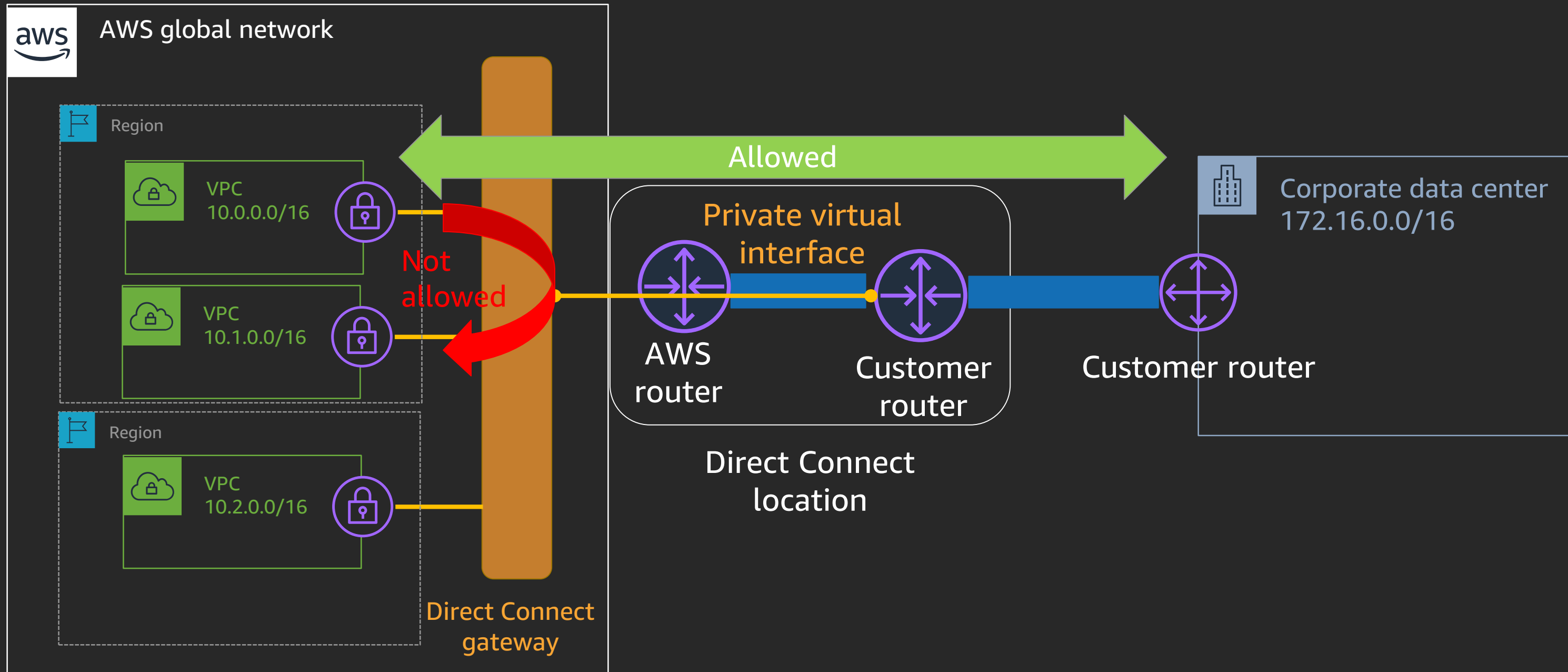
- **Private VIF** – Used to connect to Amazon VPCs using private IP addresses; directly or via Direct Connect gateway
- **Transit VIF** – Used to connect to transit gateways via Direct Connect gateway
- **Public VIF** – Used to access all AWS public services using public IP addresses

All virtual interfaces are 802.1Q VLANs with BGP peering

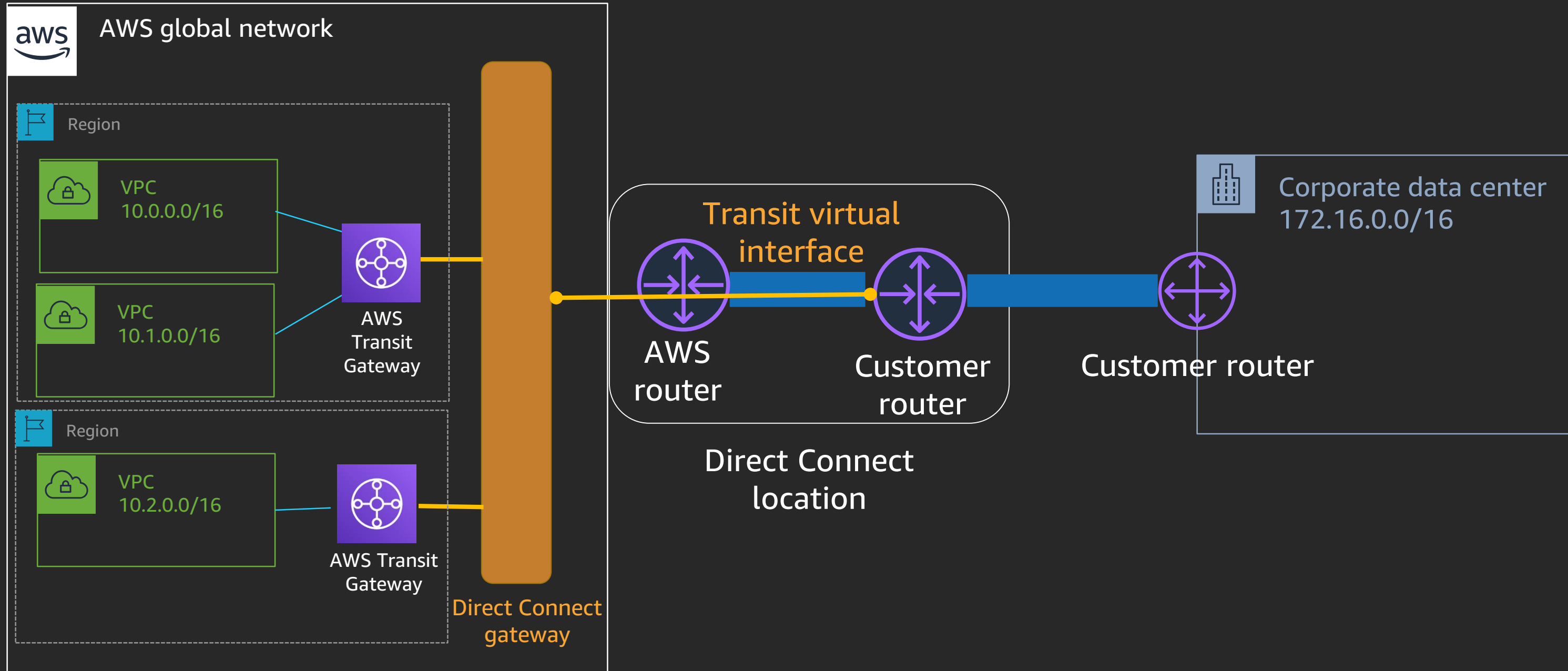
AWS Direct Connect Gateway – Private VIF



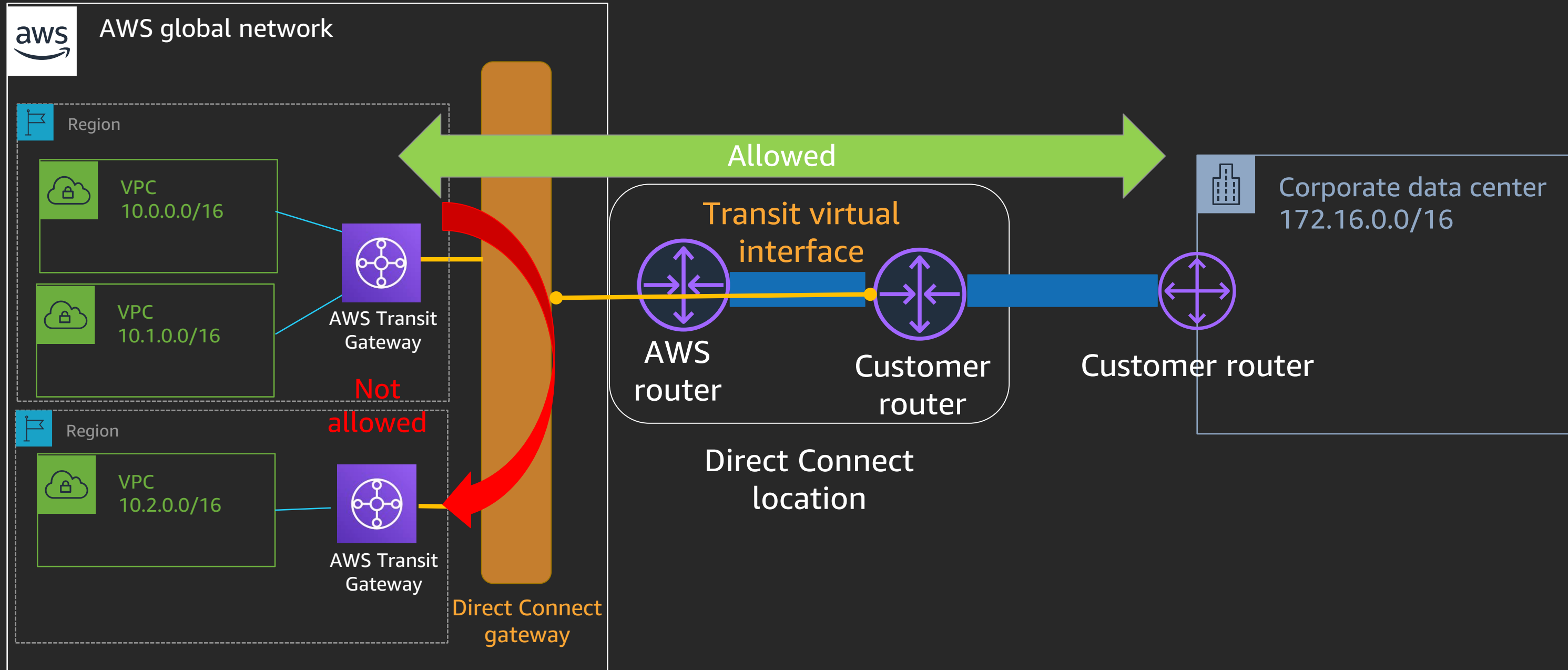
AWS Direct Connect Gateway – Traffic Flow



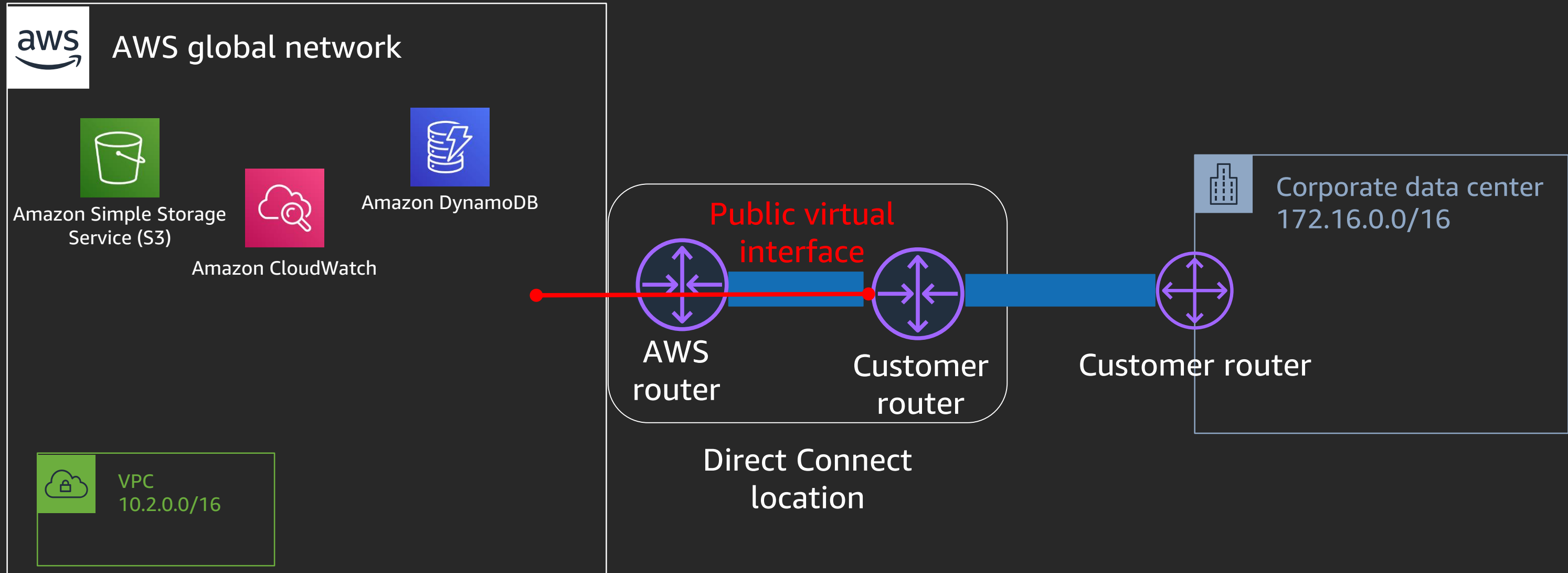
AWS Direct Connect Gateway – Transit VIF



AWS Direct Connect Gateway – Traffic Flow

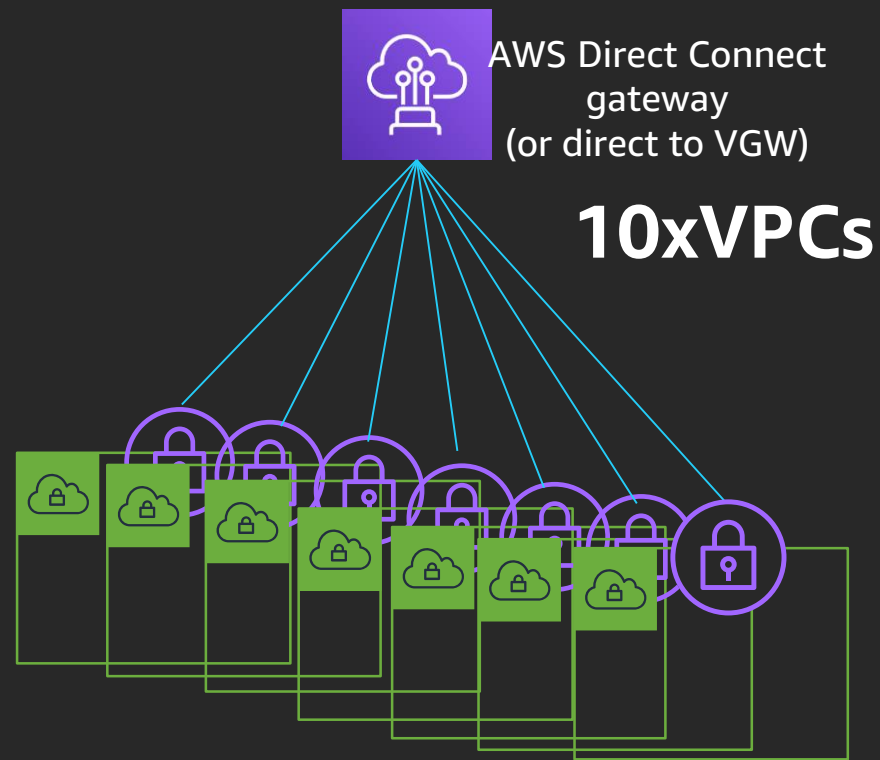


AWS Direct Connect – Public VIF

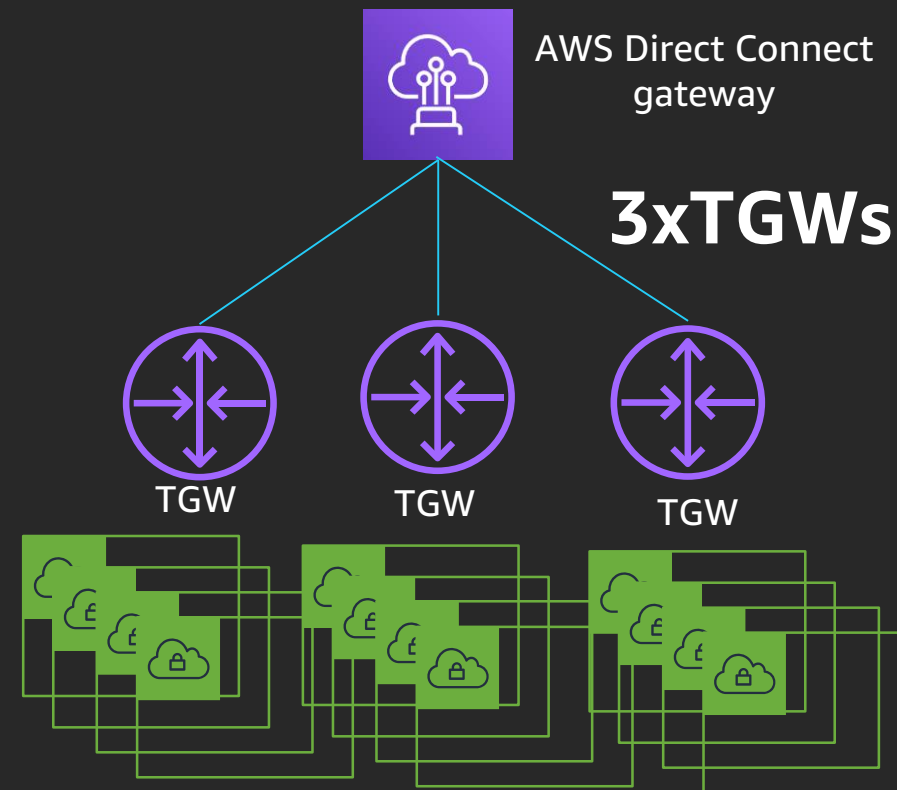


AWS Direct Connect – Interface types

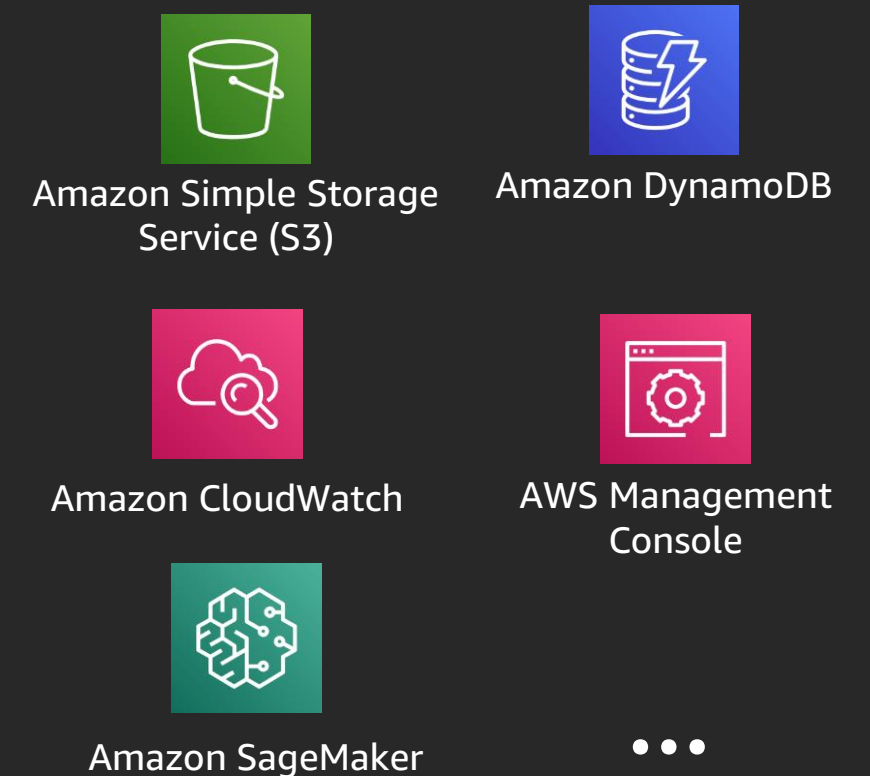
Private VIF



Transit VIF



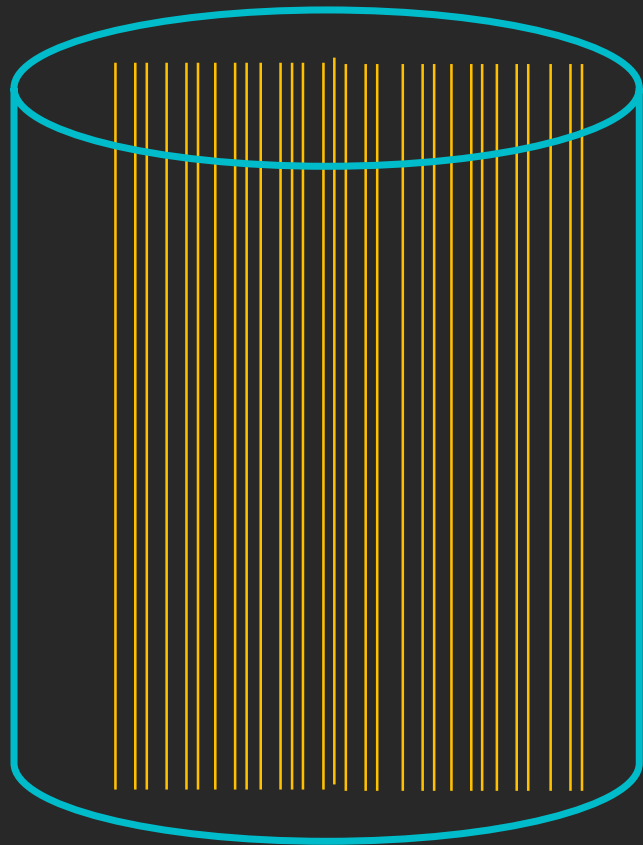
Public VIF



Direct Connect gateway allows for connecting to resources in any AWS region (except for China)

Direct Connect connection types

1 Gbps or 10 Gbps

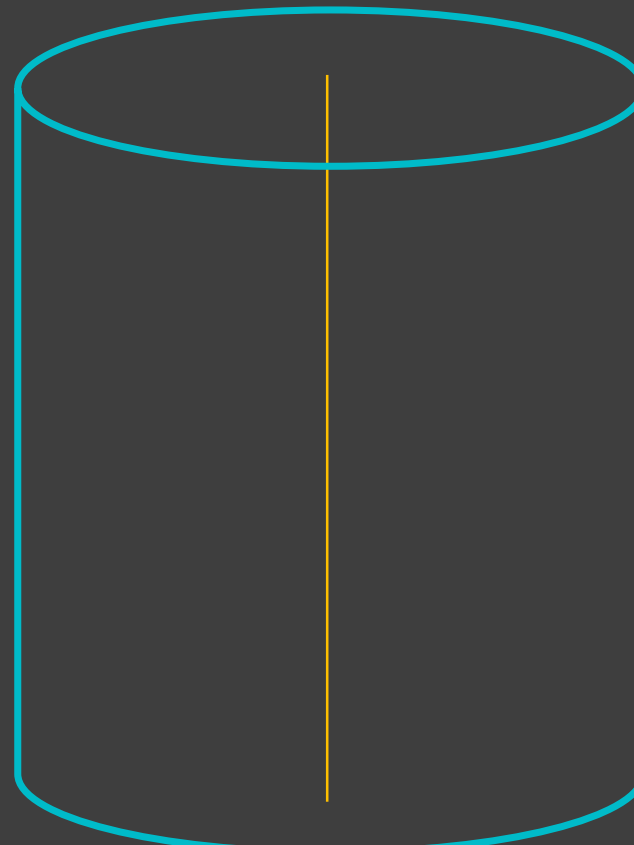


50 VIFs

AND 1 transit VIF

Dedicated connection

50 Mbps -> 10 Gbps



1 VIF **OR**

1 transit VIF (1 Gbps + only)

Hosted connection

50 Mbps -> 10 Gbps
(can be oversubscribed)

1 VIF

No transit VIF

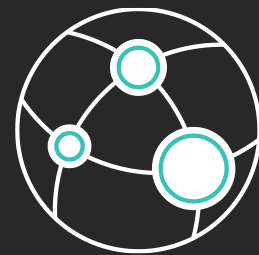
(Partner) Hosted virtual interface

ONLY FROM PARTNERS

Now it's your turn ... Questions?

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate networking skills



Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and Introduction to Amazon VPC



Validate expertise with the **AWS Certified Advanced Networking - Specialty** exam

Visit aws.amazon.com/training/paths-specialty

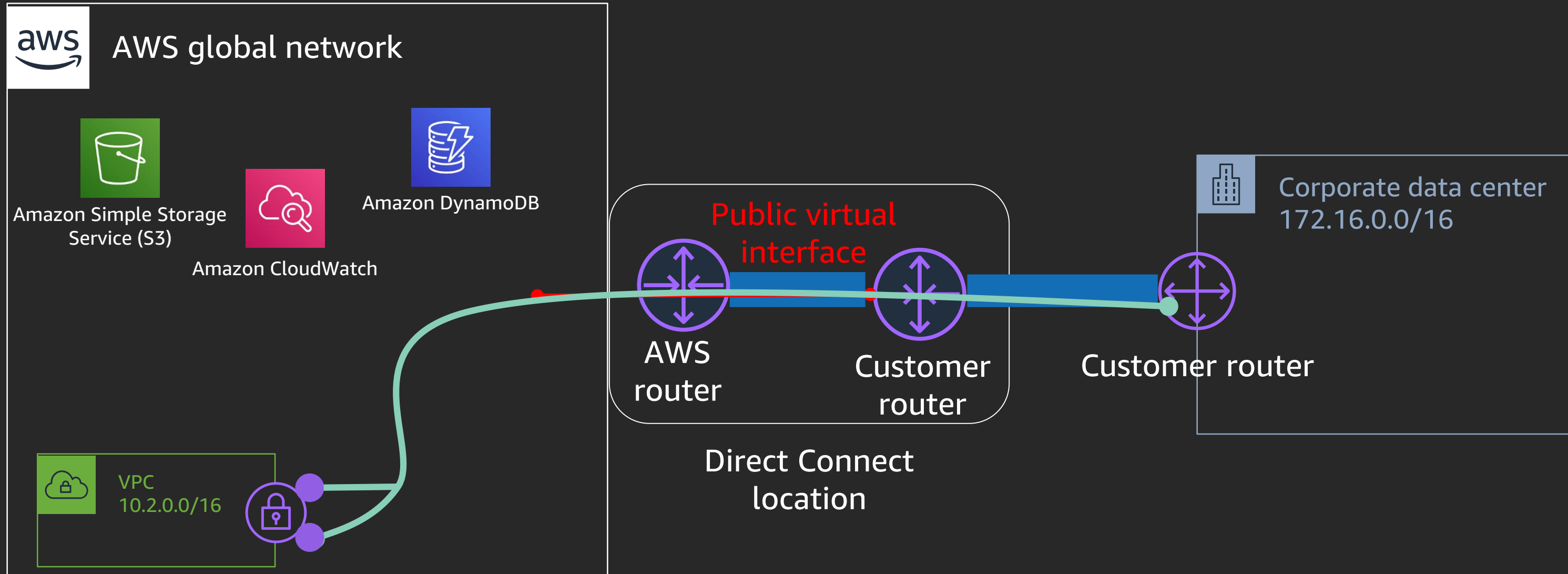
Thank you!



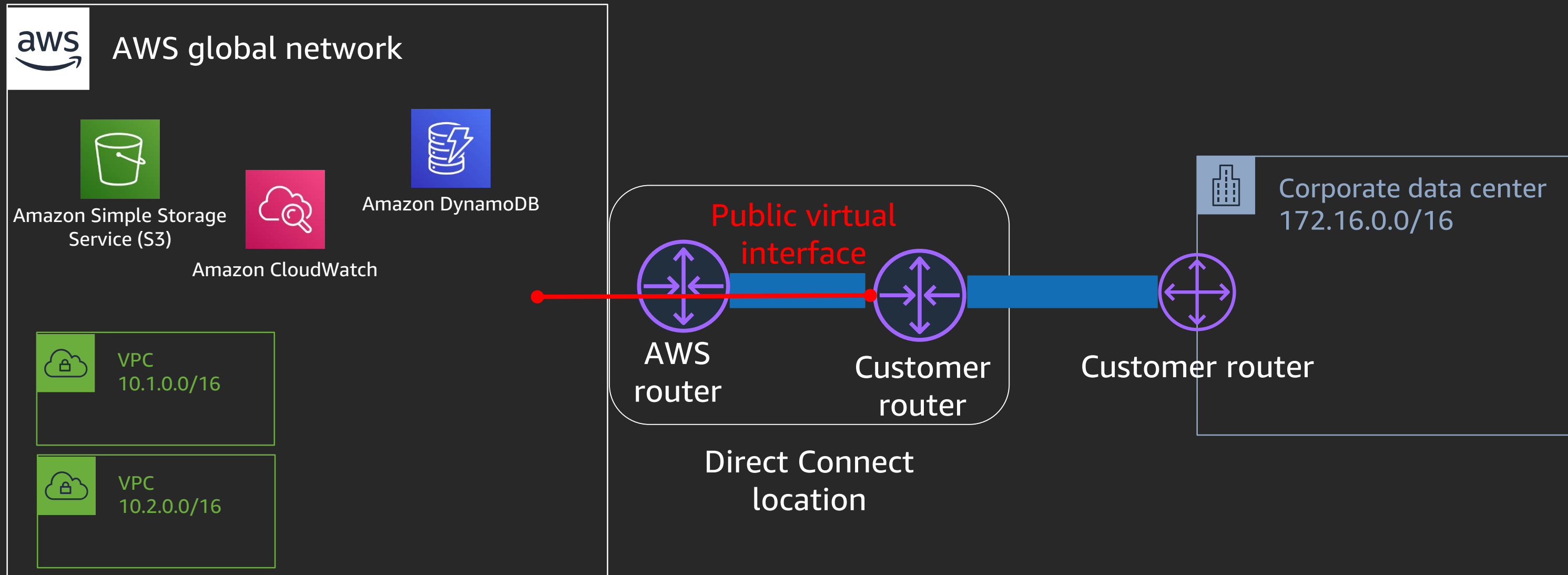
Please complete the session survey in the mobile app.

Appendix

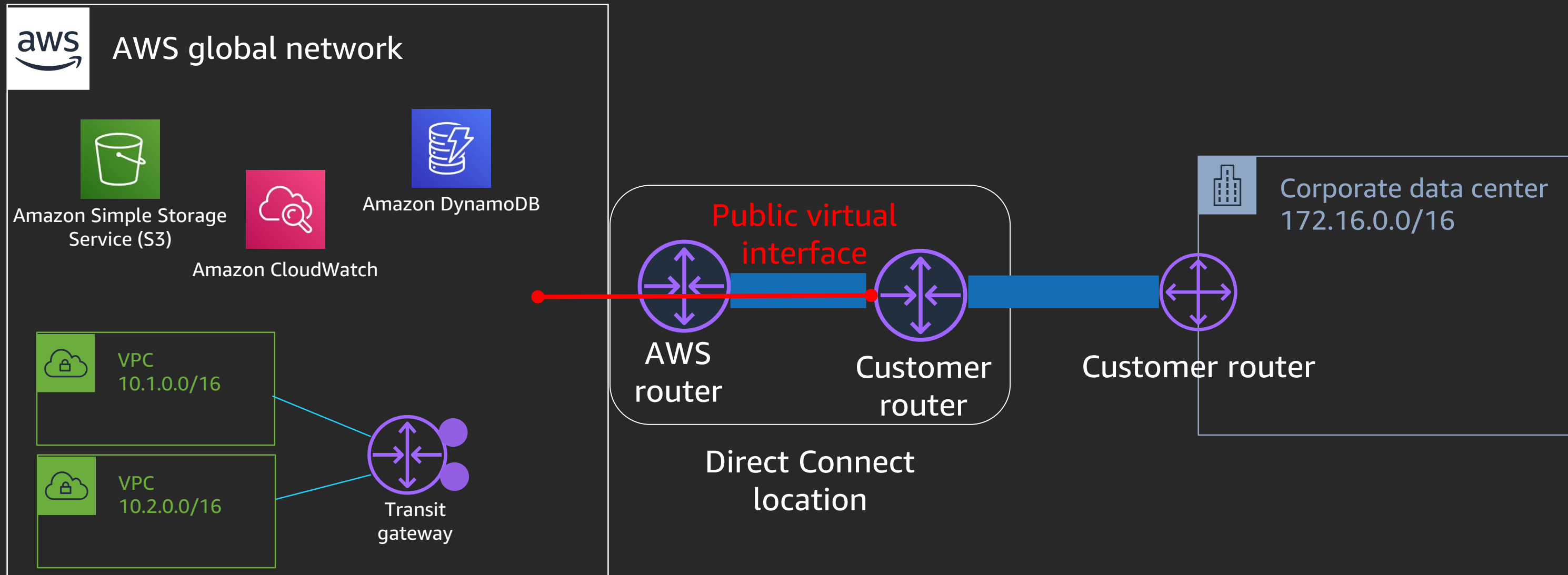
AWS Direct Connect – Public VIF + AWS VPN



AWS Direct Connect – Public VIF + AWS VPN



AWS Direct Connect – Public VIF + AWS VPN



AWS Direct Connect – Public VIF + AWS VPN

