AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

NET306

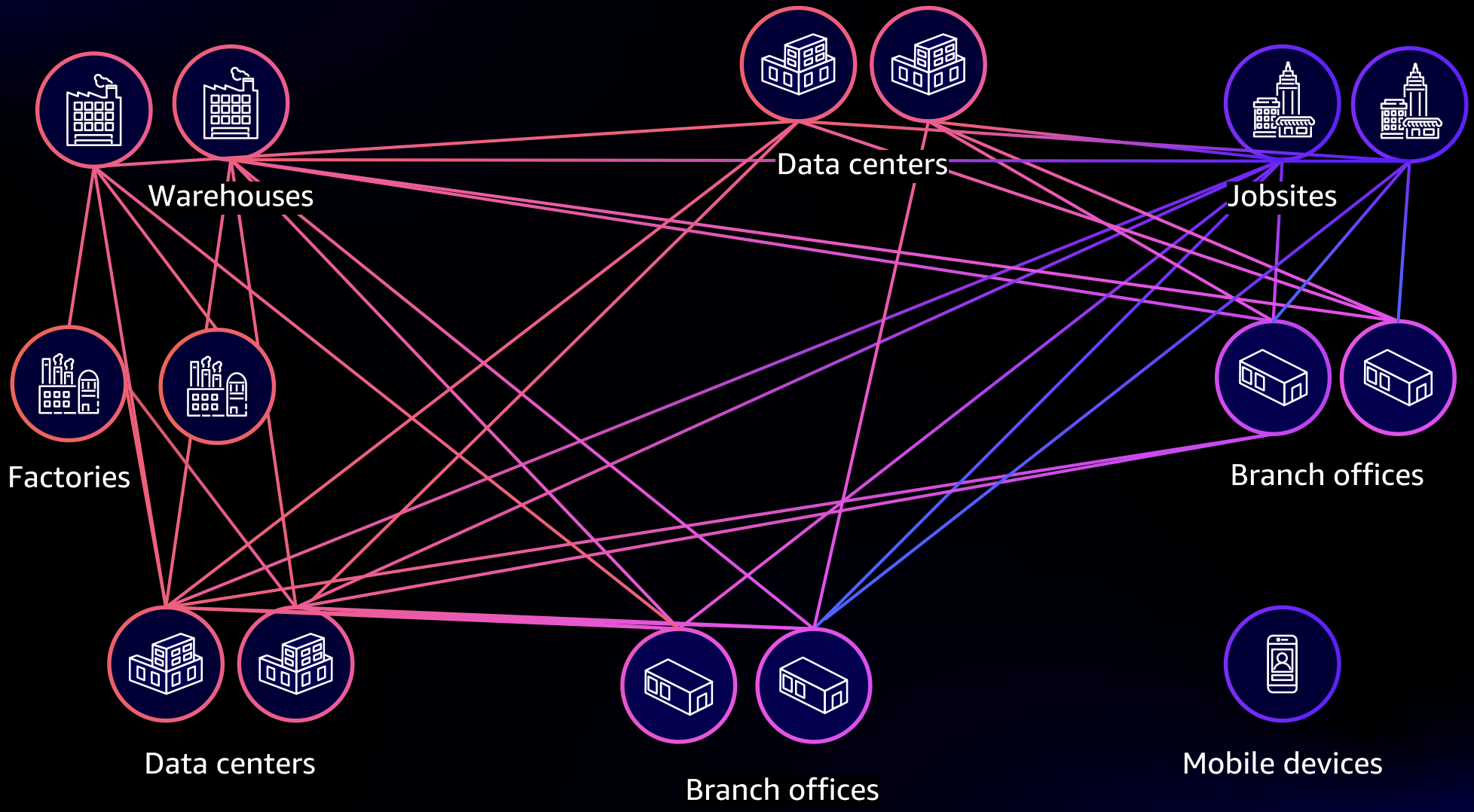
AWS Well-Architected Framework for hybrid networks

Aarthi Raju
Sr. Manager, Solutions Architecture
AWS

Rohit Aswani
Senior Specialist Solutions Architect – Networking
AWS

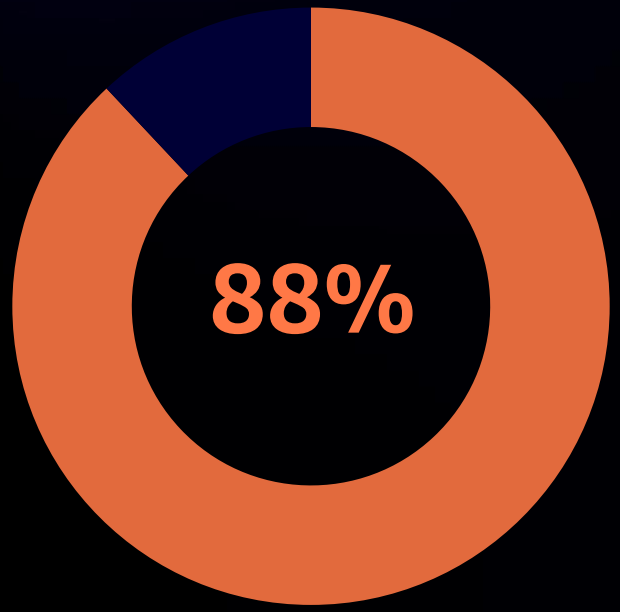
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional enterprise networks are complex

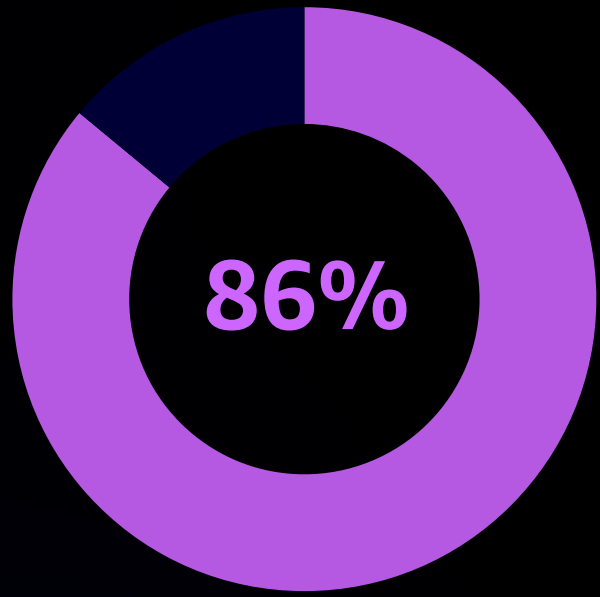


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

It’s still a hybrid world



Enterprises that have a cloud-first strategy



Infrastructure spend still on premises

Source: Gartner Market Trends: Cloud Shift — 2020 Through 2024

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS networking vision

FROM THE EDGE TO THE DATA CENTER



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Today’s storyboard

Key **architectural considerations** and design principles

Lessons learned and **best practices**

Choosing the **right service** for your hybrid networks

Technical resources and follow-up **documentation**

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pillars of the Well-Architected Framework



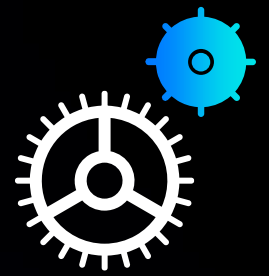
Reliability



Security



Performance efficiency



Operational excellence



Cost optimization

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reliability



Reliability

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Building reliable networks

- Distributed network architectures and potential issues
- Availability
- Resiliency and recovery planning



AWS Transit Gateway



AWS Direct Connect



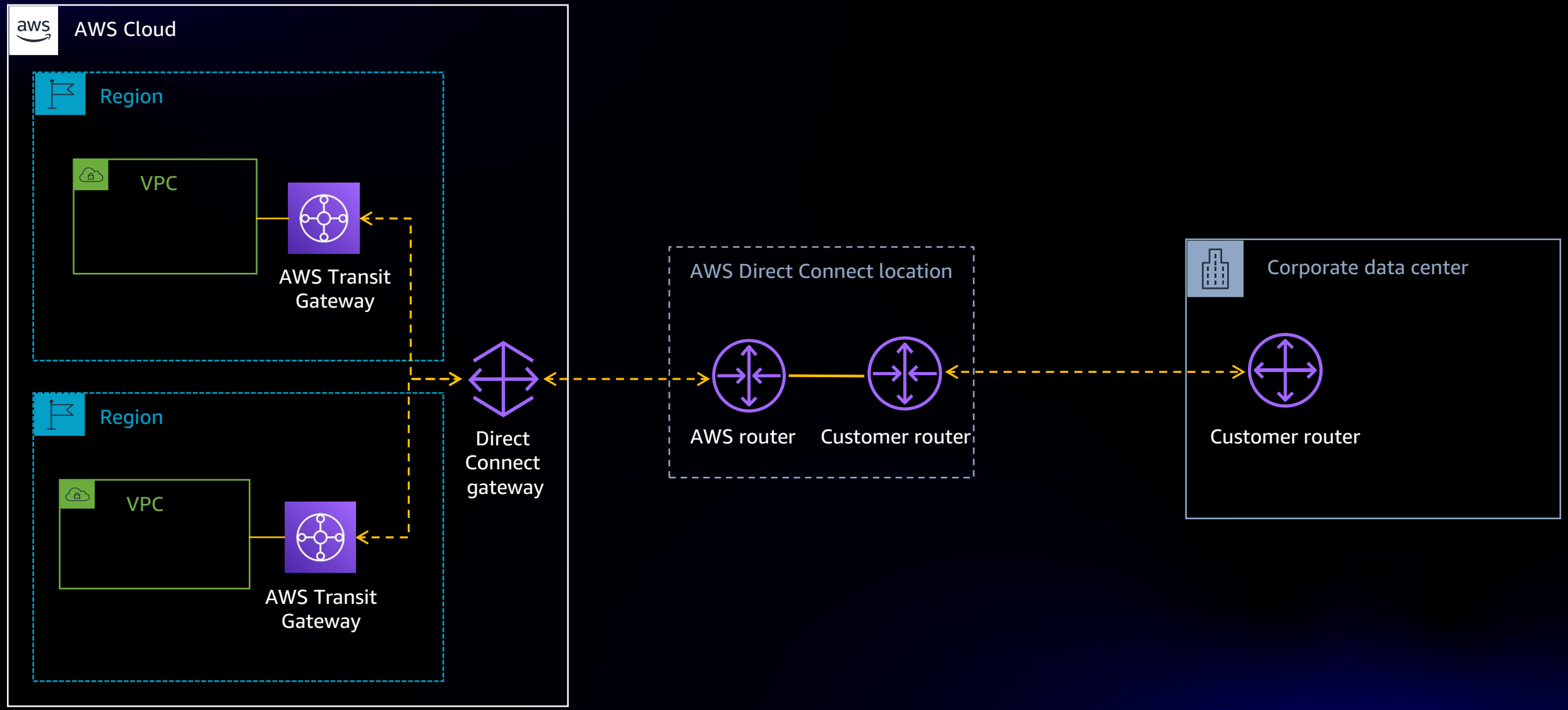
AWS Site-to-Site VPN



AWS Client VPN

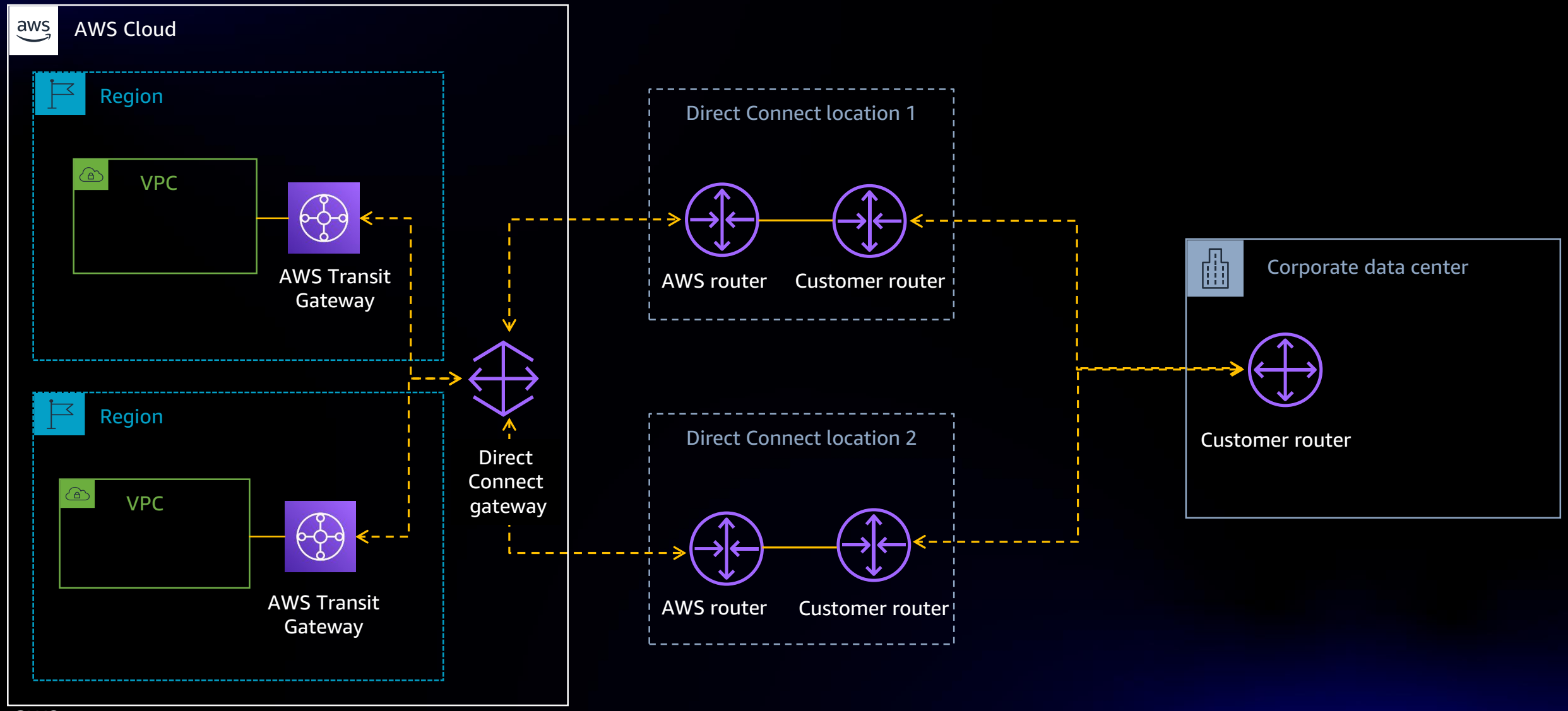
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Connectivity using AWS Direct Connect



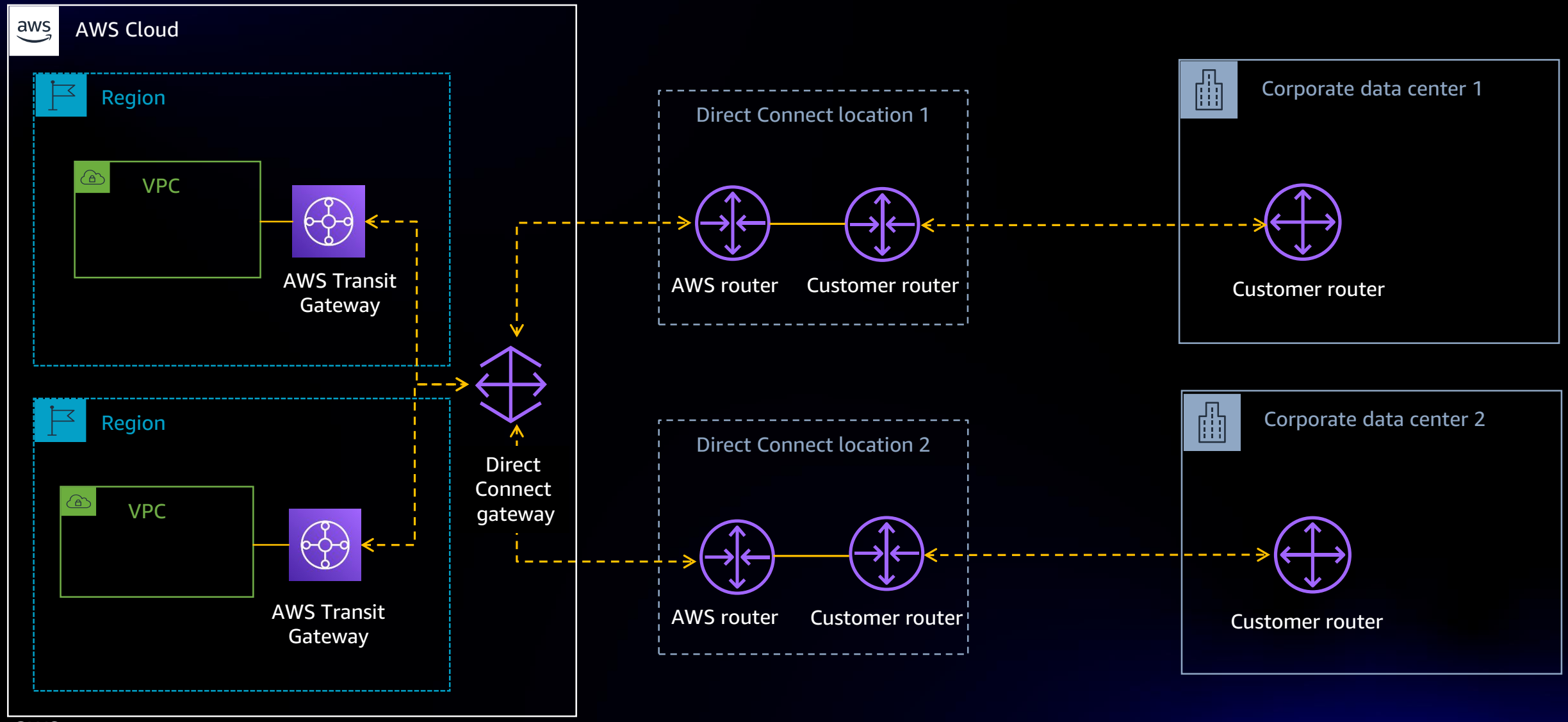
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Building high resiliency for Direct Connect



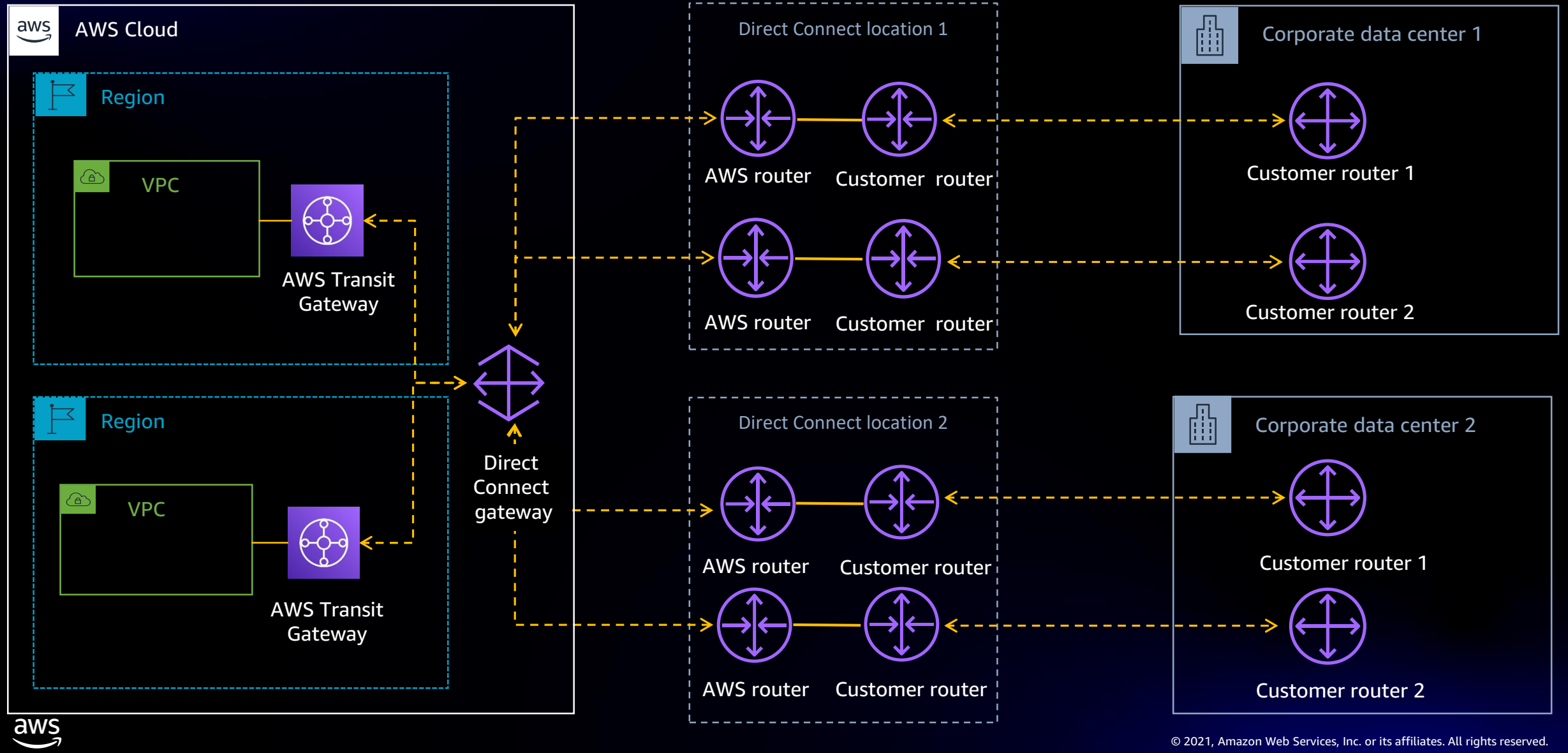
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect – High resiliency



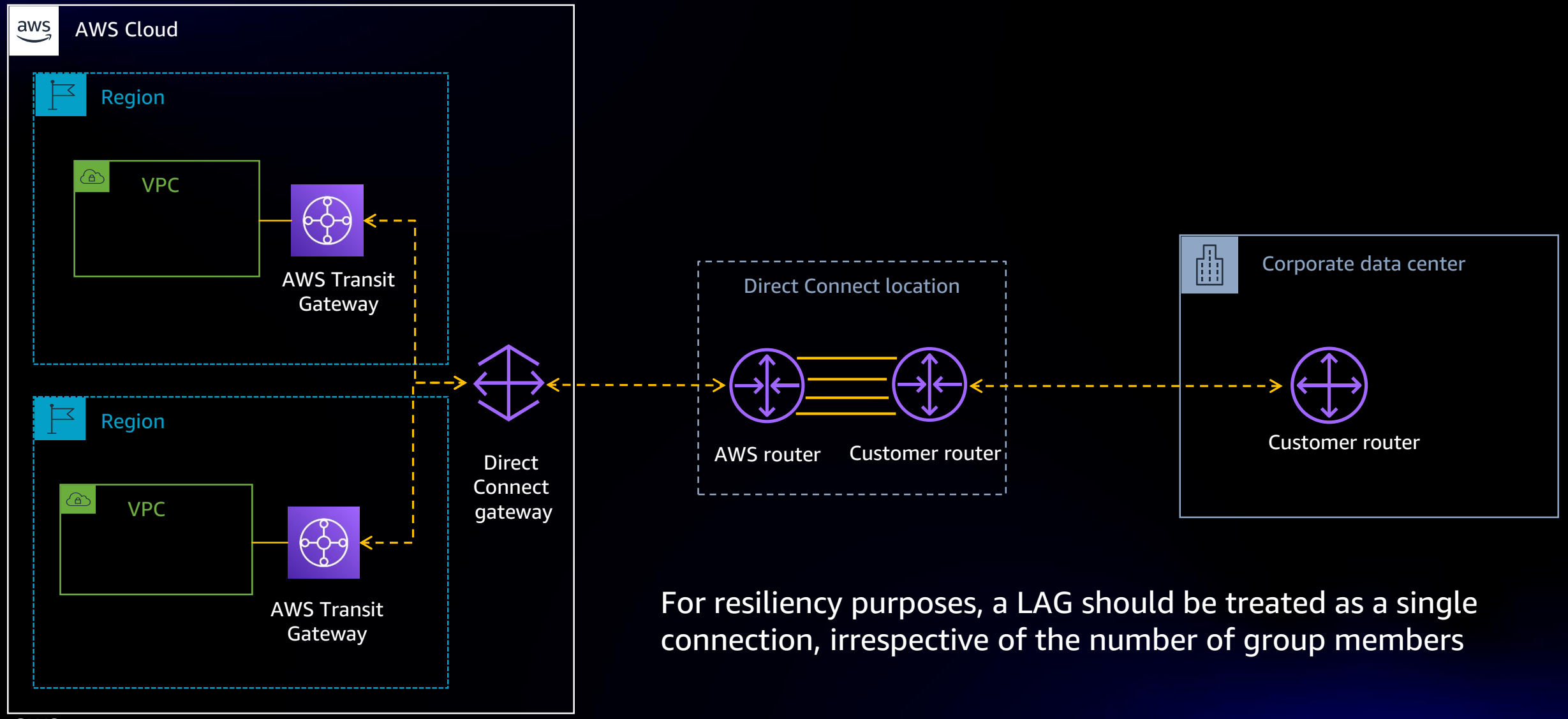
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect – Maximum resiliency



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Link Aggregation Group (LAG)



For resiliency purposes, a LAG should be treated as a single connection, irrespective of the number of group members

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect availability

- May be eligible for service-level agreement (SLA)
  - 99.9% for 2 Direct Connect locations with a total of 2 connections
  - 99.99% for 2 Direct Connect locations with a total of 4 connections

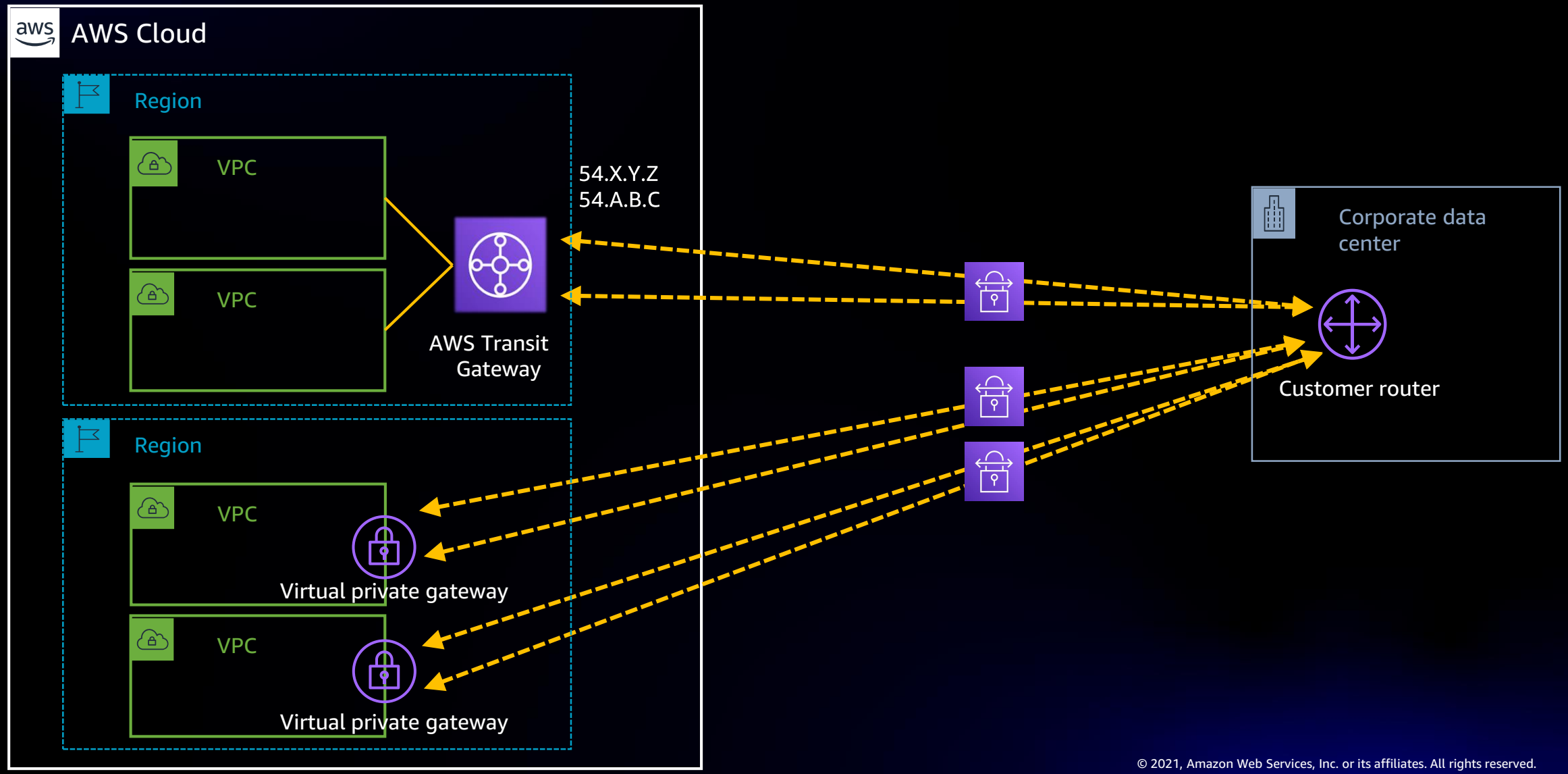


- Single AWS Direct Connect connections have maintenance
  - Look at a second Direct Connect connection or VPN for backup
  - Use Resiliency Toolkit and perform failover testing



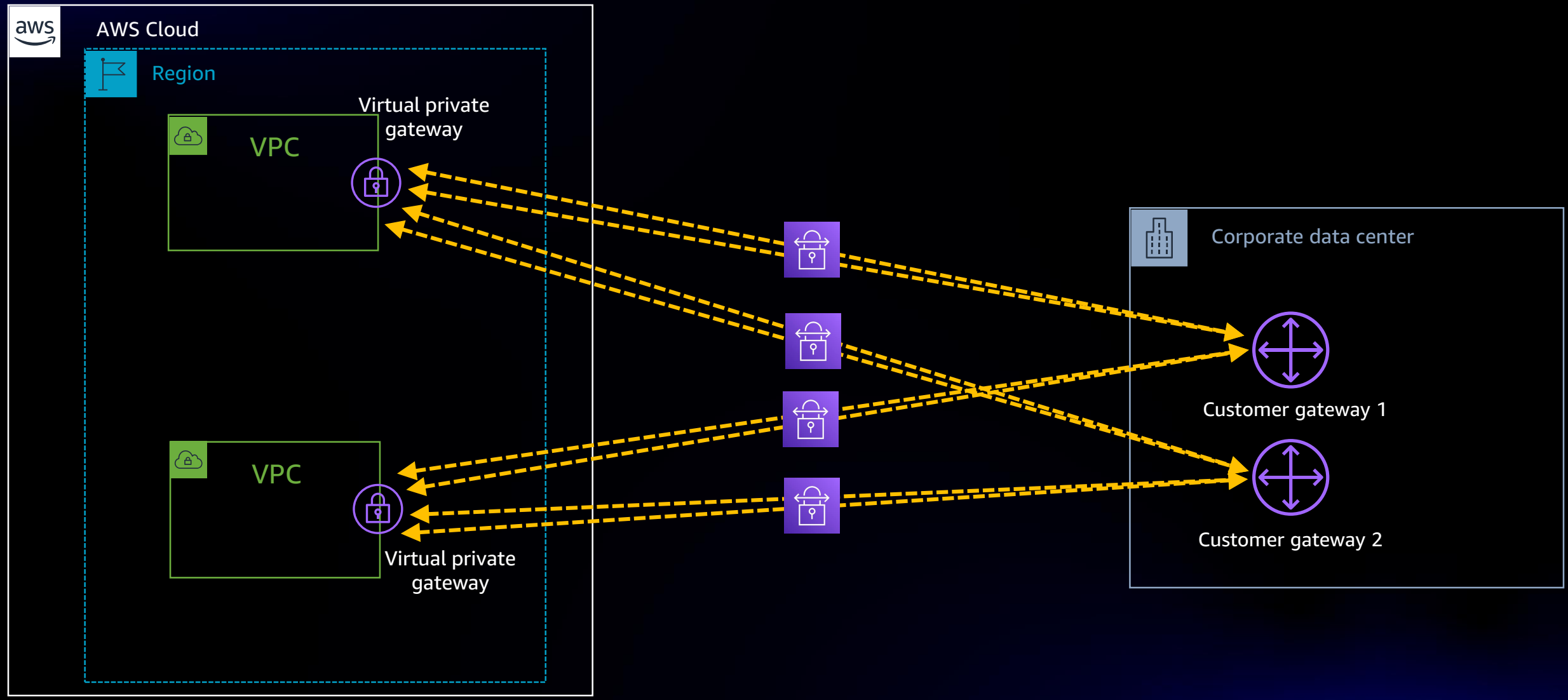
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Connectivity using AWS Site-to-Site VPN



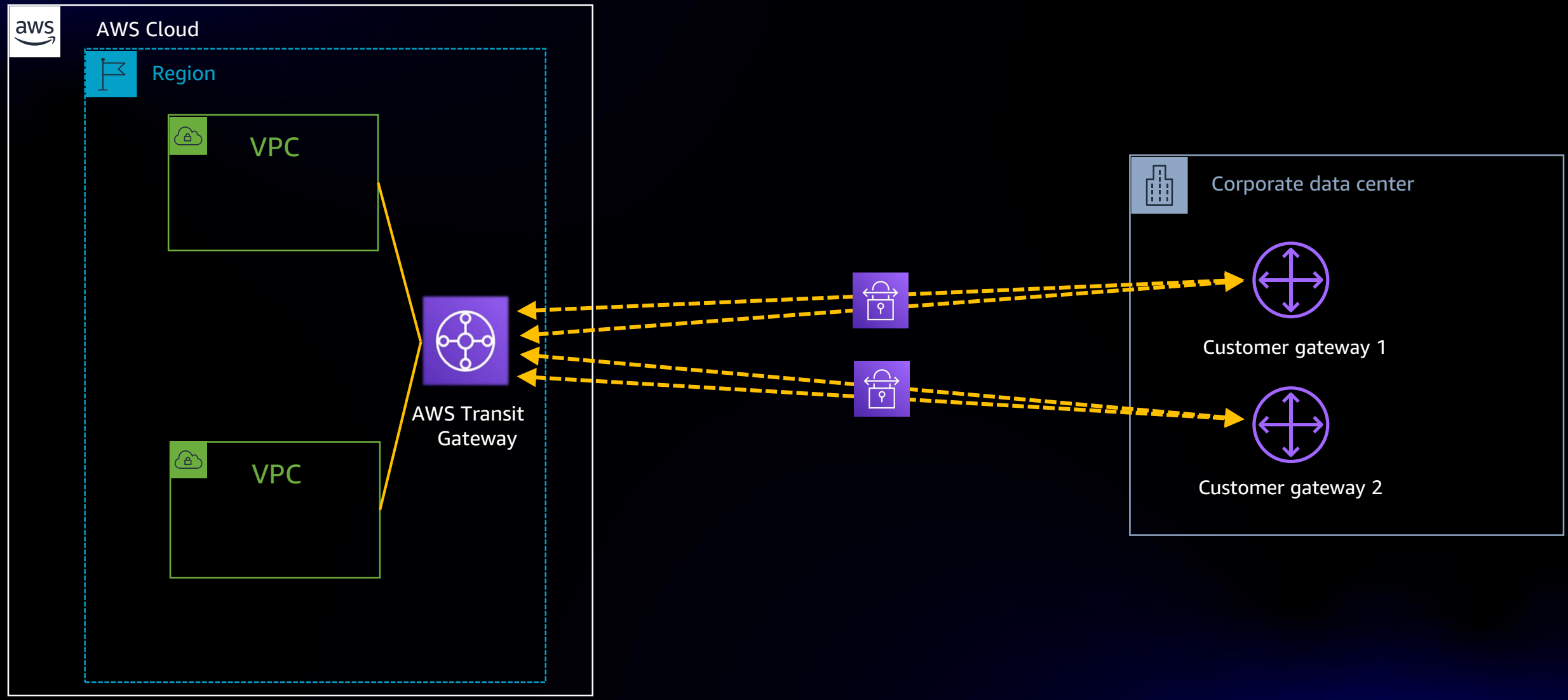
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Site-to-Site VPN – Virtual private gateway



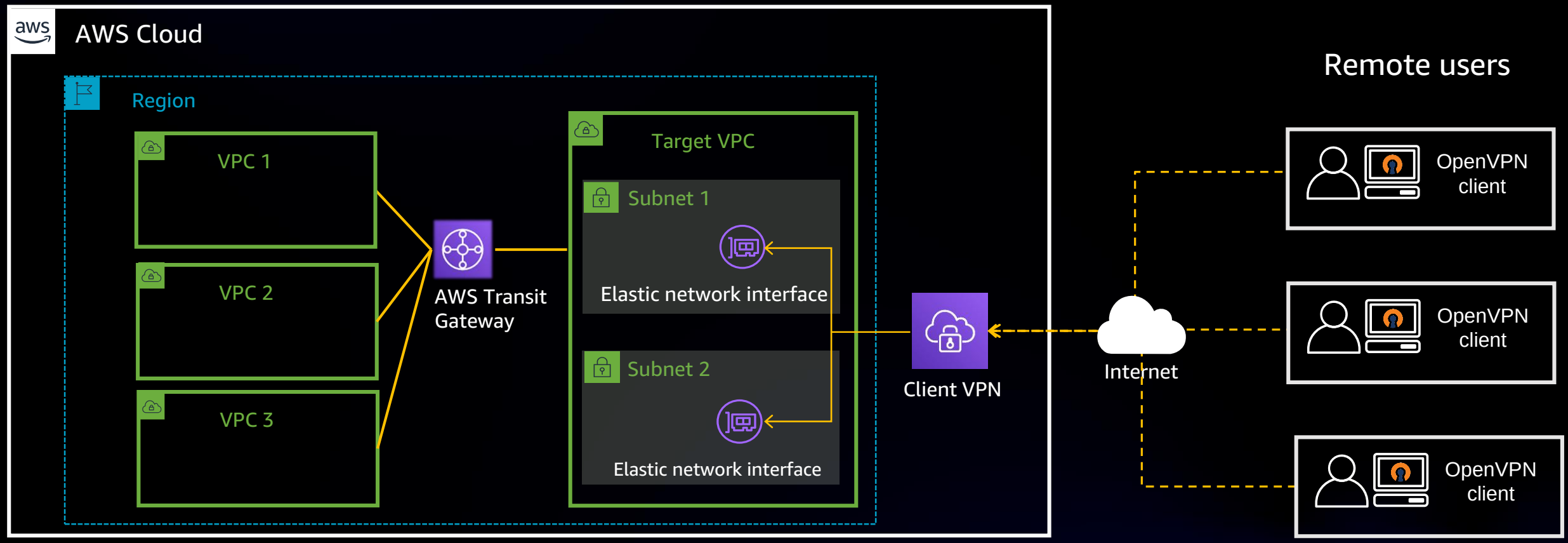
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Site-to-Site VPN – Transit Gateway



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Connectivity using AWS Client VPN



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices for connectivity within VPC

- Use multiple Availability Zones to deploy your workloads within VPC
- Use multiple subnets (1 per AZ) for AWS Transit Gateway VPC attachments and for the target VPC for Client VPN endpoint
- Use a separate subnet for Transit Gateway VPC attachment, different from your workload subnets
- Be aware of your VPC service quotas

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Service quotas that may affect your availability

Direct Connect

- 50 private or public and **1 transit virtual interface** per Direct Connect dedicated connection
- 10 virtual private gateways per Direct Connect gateway
- **100** routes per BGP session on a private or transit virtual interface
- **20** prefixes (**IPv4 + IPv6**) per Transit Gateway from AWS to on-premises on a transit virtual interface

Transit Gateway

- 5,000 attachments per transit gateway
- **3** transit gateways per AWS Direct Connect gateway

Site-to-Site VPN

- 1,000 routes advertised from a virtual private gateway to a customer gateway device
- **1,000** dynamic routes (**an increase from 100**) from a customer gateway device to a Transit Gateway
- **5,000** routes (**an increase from 1,000**) from Transit Gateway to a customer gateway device

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

References



“Hybrid Connectivity” whitepaper



AWS Direct Connect resiliency recommendations



AWS Direct Connect service quotas

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

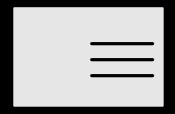
Security



Security

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS security solutions



Identity and access management



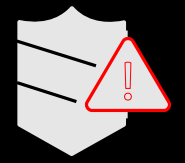
Detective controls



Infrastructure protection



Data protection



Incident response

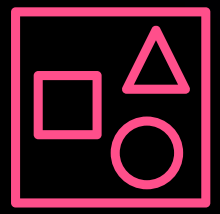
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices – Identity and access management



AWS Identity and Access Management (IAM)

Implement the principle of least privilege



Account

Create a separate networking account to host hybrid networking resources

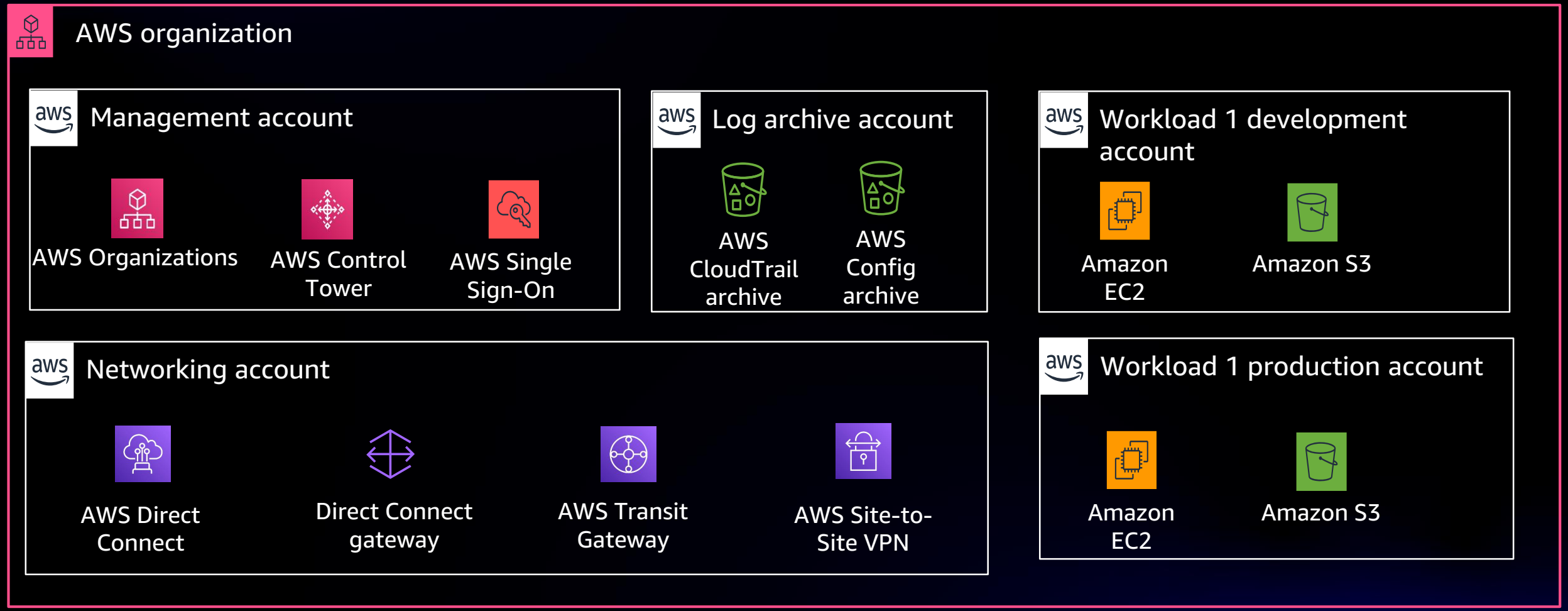


AWS Control Tower

Implement AWS Control Tower for deploying your AWS environment

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices – Account segmentation



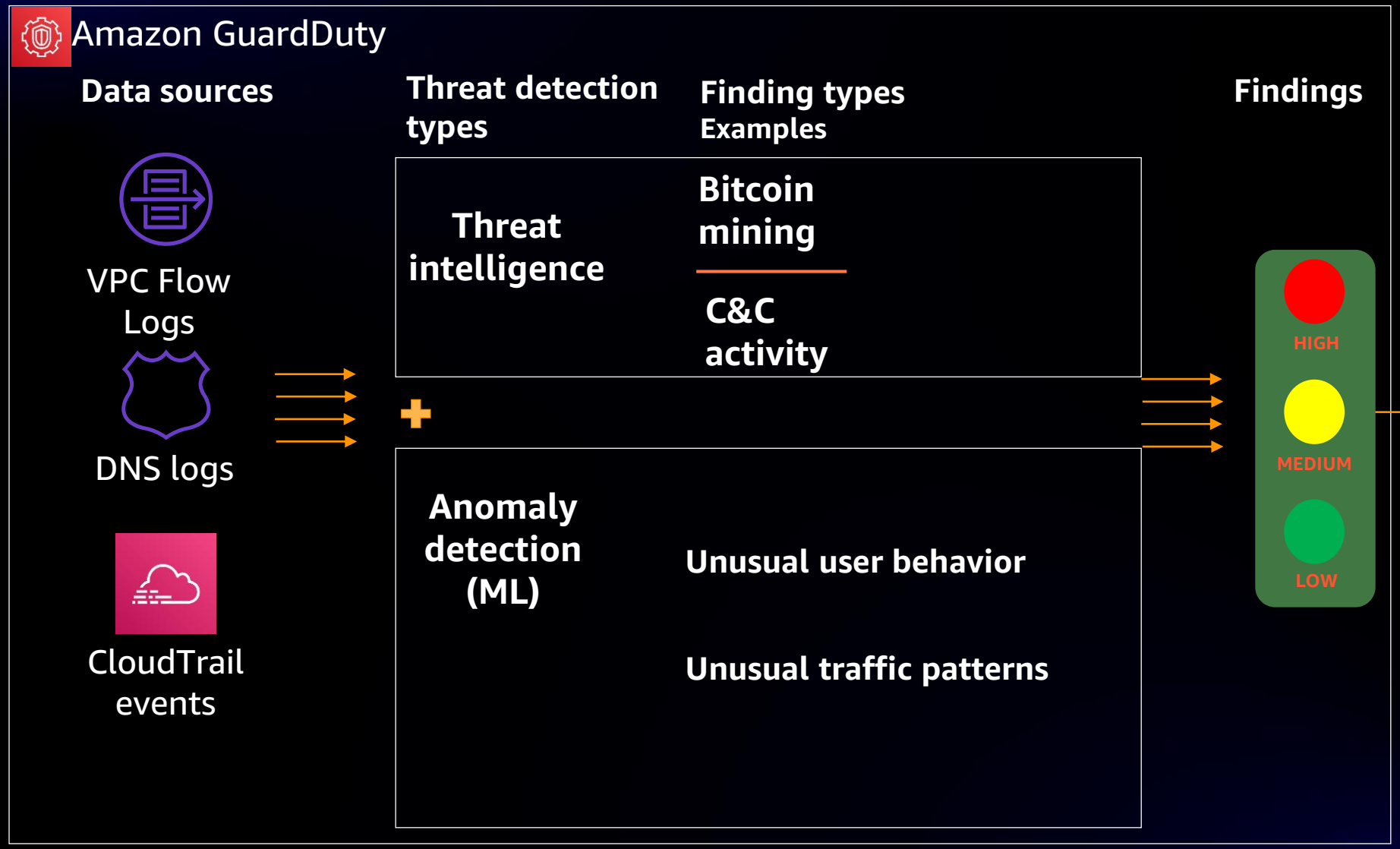
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Permissions management

- Networking team owns provisioning hybrid resources such as Transit Gateway, AWS Direct Connect, and VPN connections
- **Restrict** access to **Create and Delete API** calls to networking team
- **Tag** your networking resources

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detective controls



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

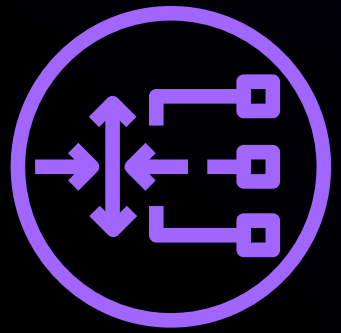
Infrastructure protection

Control traffic at all layers

- Security groups
- Network ACLs
- VPC route tables
- Transit Gateway route tables

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure protection



Gateway Load Balancer



AWS Network Firewall



Amazon Route 53 Resolver DNS Firewall

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection

- Encrypt your AWS Direct Connect connection
- Use AWS Site-to-Site VPN provided encrypted tunnels
- Encrypt your application layer traffic using TLS
- Leverage certificates for authentication wherever applicable

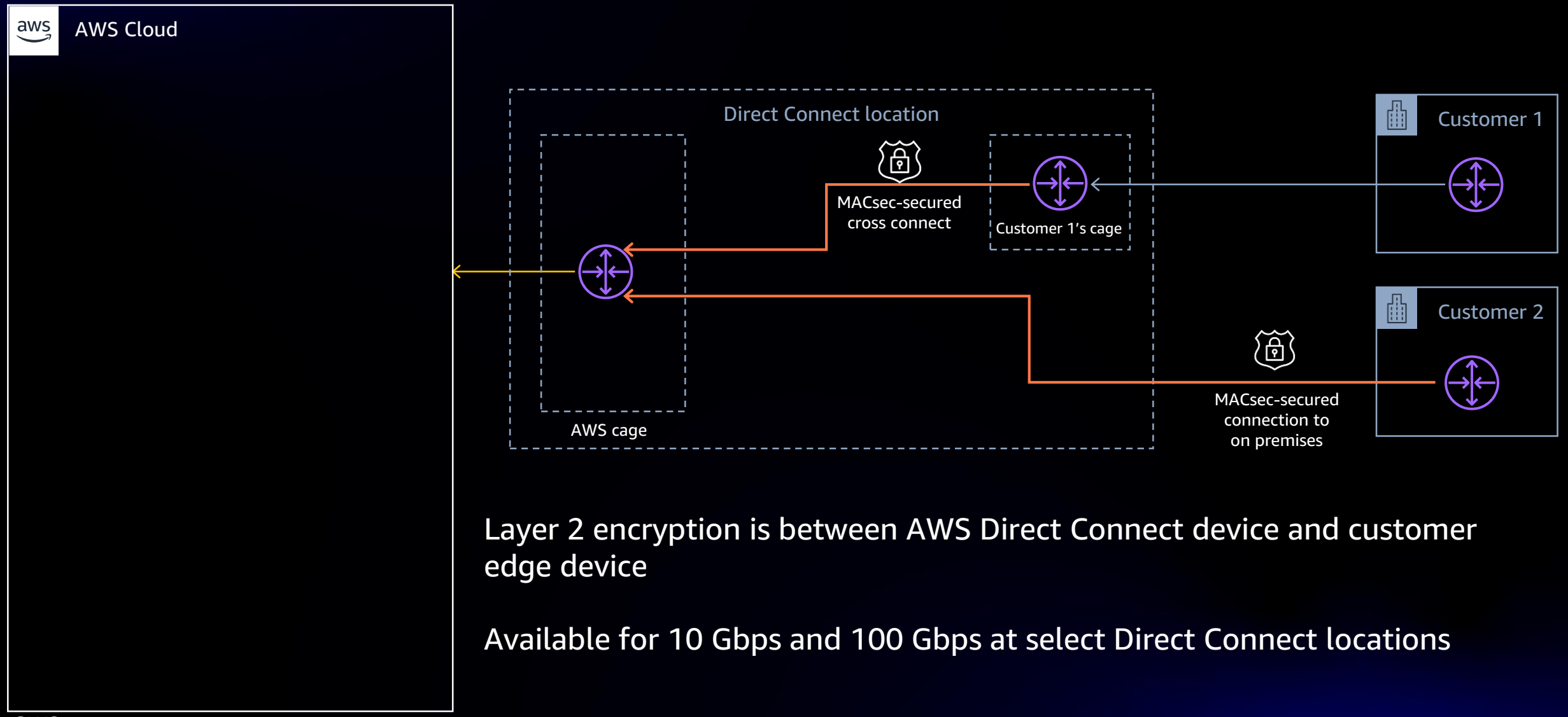
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Encrypting Direct Connect connection

- MACsec support for AWS Direct Connect dedicated connection
- Encrypt using TLS
- Site-to-Site VPN terminating on Transit Gateway or virtual private gateway over Direct Connect public virtual interface
- Software VPN to a virtual appliance over Direct Connect virtual interfaces

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect – MACsec support

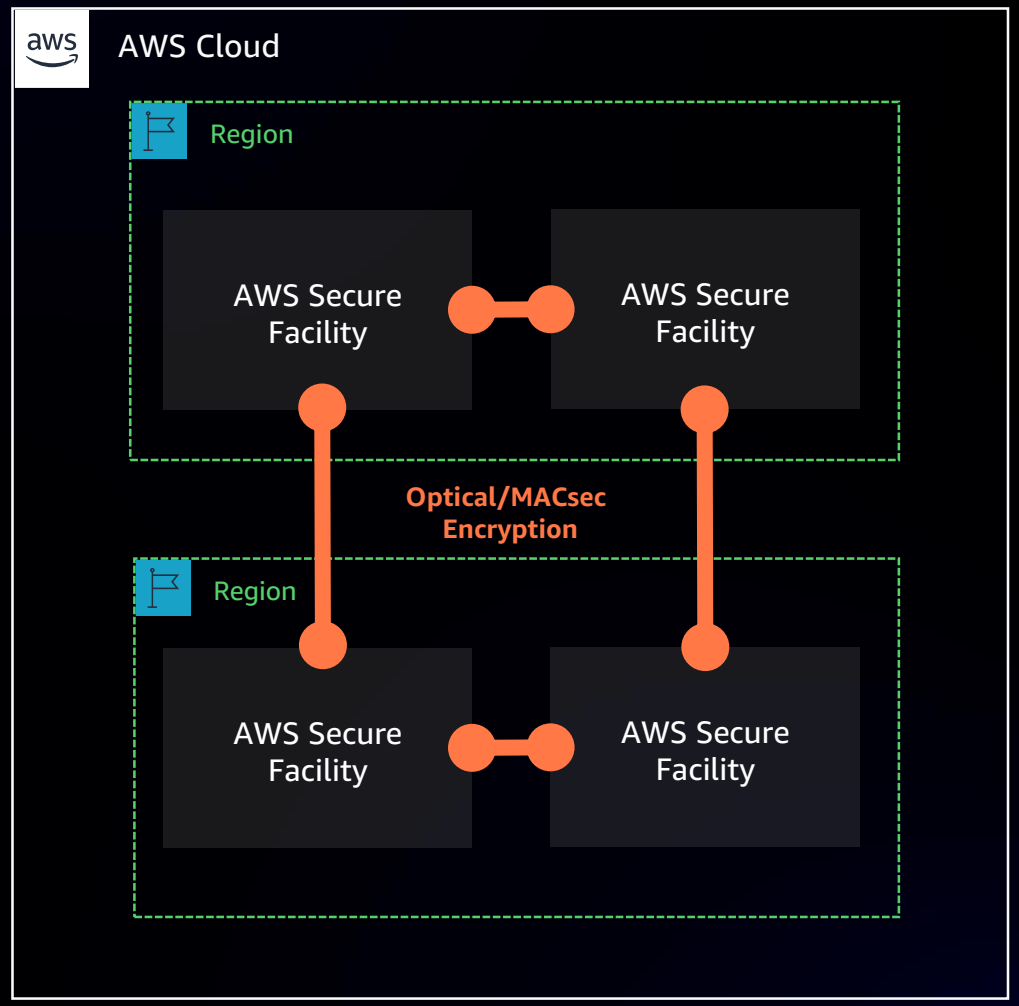


Layer 2 encryption is between AWS Direct Connect device and customer edge device

Available for 10 Gbps and 100 Gbps at select Direct Connect locations

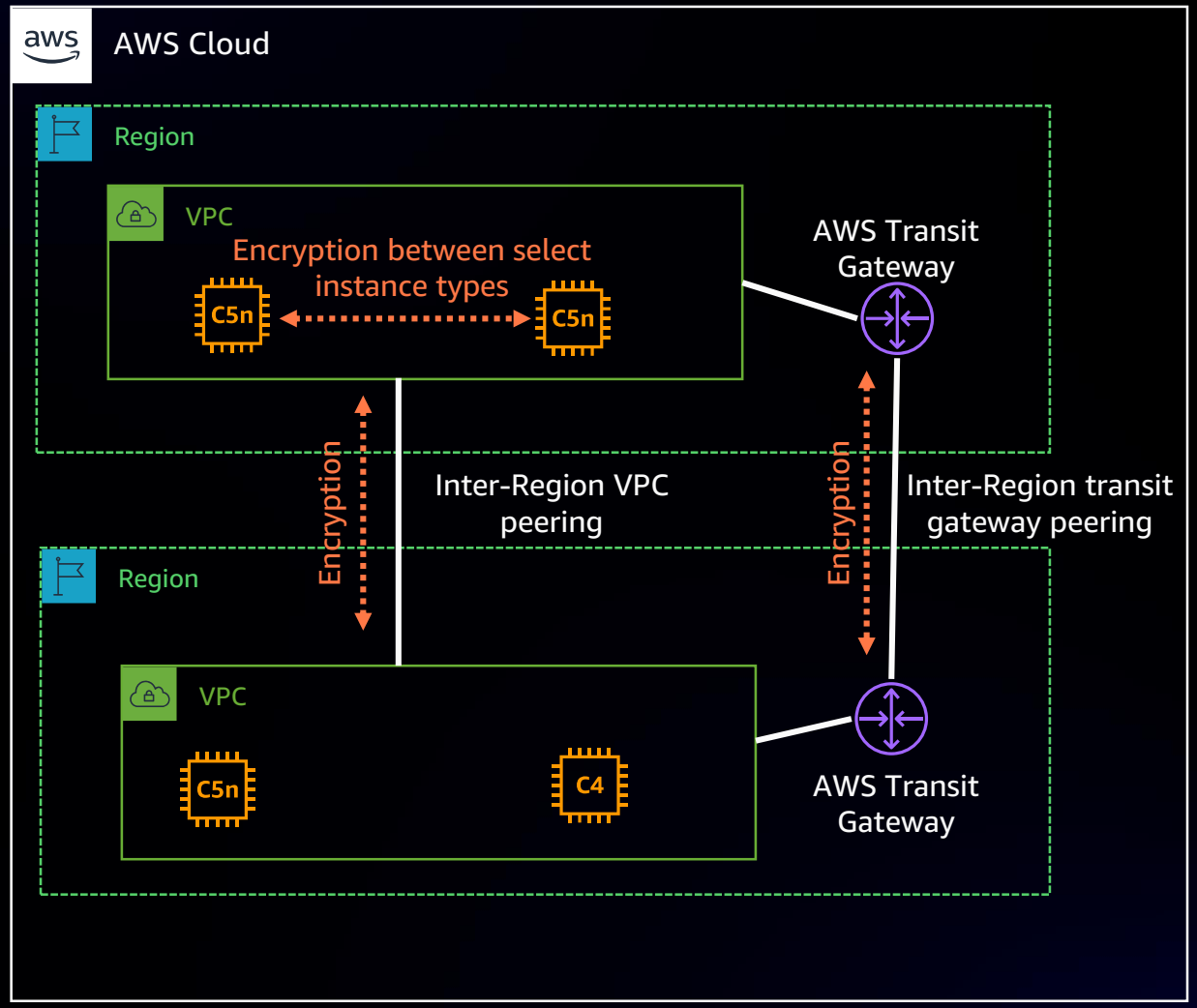
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS-provided network layer encryption



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS-provided network layer encryption



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incident response



Incident Response

Automate incident response to reduce containment time and prevent alert fatigue



Amazon GuardDuty

Use Amazon GuardDuty to monitor AWS environment to protect against malicious activity



AWS Security Hub

Automate and detect your incident response with AWS Security Hub



Amazon EventBridge

Take automated action with Amazon EventBridge

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

References



Data protection in Amazon EC2



Securely scale multi-account architecture with AWS Network Firewall and AWS Control Tower



Automatically block suspicious traffic with AWS Network Firewall and Amazon GuardDuty

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Performance



Performance efficiency

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Planning for performance

- Connectivity options
- Infrastructure location options
- Application performance


AWS Site-to-Site VPN


AWS Direct Connect

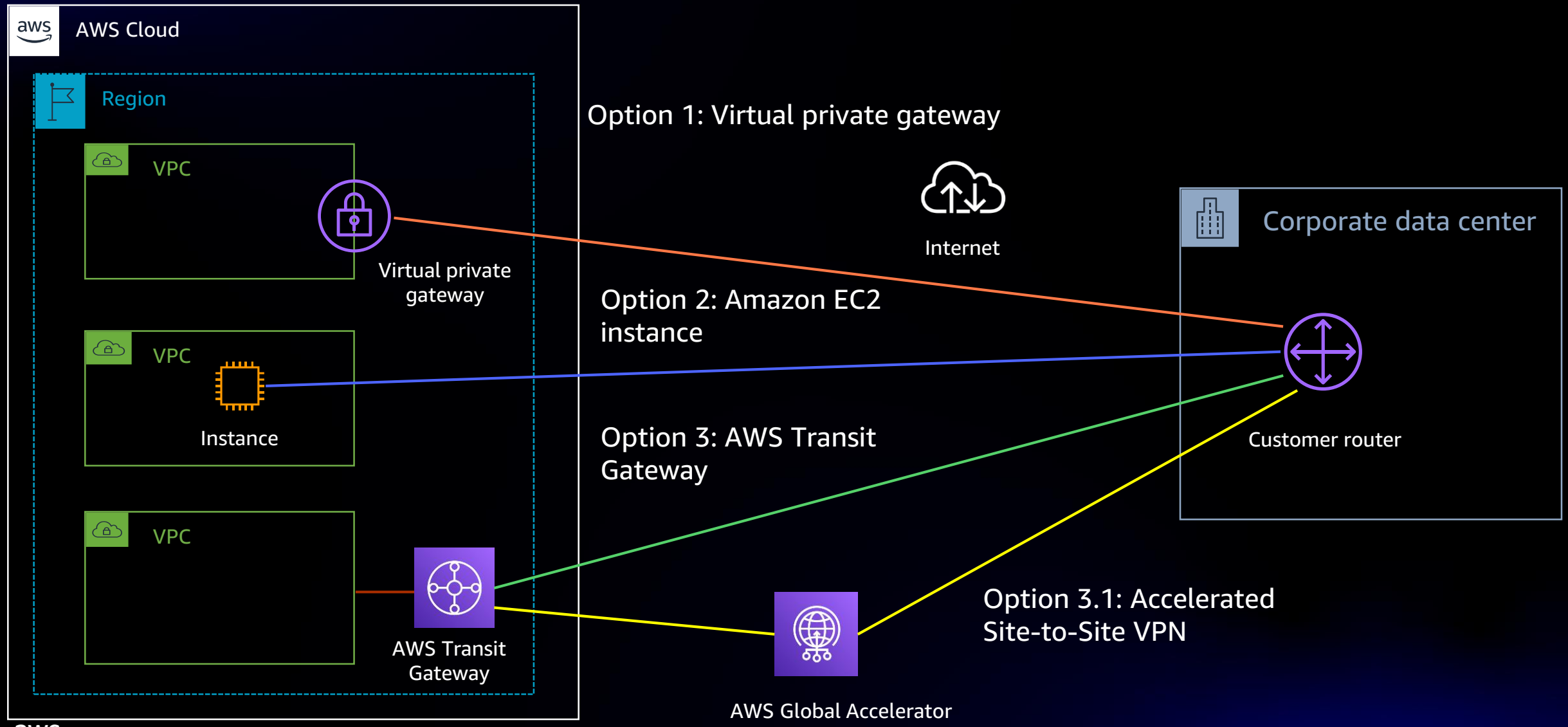

AWS Local Zones


AWS Outposts


Amazon EC2

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPN connectivity options



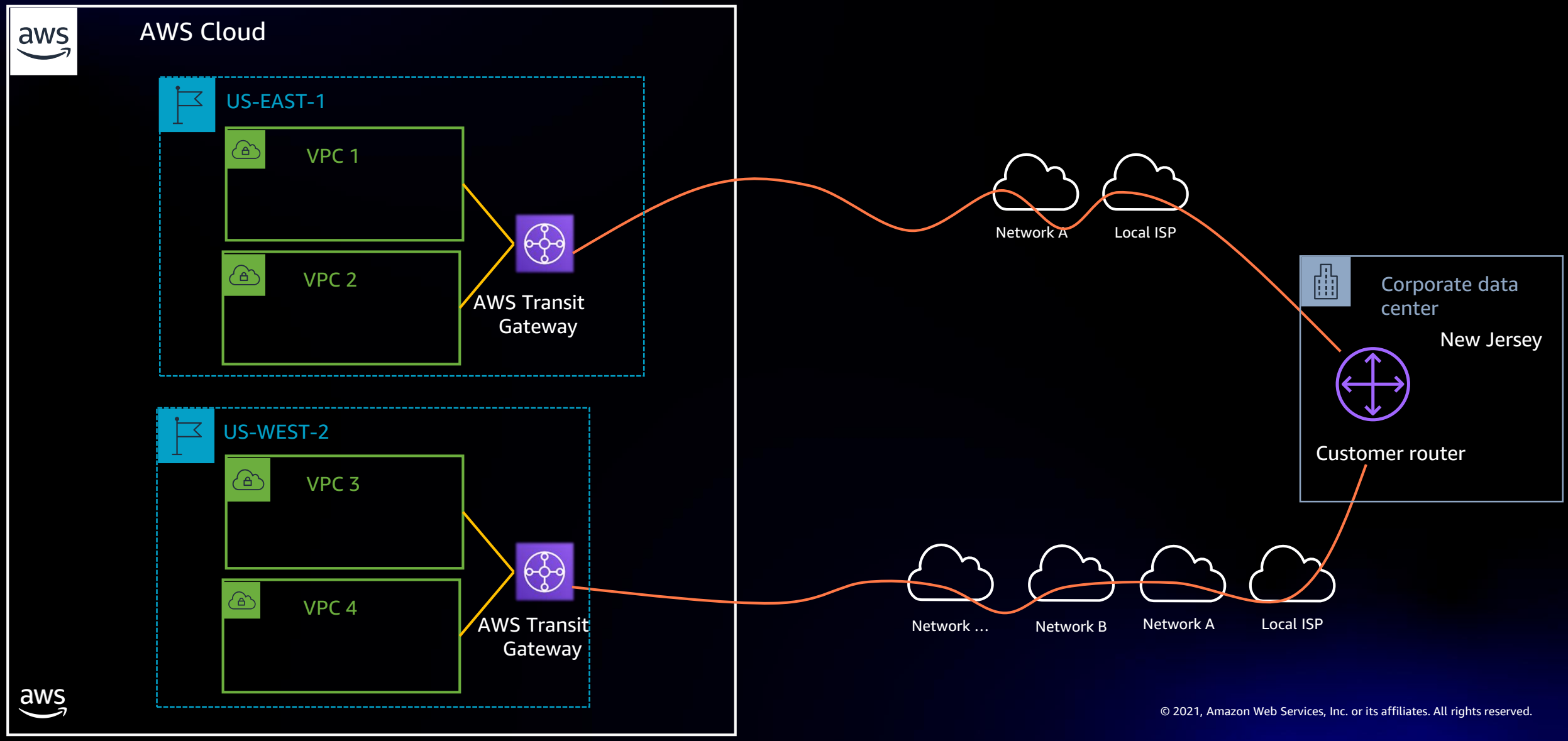
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPN – Throughput considerations

Virtual private gateway	Amazon EC2 instance	AWS Transit Gateway
• 1 VPN connection = 1 VPC • Throughput per tunnel = 1.25 Gbps • No ECMP support	• 1 VPN connection = 1 VPC • Throughput depends on EC2 instance type and is vendor-specific • ECMP support depends on the vendor	• 1 VPN connection = Many VPCs • Throughput per tunnel = 1.25 Gbps • ECMP supported with dynamic routing

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

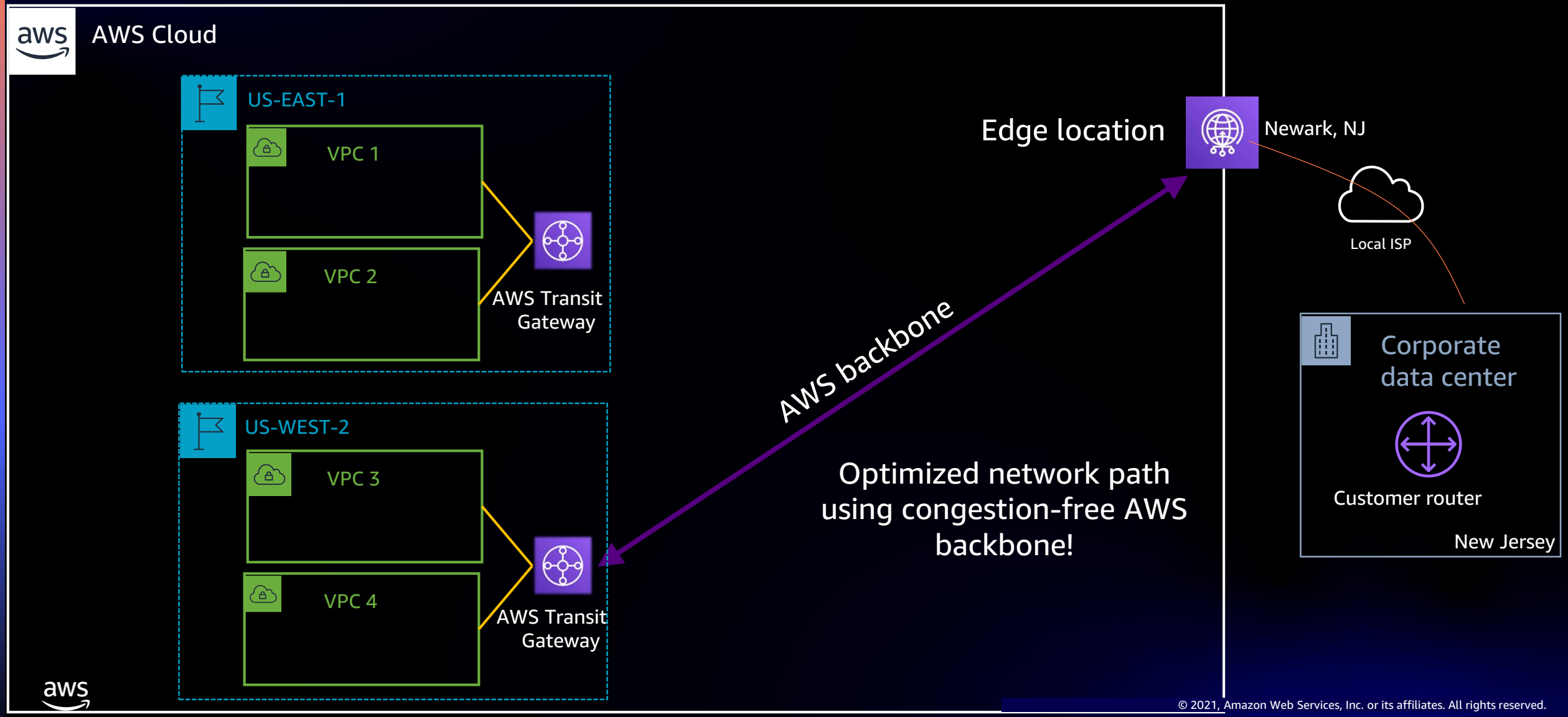
AWS Site-to-Site VPN



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

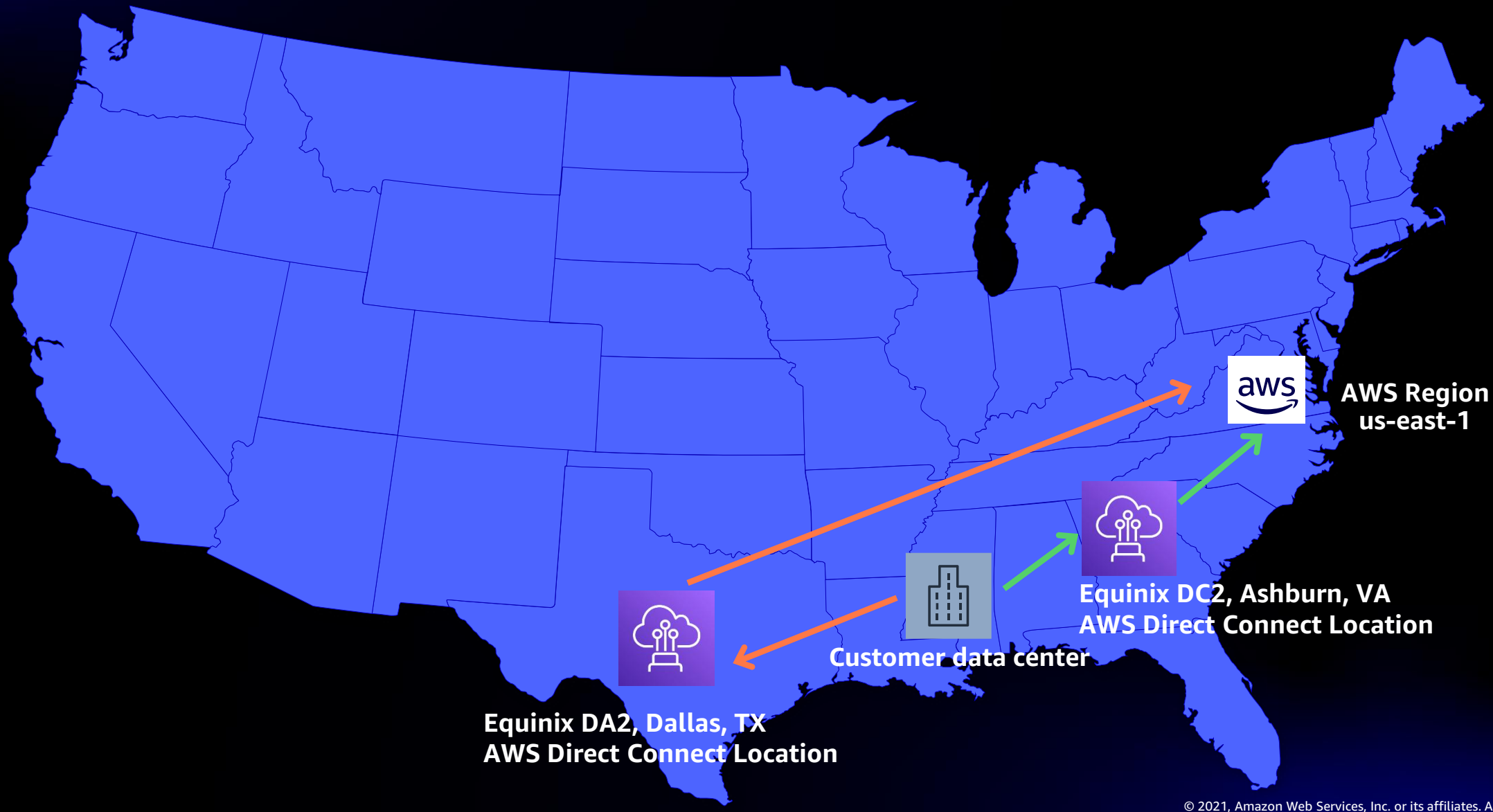
Accelerated Site-to-Site VPN

96 points of presence in 84 cities across 46 countries



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

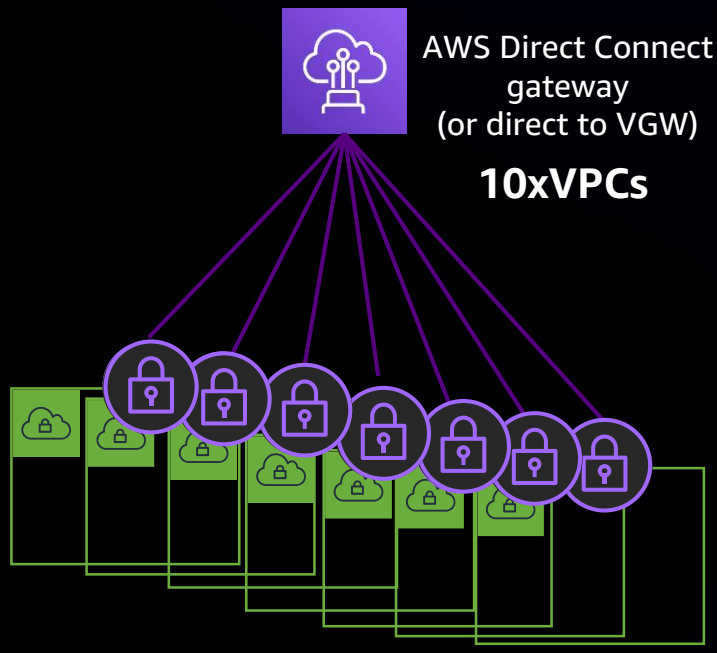
Choosing the right Direct Connect location



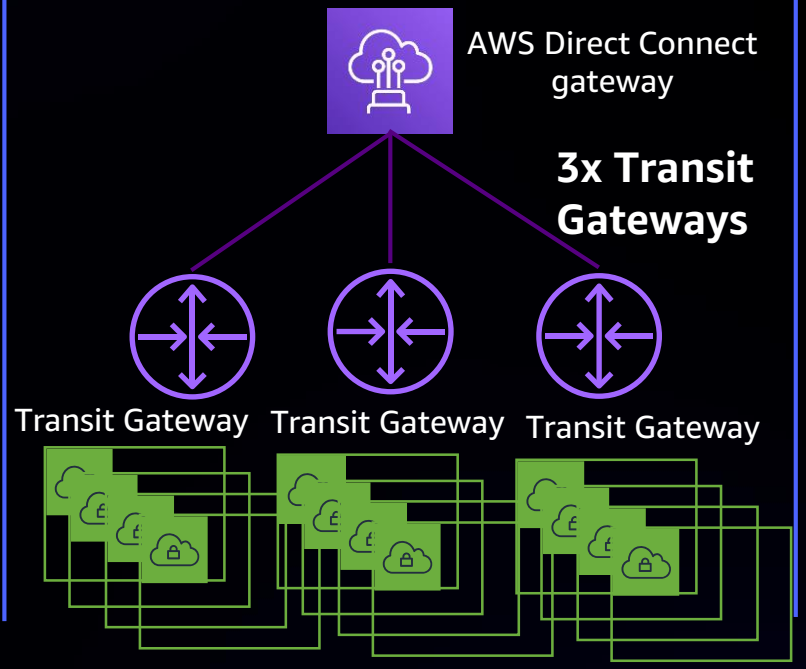
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect – Types of virtual interfaces

Private VIF



Transit VIF



Public VIF


Amazon S3


Amazon DynamoDB


Amazon CloudWatch


AWS Management Console


Amazon SageMaker

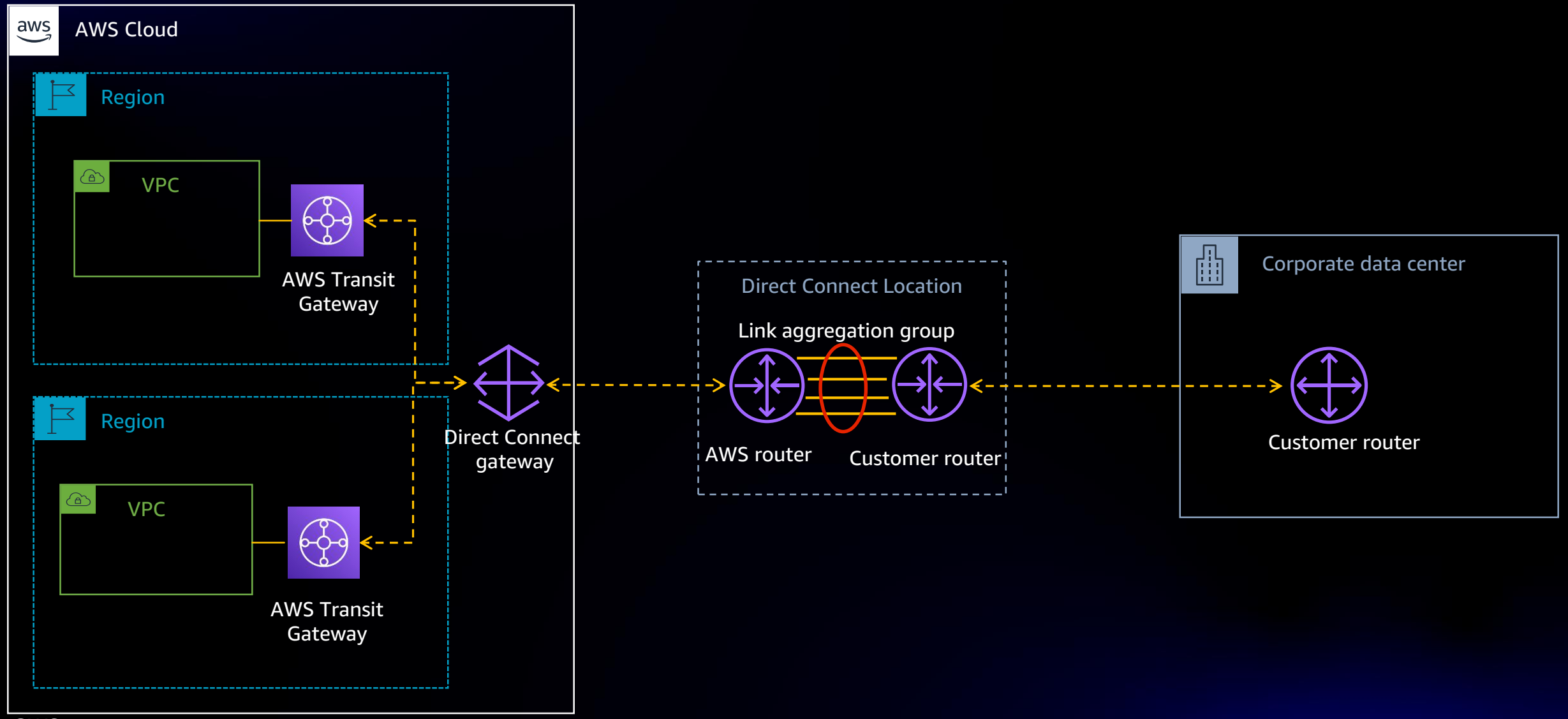
• • •

Supports IPv4 and IPv6 BGP peering sessions on all the above virtual interface types

aws

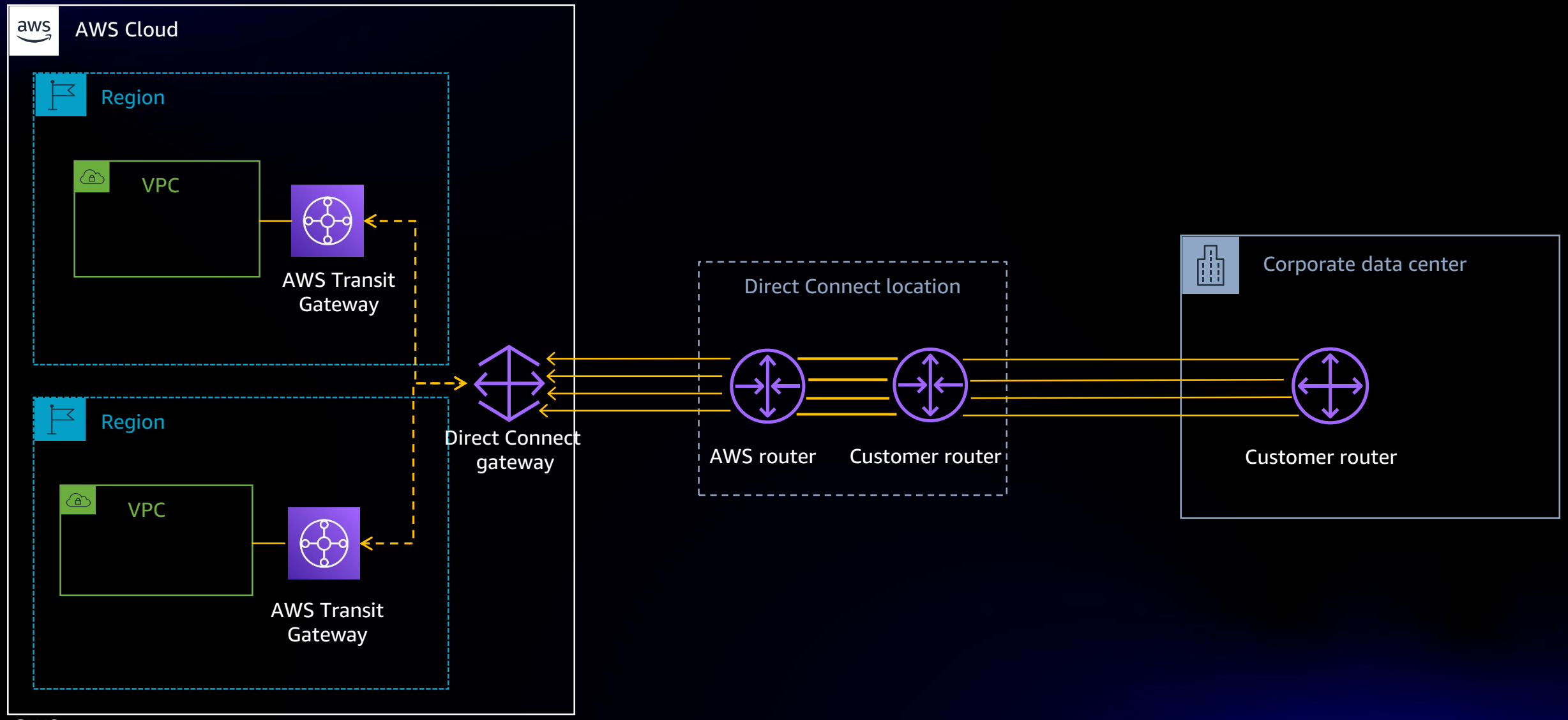
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect Link Aggregation Group (LAG)



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect – BGP with ECMP



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway and Site-to-Site VPN scaling considerations

Name	Default
Maximum bandwidth per VPC, AWS Direct Connect gateway, or peered transit gateway connection	Up to 50 Gbps
Maximum packets per second (PPS) per transit gateway attachment (VPC, VPN, AWS Direct Connect, and peering attachments)	Up to 5,000,000
Maximum bandwidth per VPN tunnel	Up to 1.25 Gbps
Maximum PPS per VPN tunnel	Up to 140,000

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Choosing the right AWS infrastructure location

AWS Regions



For most use cases

AWS Outposts



- AWS infrastructure and services **on premises**
- Migration, local critical applications, data residency
- Expandable capacity in customer's data center; collocated, on-premises location

AWS Local Zones



- AWS infrastructure and services **in large metro centers**
- Migration, low latency, local data processing
- Scalable capacity in AWS-managed and operated facility

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Choosing the right Amazon EC2 instance type

- Choose newer instance types based on performance needs
- Elastic Network Adapter (ENA)
- Elastic Fabric Adapter (EFA)
- Use placement groups

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EC2 instance network bandwidth

Up to 50% of the network bandwidth – for example, c5n.9xlarge that has an instance network bandwidth of 50 Gbps can now drive up to 25 Gbps

Conditions

- Current generation EC2 instances with a minimum of 32 vCPUs
- Traffic is destined to AWS Direct Connect, internet gateway and other AWS Regions

For all other instance types, traffic is limited to 5 Gbps

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

References



Routing policies and BGP communities



Whitepaper: Building a Scalable and Secure Multi-VPC AWS Network Infrastructure



Amazon EC2 instance network bandwidth

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operational excellence

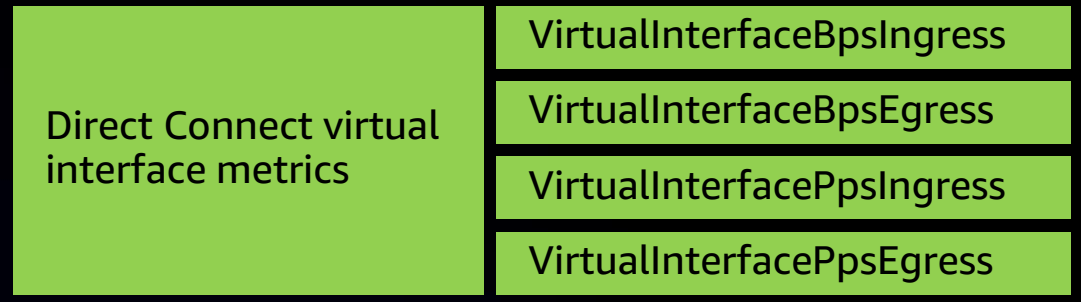


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices – Monitoring Direct Connect

Monitor your AWS Direct Connect connection and virtual interface metrics through Amazon CloudWatch and your customer device metrics





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices – AWS Direct Connect

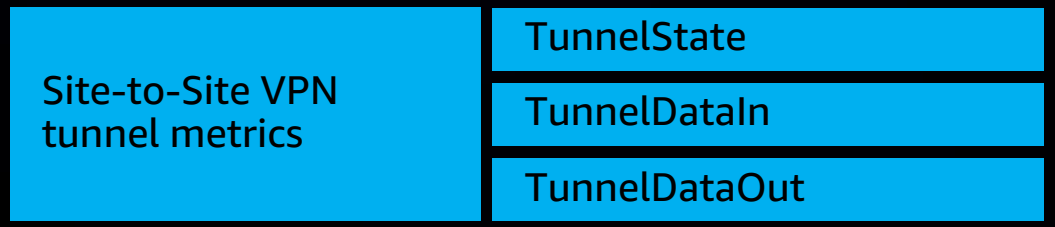


- Use AWS Personal Health Dashboard to check AWS Direct Connect maintenance notifications
- Monitoring via active probing over the different Direct Connect paths
- Enable Bidirectional Forwarding Detection (BFD) on your customer router for fast failure detection and failover
- Test your configuration periodically using AWS Direct Connect Resiliency Toolkit
- Configure a second Direct Connect connection or backup VPN connection for resiliency

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices – Site-to-Site VPN connection

- Monitor your AWS Site-to-Site VPN connections through Amazon CloudWatch and your on-premises VPN device metrics



- Create a CloudWatch alarm to notify you when one or both VPN tunnels are down

- Use AWS Personal Health Dashboard to check VPN maintenance notifications
  - Tunnel endpoint replacement notifications
  - Single-tunnel VPN notifications

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

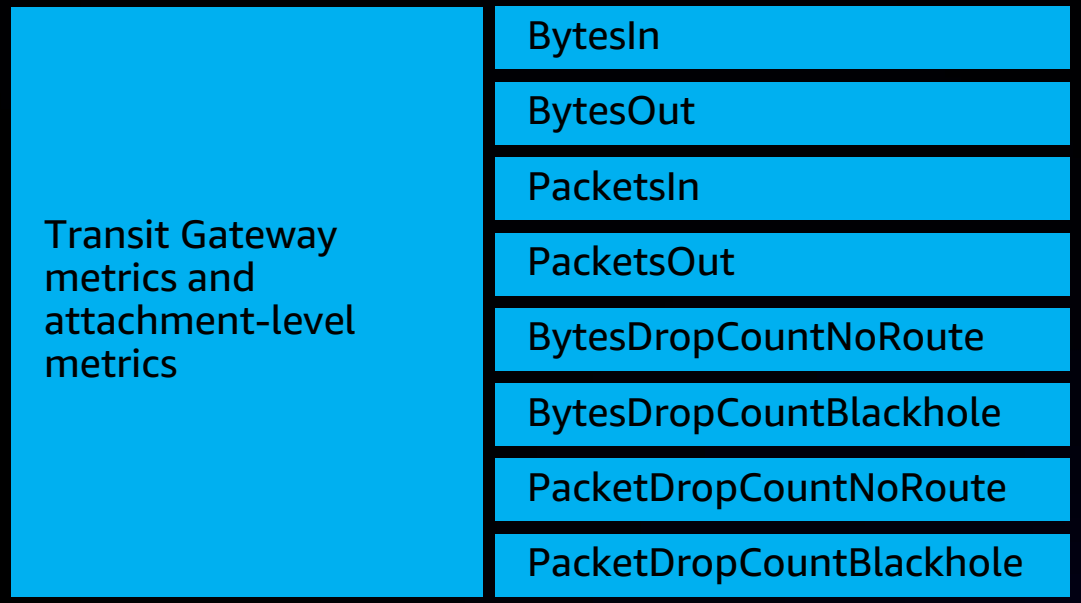
Best practices – Site-to-Site VPN connection

- Use dynamic routing (BGP) when configuring your VPN connection if your customer gateway device supports it
- Use dead peer detection for failover between tunnels
- Configure both tunnels for your VPN connection and test failover scenarios

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices – Transit Gateway

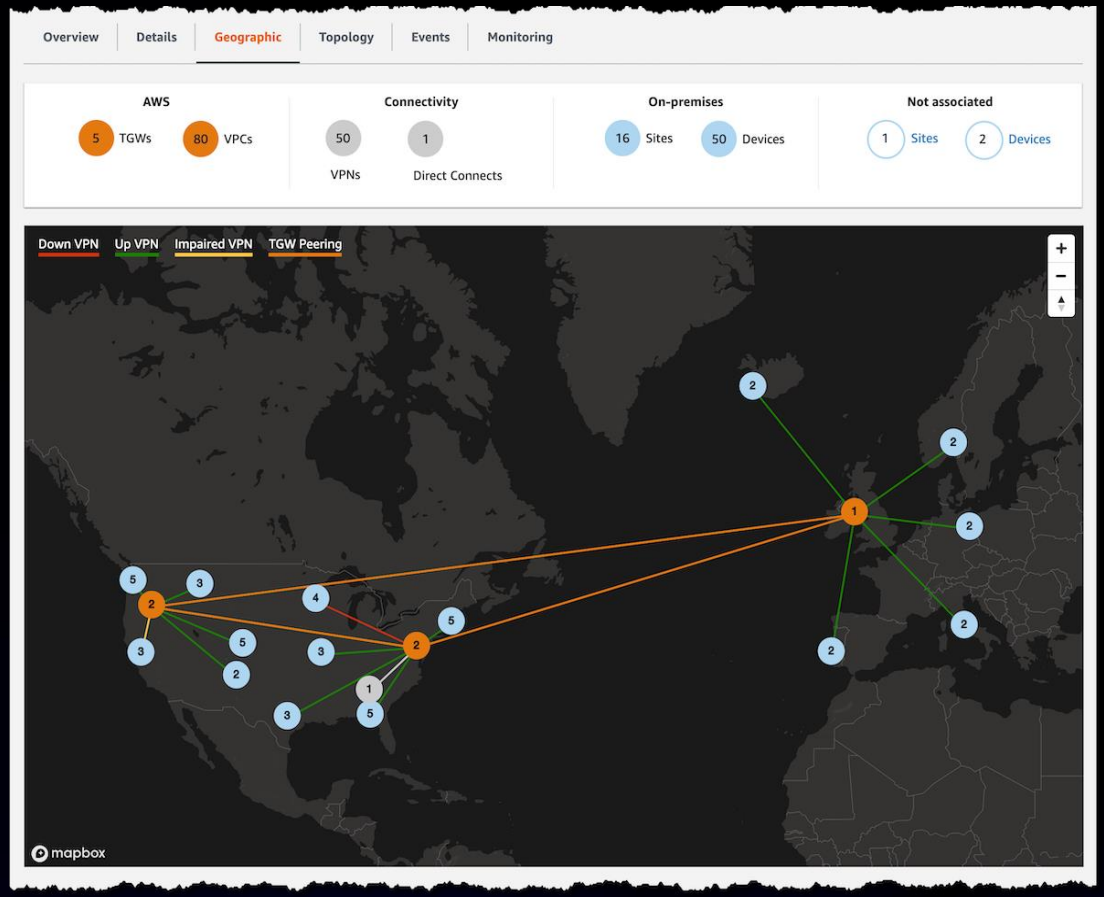
- Monitor your Transit Gateway metrics and attachment-level metrics using Amazon CloudWatch



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

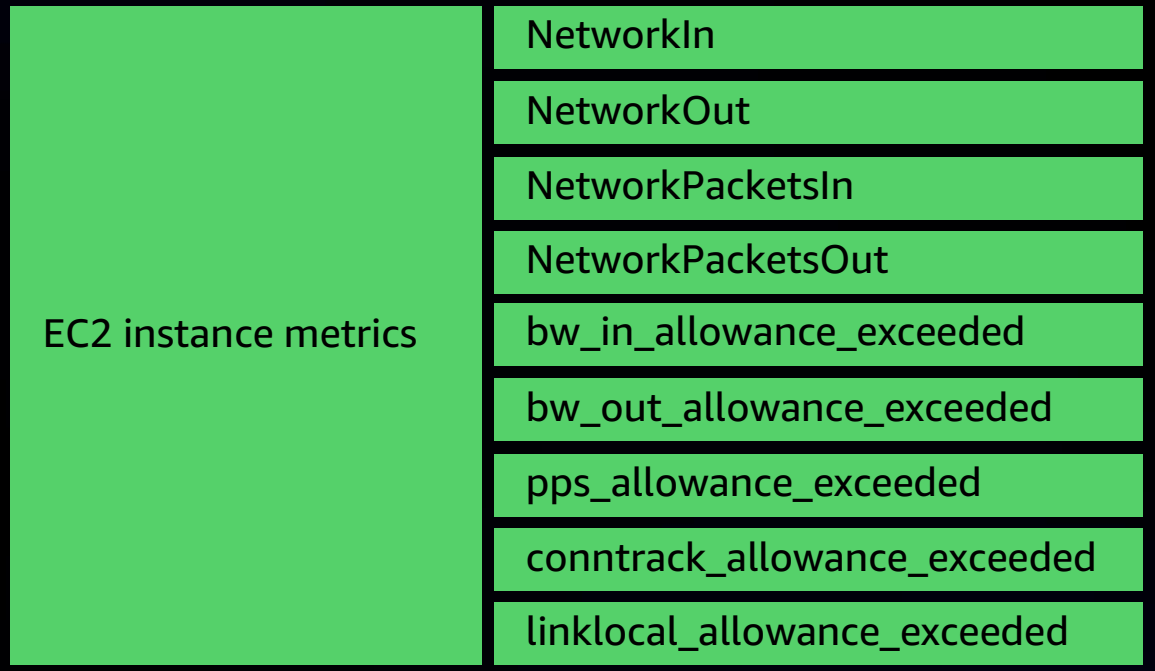
Best practices – Transit Gateway

- Create a CloudWatch alarm when packets are blackholed or dropped
  - PacketDropCountBlackhole
  - PacketDropCountNoRoute
- Use **Transit Gateway Network Manager** to visualize and monitor the health of your hybrid resources
- Use **Route Analyzer** to perform an analysis of the routes in your transit gateway route tables in your global network



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitor network performance for Amazon EC2 instances



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Define IP address and ASN allocation scheme

- Develop a **well-defined IP addressing** allocation scheme across your VPCs and on-premises networks
- Use **unique ASN** for your Direct Connect gateway, transit gateways in each region and on-premises network
- Reduce the risk of **overlapping CIDR ranges** between VPC and on-premises networks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

References



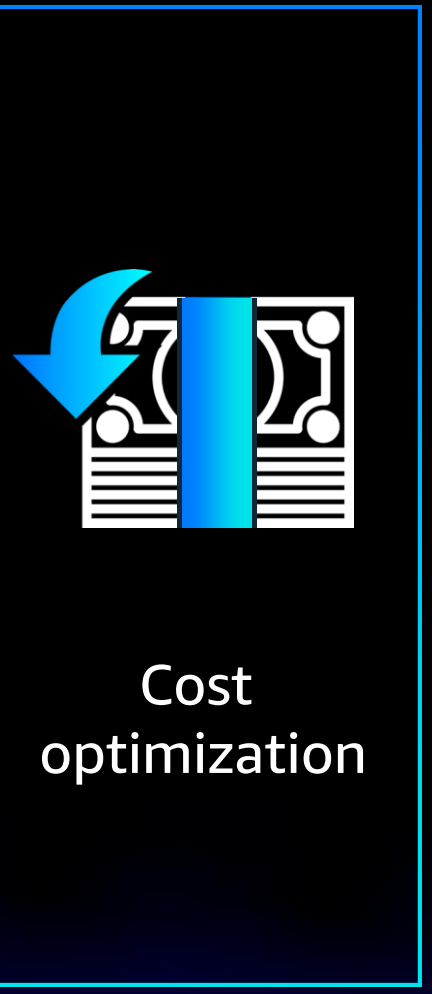
Advanced Troubleshooting with AWS Transit Gateway Network Manager Route Analyzer



Monitor network performance for your EC2 instance

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cost optimization



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Understanding your baseline costs



VPC Flow Logs

Understand top talkers and application traffic patterns



Amazon QuickSight

Visualize Amazon Athena analysis of the AWS Cost and Usage Reports to identify data transfer costs



AWS Cost and Usage Reports

Gather comprehensive data about your AWS costs



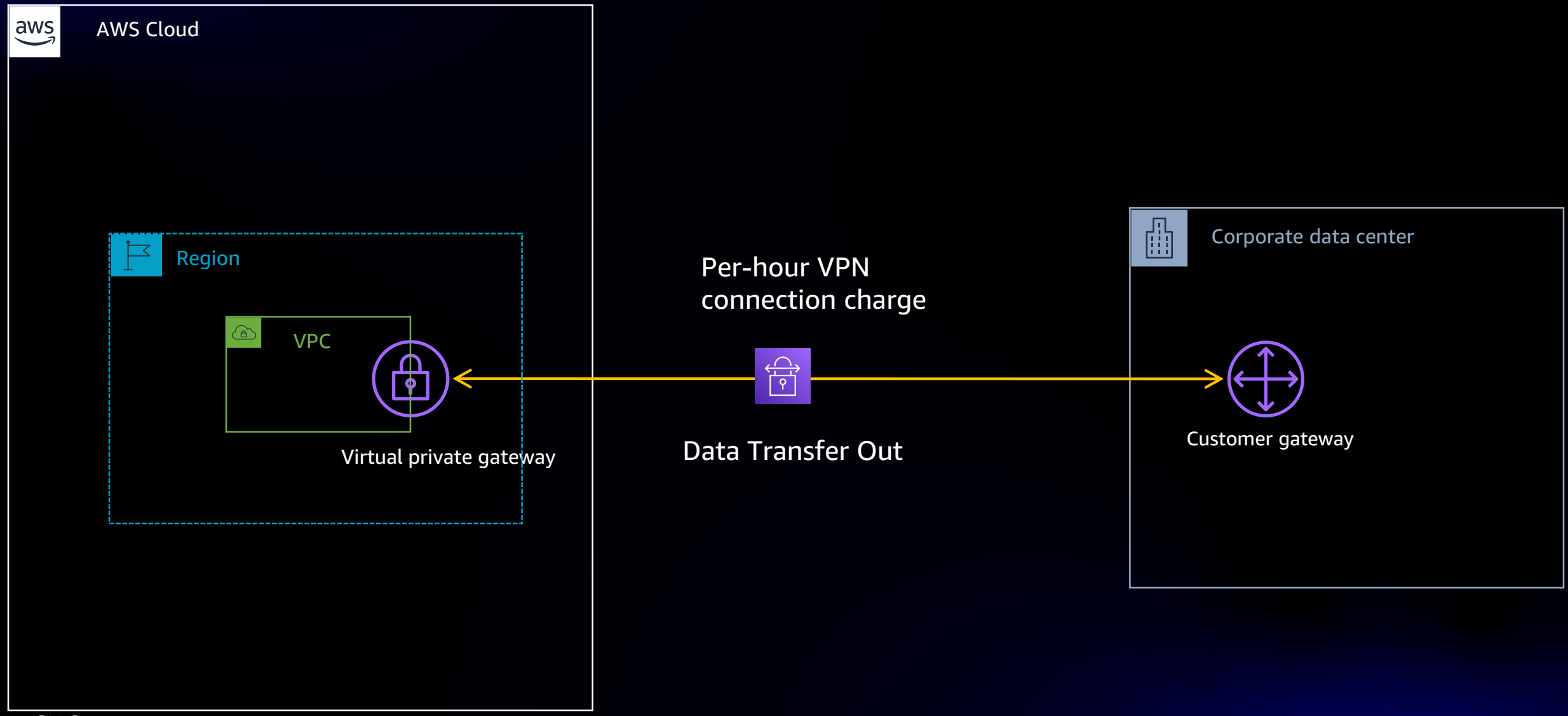
AWS Cost Explorer

Understand and manage your AWS costs and usage over time

aws

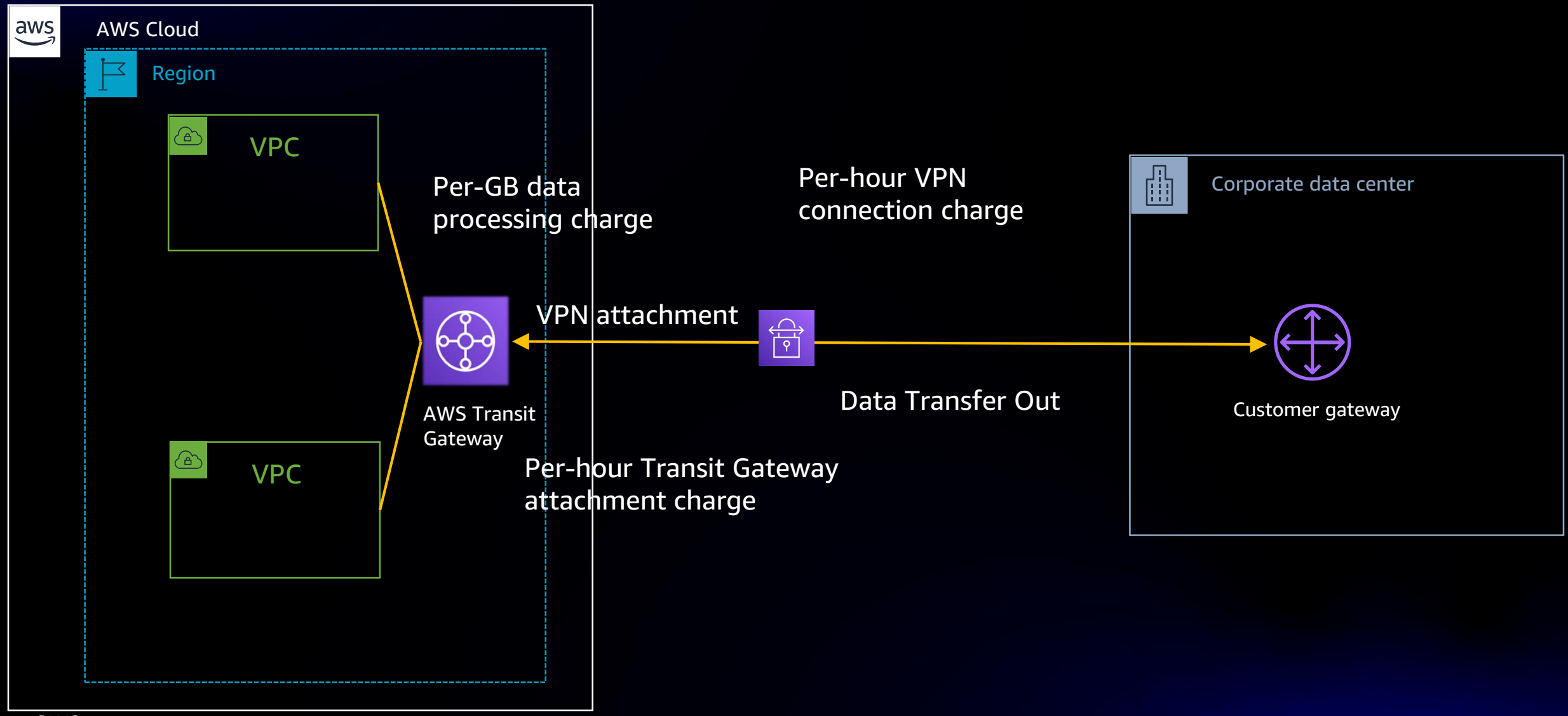
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Site-to-Site VPN – Virtual private gateway



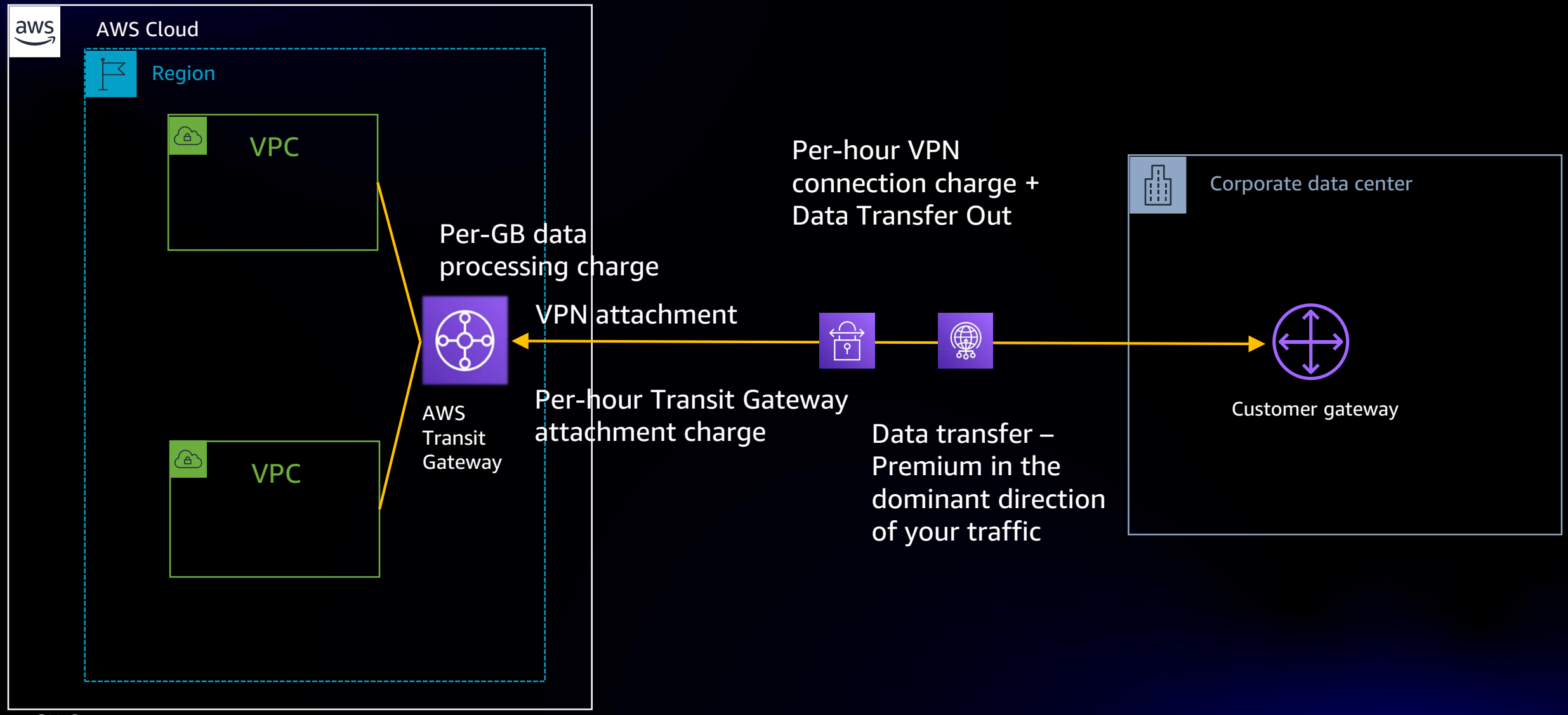
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Site-to-Site VPN – Transit Gateway



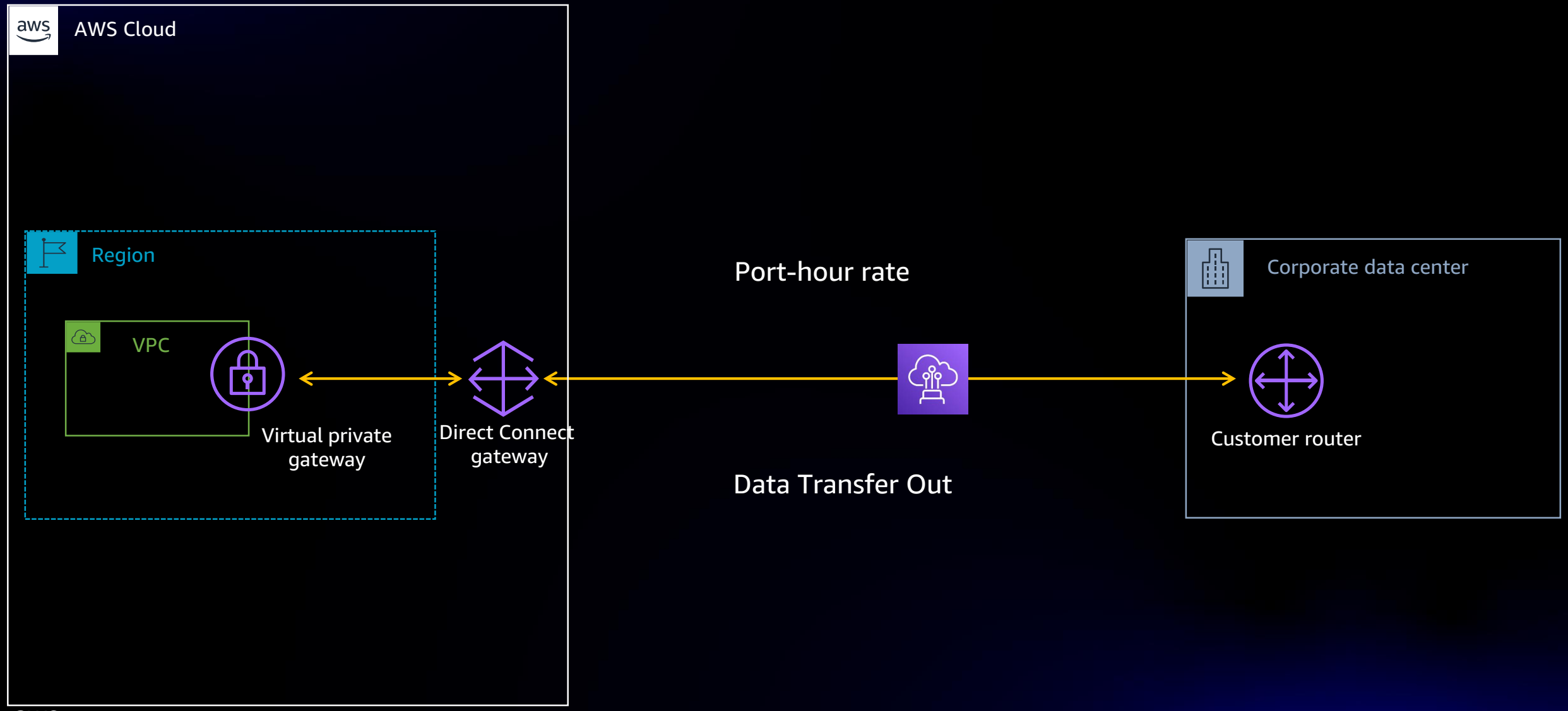
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Accelerated Site-to-Site VPN



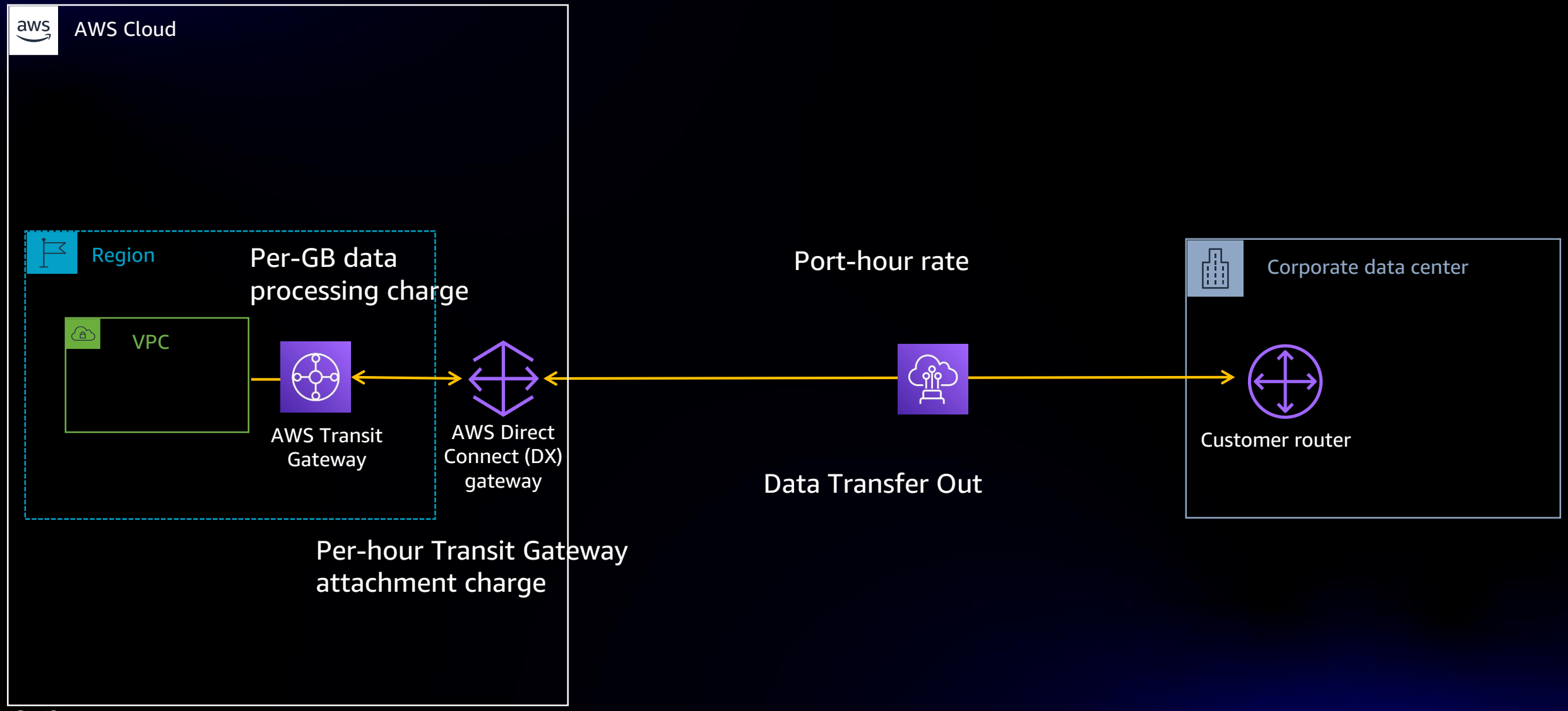
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect and virtual private gateway



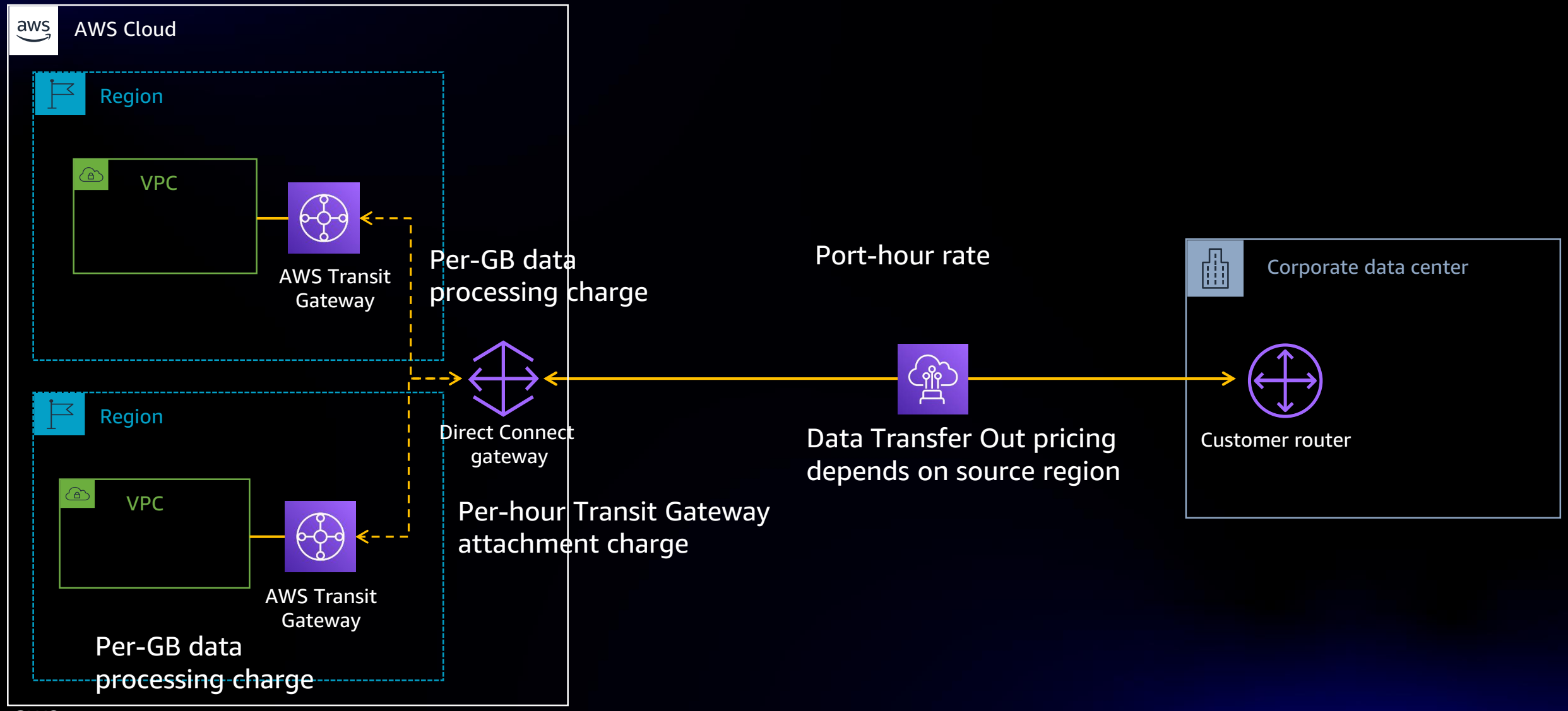
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DX and Transit Gateway – Same Region



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DX and Transit Gateway – Different Region



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cost-effective resources

Category	Customer-managed VPN or SD-WAN	AWS Site-to-Site VPN	AWS accelerated Site-to-Site VPN	AWS Direct Connect hosted connection	AWS Direct Connect dedicated connection
Requires customer internet connection	Yes	Yes	Yes	No	No
Provisioned resources cost	EC2 instance and software licensing	AWS Site-to-Site VPN	AWS Site-to-Site VPN and AWS Global Accelerator	Hosted Connection port cost	Dedicated port cost
Data transfer cost	Internet rate	Internet rate or Direct Connect rate	Internet with data transfer premium	Direct Connect rate	Direct Connect rate
Transit Gateway	Optional	Optional	Required	Optional	Optional
Data processing cost	N/A	Only with AWS Transit Gateway	Yes	Only with AWS Transit Gateway	Only with AWS Transit Gateway
Can be used over AWS Direct Connect?	Yes	Yes	No	N/A	N/A

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

References



Trends Dashboard with AWS Cost and Usage Reports, Amazon Athena and Amazon QuickSight



Overview of Data Transfer Costs for Common Architectures



Optimize performance and reduce costs for network analytics with VPC Flow Logs in Apache Parquet format

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pillars of the Well-Architected Framework



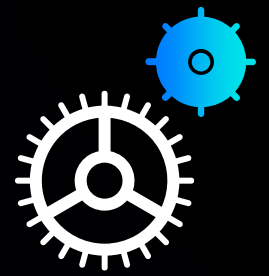
Reliability



Security



Performance efficiency



Operational excellence



Cost optimization

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Aarthi Raju
aartraju@amazon.com

Rohit Aswani
raaswani@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.