

WASHINGTON, DC | JUNE 26-27, 2024

aws SUMMIT



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NET 302

Networking essentials across AWS partitions

Chris Smith

he/him

Principal Solutions Architect,
WWPS US Federal Partners
AWS

Chuck Fuller

he/him

Senior Solutions Architect,
WWPS State and Local Government
AWS

Jeffrey Damick

he/him

Principal Software Engineer,
Amazon Route 53
AWS



Before we begin

300

NET302 is a 300-level session, not entry level nor expert level



We'll let you know when a buildout is complete for photos



Pro tip: Watch for recommendations and best practices

Agenda

AWS GovCloud (US) as a partition

AWS partitions, AWS Regions, and AWS Global Infrastructure

Customer journey in building networks on AWS

Public sector customers and DNS

Multi-partition patterns

AWS GovCloud (US)

Why and how?



Why AWS GovCloud (US) as a separate partition?

Aligns to ITAR and EAR compliance for storing and processing export-controlled data

- Resides on US soil
- Managed by US citizens
- Vetted access/accounts for customers

Compliance alignment

- FISMA FedRAMP High
- DOD SRG IL 2, 4, and 5
- CJIS
- DFARS
- NIST 800-53, 800-171
- IRS 1075



AWS GovCloud (US)

AWS GovCloud (US) accounts can also store and process data not regulated by ITAR or EAR

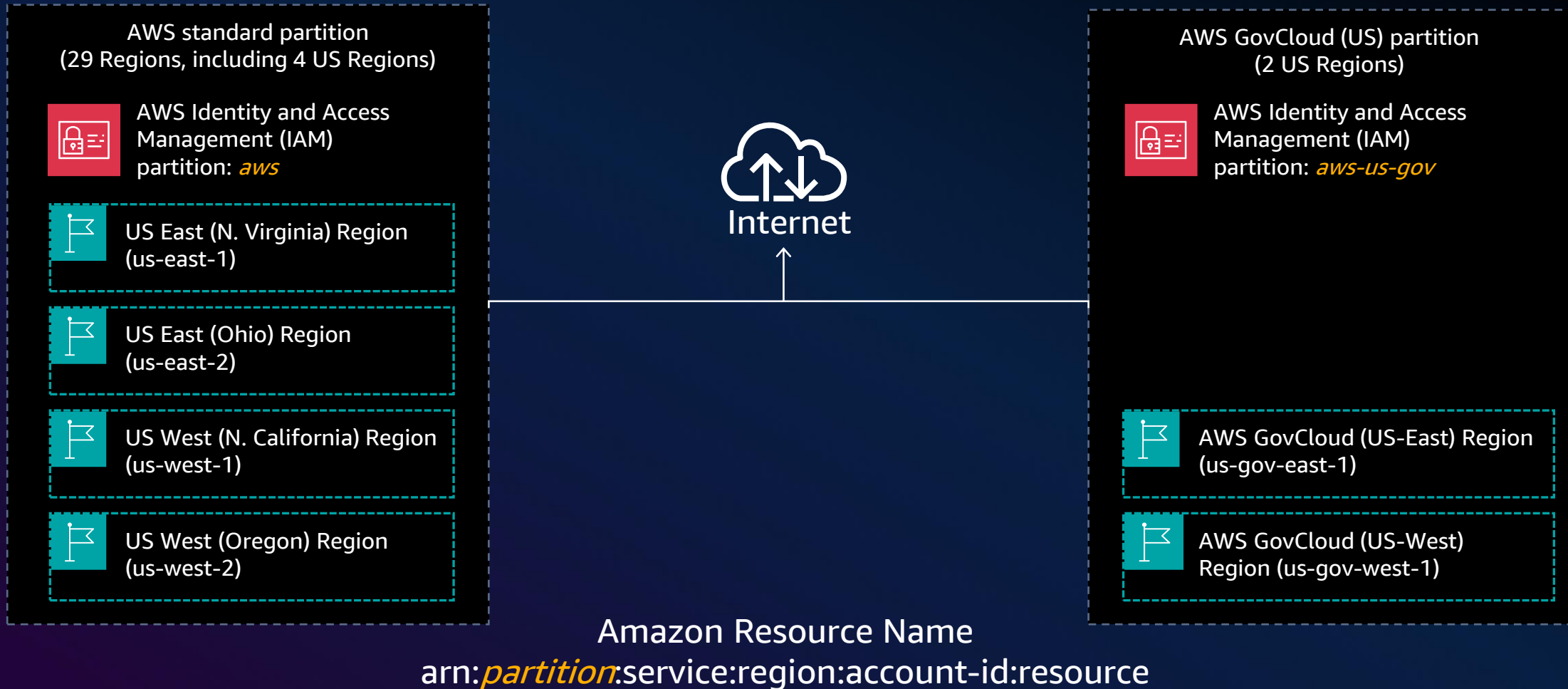


AWS partitions, AWS Regions, and AWS Global Infrastructure

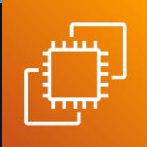







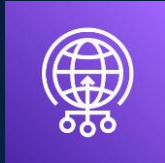
A deeper look



AWS partitions and networks



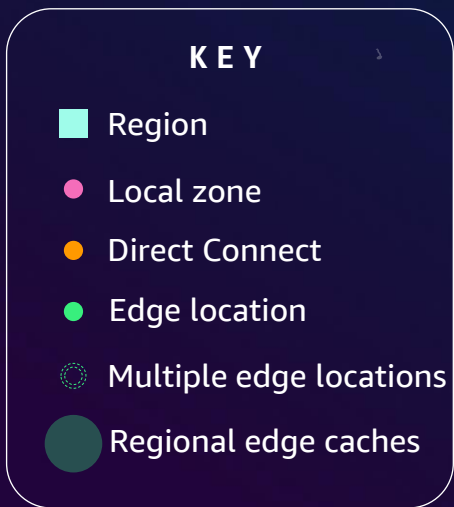
AWS services (zonal, regional, and global)

Service type	Control plane	Data plane	Service examples			
Zonal services	Regional	Zonal				
			Amazon EC2	Amazon EBS		
Regional services	Regional	Regional				...
			Amazon S3	Amazon Aurora	Amazon DynamoDB	
Global services	Hosted in a Region (e.g., us-east-1), operates globally	Distributed globally, operate independently in each Region				 ...
			AWS Identity and Access Management (IAM)	Amazon CloudFront	Amazon Route 53	AWS Global Accelerator



AWS Global Infrastructure

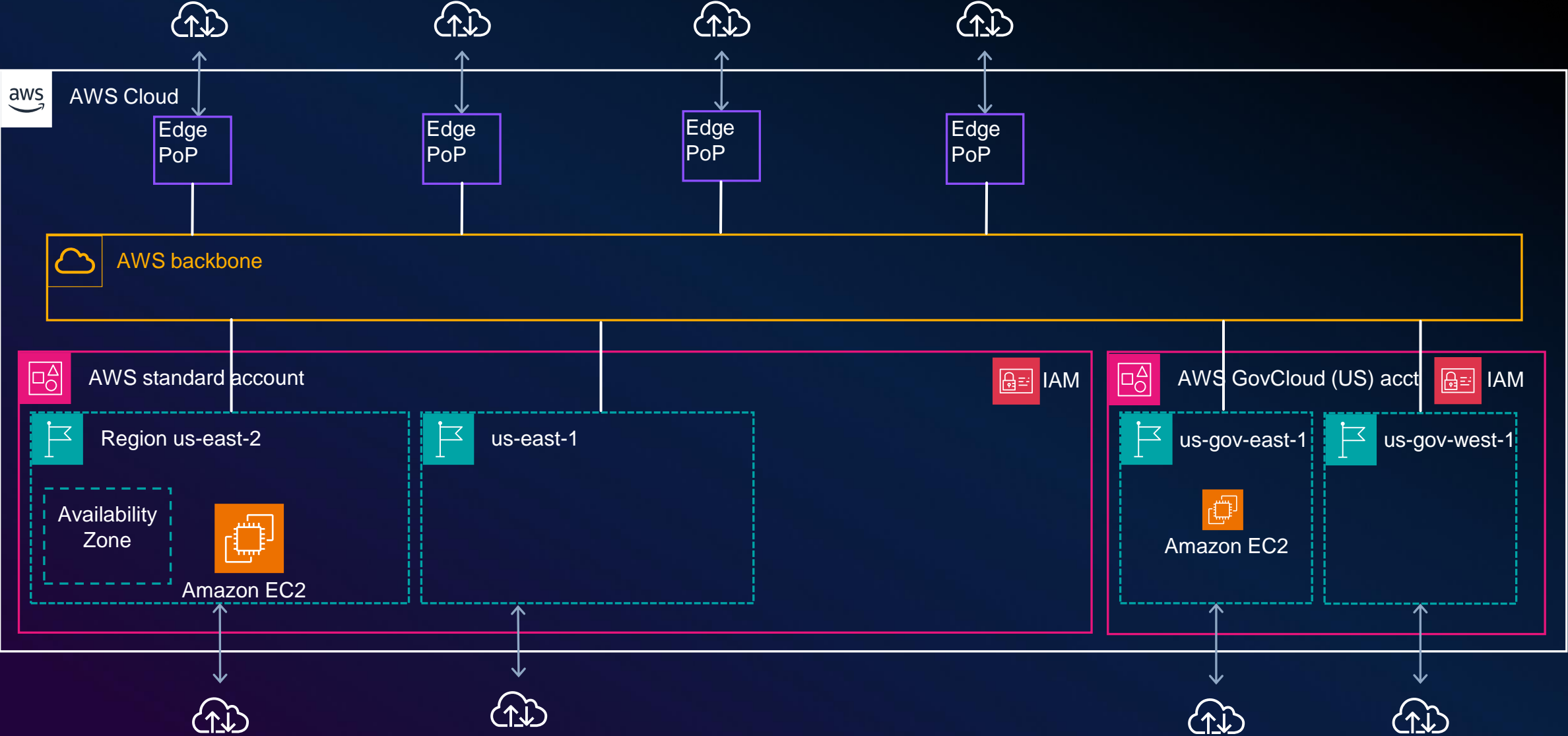
AWS REGIONS, LOCAL ZONES, EDGE LOCATIONS, AND GLOBAL BACKBONE



Always check the AWS Global Infrastructure page for the latest information: <https://aws.amazon.com/about-aws/global-infrastructure/>

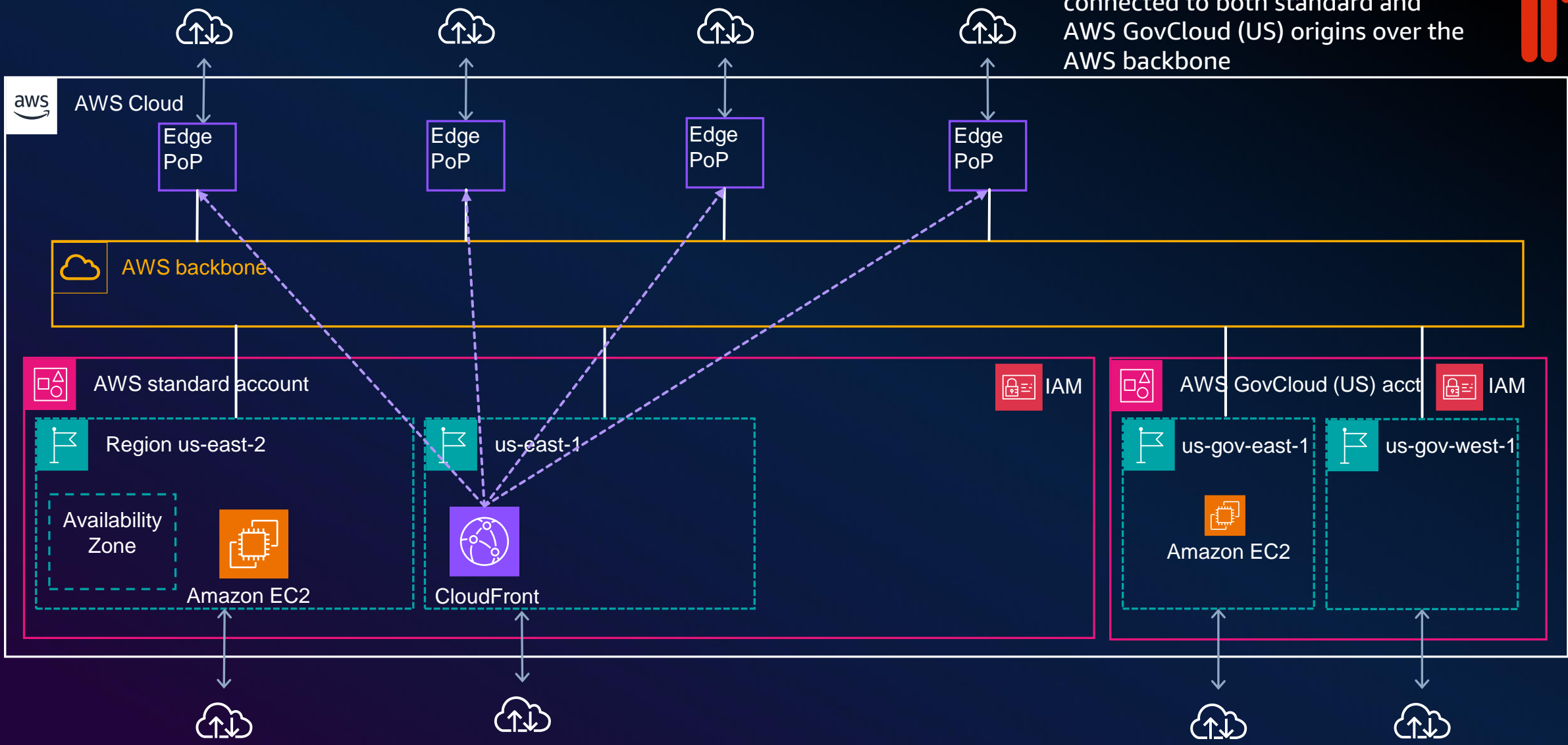


AWS service control plane and infrastructure data plane



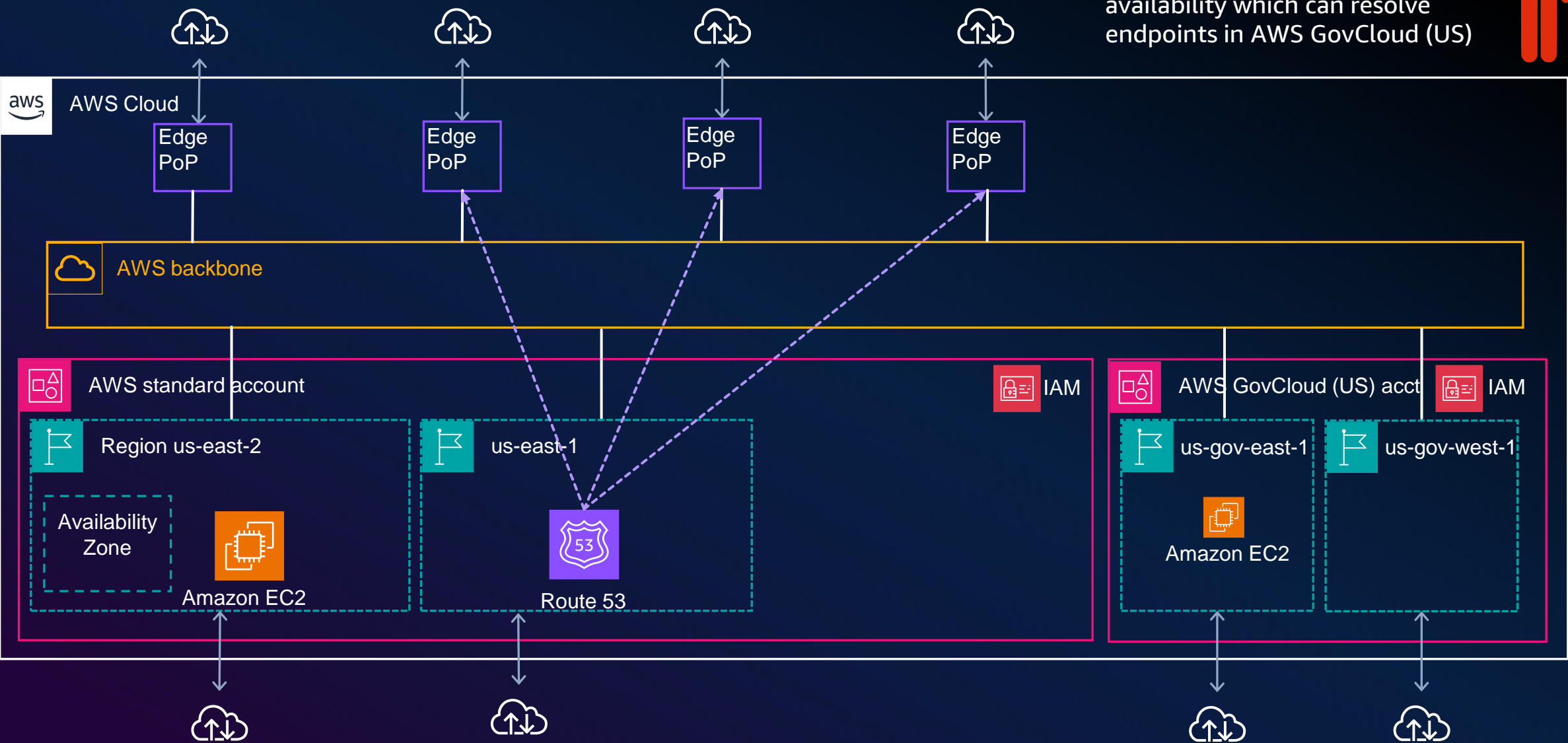
AWS edge network services

CloudFront 600+ POPs in 100+ cities across 50+ countries that can be connected to both standard and AWS GovCloud (US) origins over the AWS backbone

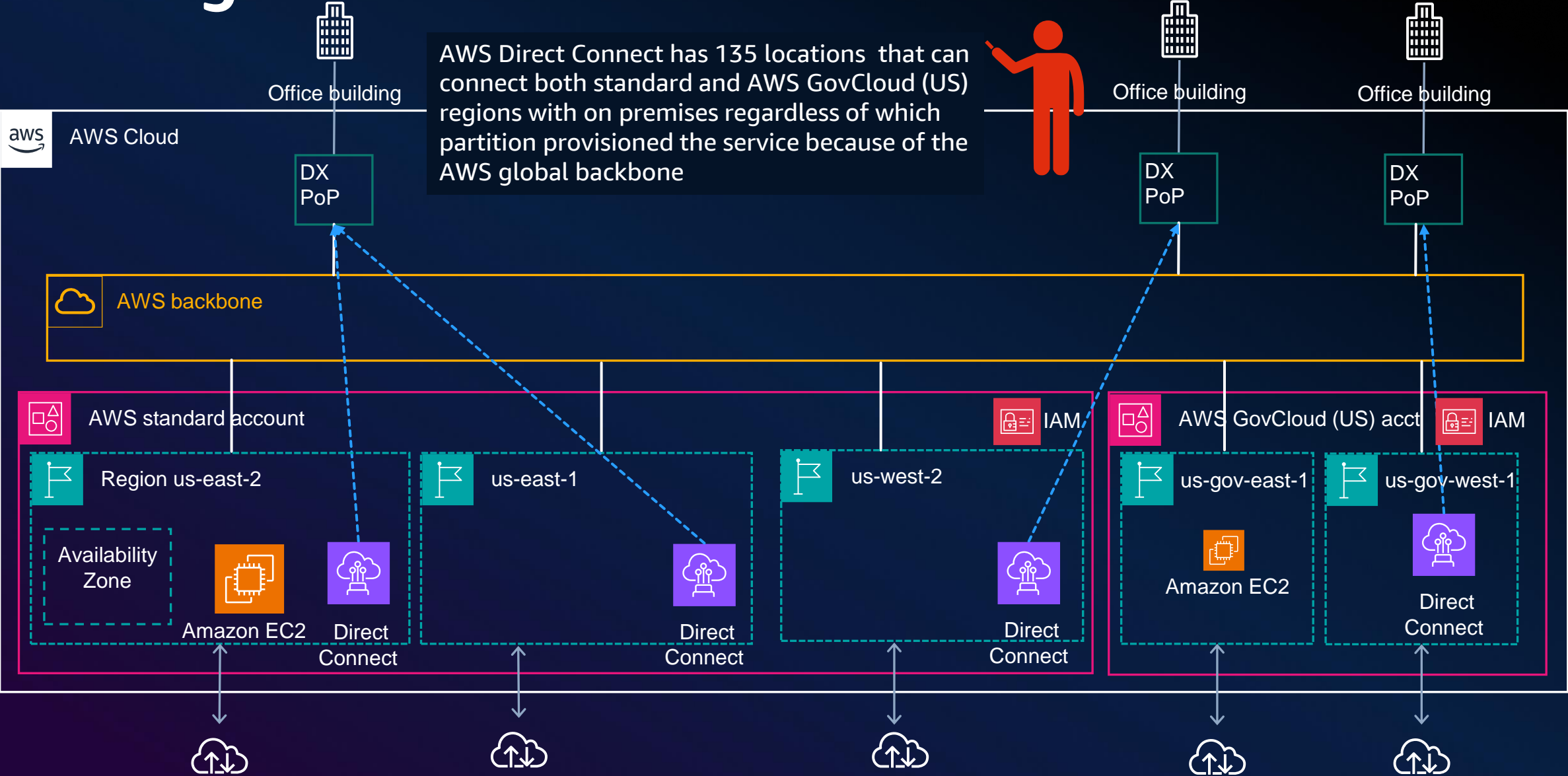


AWS edge network services

Route 53 has global presence with a 100% SLA for uptime availability which can resolve endpoints in AWS GovCloud (US)



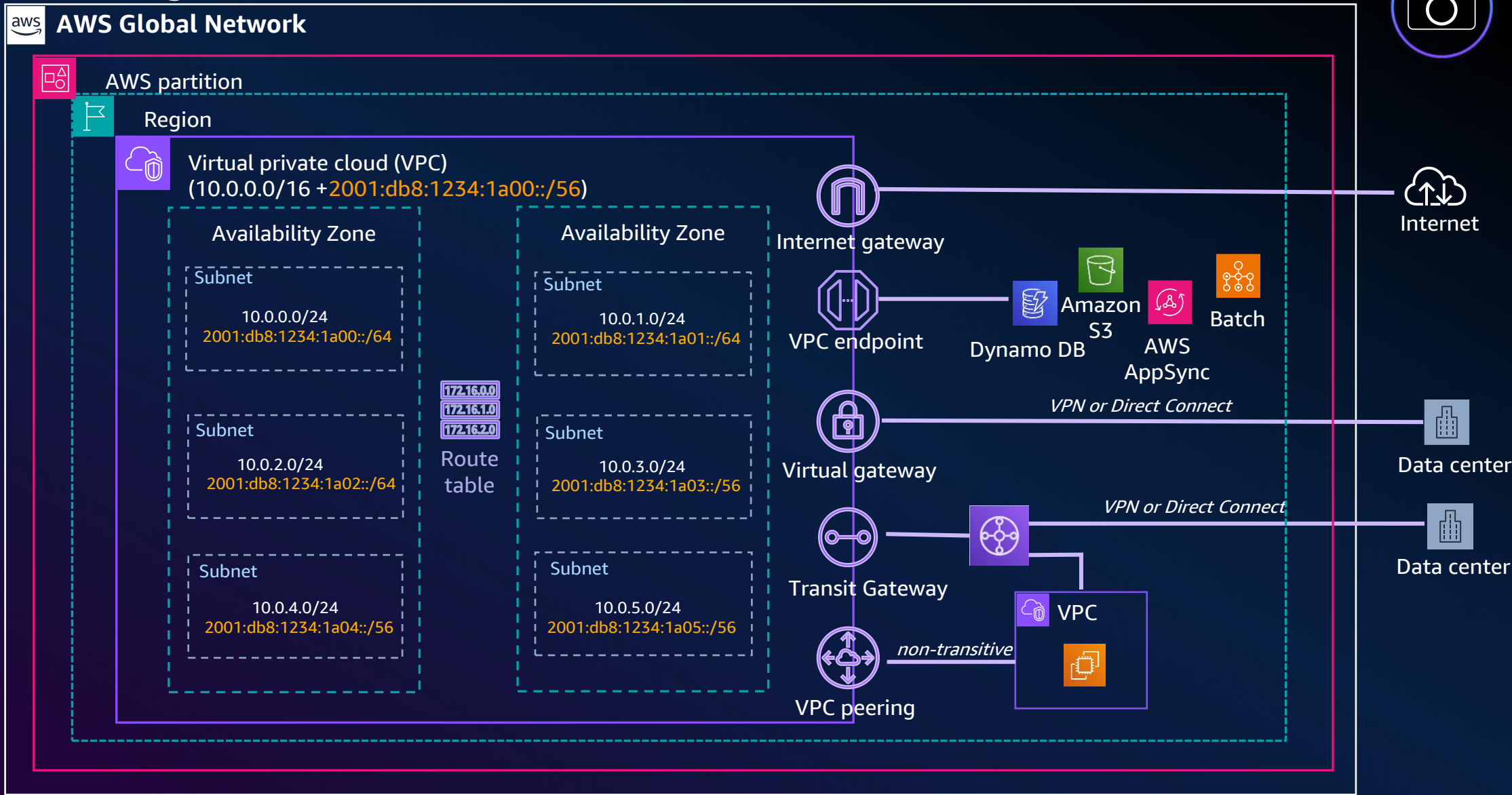
AWS edge network services



Building networks on AWS

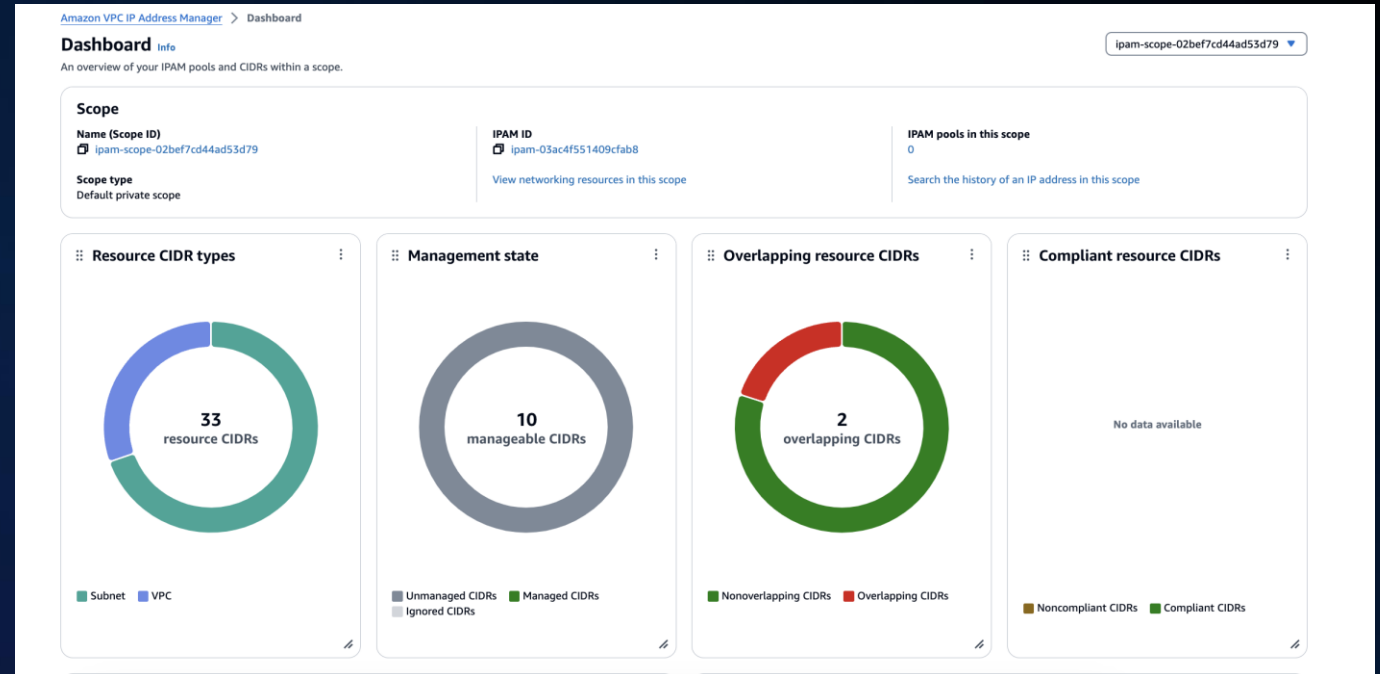


Anatomy of VPC



VPC IP Address Manager (IPAM)

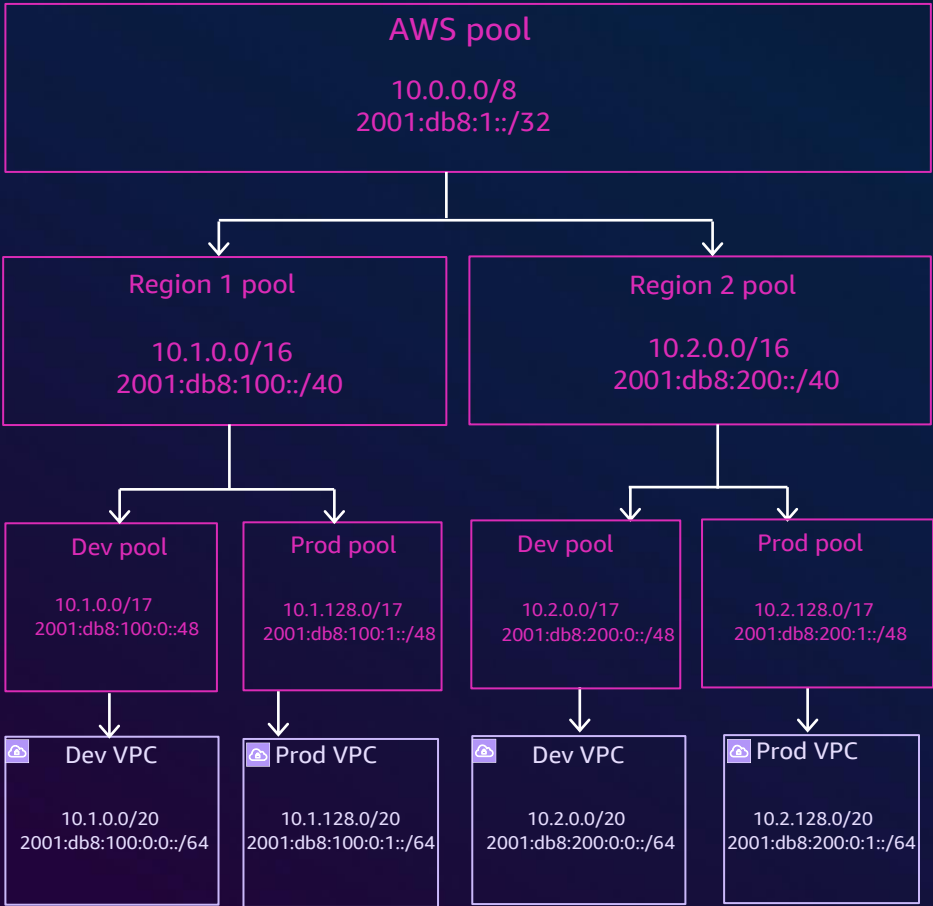
- Organize IP addresses
- Monitor IP address space
- View assignment history
- Allocate CIDRs to VPCs
- Troubleshoot
- Cross-Region BYOIP sharing



VPC IP address manager (IPAM)

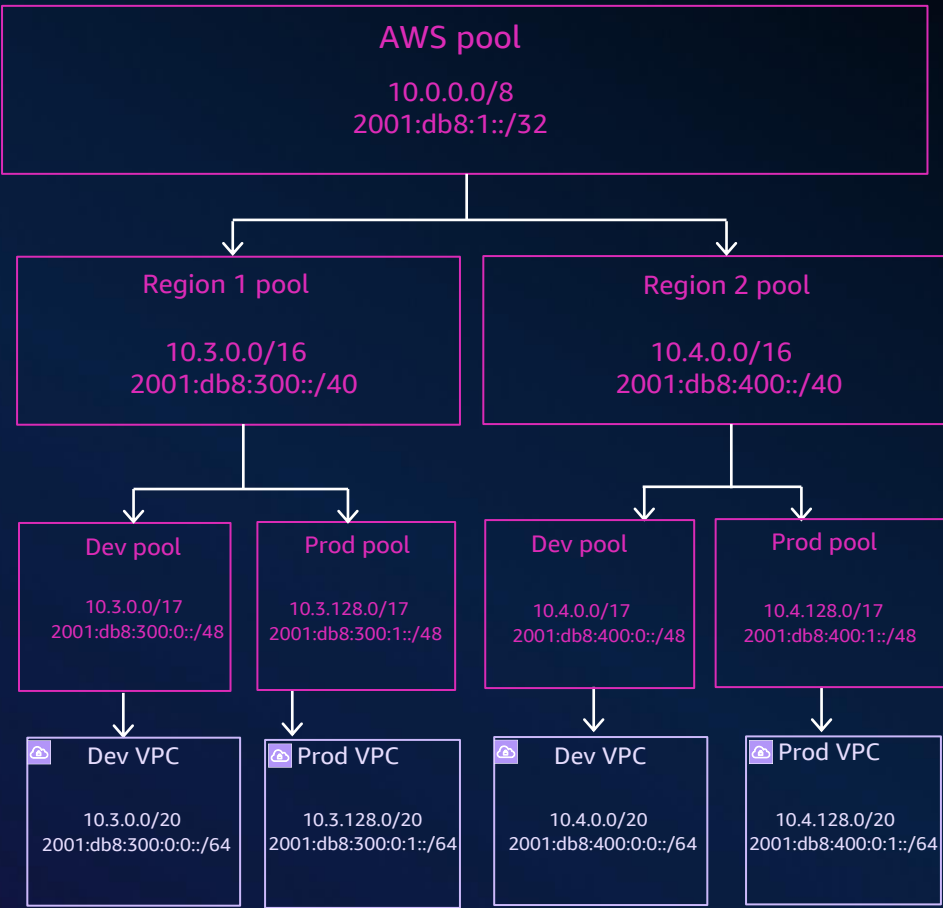
Standard partition

Multi-Region pool hierarchy



AWS GovCloud (US) partition

Multi-Region pool hierarchy



VPC IP Address Manager (IPAM)

Create IPAM [Info](#)

ⓘ We have detected you are not the IPAM delegated administrator of your organization. If you create an IPAM, it will only monitor resources in your account. If you want IPAM to monitor resources across your organization, the IPAM must be created in the delegated administrator's account. To set a delegated administrator, sign in as the management account of your organization and go to the Settings page.

Allow data replication [Info](#)

Amazon VPC IP Address Manager needs permission to replicate data from the member account(s) into the delegated admin account and from the operating Regions into the home Region. The delegated account will have access to resource and IP usage details from each of the member accounts and the Regions selected by those member accounts.

☐ Allow Amazon VPC IP Address Manager to replicate data from the member account(s) into the delegated admin account and from the operating Regions into the home Region.
You must select this checkbox to continue to create an IPAM.

IPAM tier

IPAM is offered in two tiers:
For information on what's included in each tier and pricing, see [Amazon VPC pricing > IPAM tab](#).

☐ Free Tier
Get started with IPAM. View public IPv4 usage across your Amazon Web Services Organization and manage public IP addresses in your account, at no cost.

☒ Advanced Tier
Get all the features offered in IPAM. Manage public and private IP addresses across your Amazon Web Services Organization. You will incur charges for your usage of IPAM.

ⓘ You pay an hourly rate for each active IP address that you manage using IPAM. An active IP address is an IP address or a prefix assigned to a resource such as an EC2 instance or an Elastic network interface (ENI).

IPAM settings [Info](#)

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

Description - optional
Write a brief description for the IPAM.

Operating Regions
Select Regions in which the IPAM will discover resources and manage IPs. The current Region will always be set as an operating Region.

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

IPv4 CIDR block [Info](#)

☐ IPv4 CIDR manual input

☒ IPAM-allocated IPv4 CIDR block

IPv4 IPAM pool

ipam-pool-01 (ipam-pool-02e863ebec73e5c36)
us-east-1 IPv4 Pool for demonstrations

Private ▼

The locale of the IPAM pool must be equal to the current region.

Netmask

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

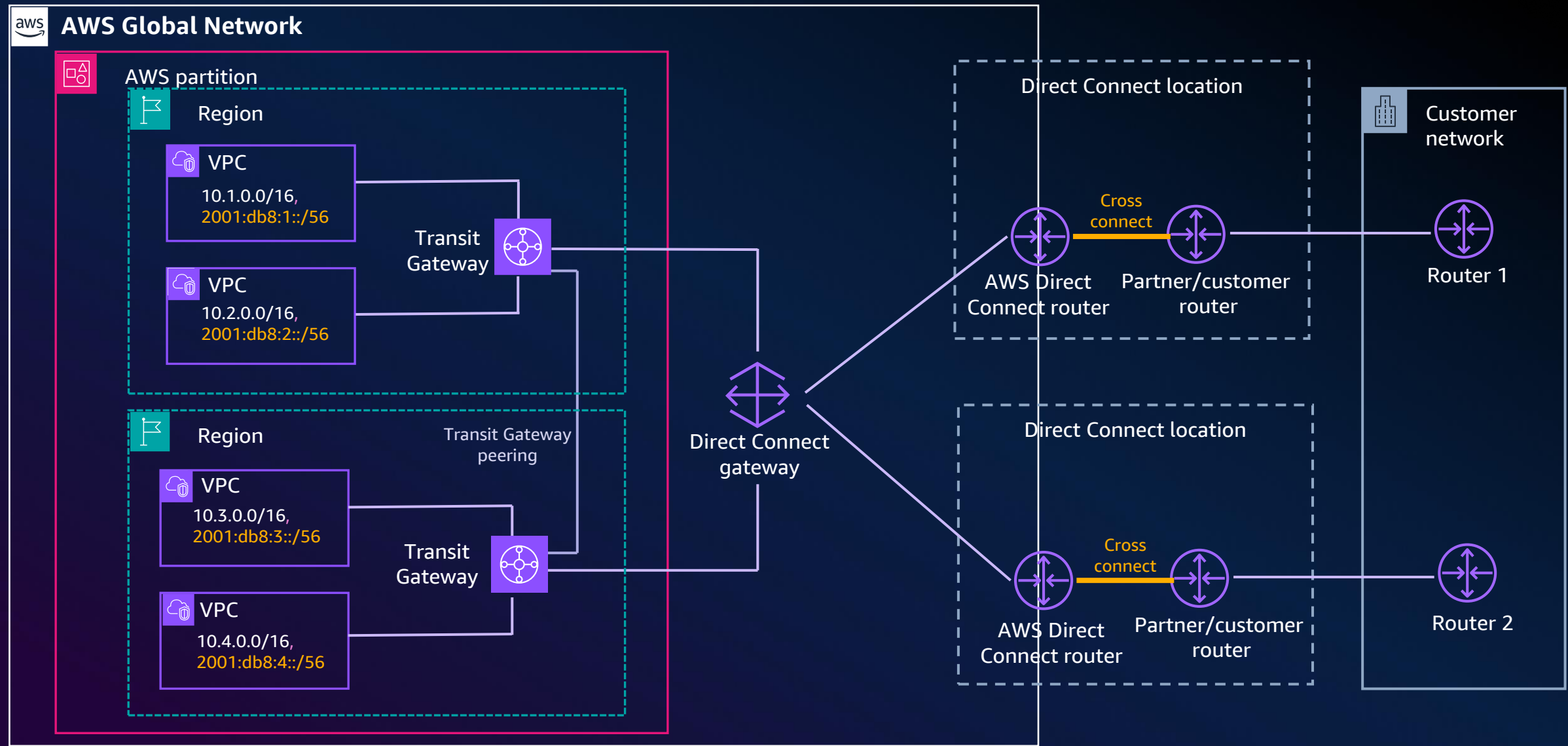
☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

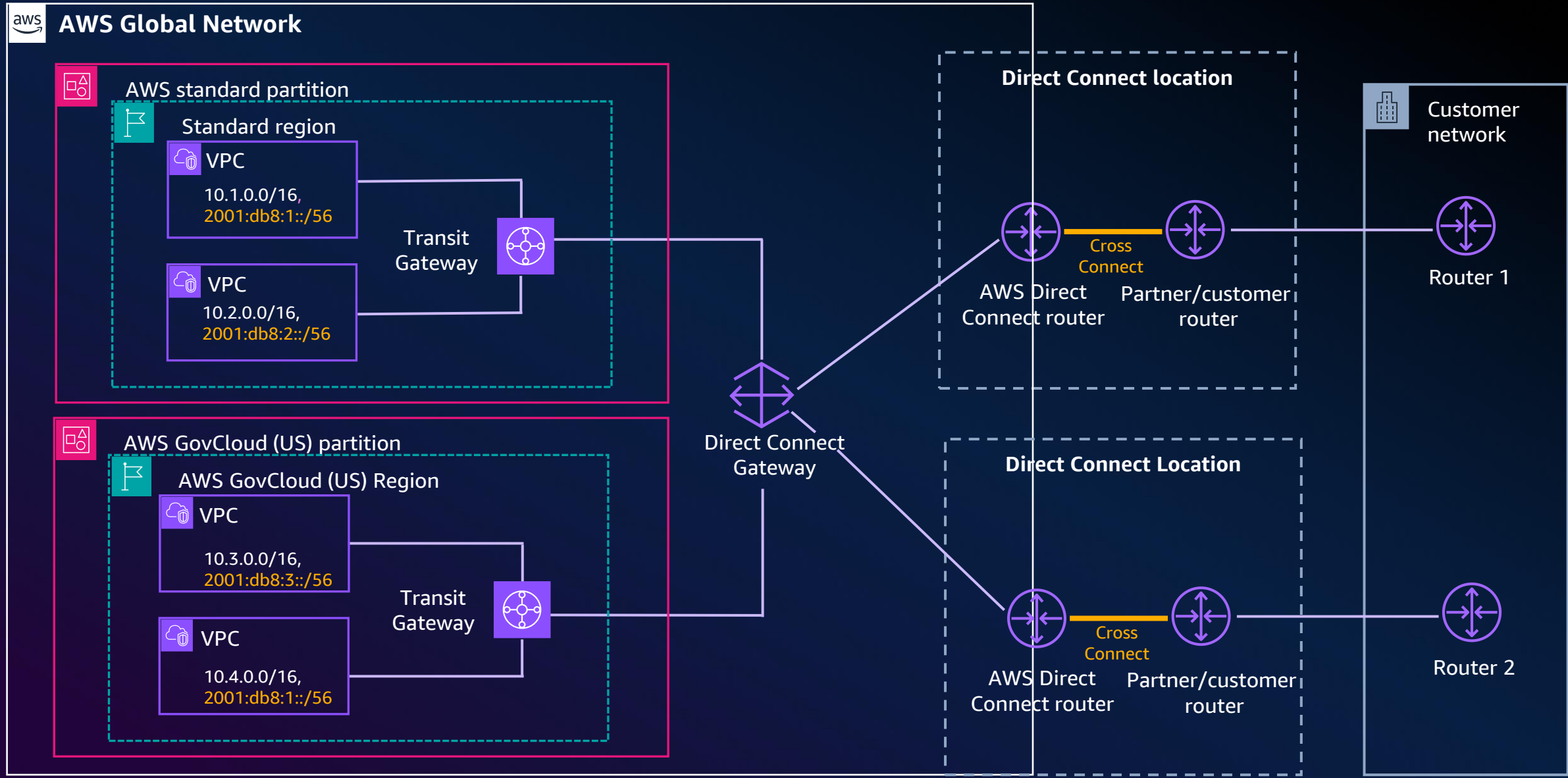
Tenancy [Info](#)

▼

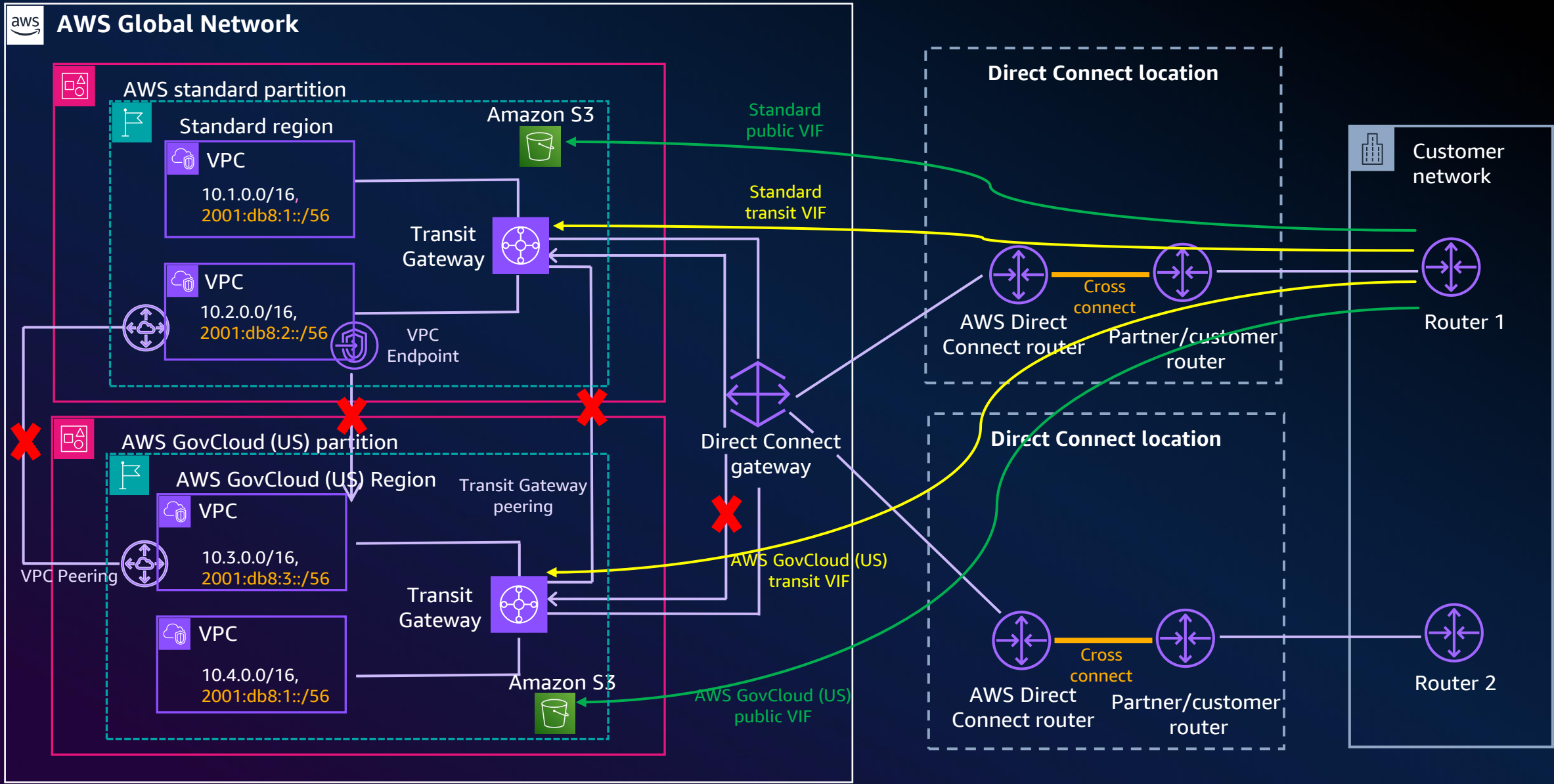
Hybrid connectivity – Single partition (Direct Connect)



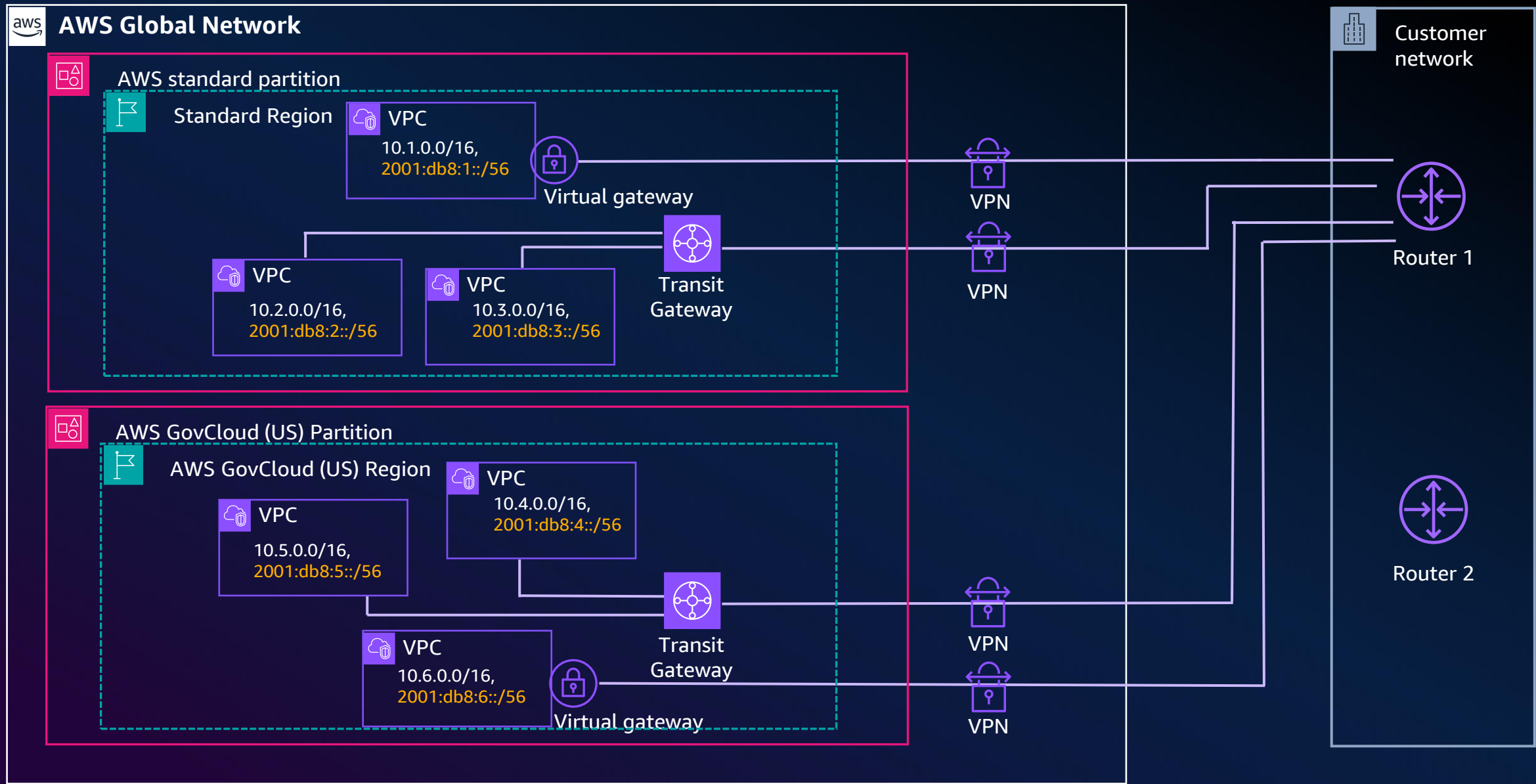
Hybrid connectivity – Multiple partitions (Direct Connect)



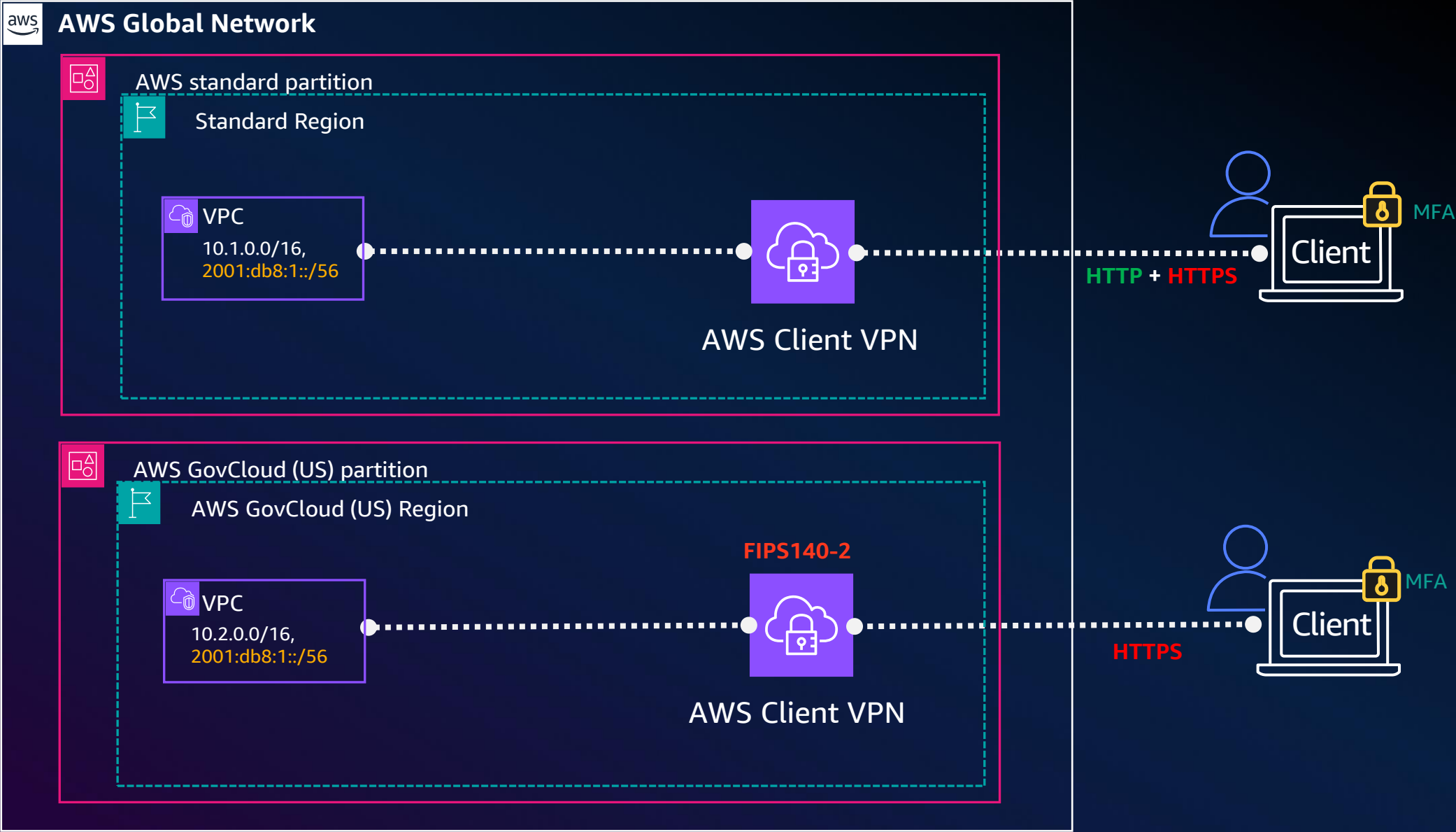
Partition isolation



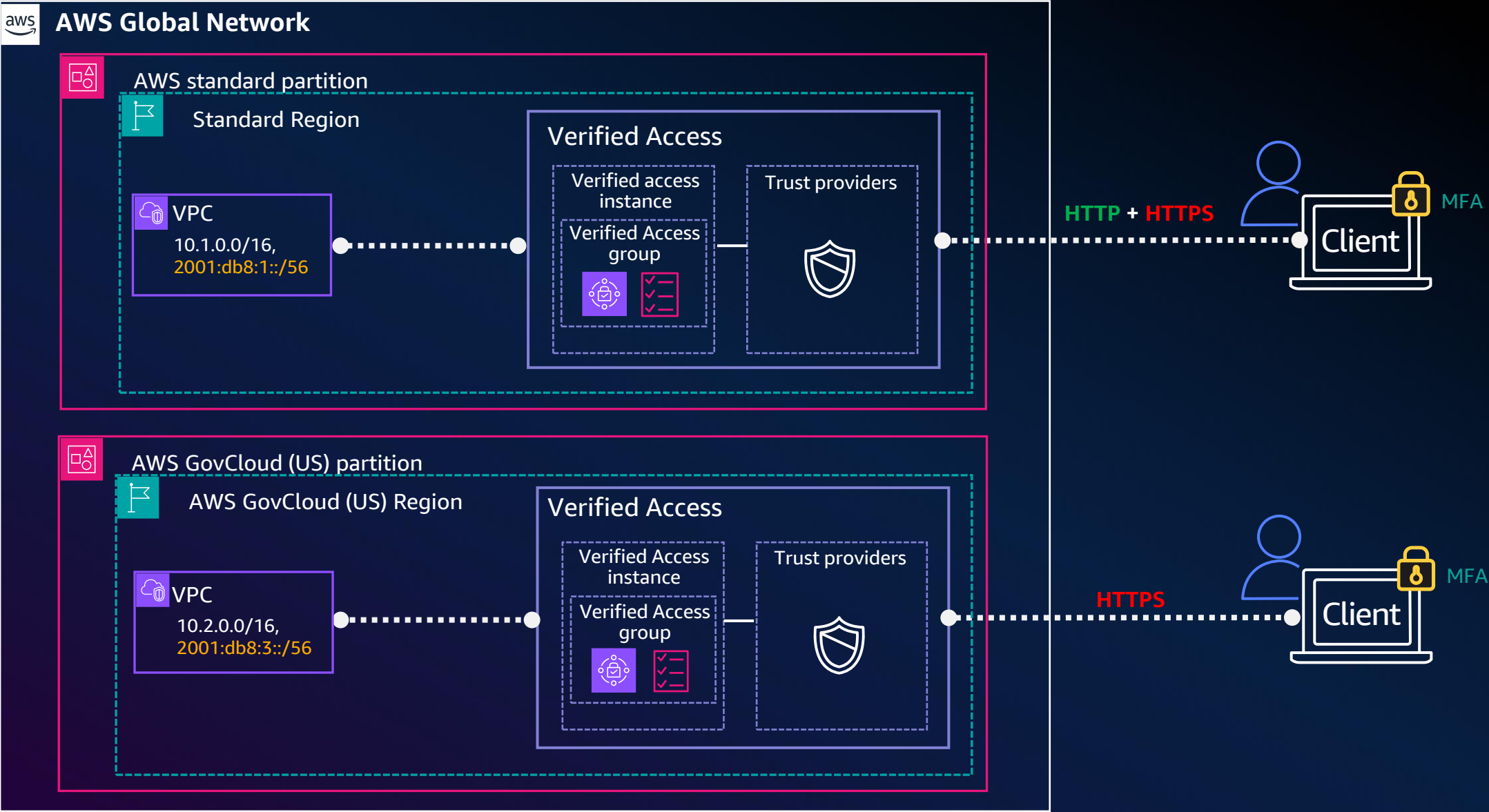
Hybrid connectivity – Multiple partitions (site-to-site VPN)



AWS Client VPN



AWS Verified Access

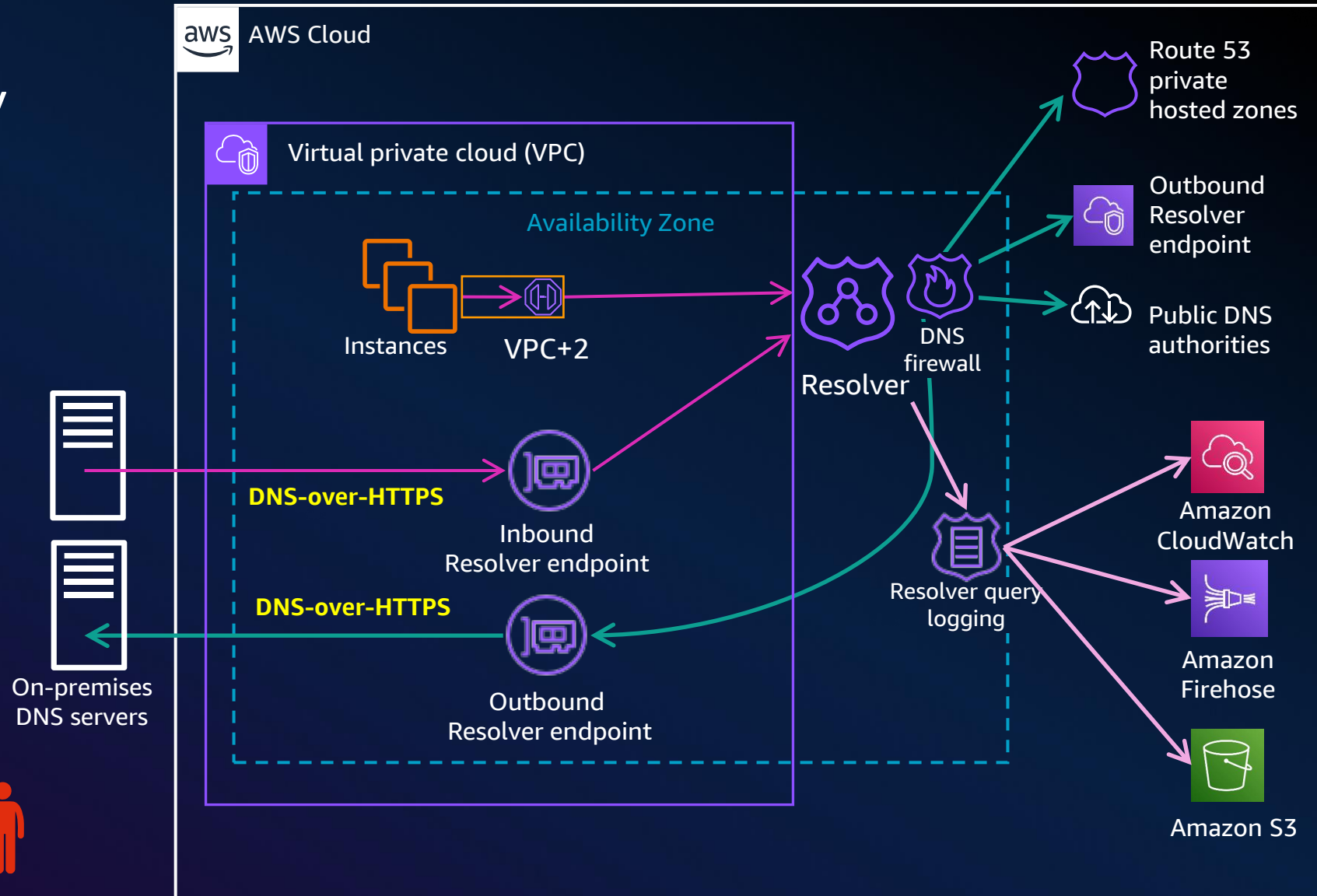


Public sector and DNS

Encrypted DNS

Use case: To meet security requirements, all DNS traffic must be encrypted

- US (M-22-09), UK, others
- DNS queries and responses transmitted encrypted
 - DNS-over-HTTPS
- FIPS inbound endpoint



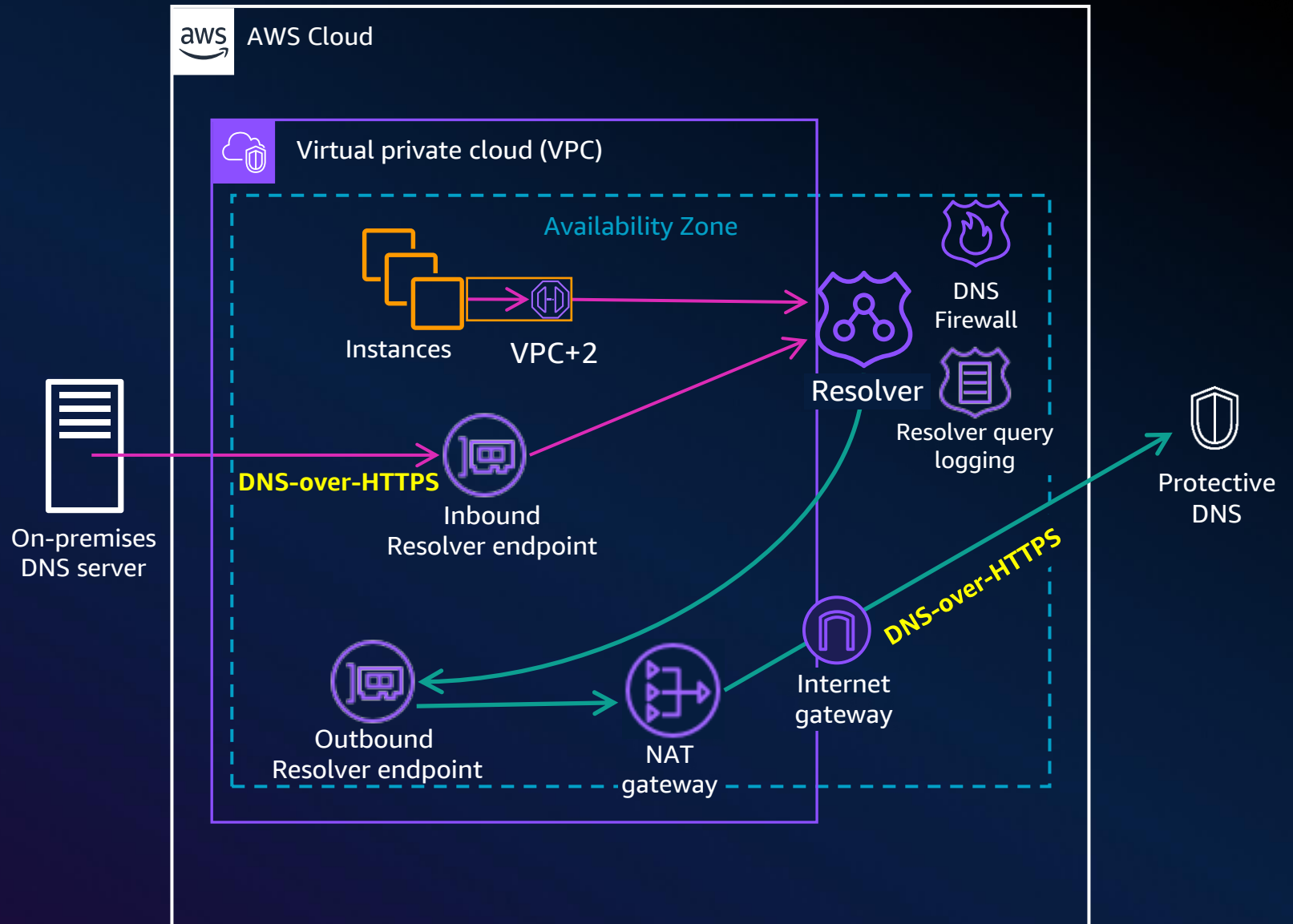
DNSSEC is not encrypted DNS



Encrypted DNS to protective DNS

Use case: All DNS queries sent to a protective DNS service

- Route 53 Resolver outbound endpoint + NAT gateway



Route 53 profiles

Use case: Similar configuration of Route 53 resources across many VPCs and accounts

- Profile can hold:
 - Private hosted zones
 - Route 53 Resolver rules
 - DNS Firewall rule groups
 - VPC DNS-related configurations
- Share across accounts with AWS Resource Access Manager (AWS RAM)
- Consistent resource enforcement and management across orgs
- Easy migration with local setting priority



Route 53 profiles

Route 53 > Profiles > Secure

Secure

Info

Delete

Share profile

You can associate DNS related resources to a profile, and then associate the profile to VPCs.

Overview

DNS Firewall rule groups

0

Private hosted zones

1

Resolver rules

0

VPCs

0

Profile Id

Owner Id

Last updated

rp- Owner Id May 15, 2024 12:04 PM (UTC-04:00)

DNS Firewall rule groups (0)

Private hosted zones (1)

Resolver rules (0)

VPCs (0)

Tags (0)

Configuration

Private hosted zones

Info

Disassociate

Associate

The associated private hosted zones determine how you want to route DNS traffic within and among your VPCs.

Find associations

< 1 >

Association name	Associated resource ARN	Status
	arn:aws:route53::hostedzone:	Associating

- DNS Firewall rule groups
- Private hosted zones
- Route 53 Resolver rules
- VPC DNS-related configurations

- VPC DNS-related configuration priority

Configuration status was updated successfully

Route 53 > Profiles > Secure

Secure

Info

Delete

Share profile

You can associate DNS related resources to a profile, and then associate the profile to VPCs.

Overview

DNS Firewall rule groups

0

Private hosted zones

1

Resolver rules

0

VPCs

1

Profile Id

Owner Id

Last updated

rp- Owner Id May 15, 2024 12:04 PM (UTC-04:00)

DNS Firewall rule groups (0)

Private hosted zones (1)

Resolver rules (0)

VPCs (1)

Tags (1)

Configuration

Configuration (3)

Edit

Applied configuration	Option
DNS Firewall failure mode configuration	Enabled
Resolver reverse DNS lookup configuration	Use local resource setting
DNSSEC configuration	Enabled

Multi-partition patterns and solutions

Multi-partition service solutions

Scenario: Route 53 public hosted zones for AWS GovCloud (US) systems

Route 53 > Hosted zones > aws-summit-demonstration.com > Create record

Create record [Info](#)

Quick create record [Switch to wizard](#)

▼ Record 1 [Delete](#)

Record name [Info](#) aws-summit-demonstration.com Record type [Info](#)

Keep blank to create a record for the root domain.

☒ Alias

Route traffic to [Info](#)

Routing policy [Info](#)

Evaluate target health ☒ No

Copy and paste the Amazon generated DNS record name in for the endpoint or use the AWS CLI to create the alias record



Common AWS GovCloud (US) networking use cases

Scenario: Host a serverless Amazon S3 static website hosting on AWS GovCloud (US) while complying with export controls?

Option A – CloudFront integration

Option B – Application Load Balancer integration

Amazon CloudFront Global Edge Network

GLOBAL NETWORK

Redundant 400 GbE network and private capacity between all regions except for the AWS China*

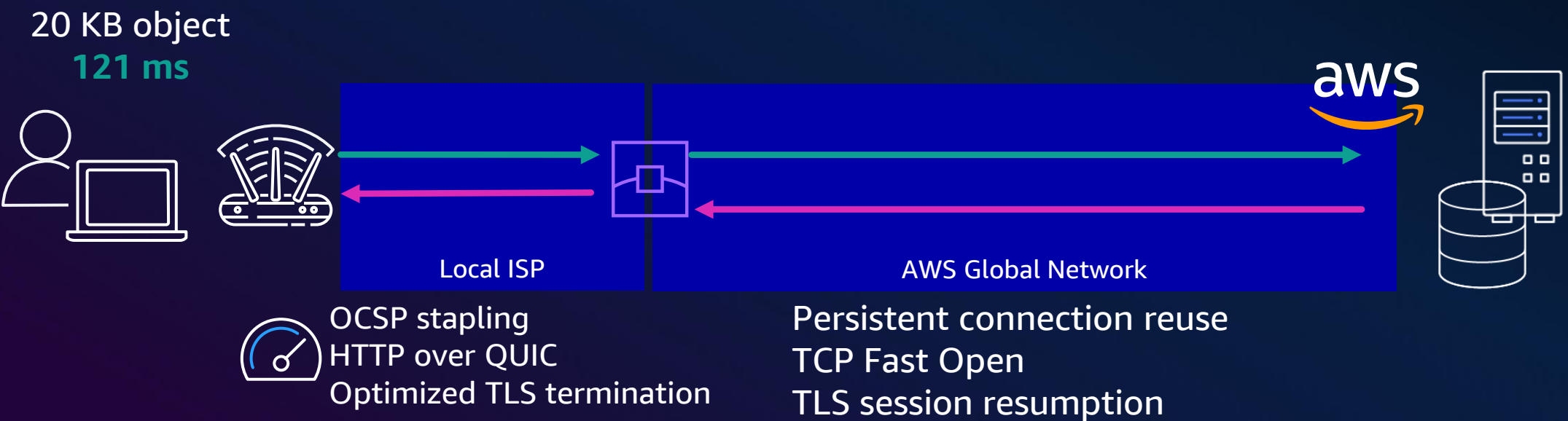
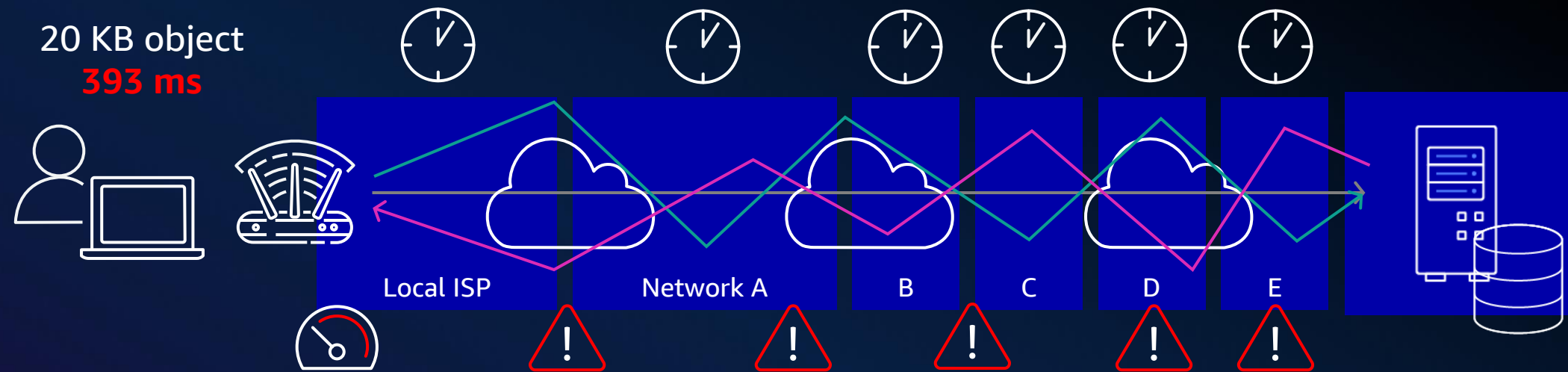
EDGE NETWORKING

600+ PoPs in 50 countries and 100+ cities, with direct peering to all major ISPs

KEY

- AWS GovCloud (US) Regions
- Edge location
- Multiple edge locations
- Regional edge caches

CloudFront: Dynamic content acceleration



Amazon CloudFront with AWS GovCloud (US) and Amazon S3

Scenario: Optimize and secure serverless web hosting out of AWS GovCloud (US)

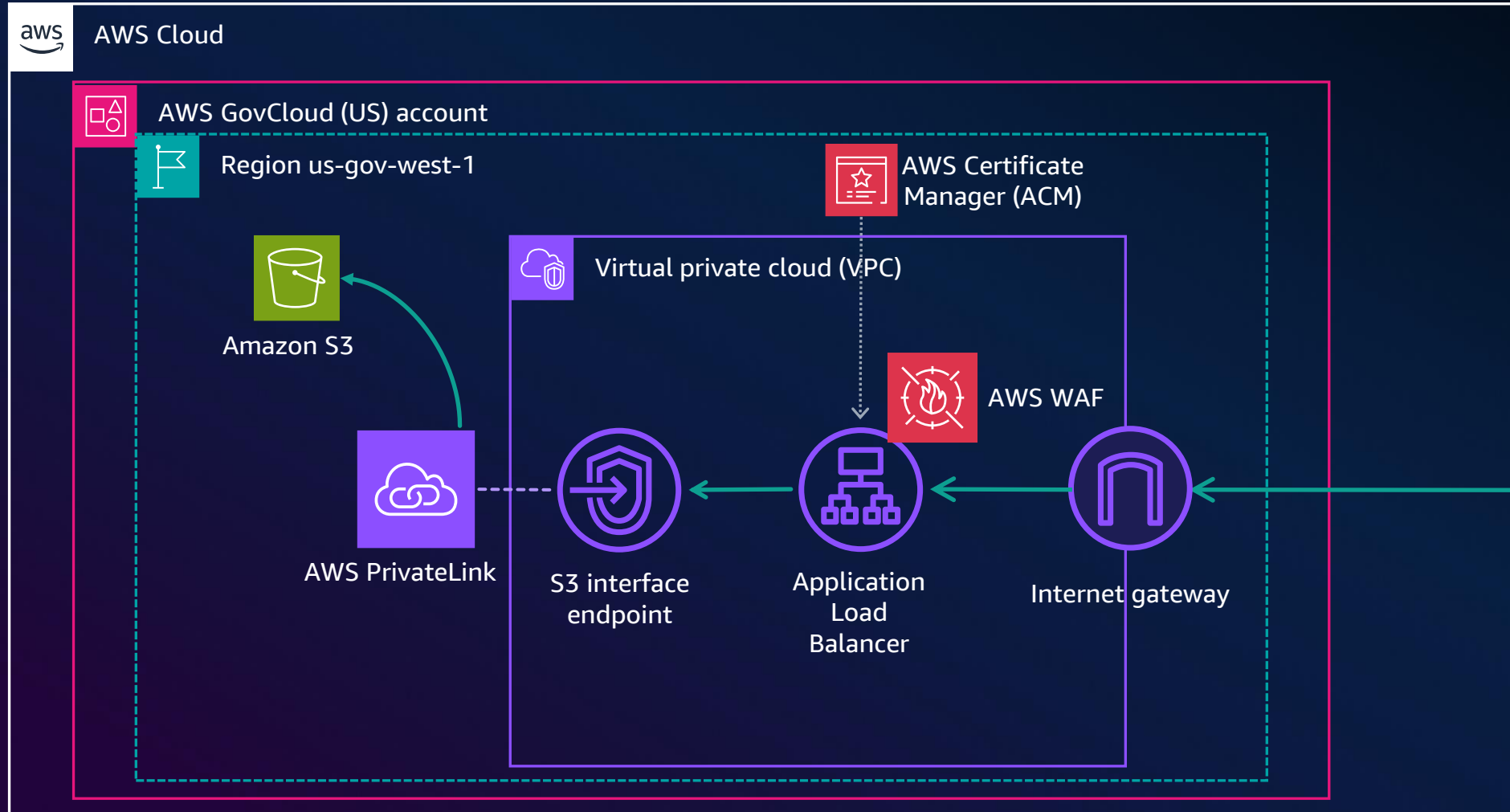


CloudFront can be used with to improve performance of dynamic, non-cached content with AWS GovCloud (US) origins. Review the AWS GovCloud (US) user guide for more details.



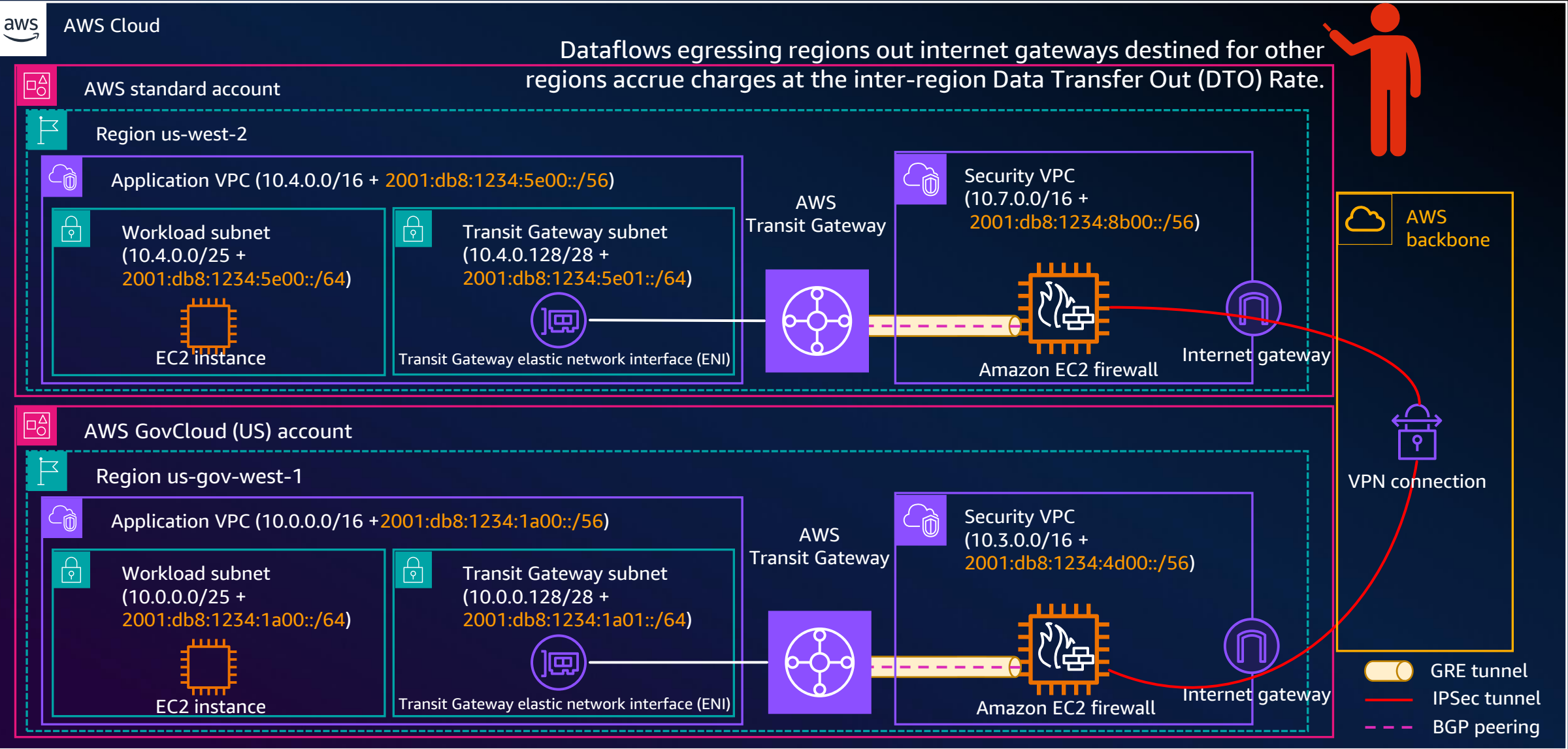
AWS GovCloud (US) Application Load Balancer

Scenario: Use only AWS GovCloud (US) resources and services for serverless, secure website hosting



[Hosting internal HTTPS static websites with Application Load Balancer, Amazon S3, and PrivateLink](#)

Cross partition private connectivity



Key takeaways

1. AWS partitions are separated **control plane** credentials and services that help customers to configure and control *physically* separated infrastructure
2. AWS standard and AWS GovCloud (US) partition-hosted services can intercommunicate over the network **data plane** *when configured by customers*, through the AWS global backbone
3. Reach out to an AWS solutions architect for more information and guidance on how to create optimized solutions

skillbuilder.aws 

Build beyond

Create a free account
on AWS Skill Builder to
gain in-demand skills