AWS re:Invent

DOP320-R

Strategies for securing code in the cloud and on premises

Lee Packham
Senior Developer Advocate
Amazon Web Services

Craig Smith
Senior Solutions Architect
Amazon Web Services

AWS re:Invent

aws

Related breakouts

EUC321 – Getting started with Amazon WorkSpaces Linux

CON320 – CI/CD pipeline integration using AWS native tools

DOP202 – Implementing GitFlow with AWS tools

NET333 – Building hybrid architectures with AWS Transit Gateway, AWS Direct Connect, and VPNs

NET412 – Become an AWS VPN and AWS Direct Connect expert

Hello world

A familiar story

- Already using version control systems on premises
- Want to use the cloud but don’t want to move their code
- Or want to move their code, but information security teams won’t let them

Definitions

Source code

Source code

- The design of your systems and software
- High level for readability
- Business logic
- Valuable intellectual property

Building code

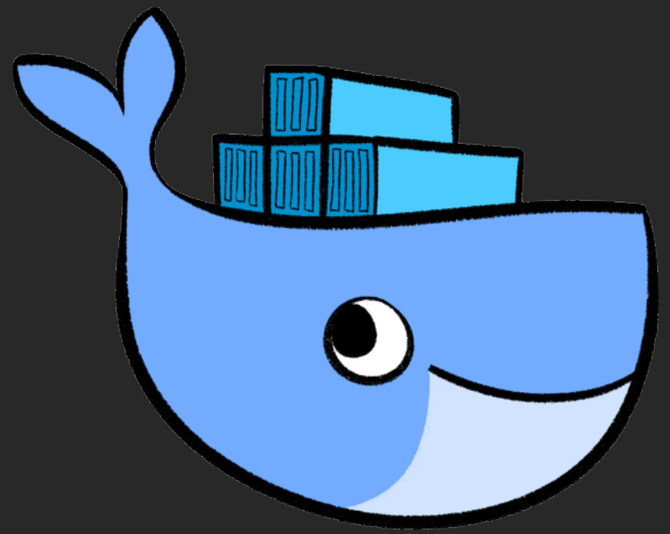
Building code

Who remembers builds that took days?

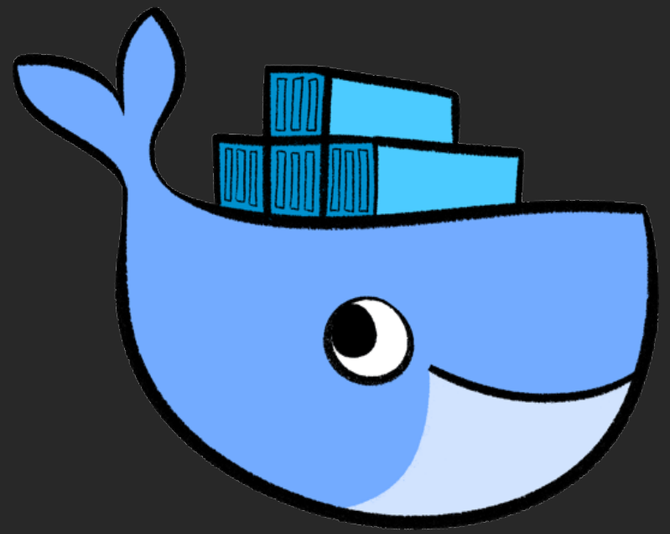
Building code

- Translation of higher-level source code into what a processor can run
- The higher-level the language, generally the slower the compiler is
- Using the cloud has changed how we build software

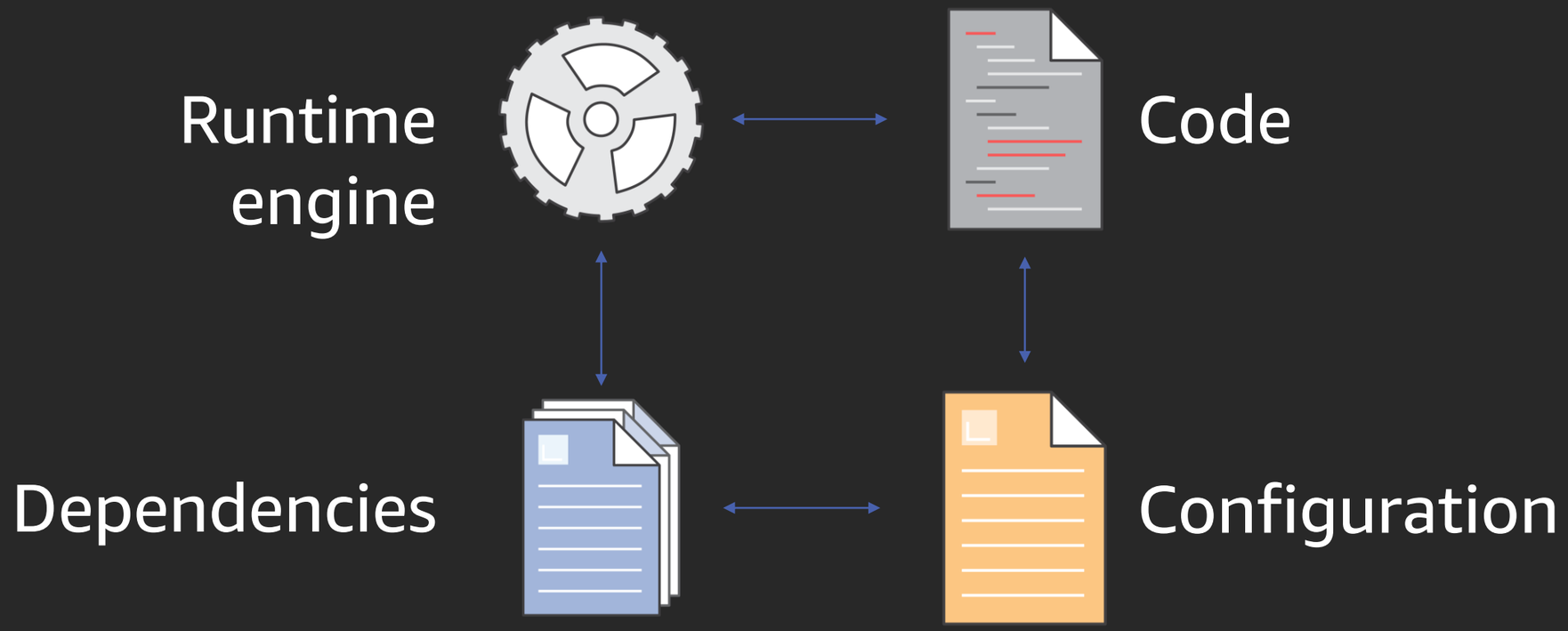
Containers



Why containers?



Application environment components

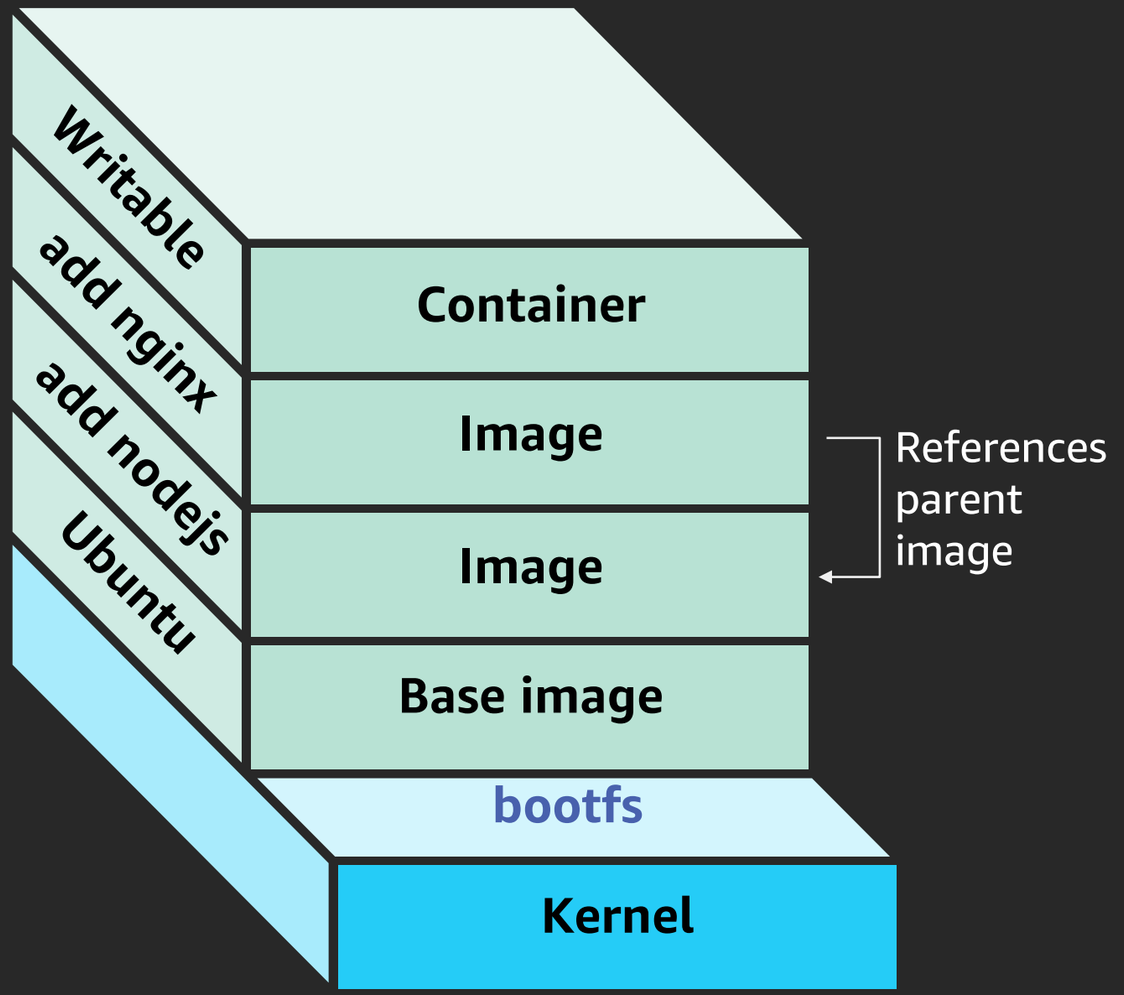


Docker container image

Read-only image that is used as a template to launch a container

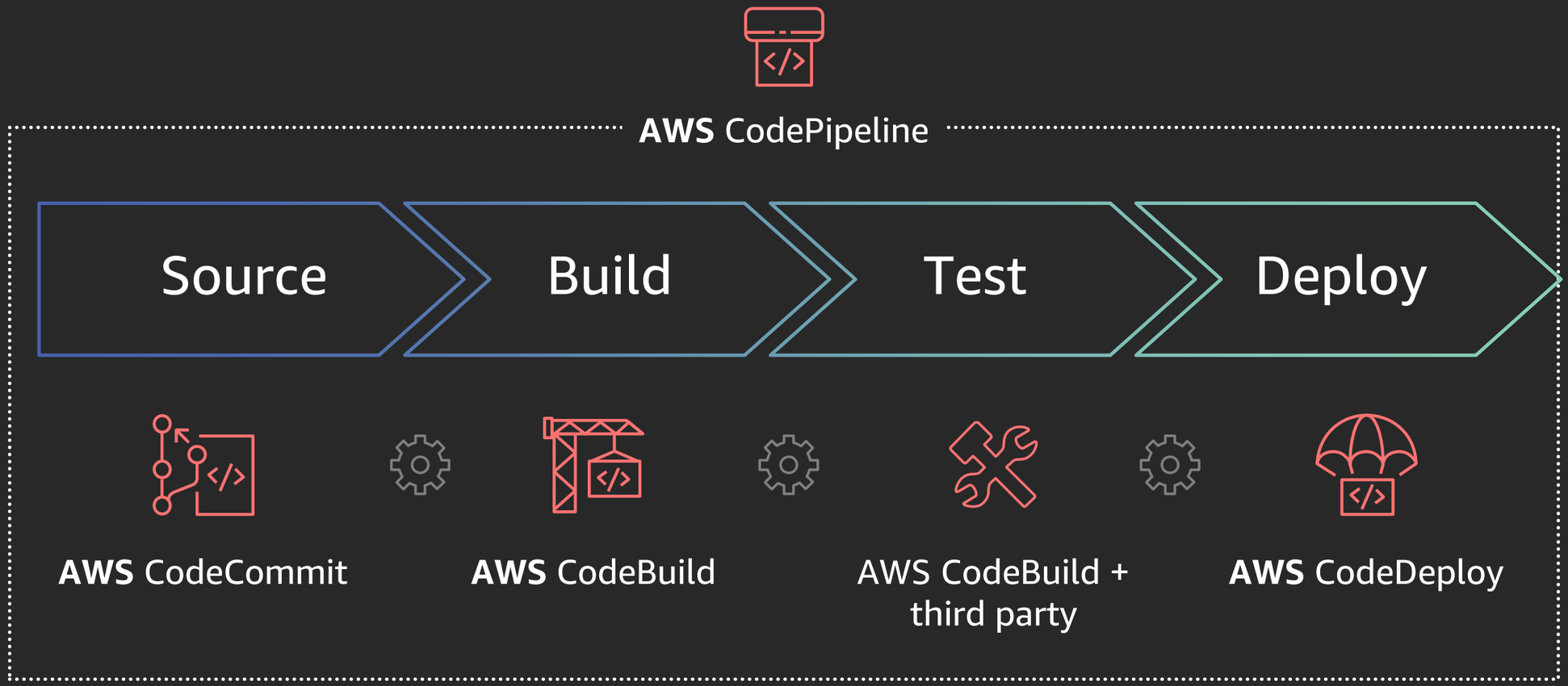
Start from base images that have your dependencies, and add your custom code

Docker file for easy, reproducible builds



Code lifecycle

Development cycle



AWS CodeCommit

- Fully managed source control service with encryption at rest and in transit that hosts secure Git-based repositories
- Supports all Git commands and works with your existing Git tools
- Highly scalable, redundant, and durable architecture
- Serverless – no servers needed to run
- No public repositories

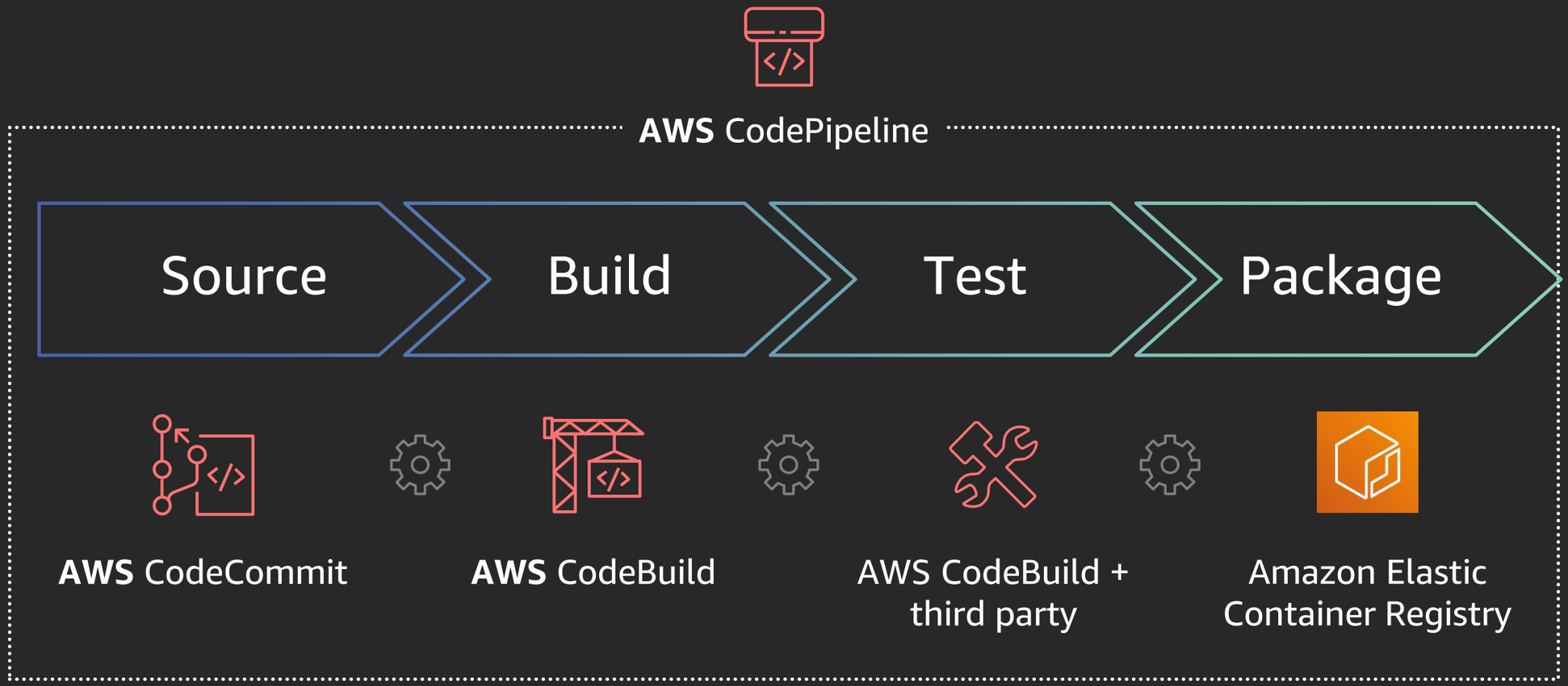
AWS CodeBuild

- Fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy

- Scales up and down automatically to meet your build volume

- Charged based on the number of minutes it takes to complete your build

Development cycle



Amazon Elastic Container Registry

- Fully managed Docker container registry
- No software to install and manage or infrastructure to scale
- Highly scalable, redundant, and durable architecture

Connectivity

What are we going to talk about?

What are the options for connectivity?

Where does AWS PrivateLink help?

The quick version!

Connecting from where you are to AWS

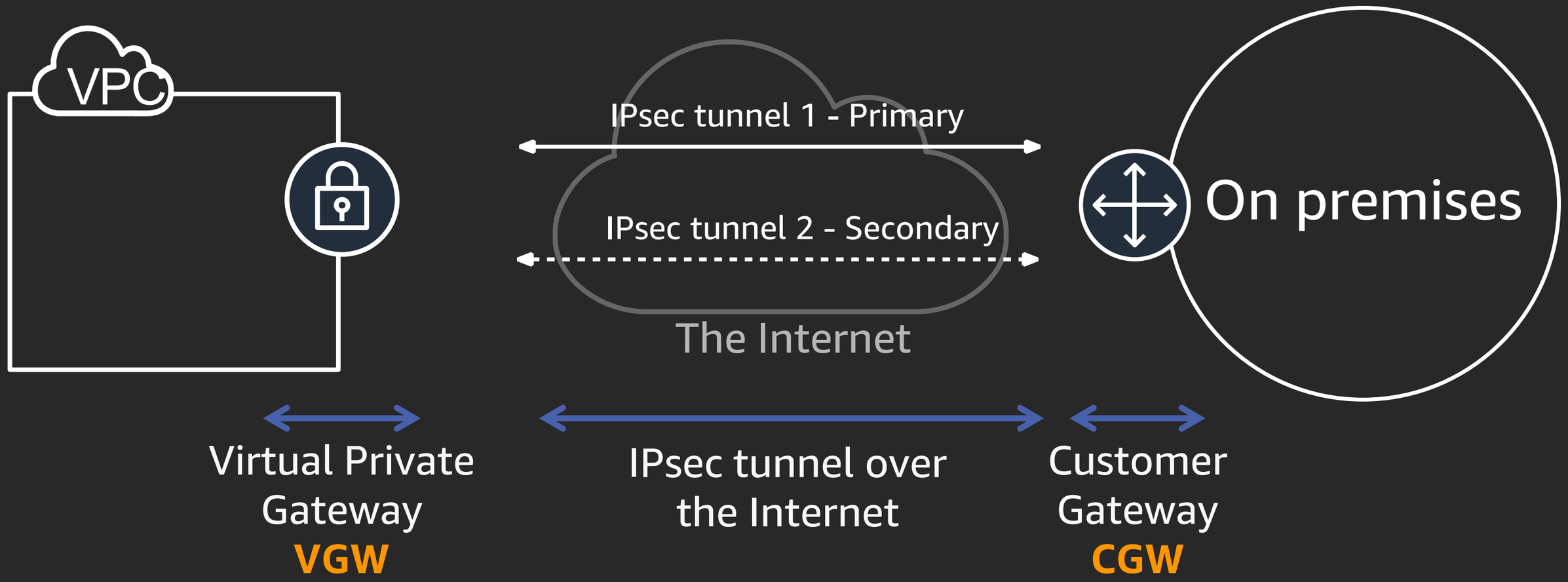
Internet

AWS Site-to-Site VPN

AWS Direct Connect

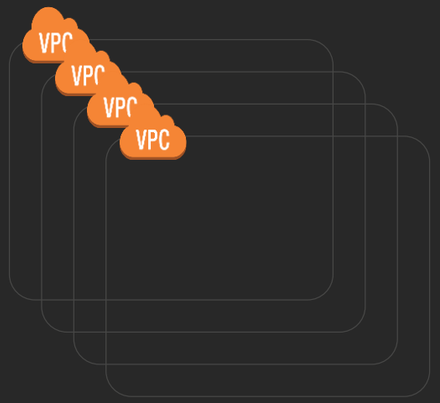
AWS Client VPN

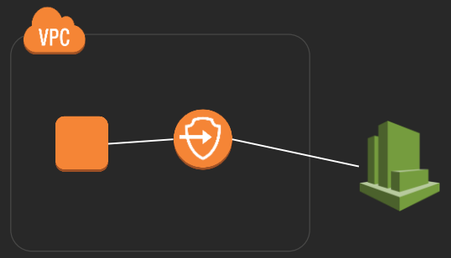
AWS Site-to-Site VPN



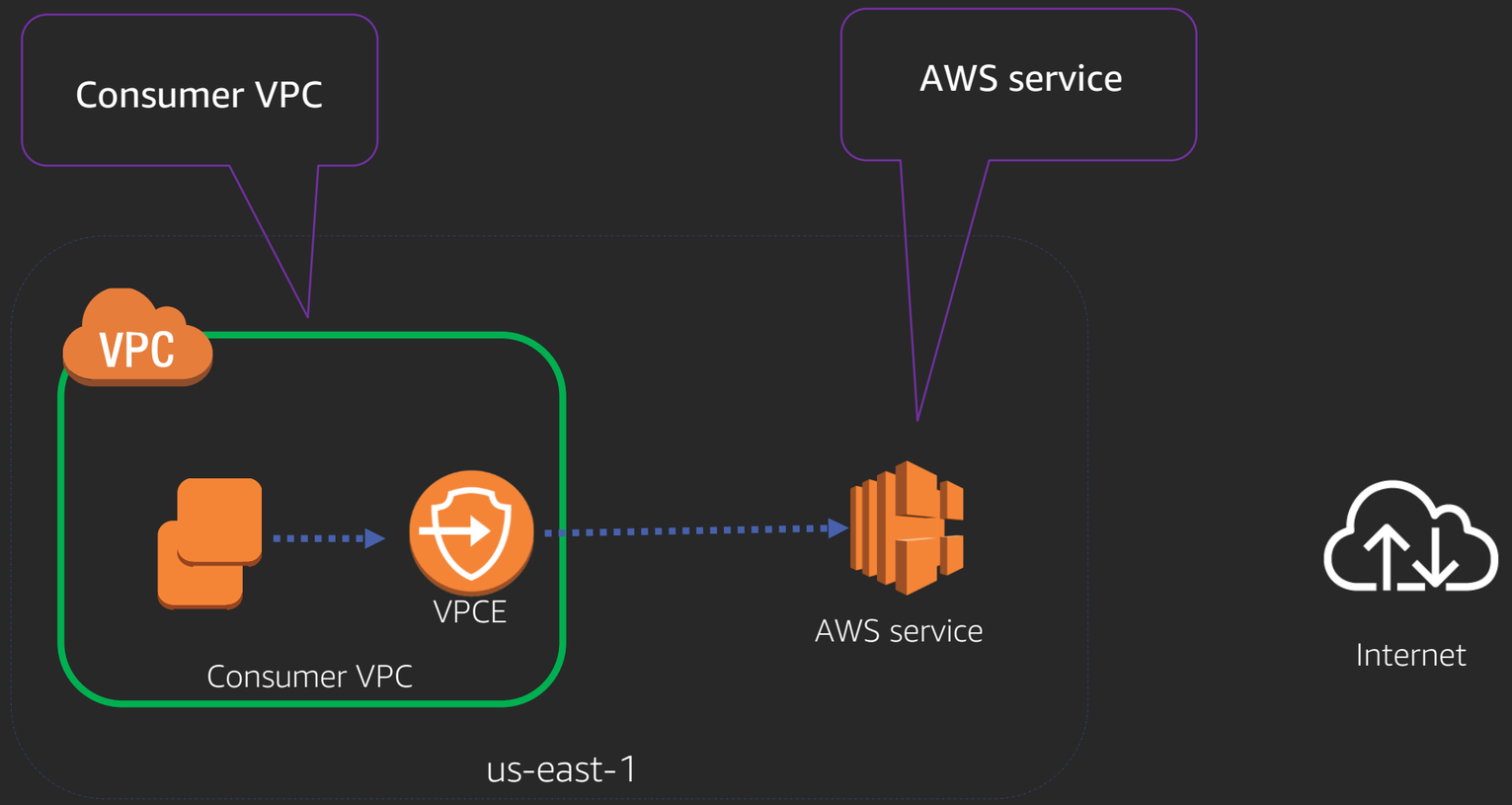
Let’s talk about AWS PrivateLink

- Customers have many VPCs
- Need private connectivity between VPCs
- Access to AWS services through private IPs
- Desire to limit/remove the need for IGWs

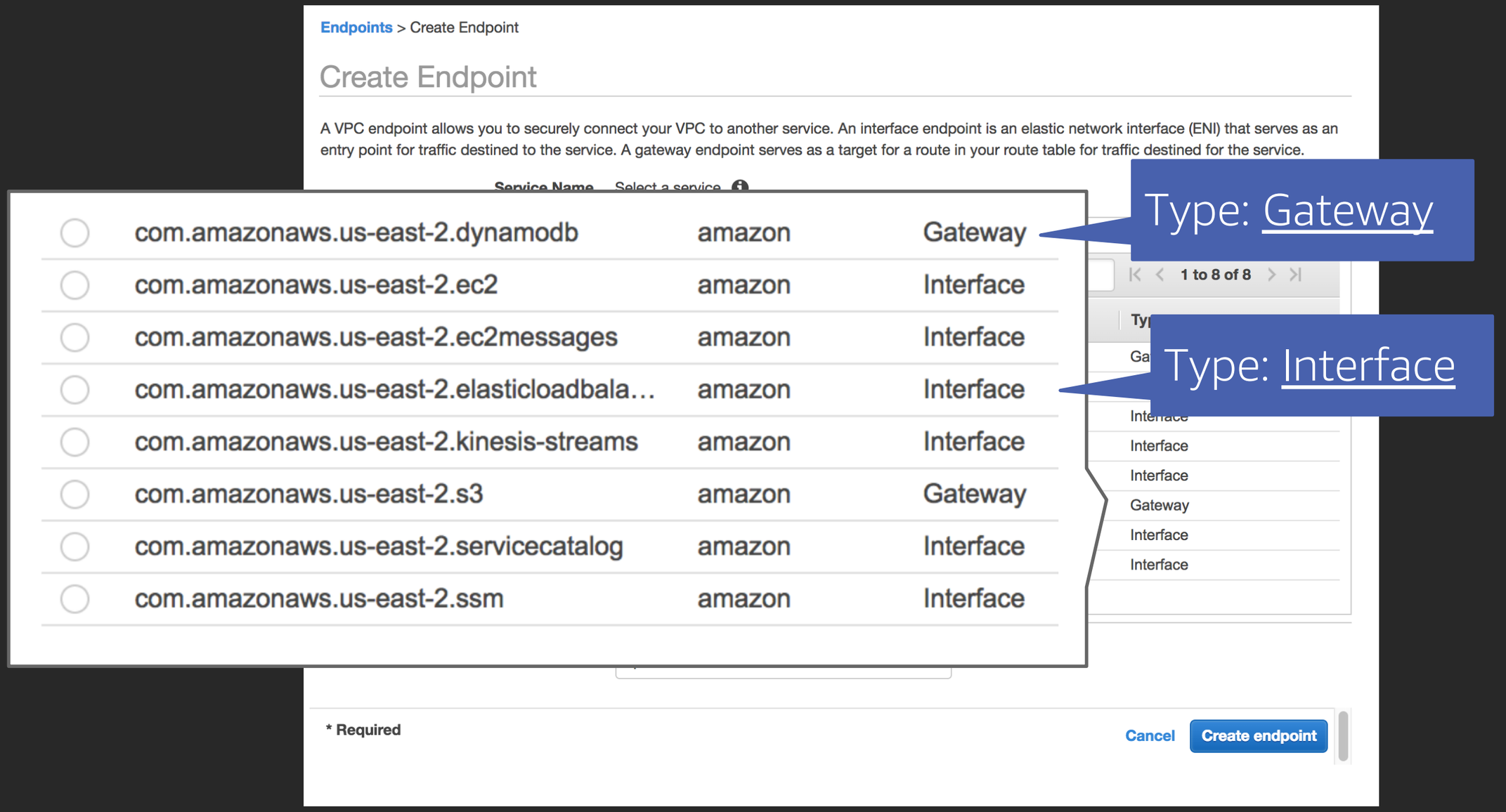




How it works for AWS services



VPC endpoints

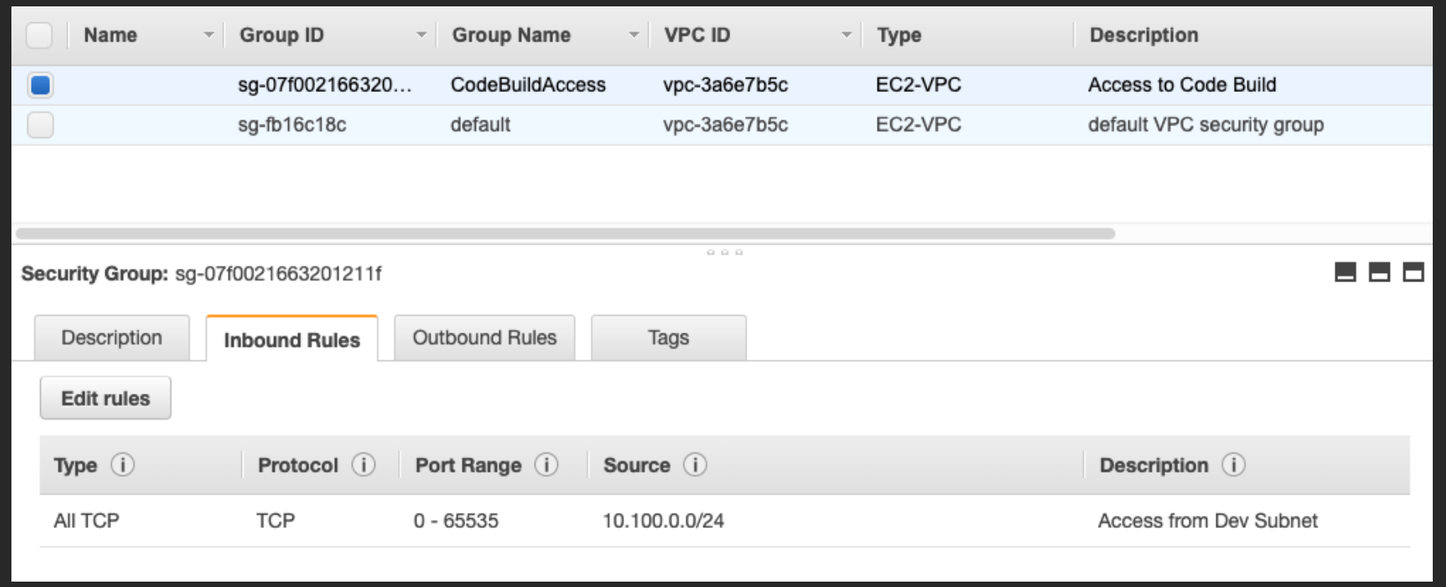


Control access from your VPC

VPC endpoint policies

- Access based on IAM users and roles
- Must contain principal
- Supported by AWS CodeBuild and AWS CodeCommit

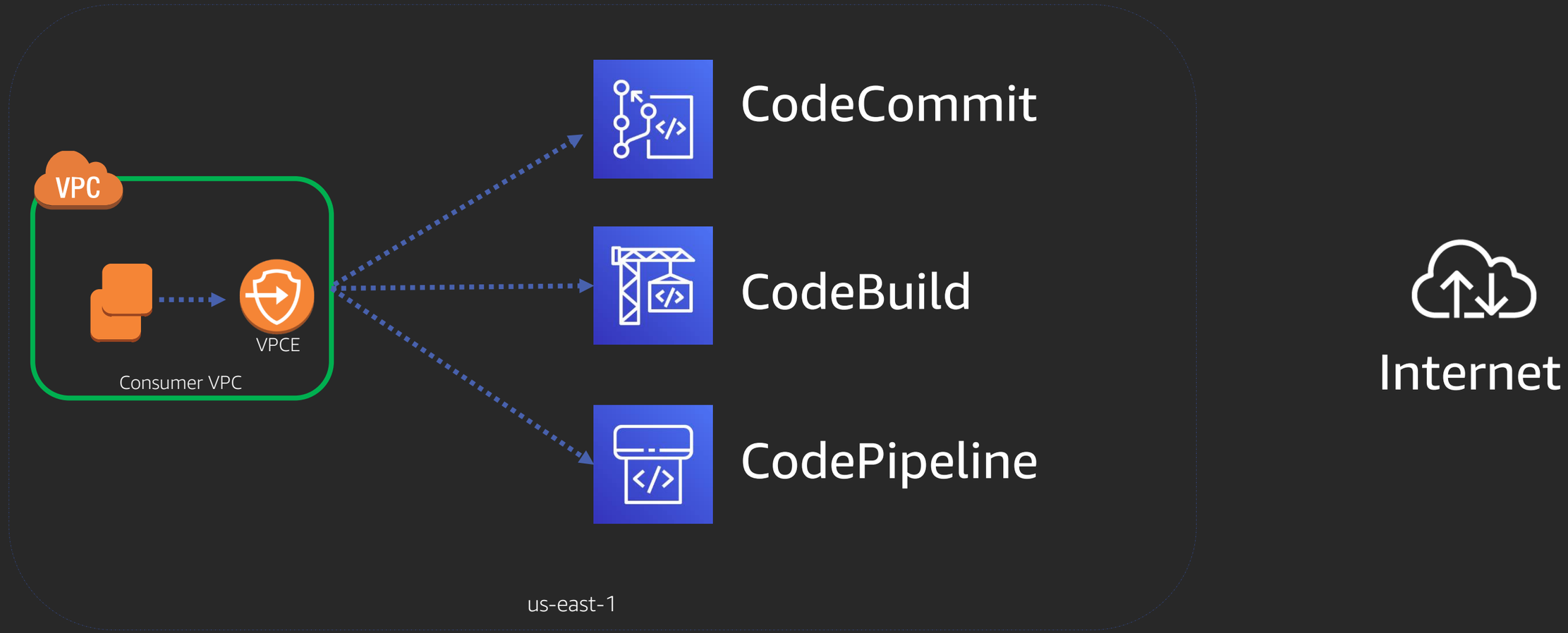
Attach a security group



Restricting subnet access to endpoints

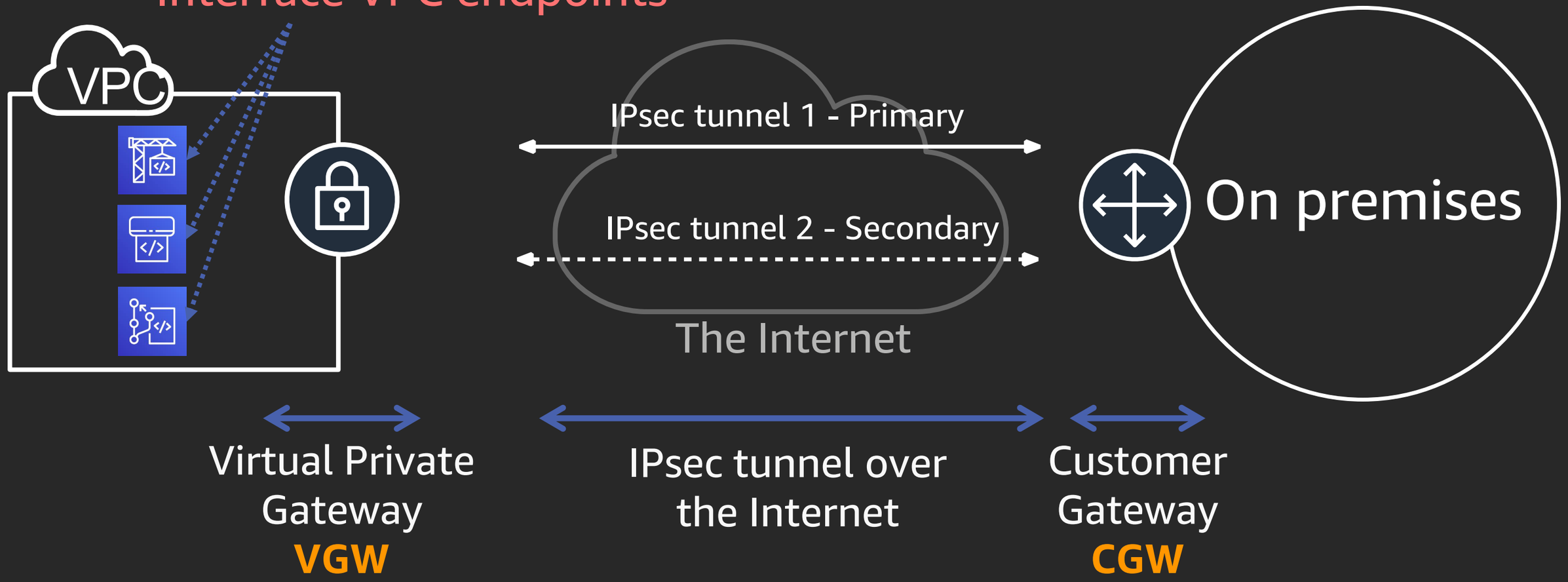
Private connections to AWS services

You can access CodeBuild, CodeCommit, CodePipeline over VPC endpoints powered by AWS PrivateLink



“Securely Access Services Over AWS PrivateLink” available at https://d1.awsstatic.com/whitepapers/aws-privatelink.pdf

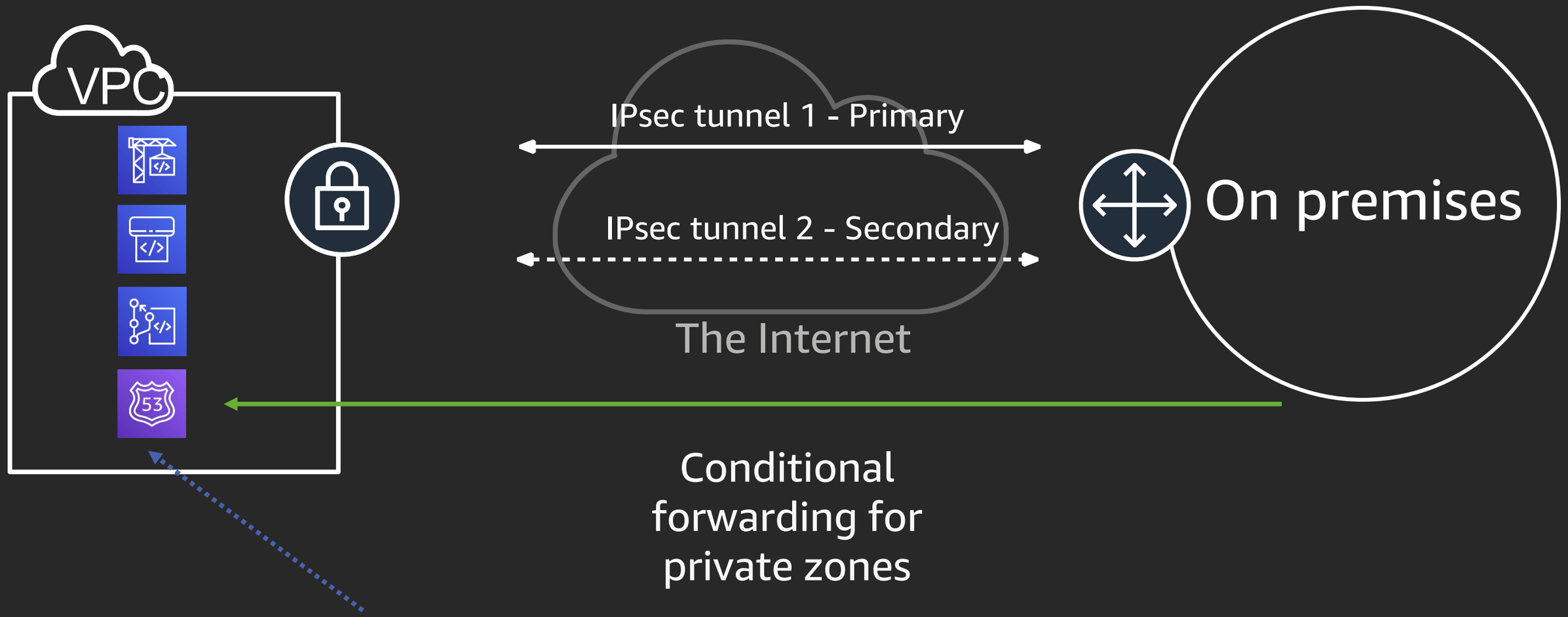
VPN to VPC endpoints



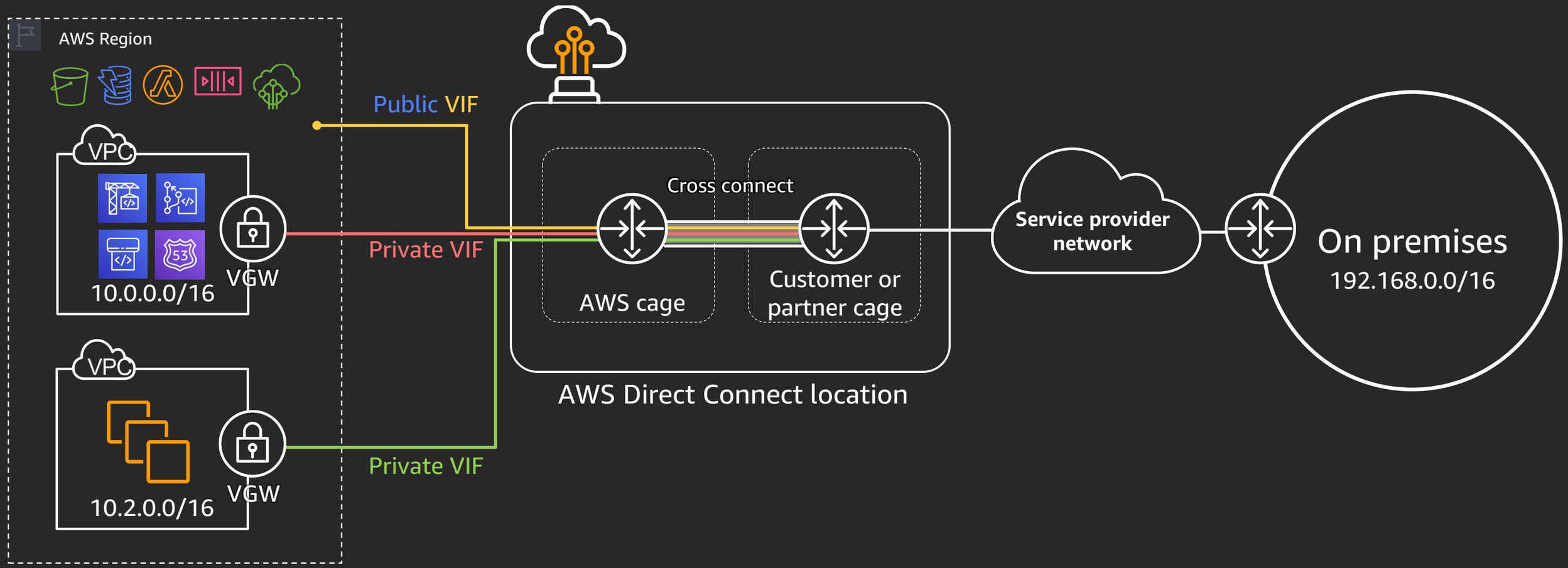
We have IP routing.

What about DNS?

Amazon Route 53 Resolver

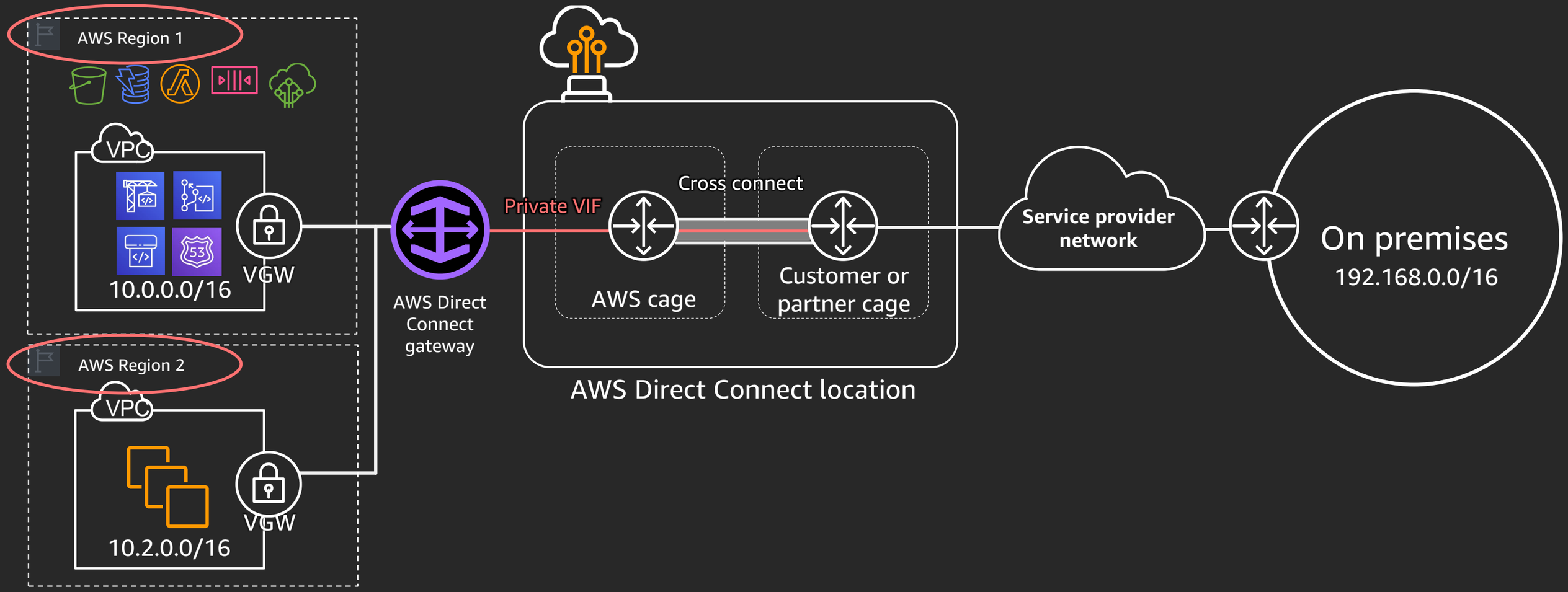


AWS Direct Connect



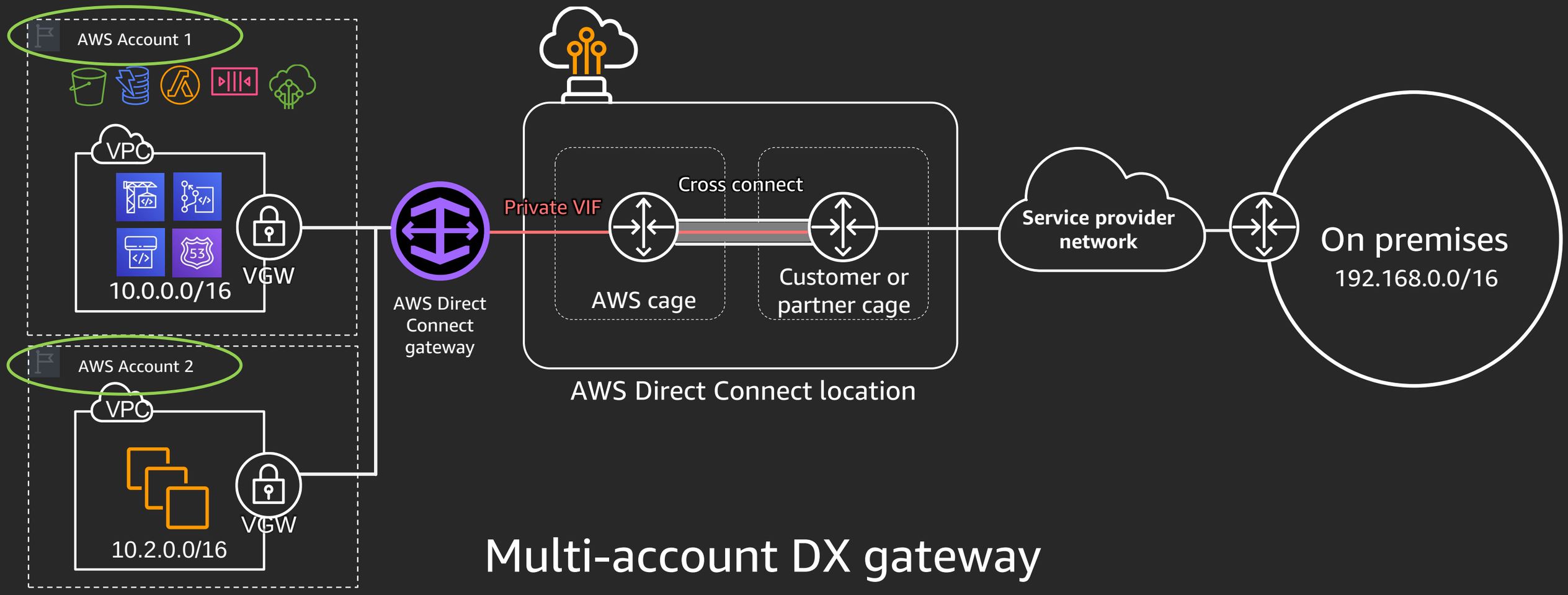
AWS Direct Connect gateway

One private VIF → many VPCs across Regions



AWS Direct Connect gateway

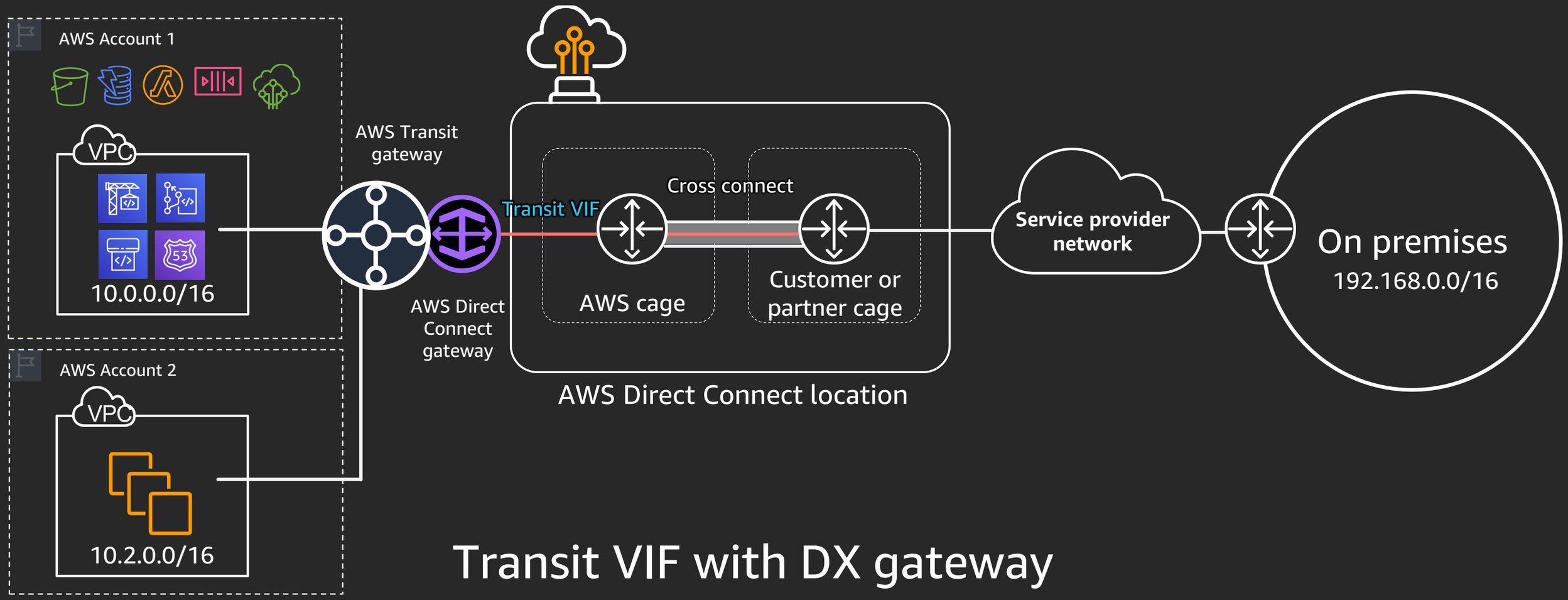
One private VIF → many VPCs across accounts



Multi-account DX gateway

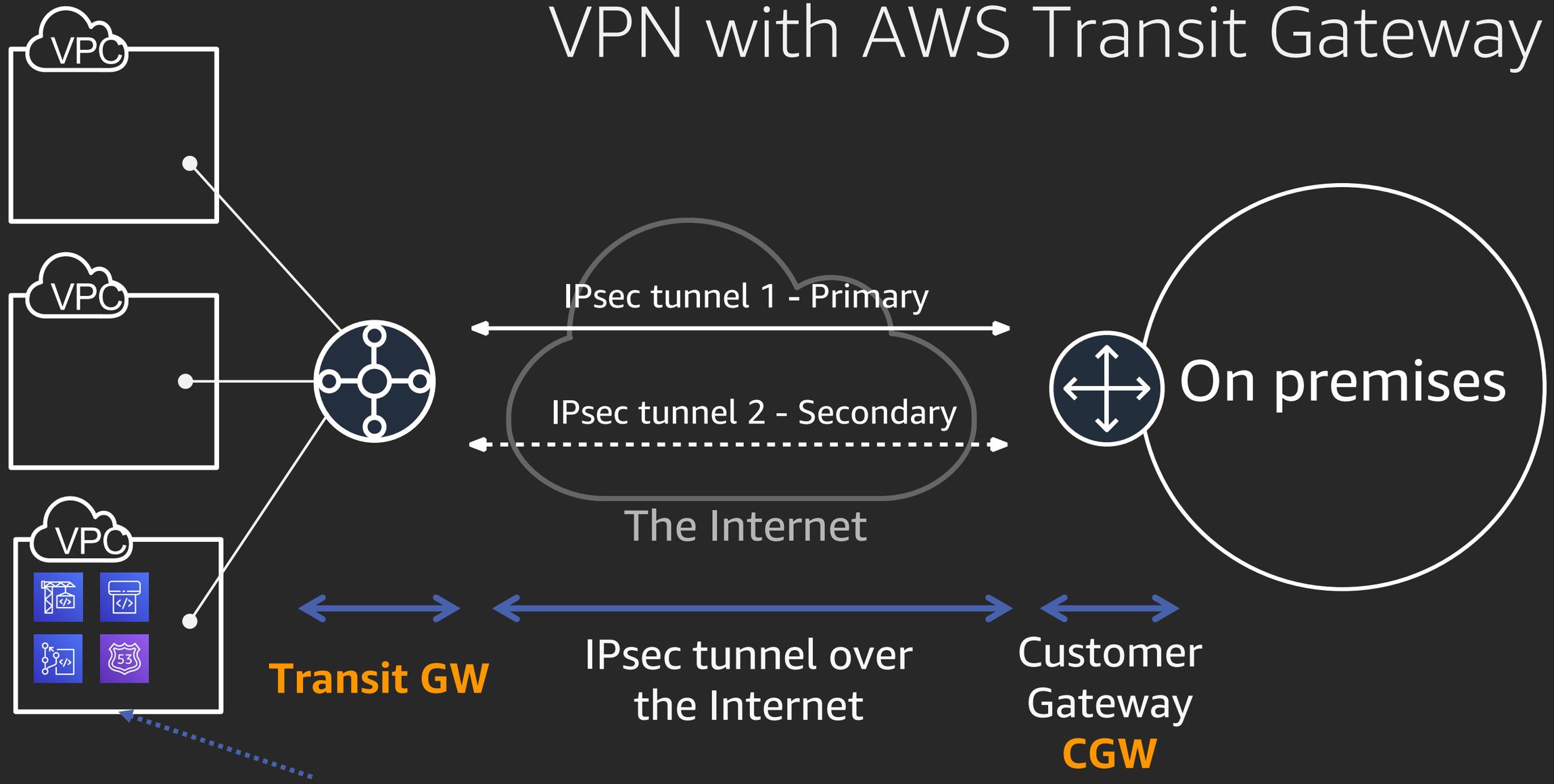
AWS Direct Connect gateway

One **transit** VIF → many VPCs

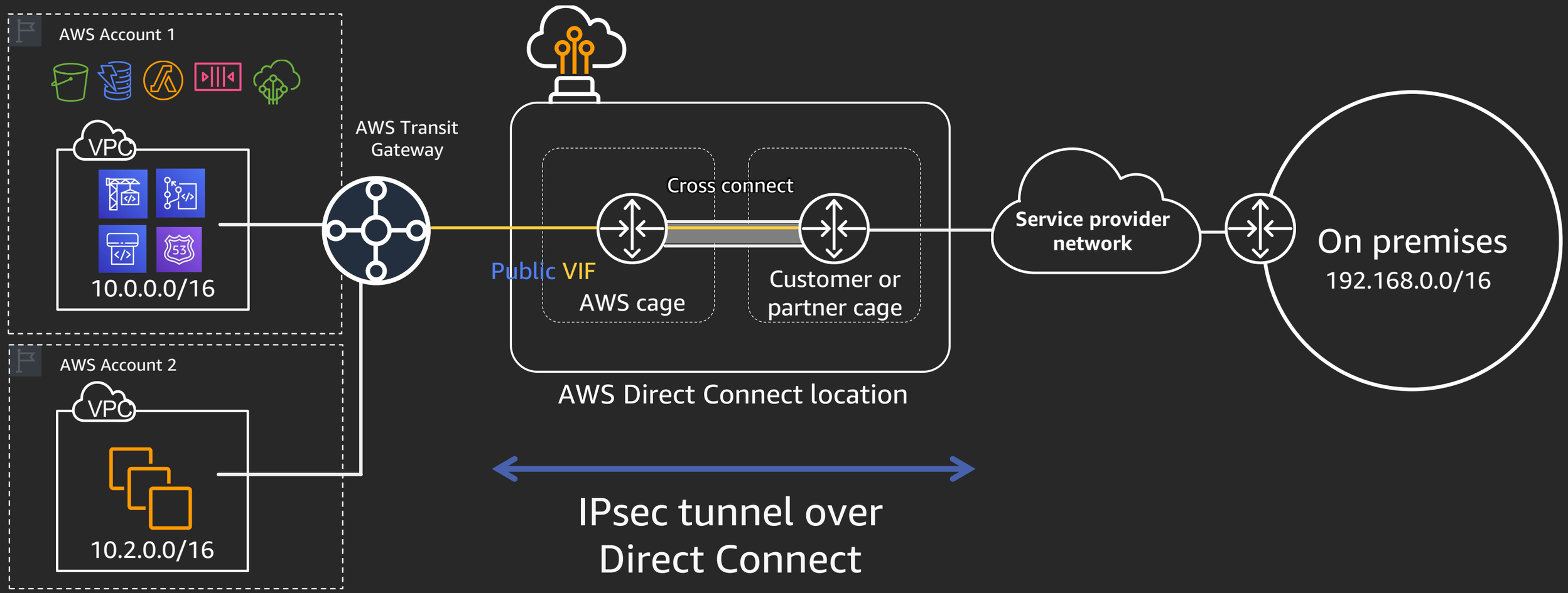


Transit VIF with DX gateway

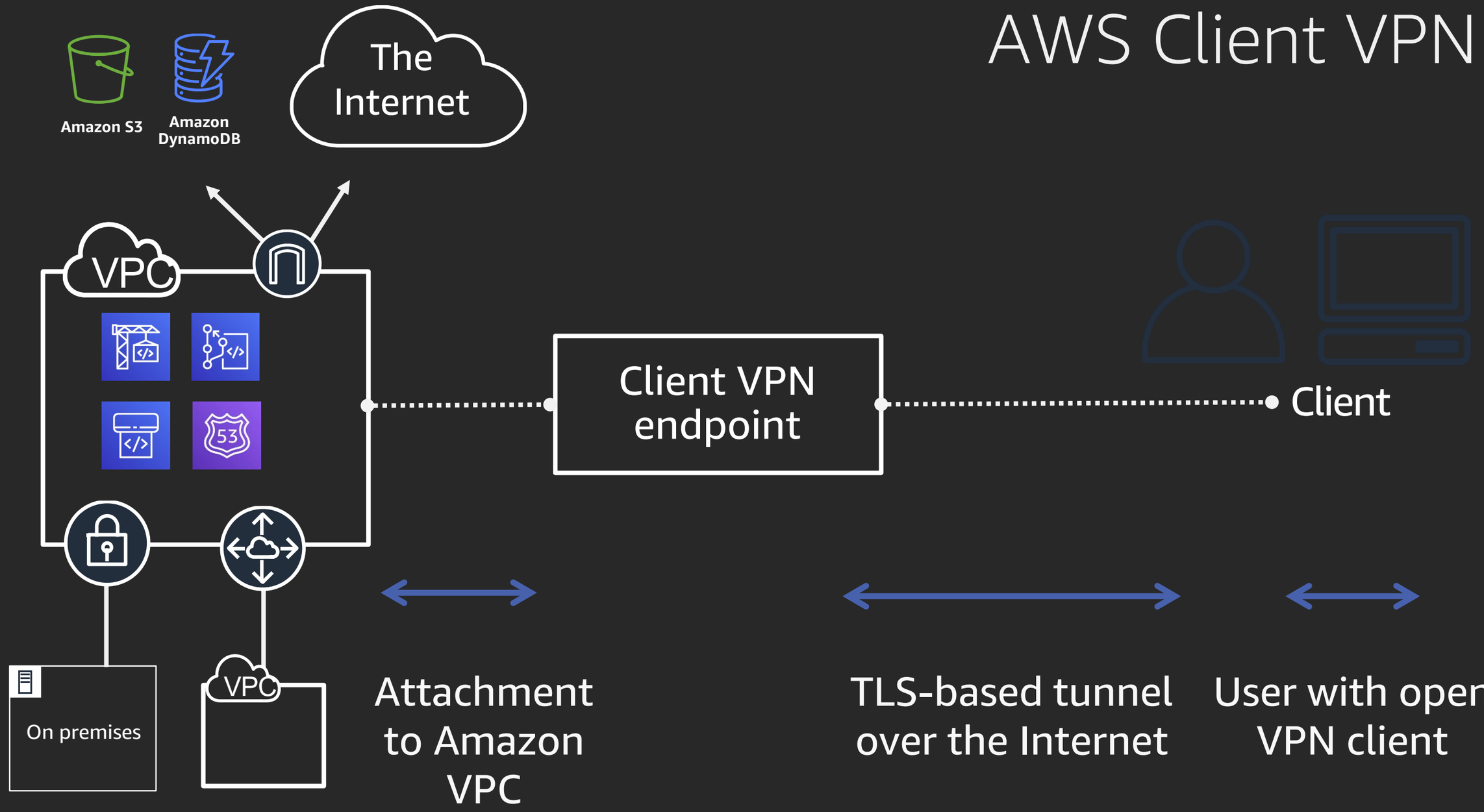
VPN with AWS Transit Gateway



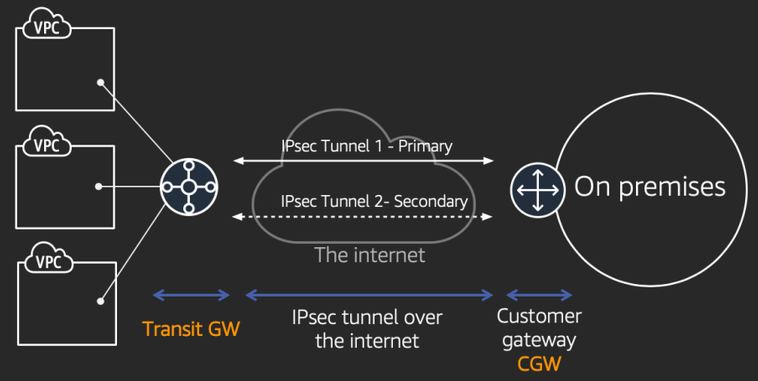
AWS Direct Connect with VPN

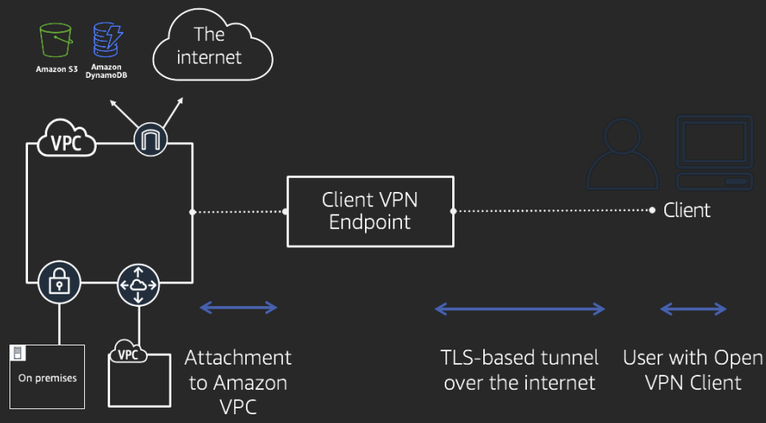


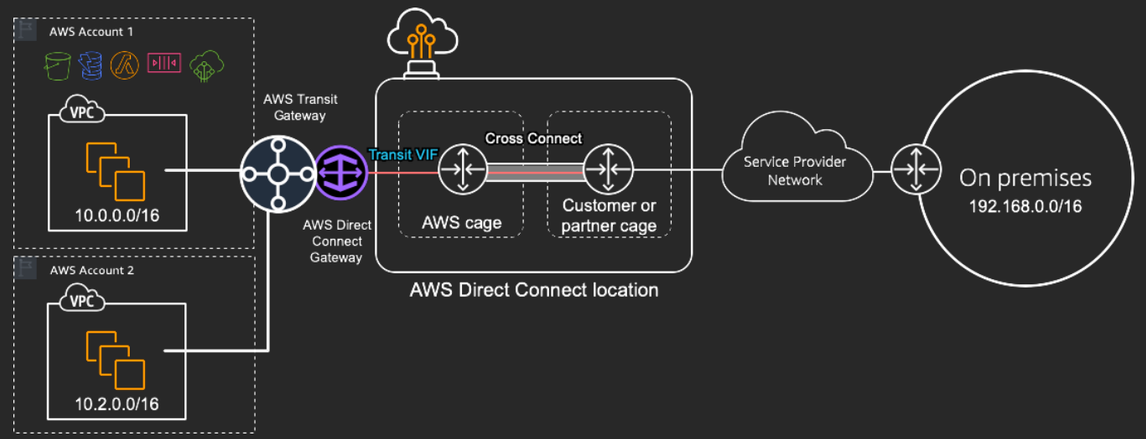
AWS Client VPN



Further sessions







NET333 – Building hybrid architectures with AWS Transit Gateway, AWS Direct Connect, and VPNs

NET412 – Become an AWS VPN and AWS Direct Connect expert

Building and deploying code

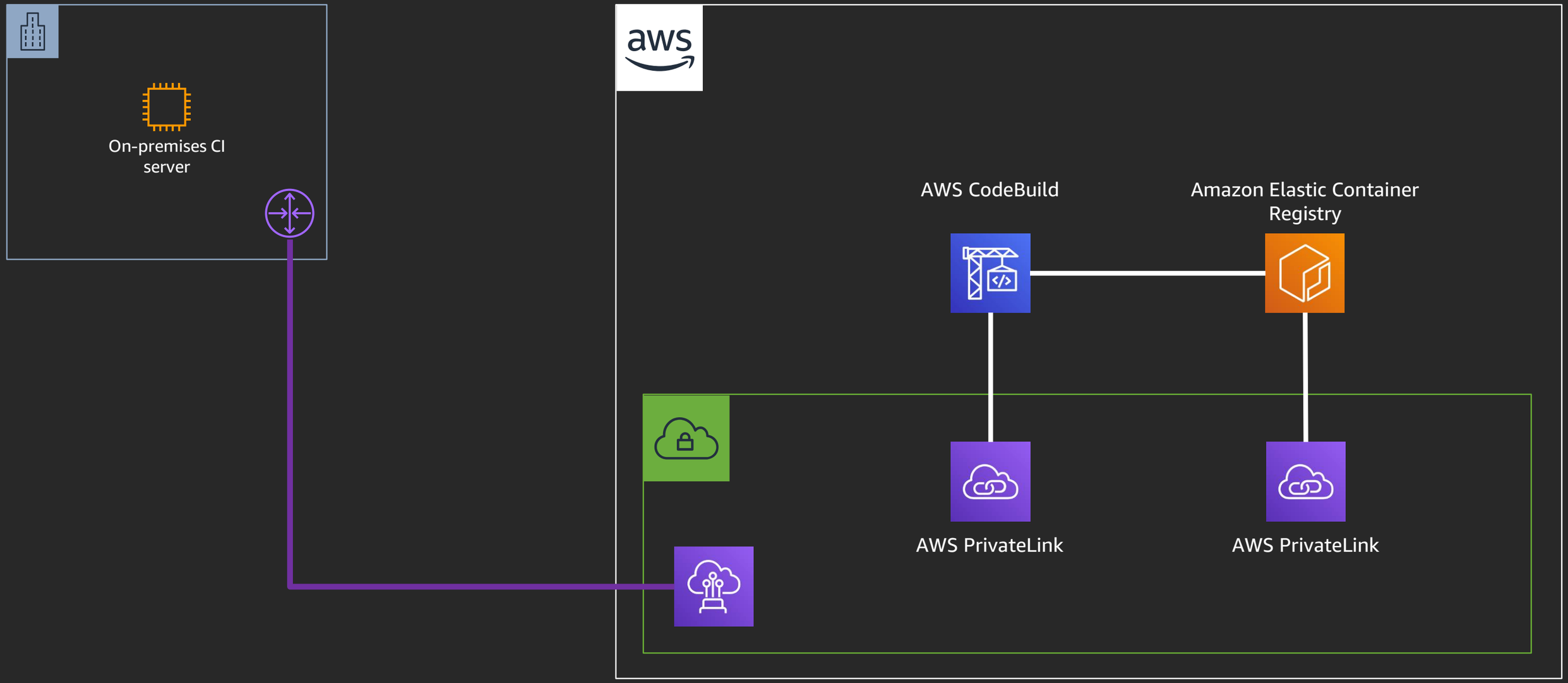
AWS CodeBuild

- Fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy

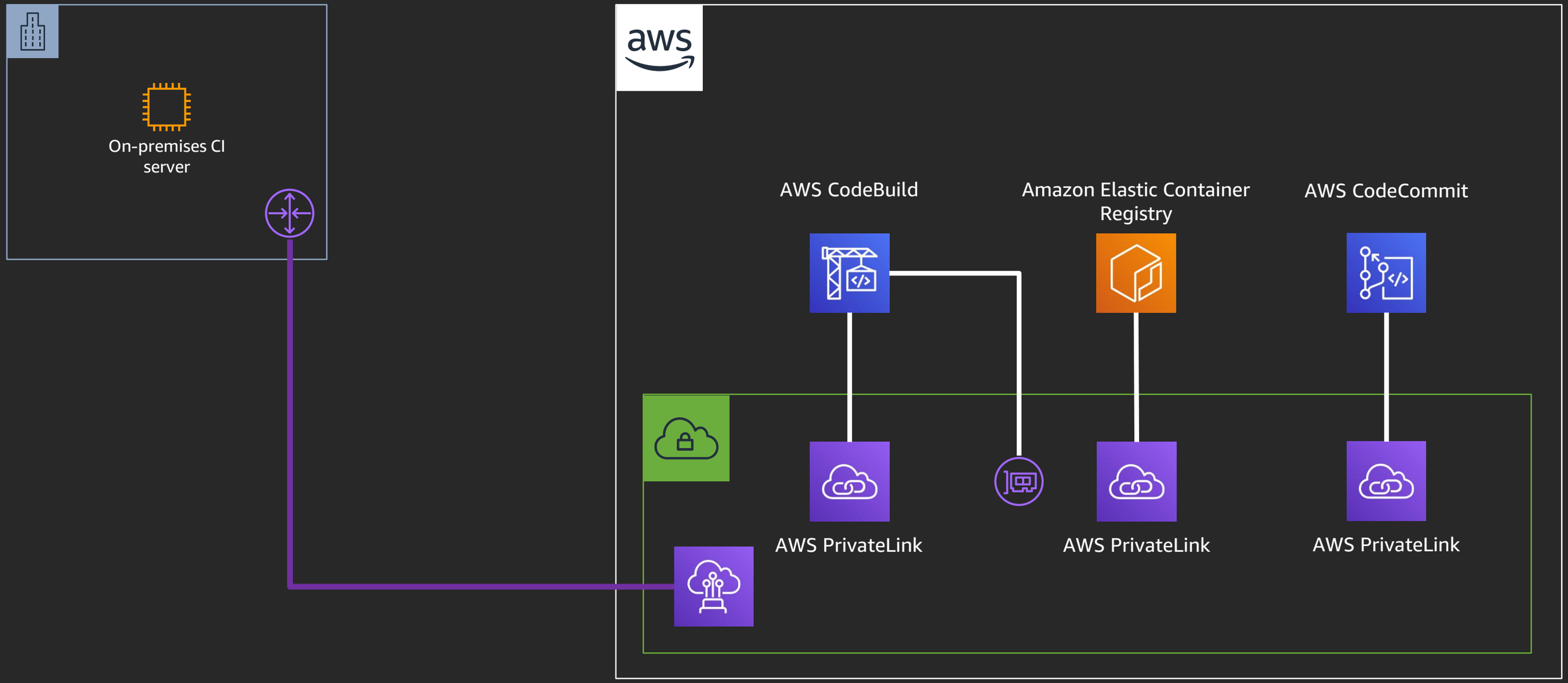
- Scales up and down automatically to meet your build volume

- Charged based on the number of minutes it takes to complete your build

AWS CodeBuild and Amazon Elastic Container Registry



AWS CodeBuild and Amazon Elastic Container Registry



A more realistic flow

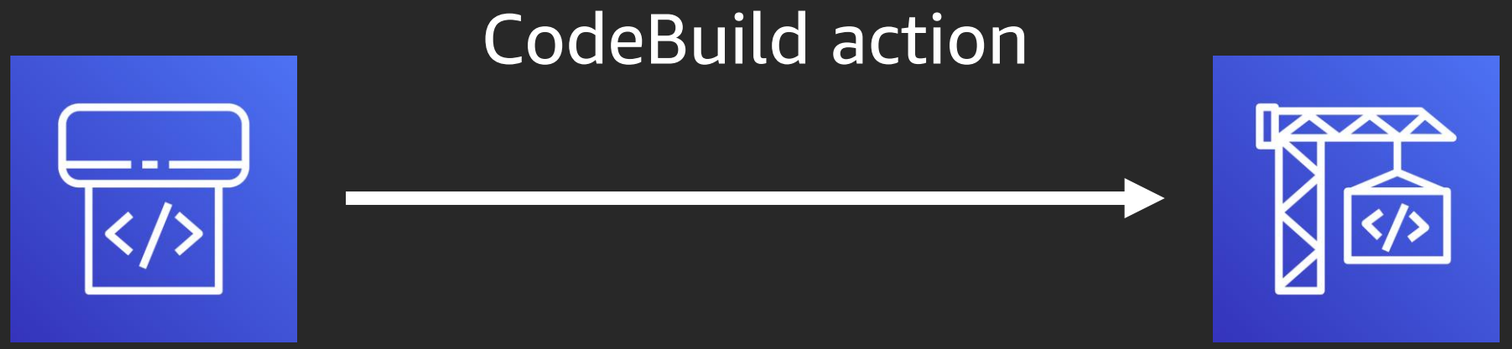
- Developer writes some code and pushes it to a Git repository such as AWS CodeCommit

A more realistic flow

- AWS CodePipeline is notified of the commit

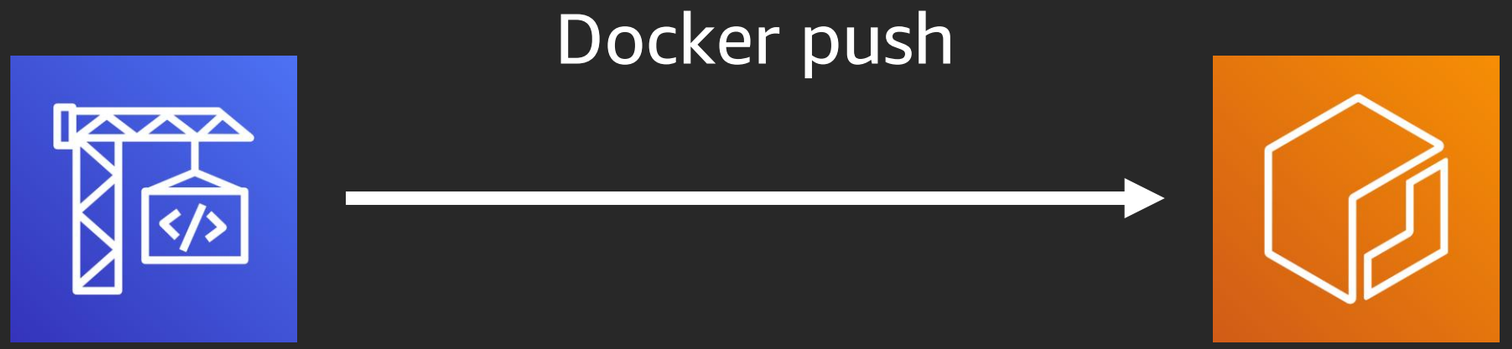
A more realistic flow

- AWS CodePipeline uses AWS CodeBuild to build Docker image



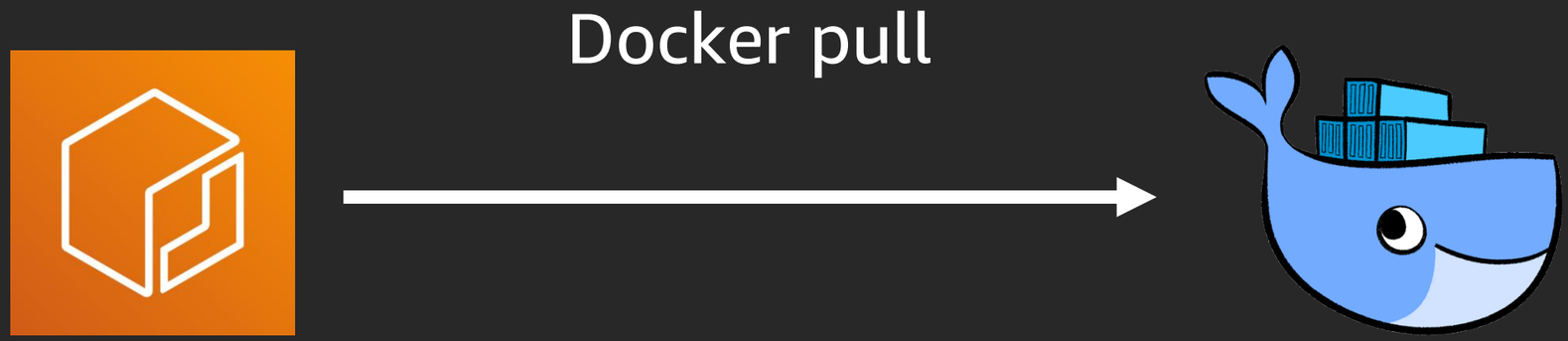
A more realistic flow

- AWS CodeBuild pushes image to Amazon Elastic Container Registry



A more realistic flow

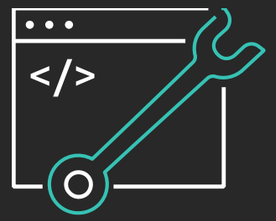
- An on-premises Docker server (such as Kubernetes or plain Docker) is used to deploy the new container



Demo

Learn DevOps with AWS Training and Certification

Resources created by the experts at AWS to propel your organization and career forward



Take free digital training to learn best practices for developing, deploying, and maintaining applications

Classroom offerings, like DevOps Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified DevOps Engineer - Professional** or **AWS Certified Developer - Associate** exams

Visit aws.amazon.com/training/path-developing/

aws training and certification

Thank you!

Lee Packham
@joolz

Craig Smith
@limivorous

AWS re:Invent

aws

Please complete the session survey in the mobile app.