aws SUMMIT

WASHINGTON DC | JUNE 07, 2023

DEV203

Building Cloud Grade Network Segmentation using Transit Gateway and Terraform

William Collins

Principal Cloud Architect
Alkira

aws

Agenda

- ***How*** did we get here?

- Benefits of ***Segmentation***

- Thinking through the ***Workflow***

- Let's ***Demo***!

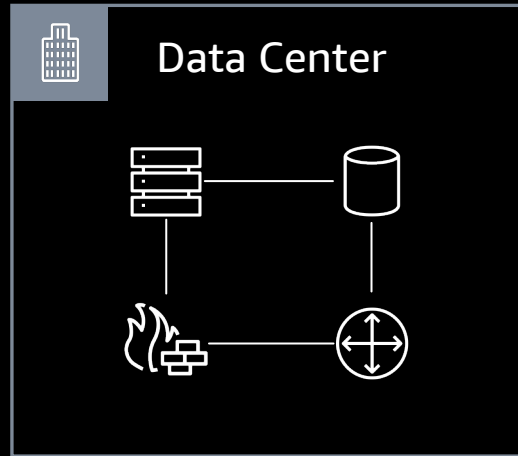# How did we get here?

🏢 Enterprise

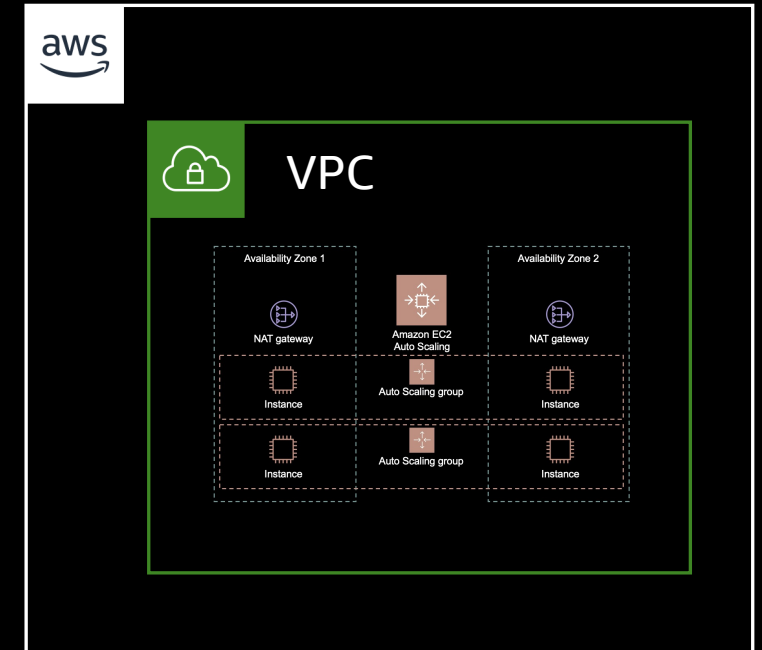*(15K or more employees)*

100 – 2,000

Applications

Data Center

How did we get here?

Data Center

Cloud Adoption →

VPC

Availability Zone 1 — Availability Zone 2

NAT gateway — Amazon EC2 Auto Scaling — NAT gateway

Instance — Auto Scaling group — Instance

Instance — Auto Scaling group — Instance
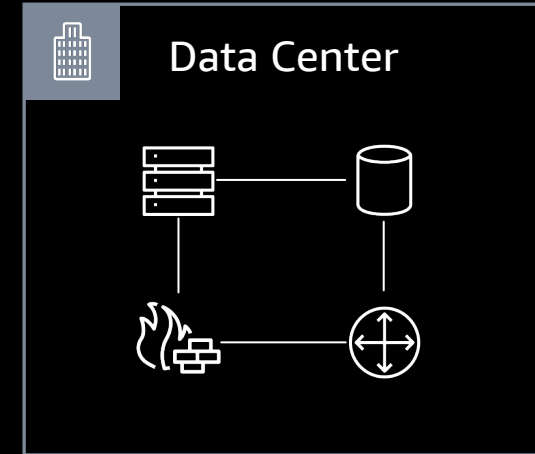
Transition business units, teams, technologies, and processes to leverage AWS

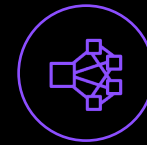# Benefits of Segmentation

Reduce attack
surface

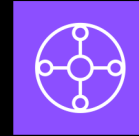Compliance
Enforcement

Environment
Isolation

Optimize
Performance

Thinking through the Workflow

VPCs

Acceleration in AWS adoption for large enterprises leads to an increase in VPCs over time
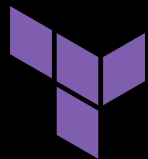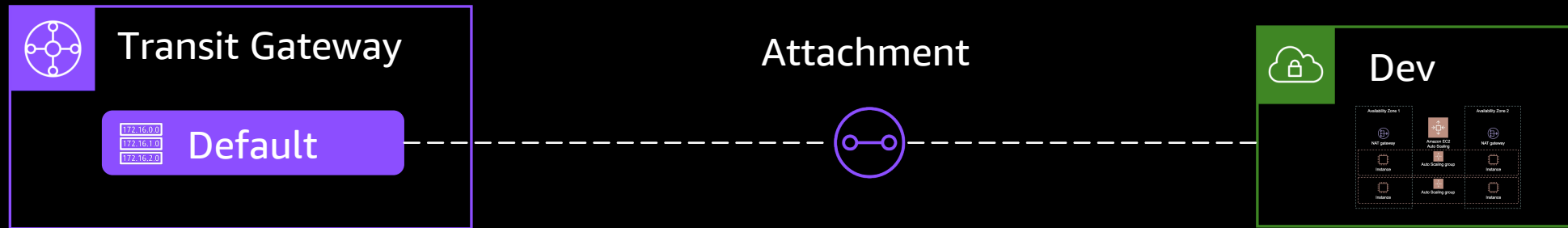
Transit Gateway

Simplifies connectivity at scale for VPCs and on-premises networking

Terraform

Infrastructure-as-Code tool that uses a declarative approach for managing cloud resources
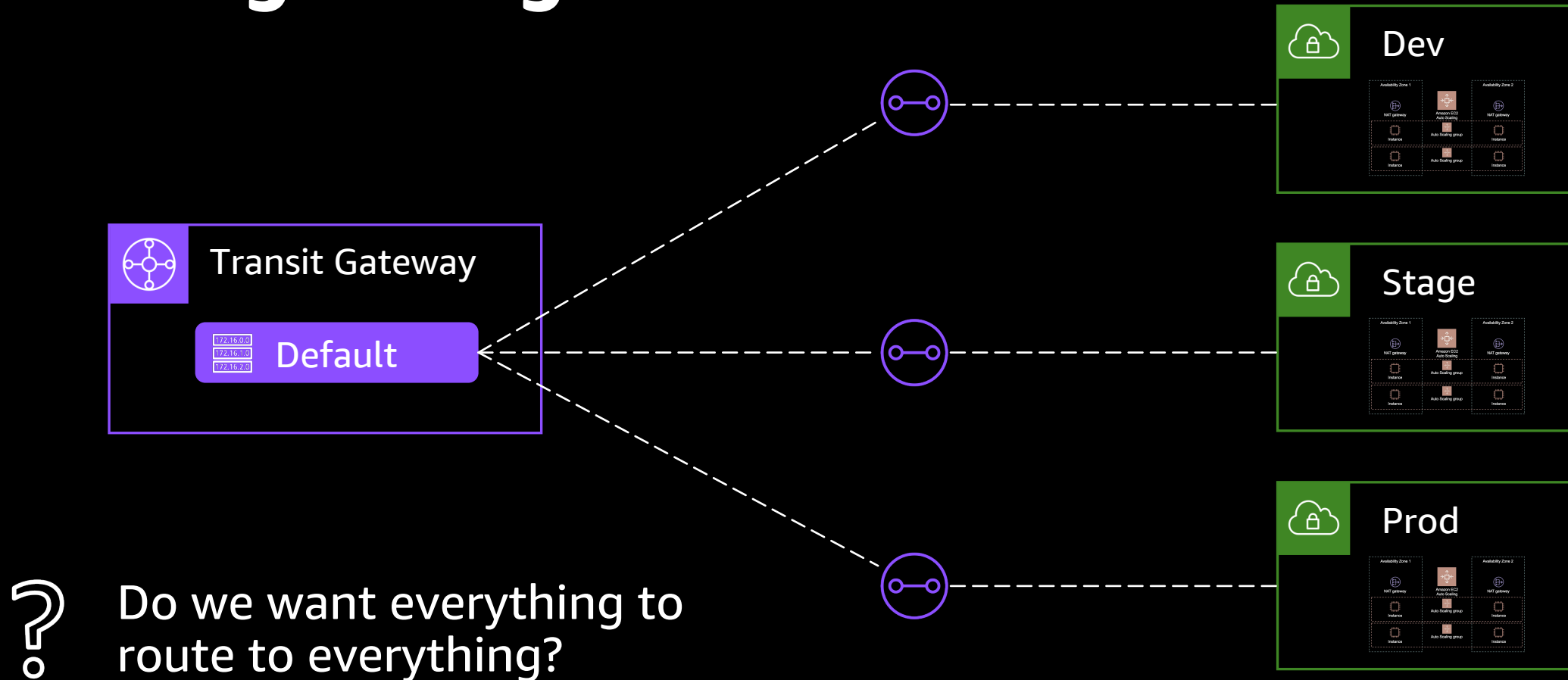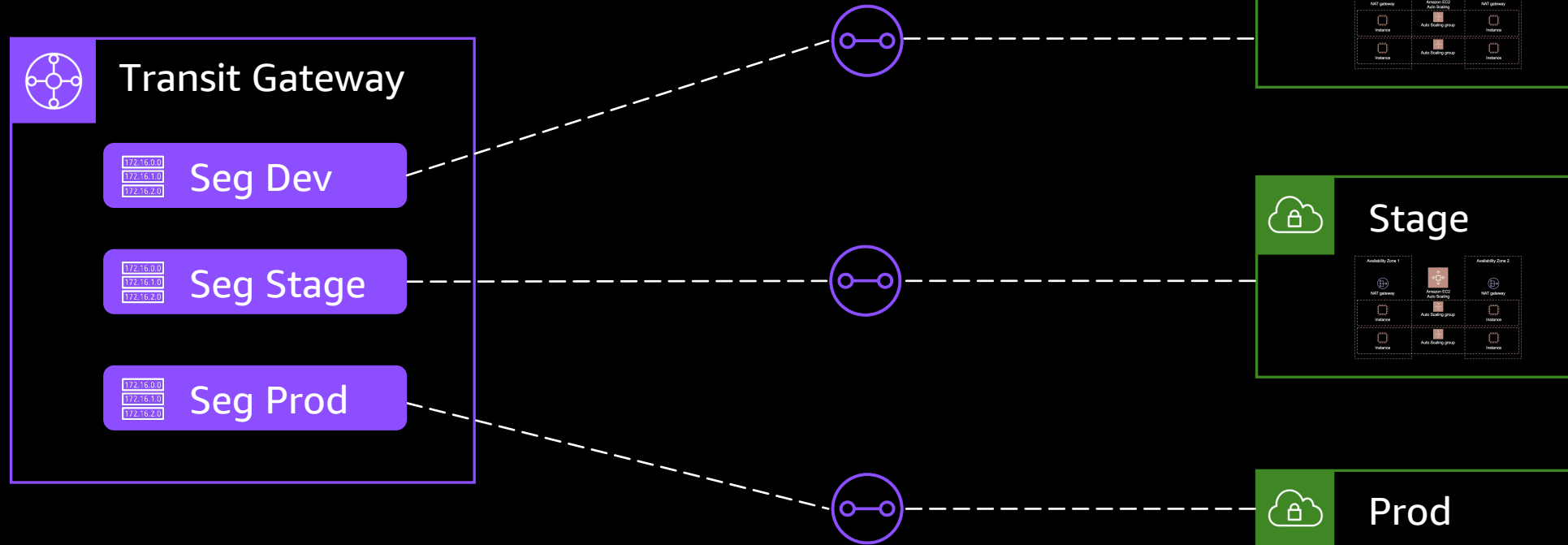
Thinking through the Workflow

Default provider behavior will associate attachments with Transit Gateway's default route table and propagate routes

# Thinking through the Workflow

Transit Gateway

172.16.0.0
172.16.1.0
172.16.2.0
Default

Dev

Stage

Prod

? Do we want everything to route to everything?

Thinking through the Workflow

Transit Gateway

Seg Dev — 172.16.0.0 / 172.16.1.0 / 172.16.2.0

Seg Stage — 172.16.0.0 / 172.16.1.0 / 172.16.2.0

Seg Prod — 172.16.0.0 / 172.16.1.0 / 172.16.2.0

Dev

Stage

Prod

💡 Let's create custom route tables for *network segmentation*!

Demo!

- *'Shared'* can reach all VPCs

- *'Dev'* and *'Stage'* have reachability to each other but not to *'Prod'*
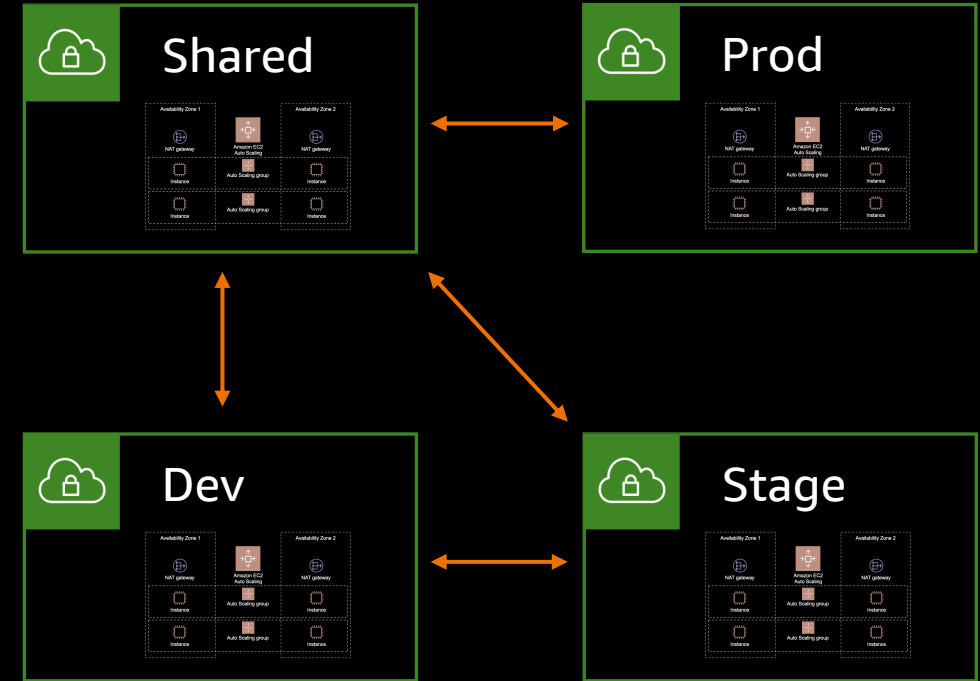
Thank you!

William Collins

🐦 @wcollins502

💼 linkedin.com/in/william-collins

🔗 wcollins.io

Please complete the session survey in the mobile app