WEBINAR

Secure and Scalable Connectivity for Modern Apps with AWS

Azeem Ayaz

Specialist TAM - Networking
AWS

Barbara Bogdanescu

Sr. Technical Account Manager
AWS

App Owner’s top Priorities

Scalable Network Connectivity

Security

Autonomy for Developers

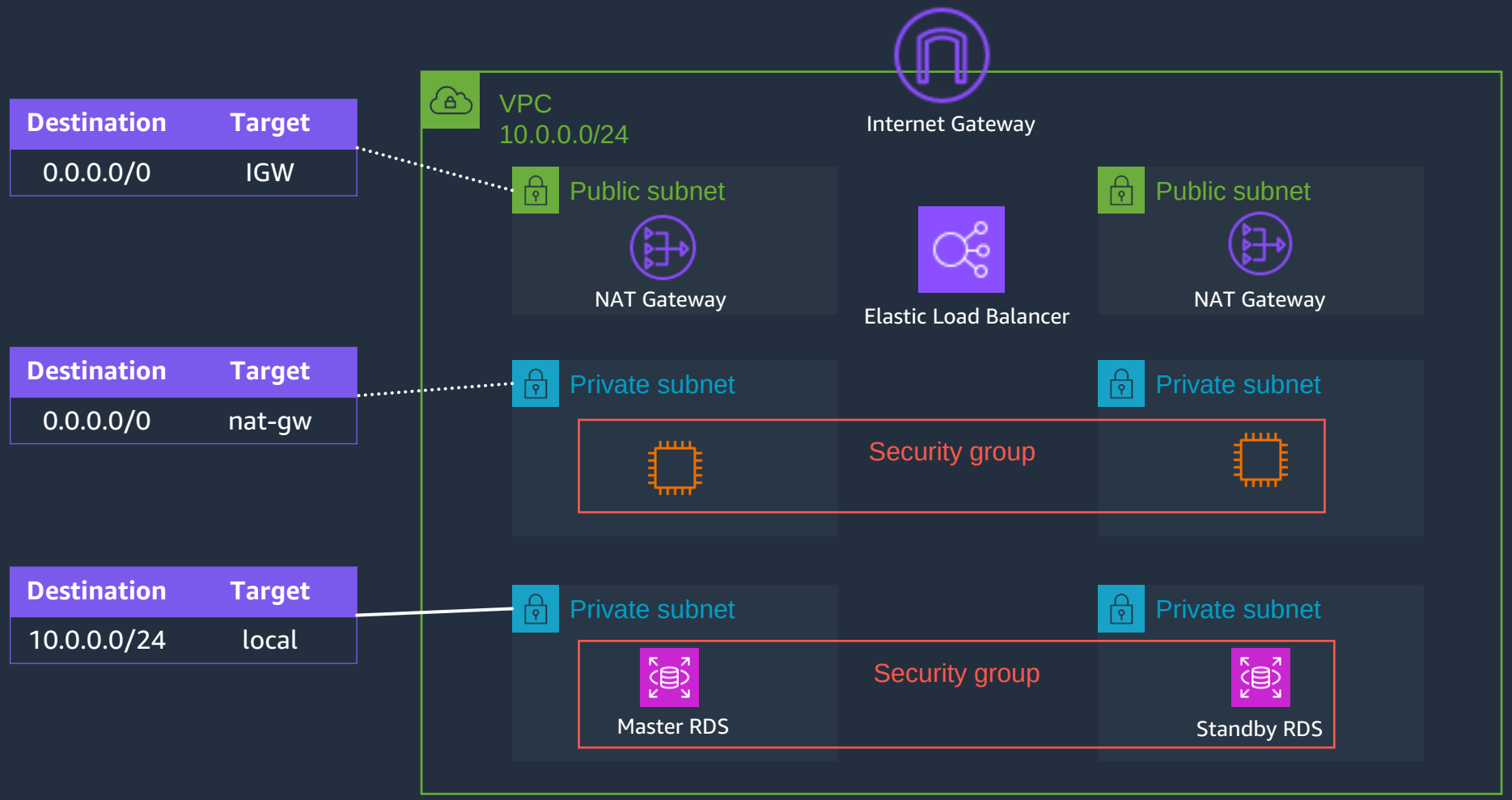
Monitoring and Observability

What are we going to discuss today ?

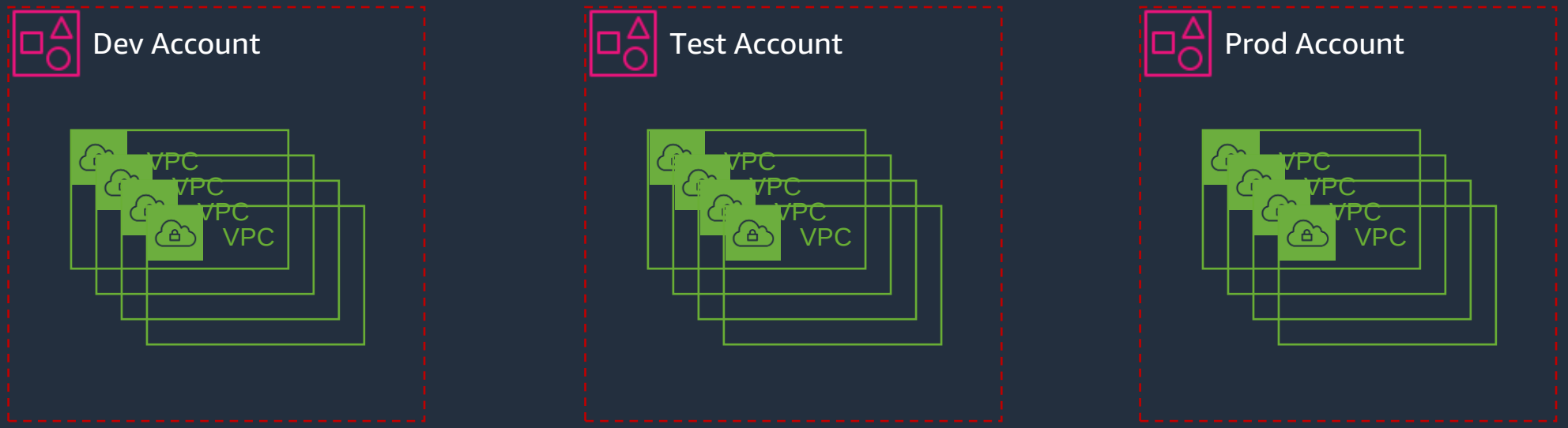
…Starting from the Network

Moving to the Application…

It starts here …

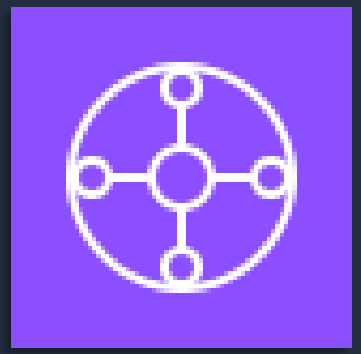


Muti-VPC Architectures



Connectivity at Scale

AWS Transit Gateway

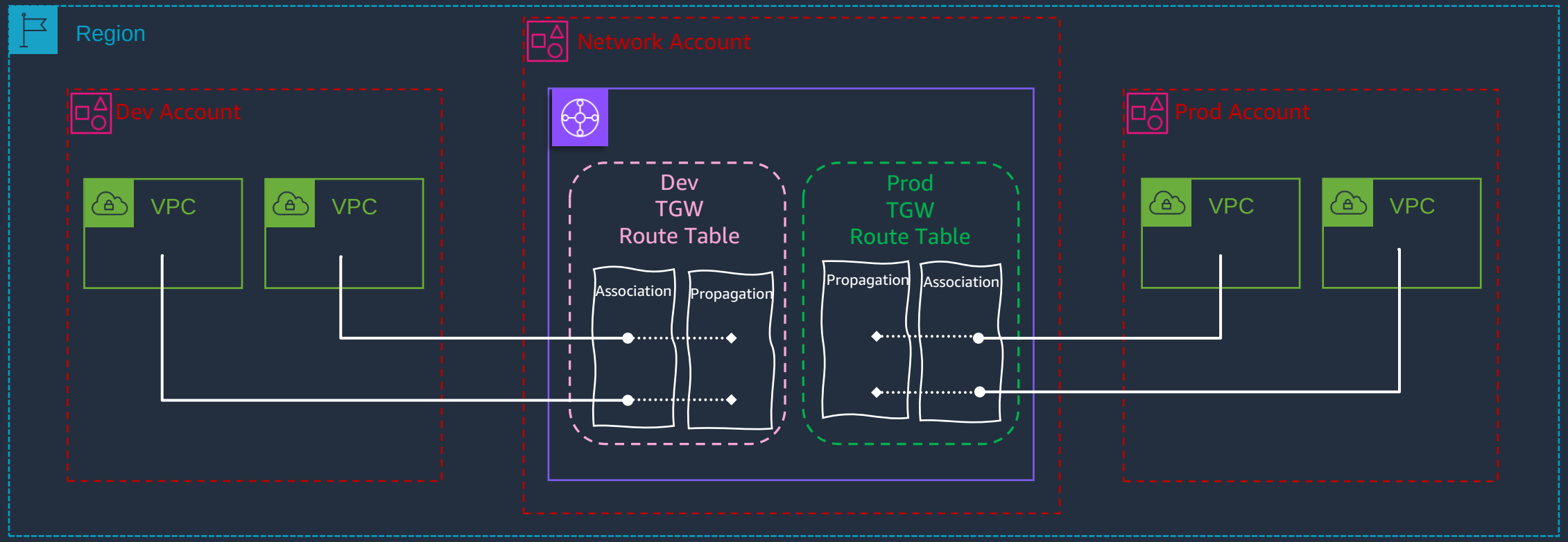


AWS Transit Gateway (TGW) is a centralized regional network hub.

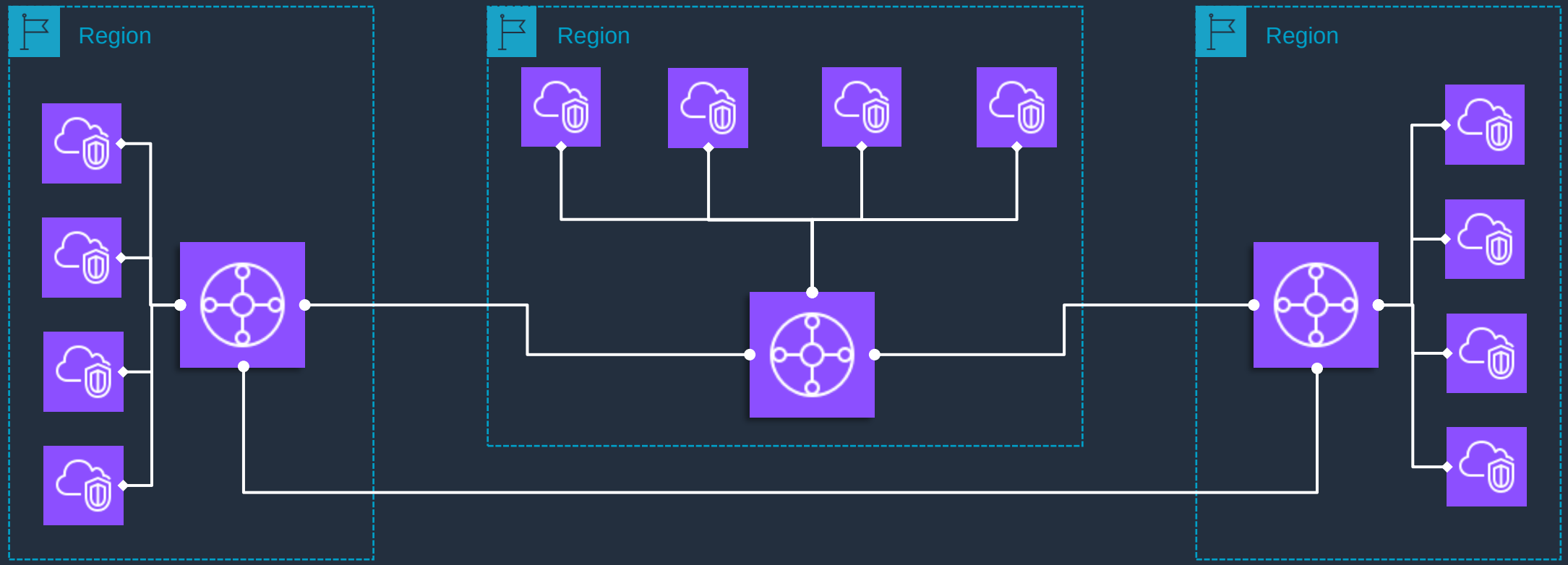
Simplifies interconnection of multiple VPCs and on-prem networks.

Allows traffic segmentation.

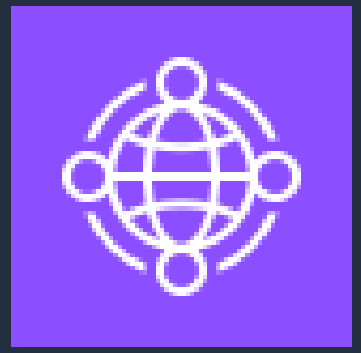
Transit Gateway: Deep Dive



Transit Gateway: Multi Region



AWS Cloud WAN

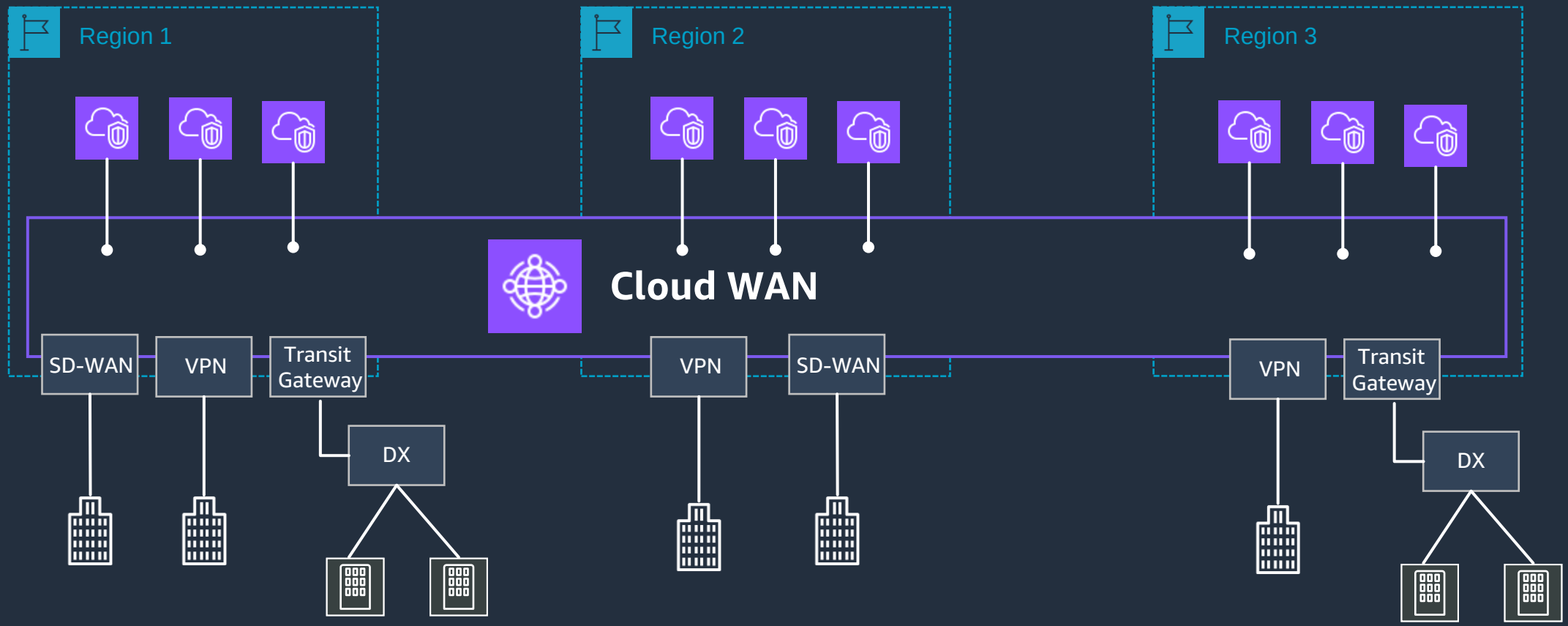


AWS Cloud WAN is a centralized global **network** hub.

Provides built-in automation, segmentation and confirmation management for building and operating global networks

Automated VPC attachments

Cloud WAN



AWS Cloud WAN: Core Components

Core Network: The part of your global network managed by AWS, operating in the AWS Regions defined in your Core Network Policy document

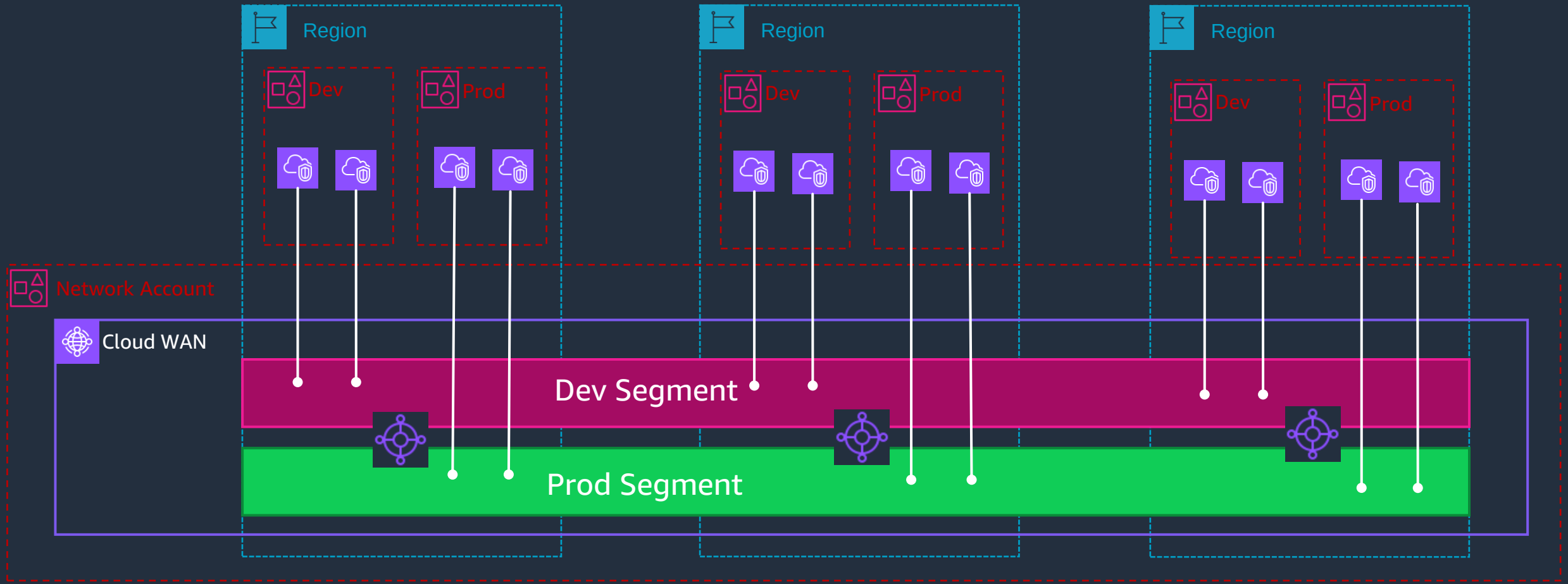
Core Network Policy: A single document that defines the global configuration of your Core Network

Core Network Edge: The Regional connection point managed by AWS in each Region. Every Cloud WAN attachment connects to a Core Network Edge

Segments: Dedicated routing domains (e.g. prod, dev, engineering, etc.)

Attachments: Attachments are any connections or resources you want to add to your Core Network

Cloud WAN: Deep Dive



Selecting the best fit for you needs

AWS Transit Gateway

Managed by customers,
controlled regionally

- Full configuration or DIY automation
  - Register to a global network
  - Use your existing automation
- Can peer with a core network edge
- Transit virtual interface for Direct Connect

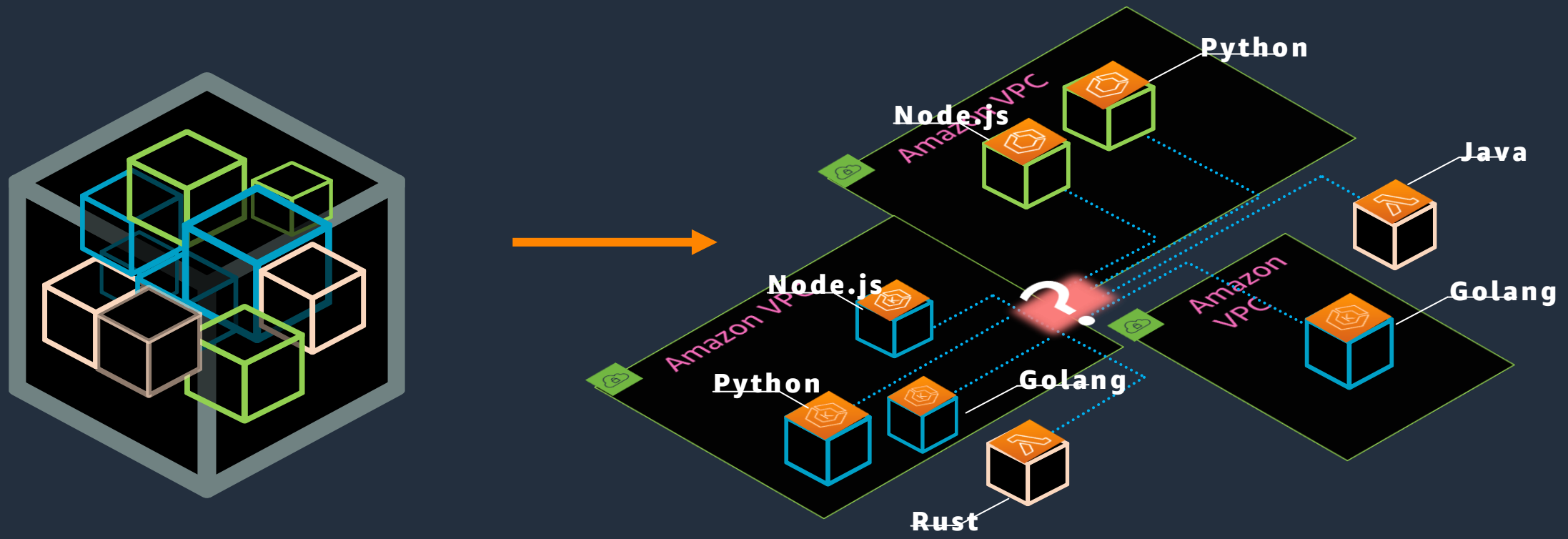
AWS Cloud WAN

Managed by AWS,
controlled globally

- Similar to AWS Transit Gateway
- Supports “Connect” (SD-WAN) attachments
- Segment across Regions
- Supports Transit Gateway integrations
- Direct Connect through Transit Gateway peering

Developers

State of the Application



Application Owner’s Conundrum

Connectivity

Security

Observability & Cost

Application Networking

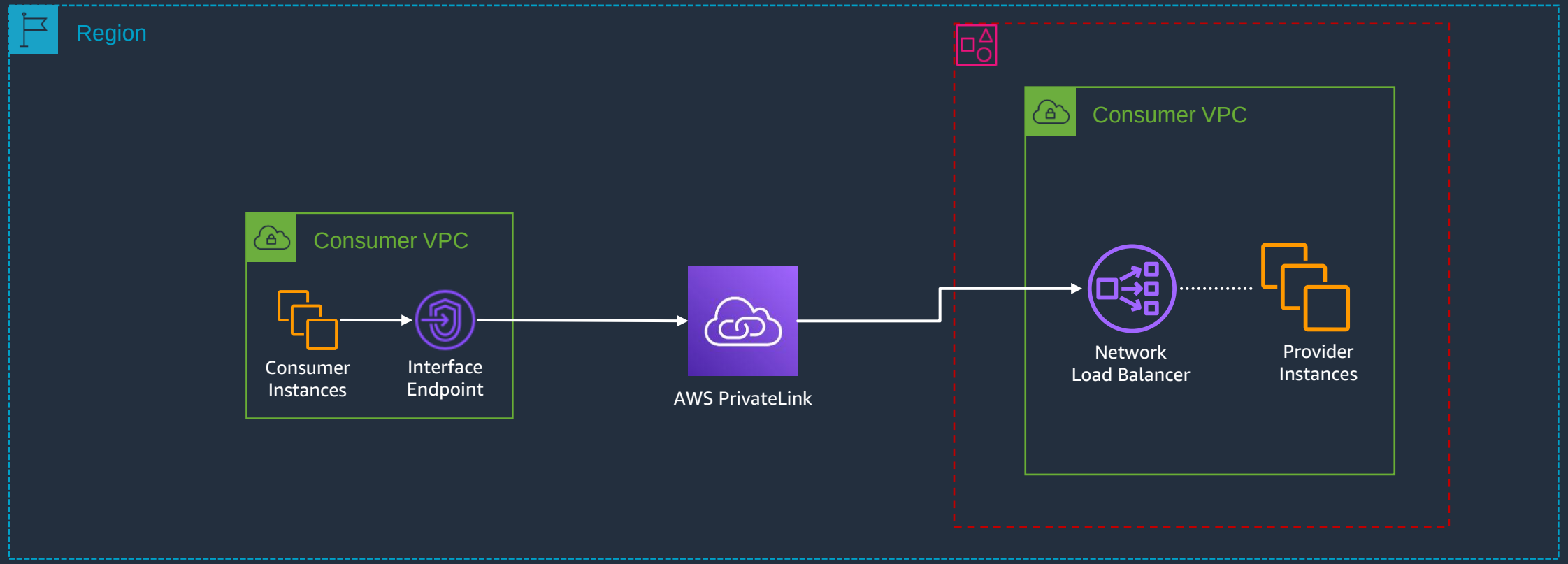
AWS PrivateLink

Allow provisioning applications in Software as a Service model.

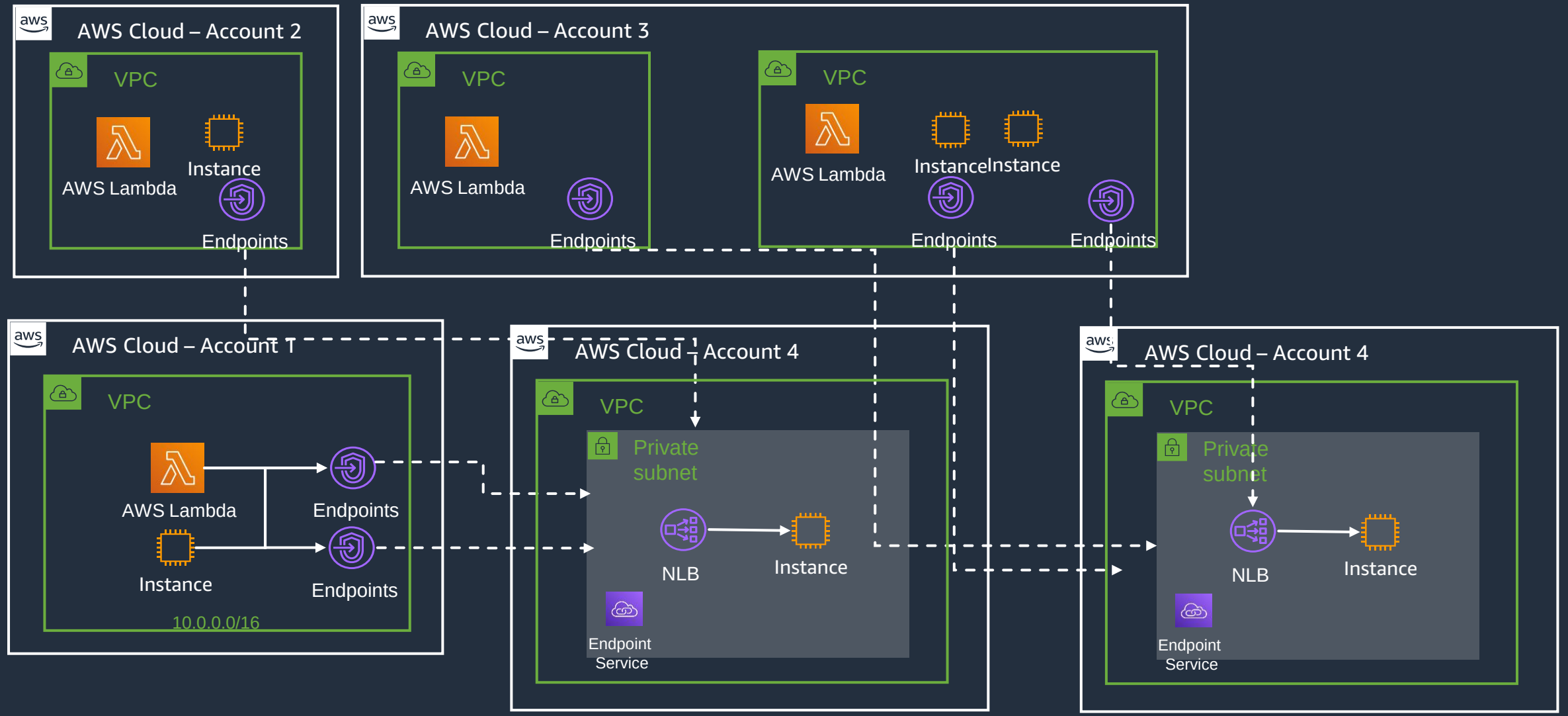
Granular Access Control

Simplified connectivity between consumer and service provider

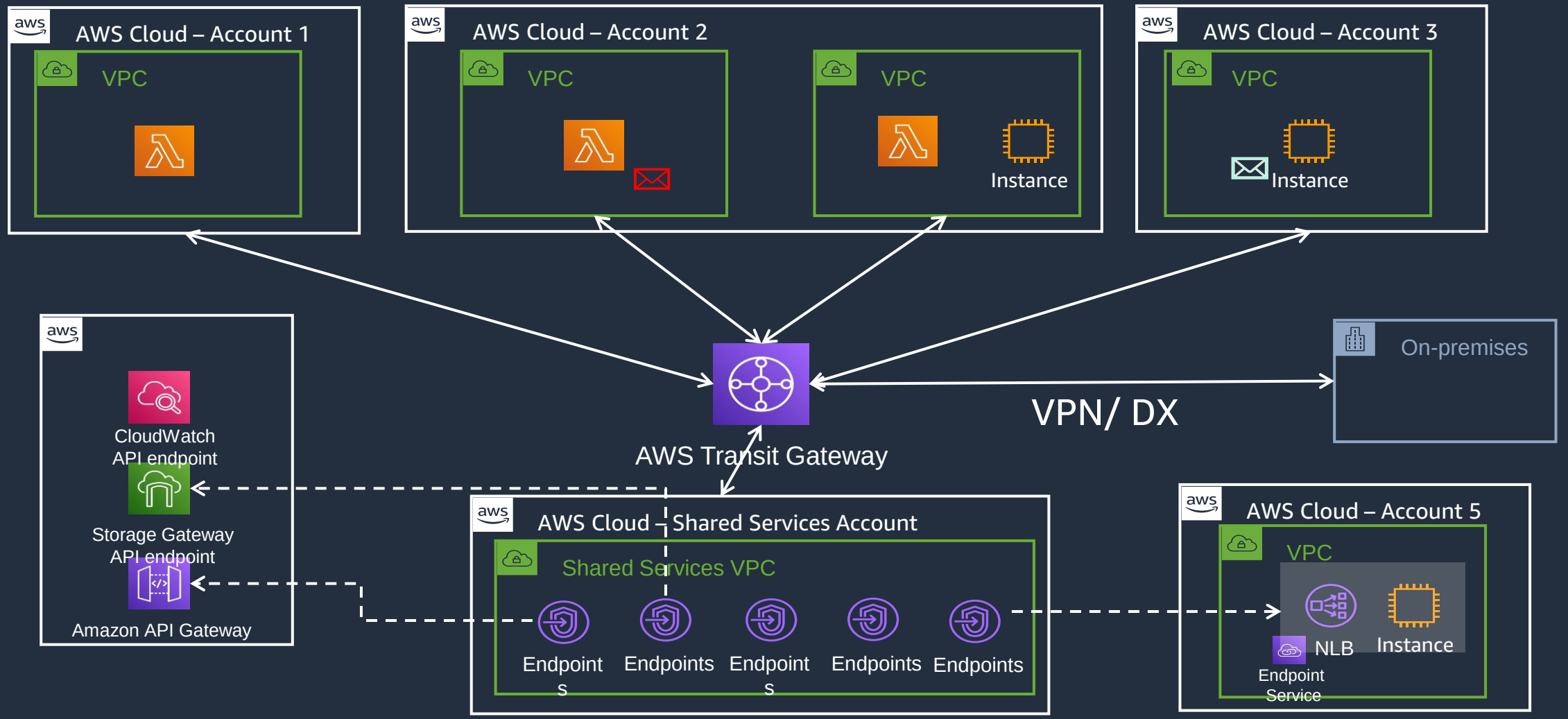
AWS Private Link: Components



AWS PrivateLink Scaling: Distributed



AWS PrivateLink Scaling: Centralized



AWS PrivateLink

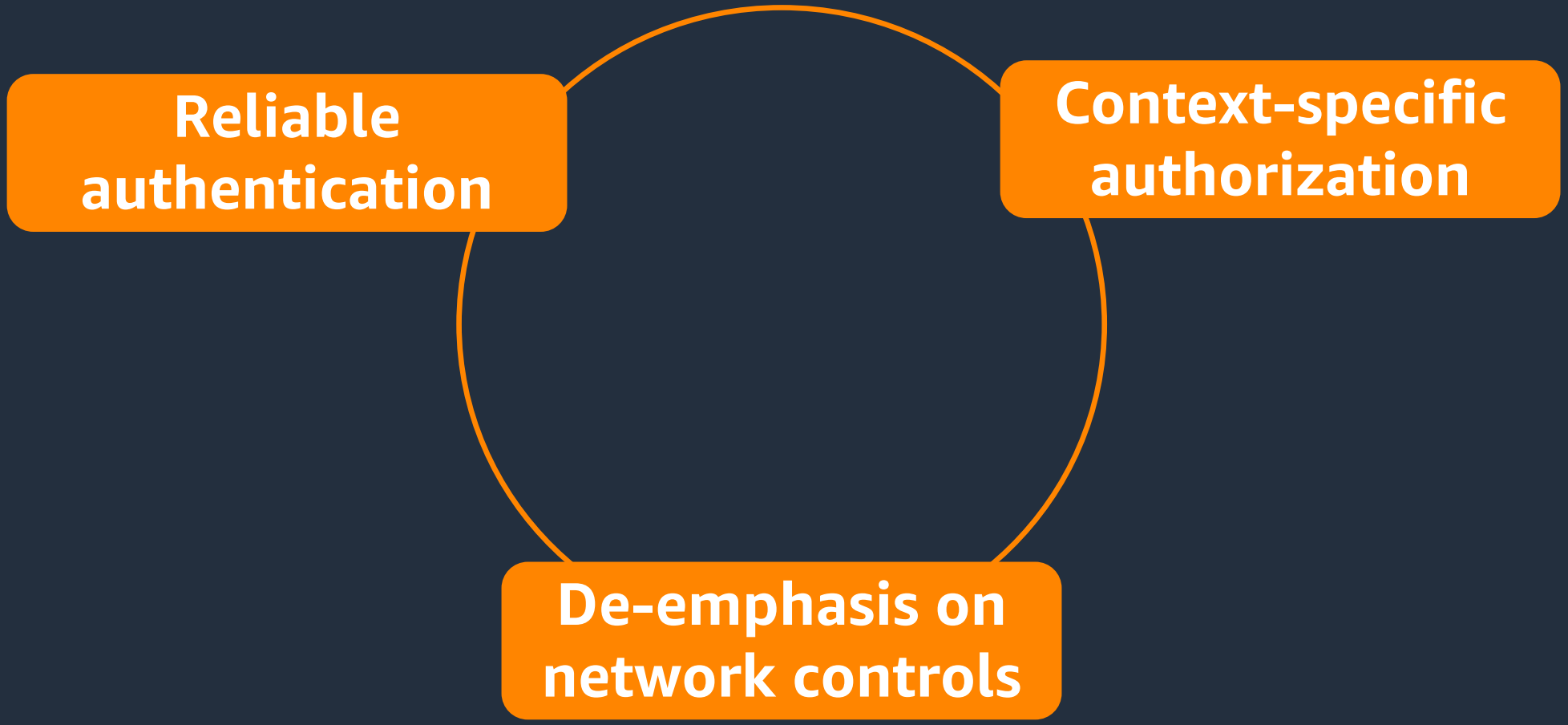
Benefits

Developers no longer need to deploy complex connectivity solutions.
Overlapping IPs no longer an issue.
Granular security control per app instead of network boundaries.

Outstanding Challenges

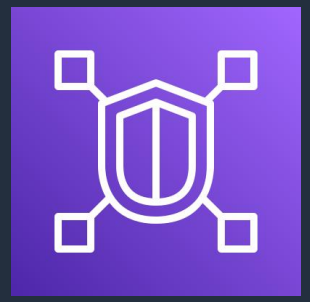
Security of applications still remain core responsibility of the service team.
Admins have no monitoring visibility of the applications.
Scaling up might bring back some of the connectivity & management requirements

Moving towards Zero Trust?



Amazon VPC Lattice

BUILT FOR DEVELOPERS, BUT WITH THE TOOLS AND CONTROLS ADMINS REQUIRE TO AUDIT AND ENFORCE



Simplifies the way developers connect, secure, and observe communication, with application layer networking between services

Connectivity

- Cross-account, cross-VPC connections to services
- Application-aware routing

Consistency across compute services

- Integration with Amazon EC2, Amazon ECS, AWS Lambda, and Amazon EKS/Kubernetes

Observability and traffic control

- Logs or metrics export to Amazon S3, Amazon CloudWatch, and Amazon Kinesis Data Firehose
- Advanced layer 7 routing and resiliency controls

Security

- Access policy for Zero Trust architectures
- Centralized control of inbound and outbound traffic

Amazon VPC Lattice benefits

< \ >

Increased developer productivity

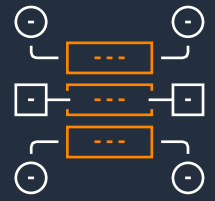
Simplified service discovery and connectivity

Enhanced security posture

Granular access control with IAM roles

Optimized compute choice

Support for EC2/ Auto Scaling groups, EKS, Lambda



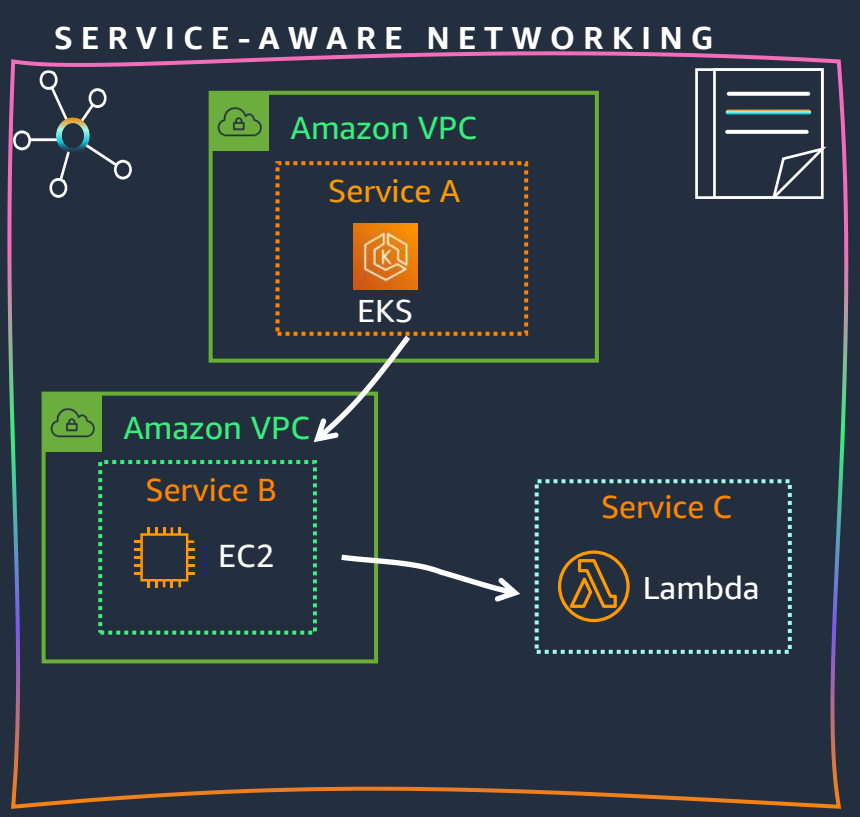
Improved scale and resilience

Fully managed control plane and data plane

Reduced Day 2 operations costs

Operate large environments with fewer resources

Amazon VPC Lattice concepts



Service network

- Define logical boundary across VPCs and accounts
- Apply common access and observability policy

Service

- Unit of application
- Extends across all compute – instances, containers, serverless

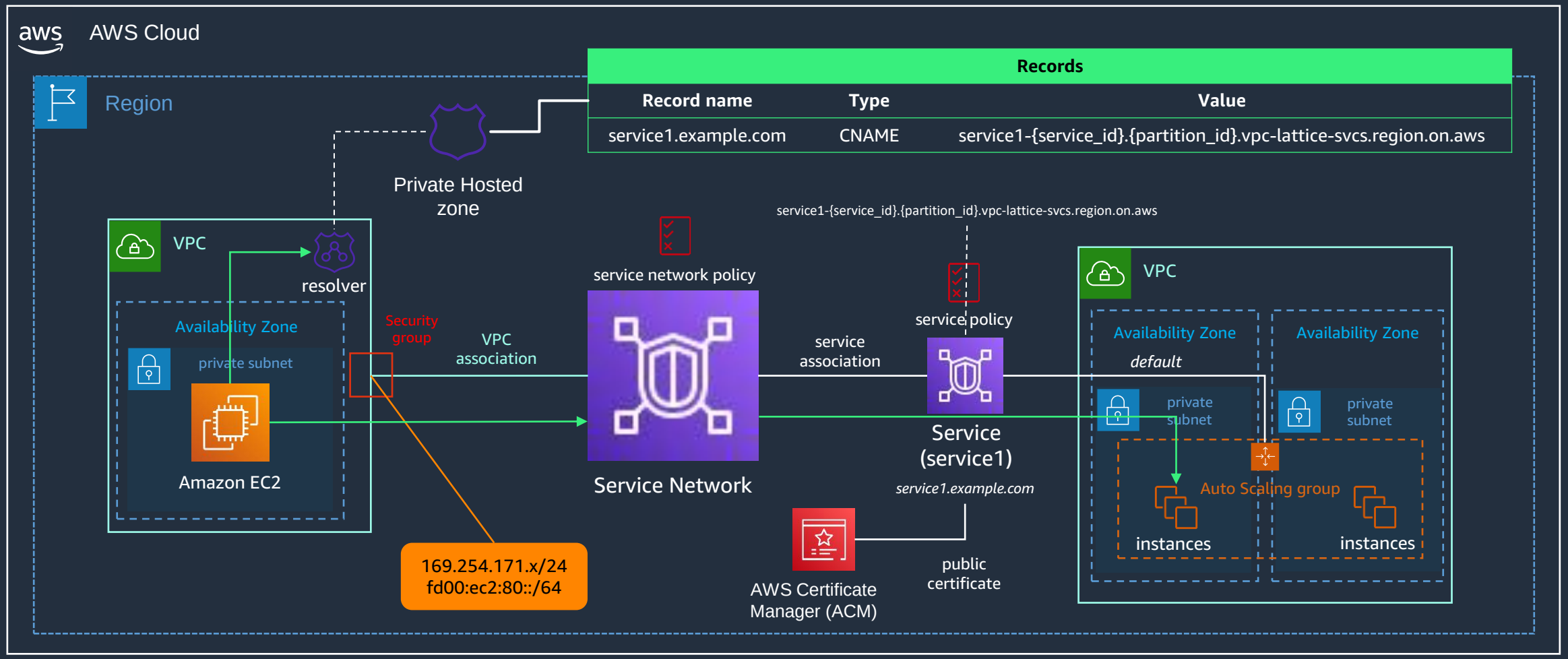
Service directory

- Centralized registry of services

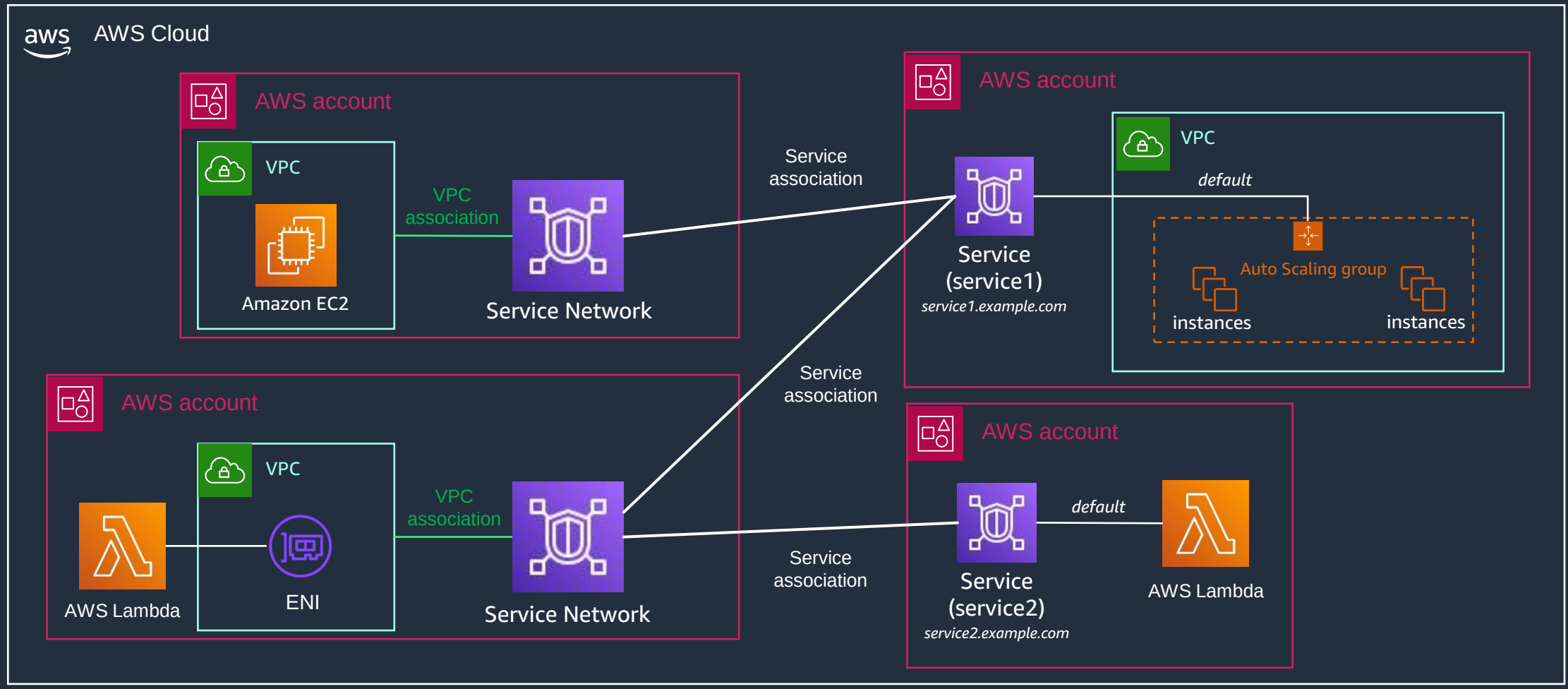
Auth policies

- Declarative policies for access, observability, and traffic management
- Applied at the service, gateway, or application network level

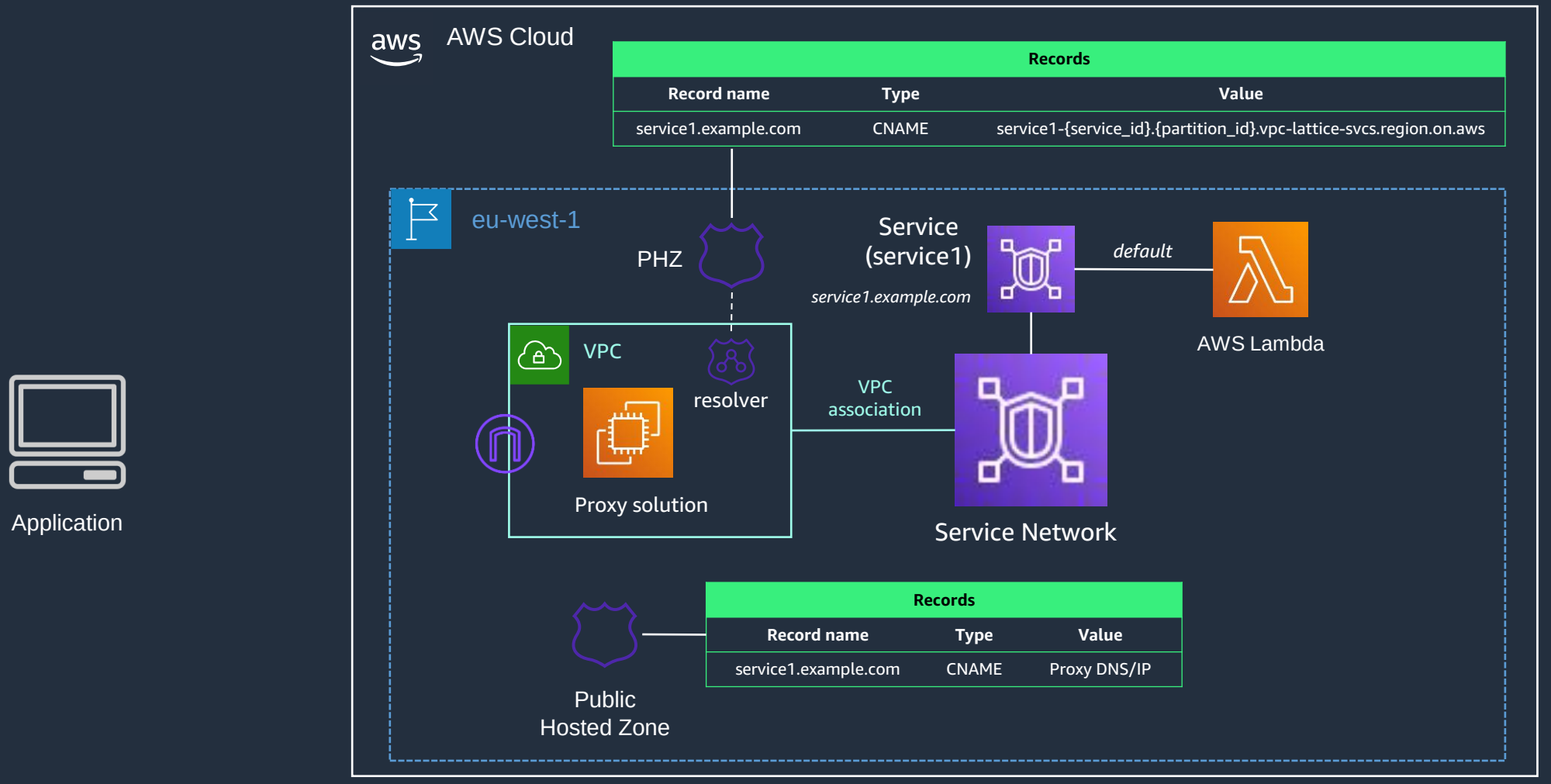
Amazon VPC Lattice Traffic Flow



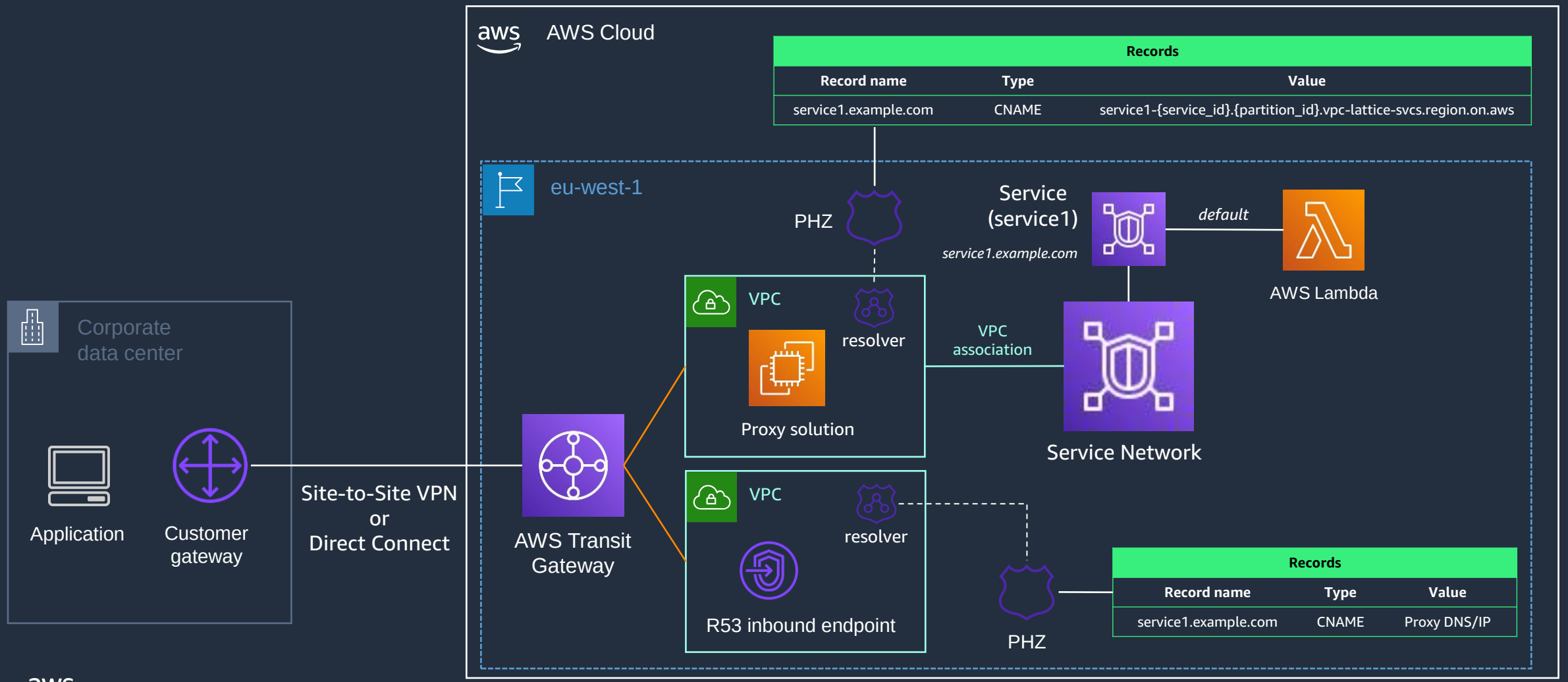
Amazon VPC Lattice Patterns - Distributed



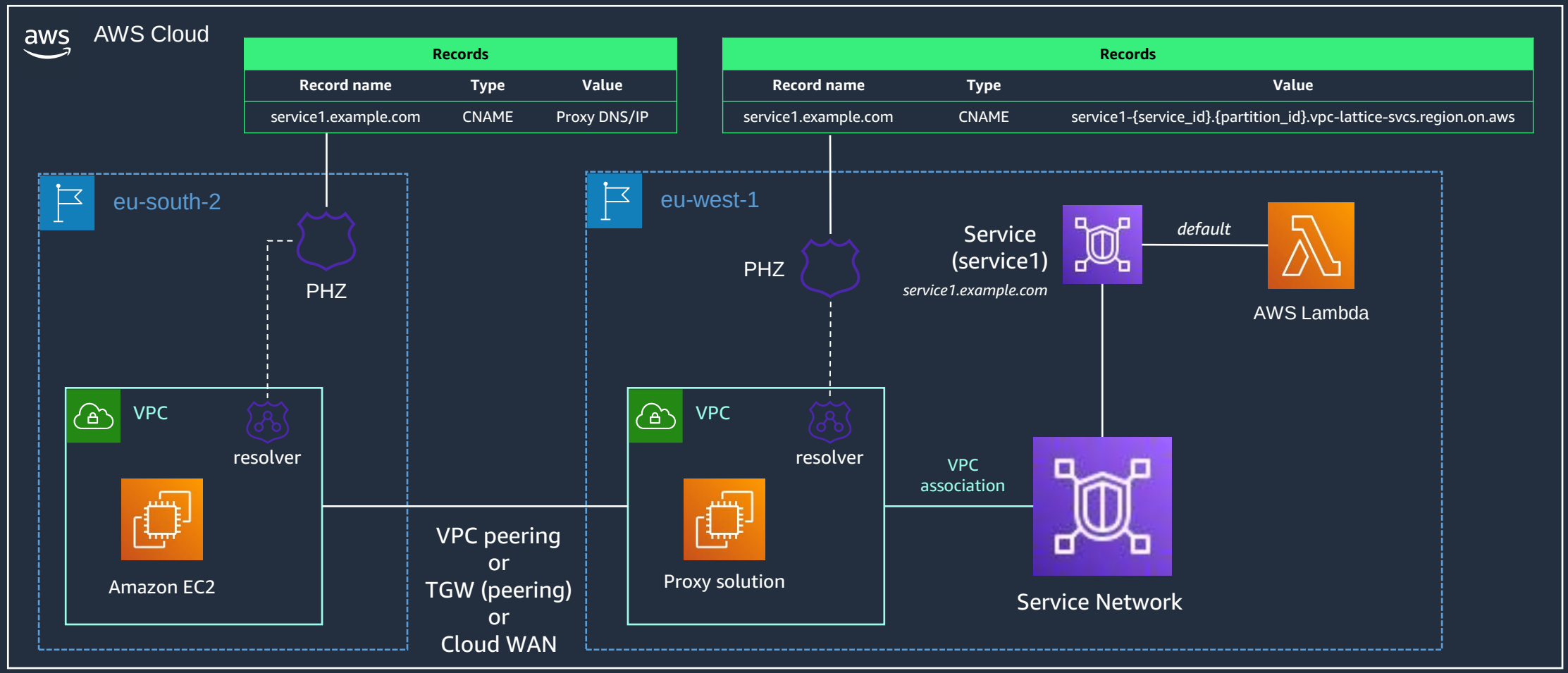
Amazon VPC Lattice – Ingress (External)



Amazon VPC Lattice – Ingress (Hybrid)



Amazon VPC Lattice – Ingress (Cross-region)



Selecting the best fit for you needs

AWS PrivateLink

Fast, simple, scalable and secure service access

- TCP only
- Suited for unidirectional session creation, SaaS offerings.

private cross-VPC or hybrid connectivity

- Highly scalable in terms of throughput/resilience

AWS VPC Lattice

Zero Trust L7 Application Routing

- HTTP/S support only (at the moment)
- Granular policy based AuthN and AuthZ
- Support for complex L7 and weight-based routing

Thank you!

Azeem Ayaz
Specialist TAM - Networking

Barbara Bogdanescu
Sr. Technical Account Manager