aviatrix

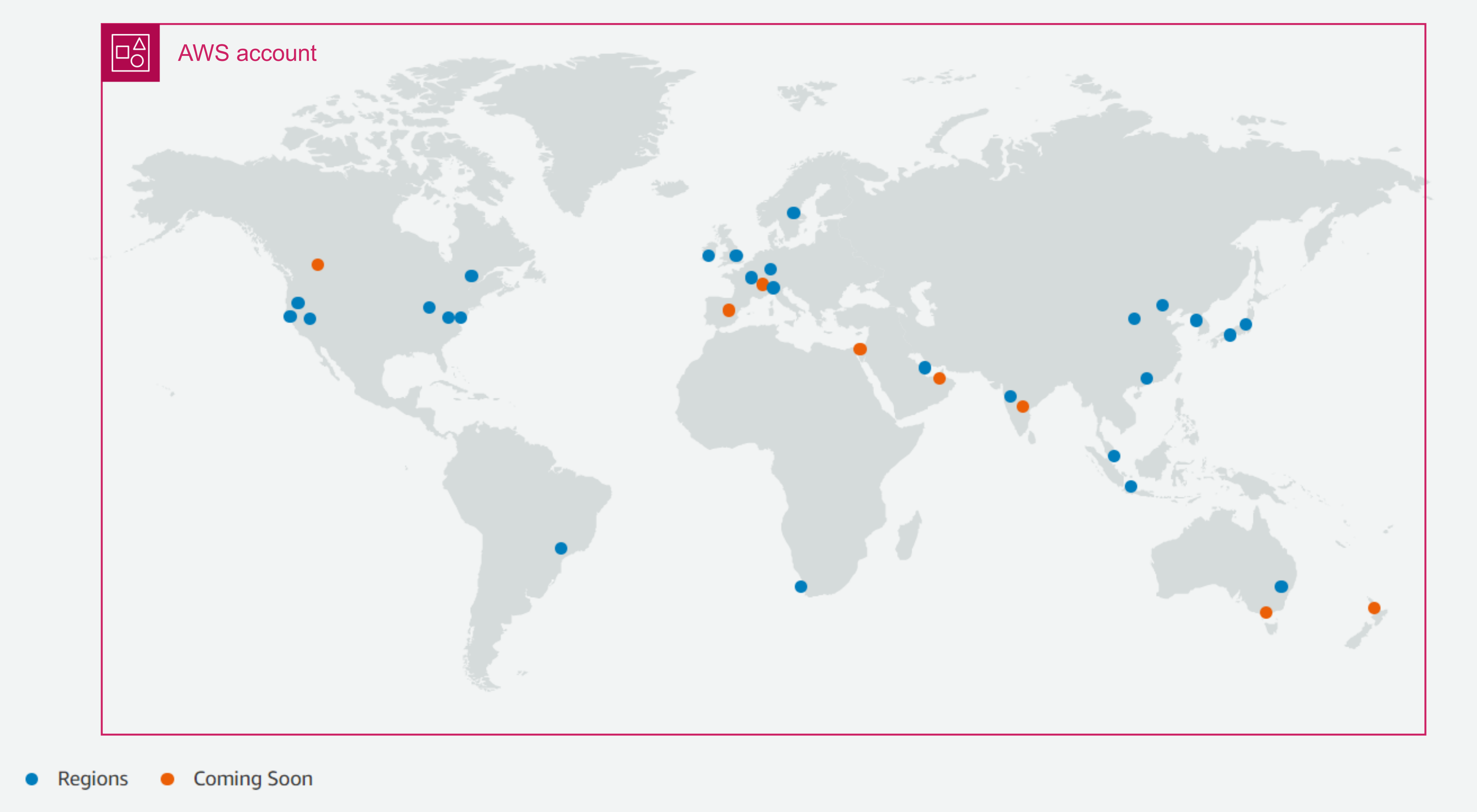
ACE

Aviatrix Certified Engineer

AWS Networking 101

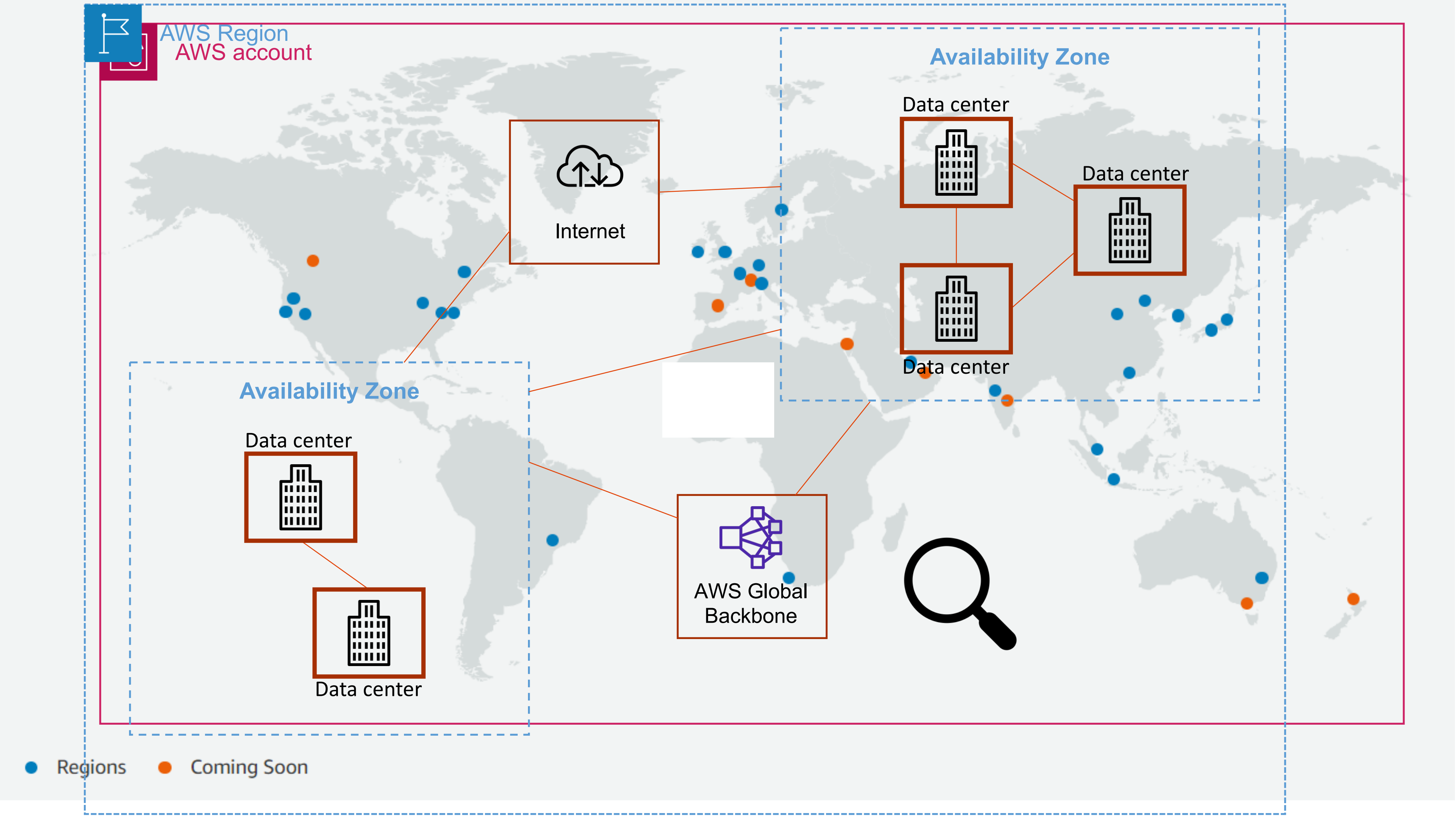
FUNDAMENTALS

AWS Region

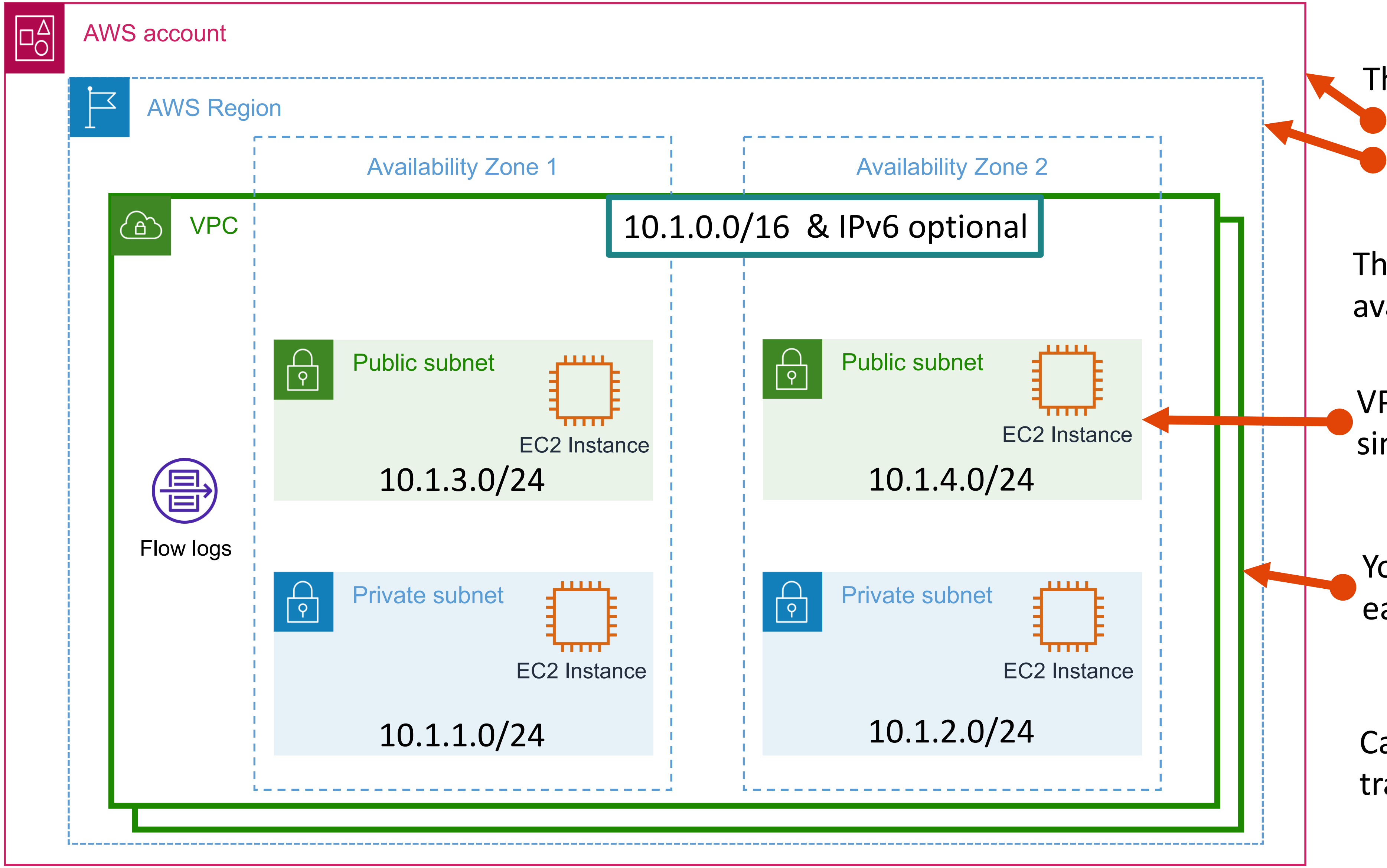


aviatrix

AWS Region


AWS Region
AWS account
Availability Zone
Data center
Data center
Data center
Internet
Availability Zone
Data center
Data center
AWS Global Backbone
● Regions
● Coming Soon

Amazon Virtual Private Cloud (VPC)



The VPC only exists within:

- One AWS Account
- One AWS Region

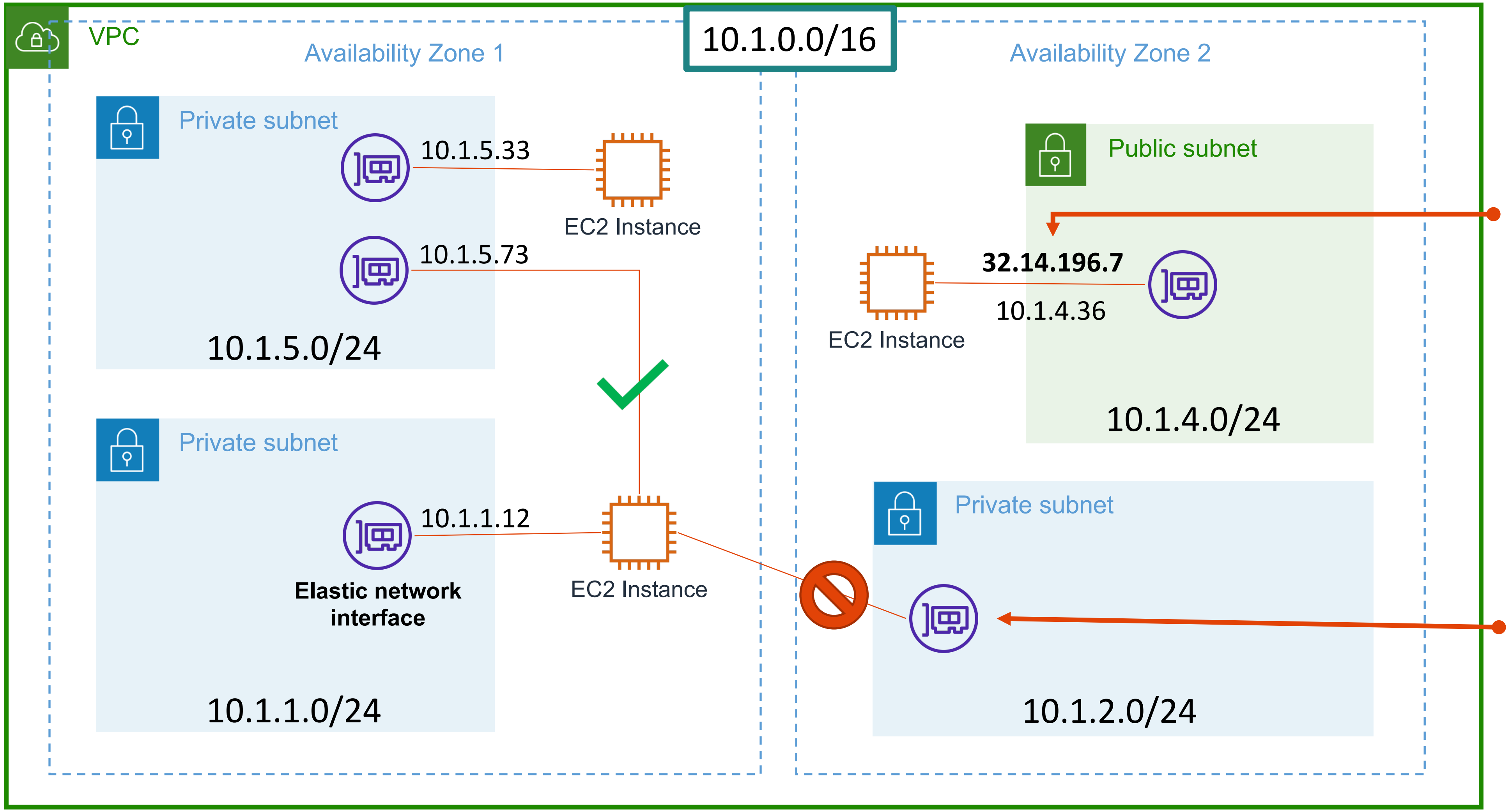
The VPC spans multiple availability zones in a region

VPC Subnet is confined to a single availability zone

You can have many VPCs in each account and region

Can enable VPC Flow logs for traffic flow data

Elastic Network Interface (ENI)

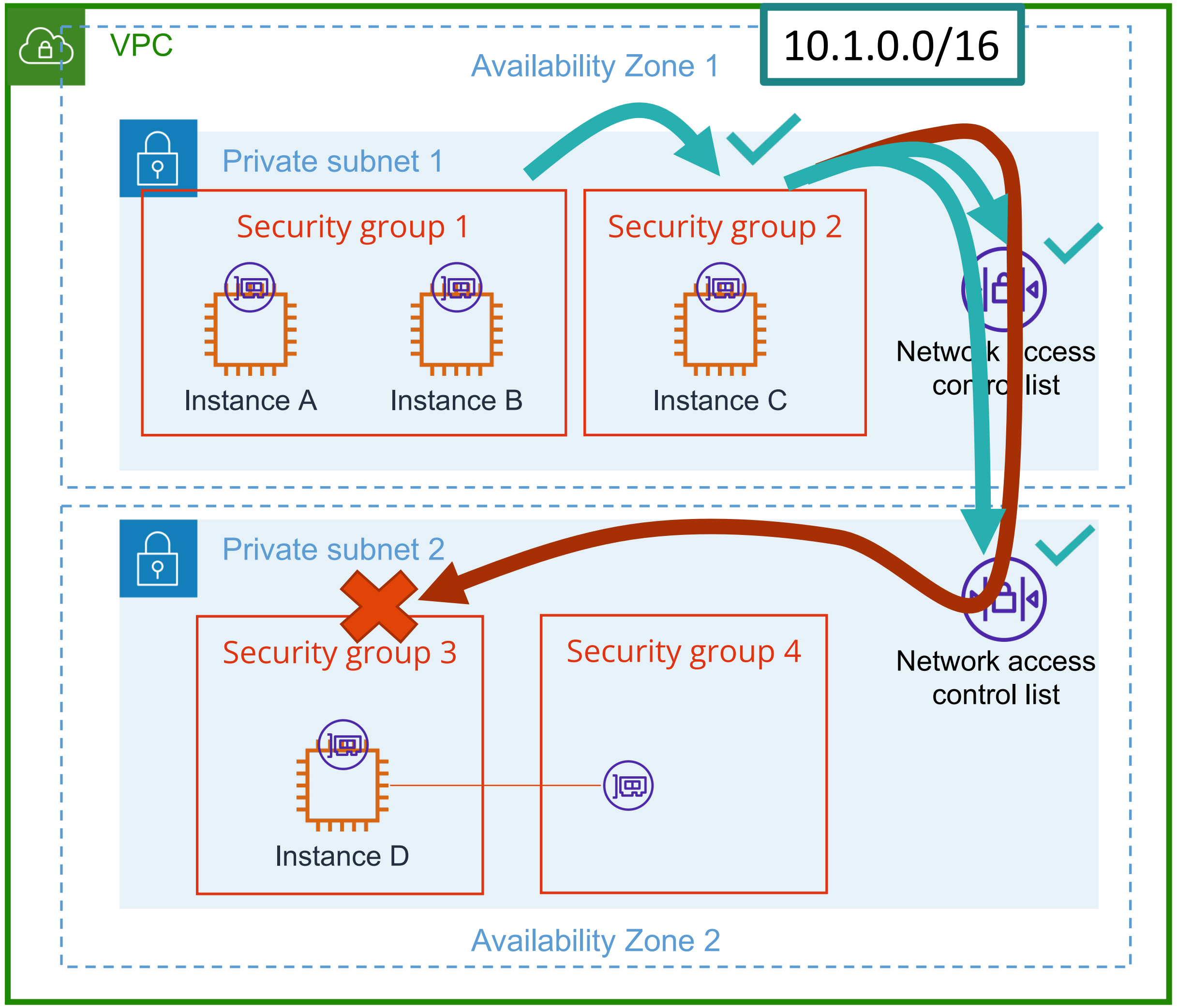


Elastic IP Address (EIP)

Can have multiple ENIs per EC2 instance

ENI and EC2 instance must be in the same availability zone

VPC Security Groups and NACLs



Security Groups

- Protect the EC2 instance
- Can write Allow rules
- Default outbound allow all rule
- Default inbound traffic blocked
- Are stateful
- Rules with IPs or Security Group IDs
- Complex to manage at scale

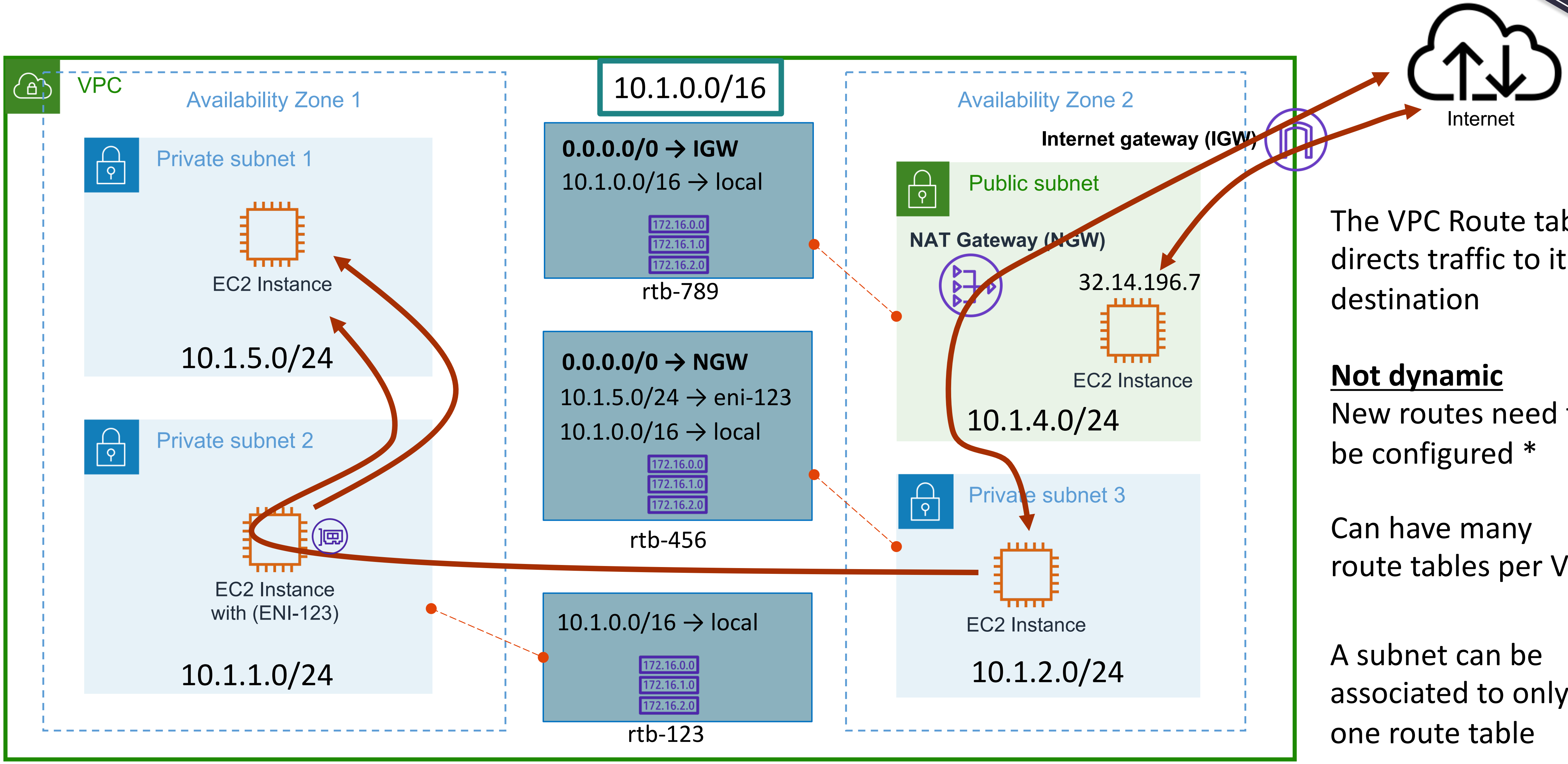
NACLS

- Protect the Subnet
- Default rules allow all inbound and outbound traffic
- Can write Allow and Deny rules
- Are stateless
- Rules with IPs

Example shown

- Security Group 2 is configured with inbound rule allowing traffic from Security Group 1
- NACLs allow by default, Security Group 3 denies inbound by default

VPC Route Tables Internet Gateways (IGW) & NAT Gateways (NGW)



The VPC Route table directs traffic to its destination

Not dynamic

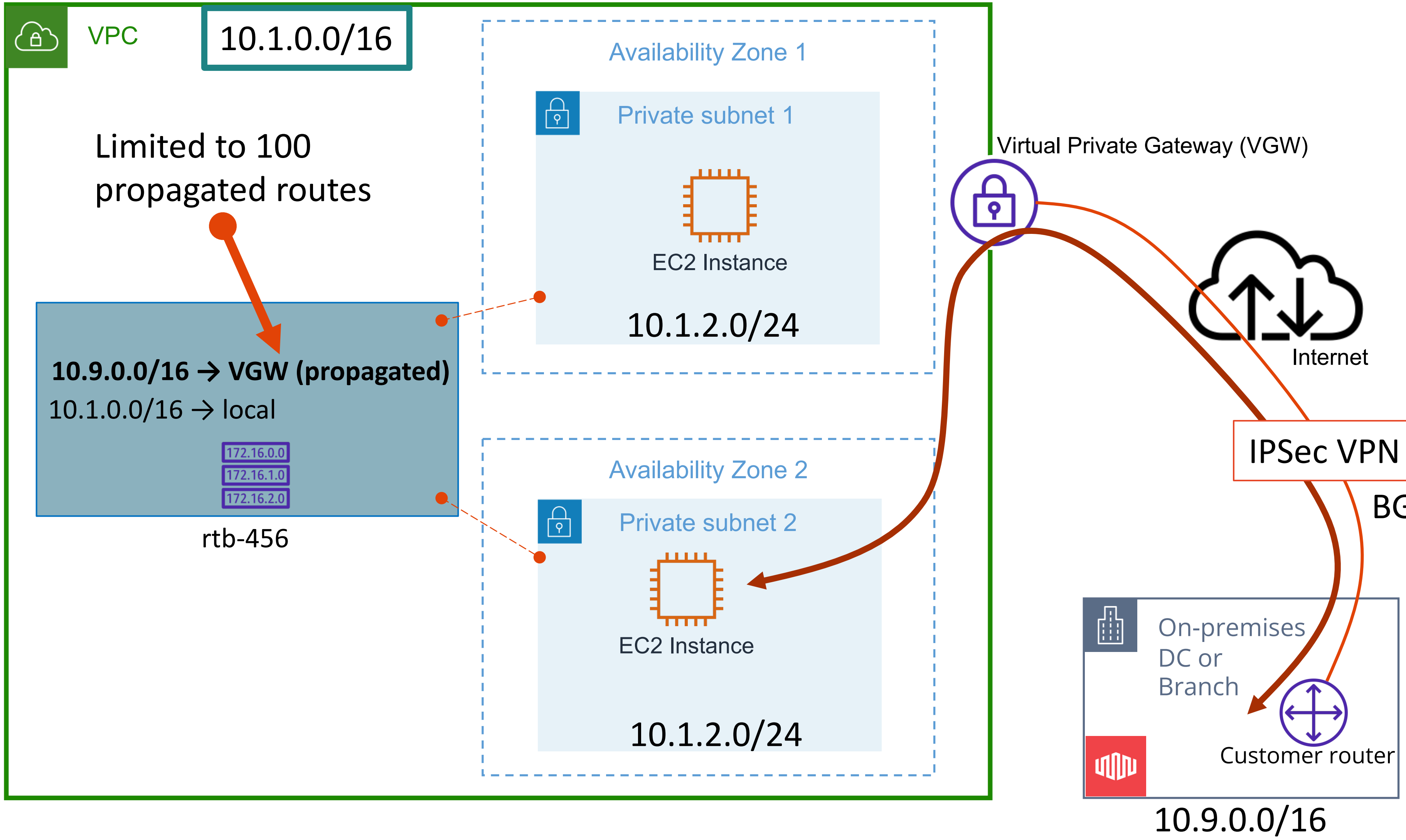
New routes need to be configured *

Can have many route tables per VPC

A subnet can be associated to only one route table

* Except for propagated routes from a VGW

Virtual Private Gateways (VGW)



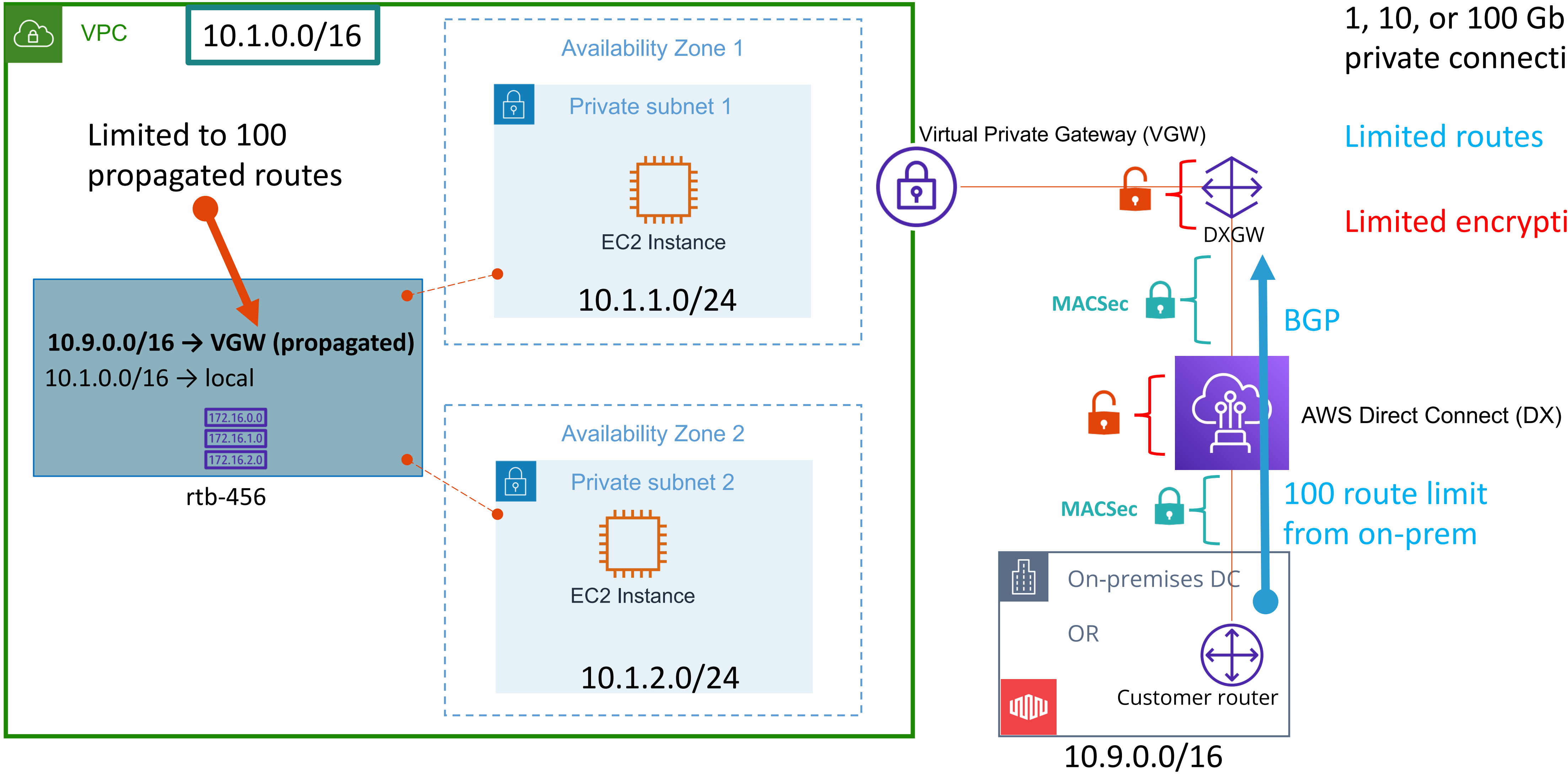
Throughput limited to 1.25 Gbps

AWS Direct Connect

1, 10, or 100 Gbps private connection

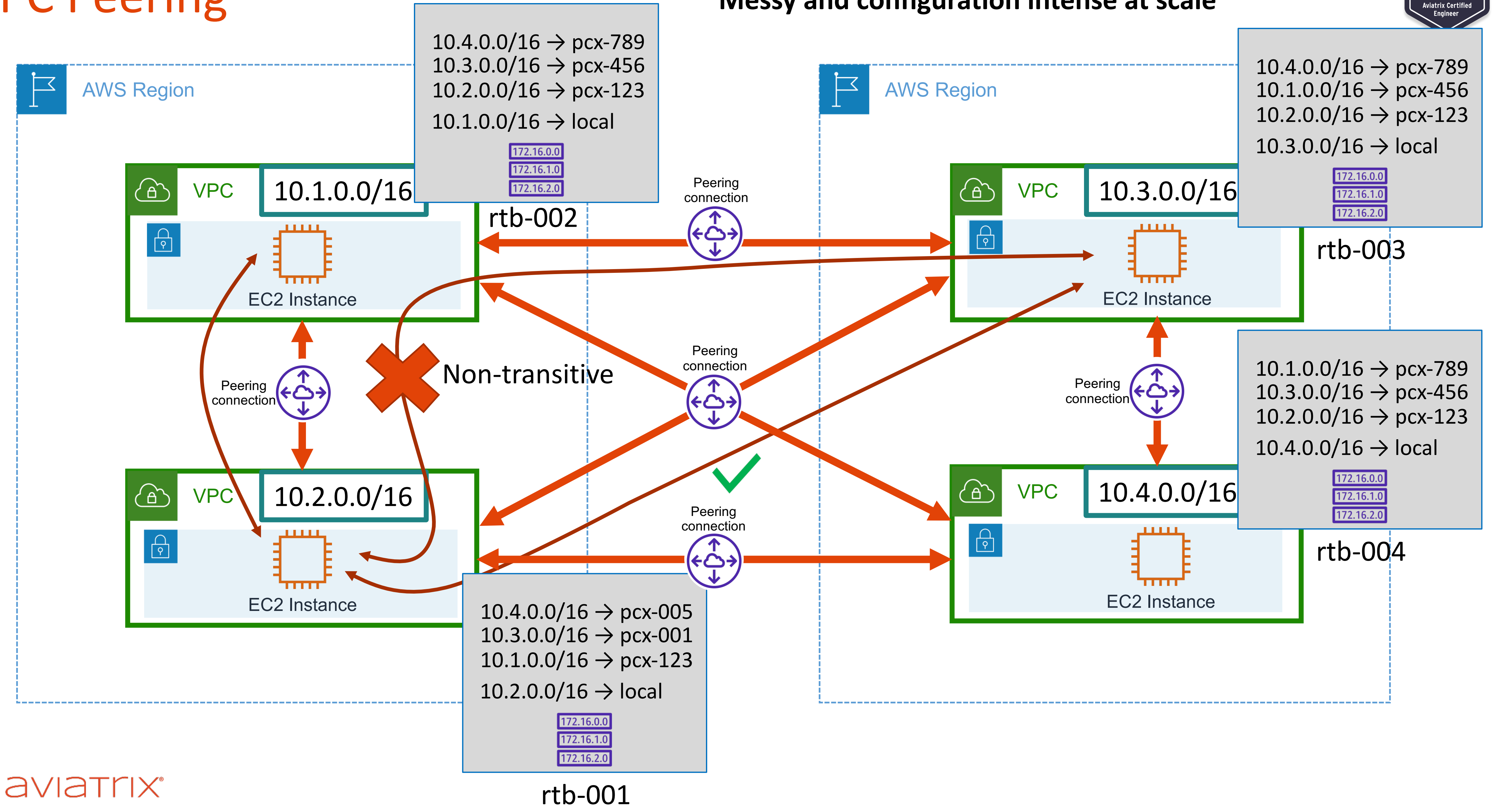
Limited routes

Limited encryption



VPC Peering

Full mesh required
Messy and configuration intense at scale



10.4.0.0/16 → pcx-789
10.3.0.0/16 → pcx-456
10.2.0.0/16 → pcx-123
10.1.0.0/16 → local

rtb-002

10.4.0.0/16 → pcx-789
10.1.0.0/16 → pcx-456
10.2.0.0/16 → pcx-123
10.3.0.0/16 → local

rtb-003

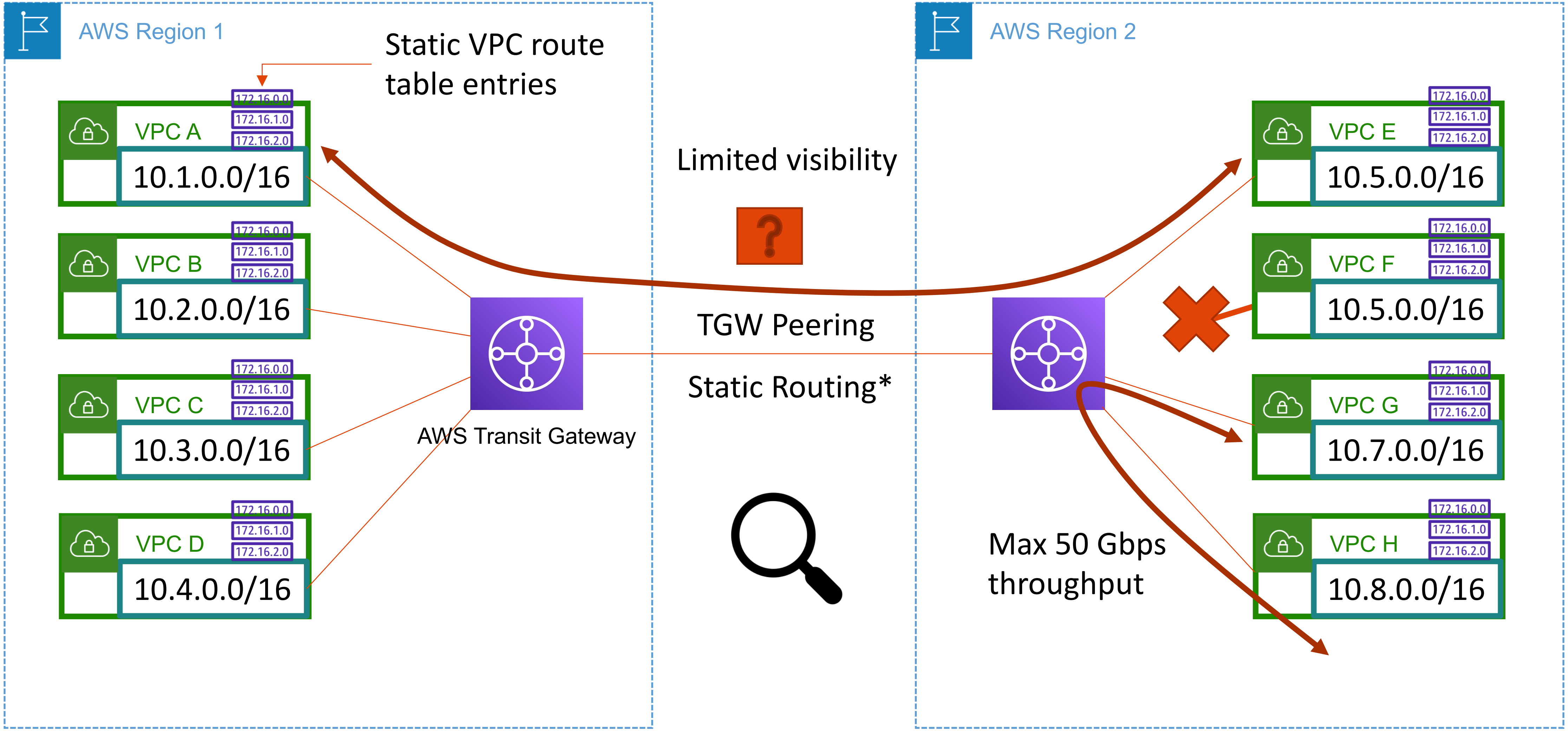
10.1.0.0/16 → pcx-789
10.3.0.0/16 → pcx-456
10.2.0.0/16 → pcx-123
10.4.0.0/16 → local

rtb-004

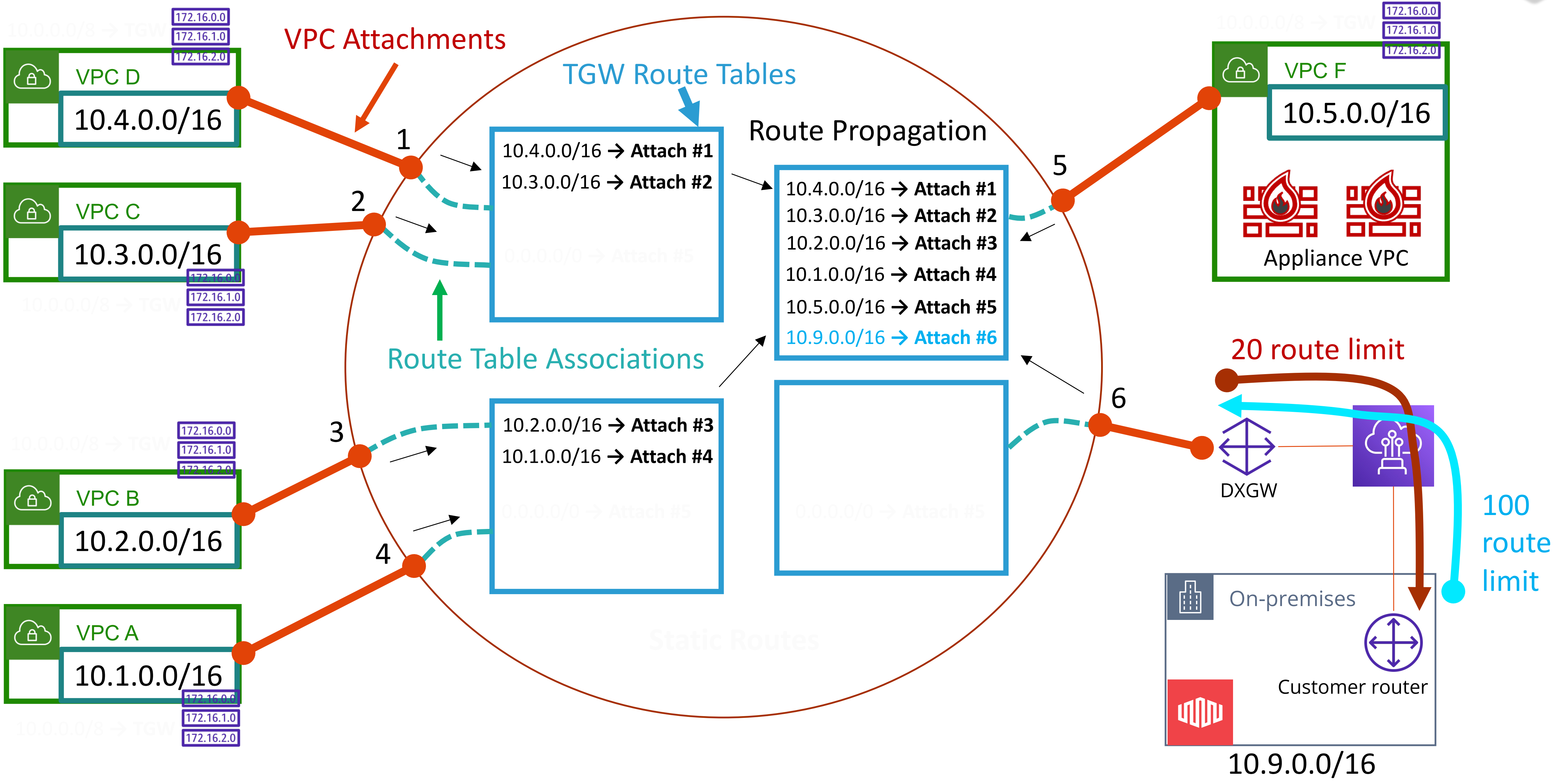
10.4.0.0/16 → pcx-005
10.3.0.0/16 → pcx-001
10.1.0.0/16 → pcx-123
10.2.0.0/16 → local

rtb-001

AWS Transit Gateway (TGW)

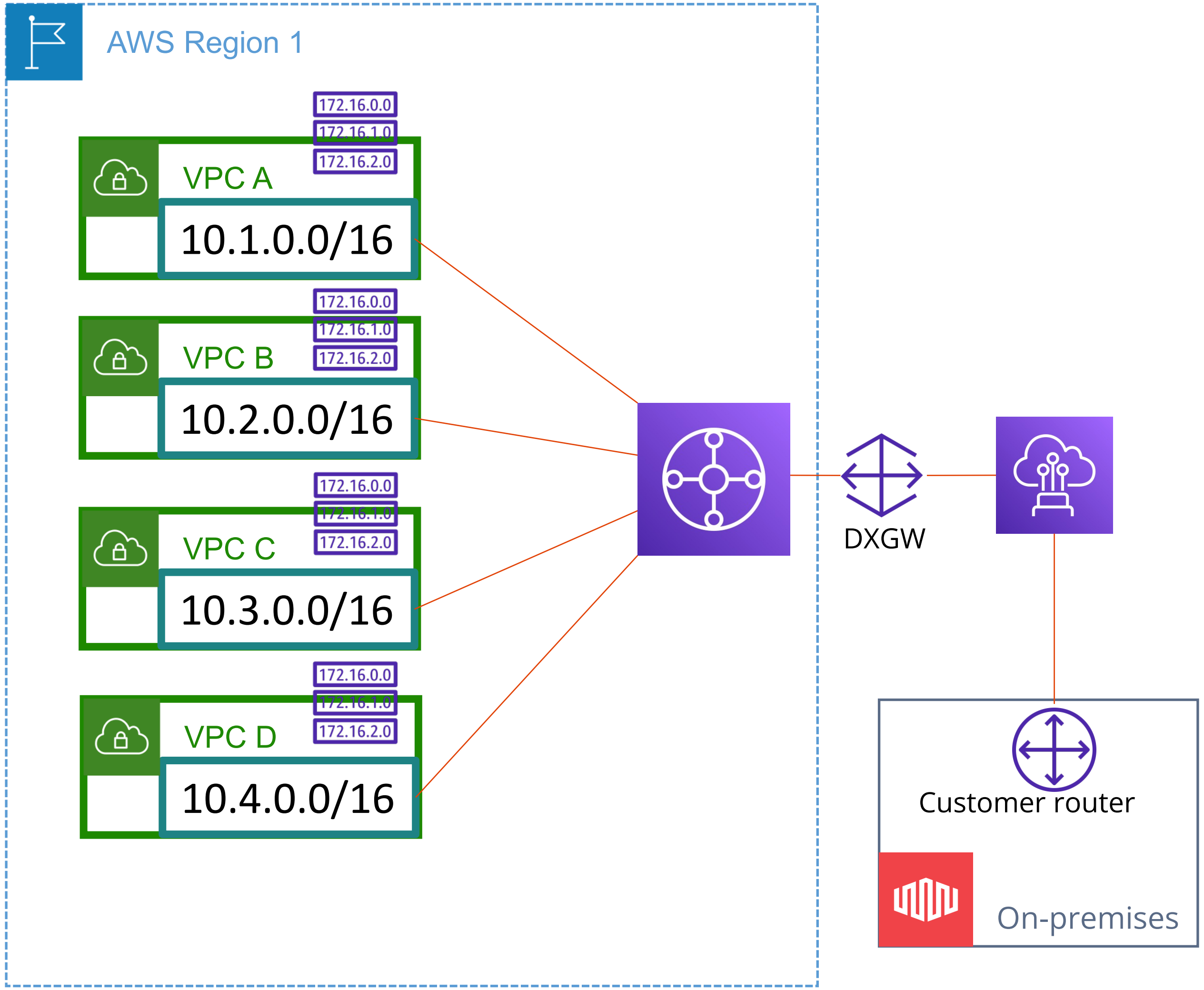


Inside the AWS Transit Gateway (TGW)



AWS Transit Gateway – Operational Visibility Considerations

- Basic Layer 3 connectivity
- Manual and complex traffic steering and isolation
- Manual VPC Route Table management
  - VPC to VPC routes
  - VPC to on-prem routes
- "Black box" – very little visibility
  - No troubleshooting tools like packet captures
- BGP Support
  - Limited routes on DX
  - 20 manually advertised routes to on-prem
  - 100 routes max to AWS (101 route break everything)
  - TGW doesn't pass any BGP attributes to peers
  - No BGP attributes shown in the route table
  - No automatic VPC CIDR summarization



aviatrix

ACE

Aviatrix Certified Engineer

Next: Azure Networking 101