aviatrix

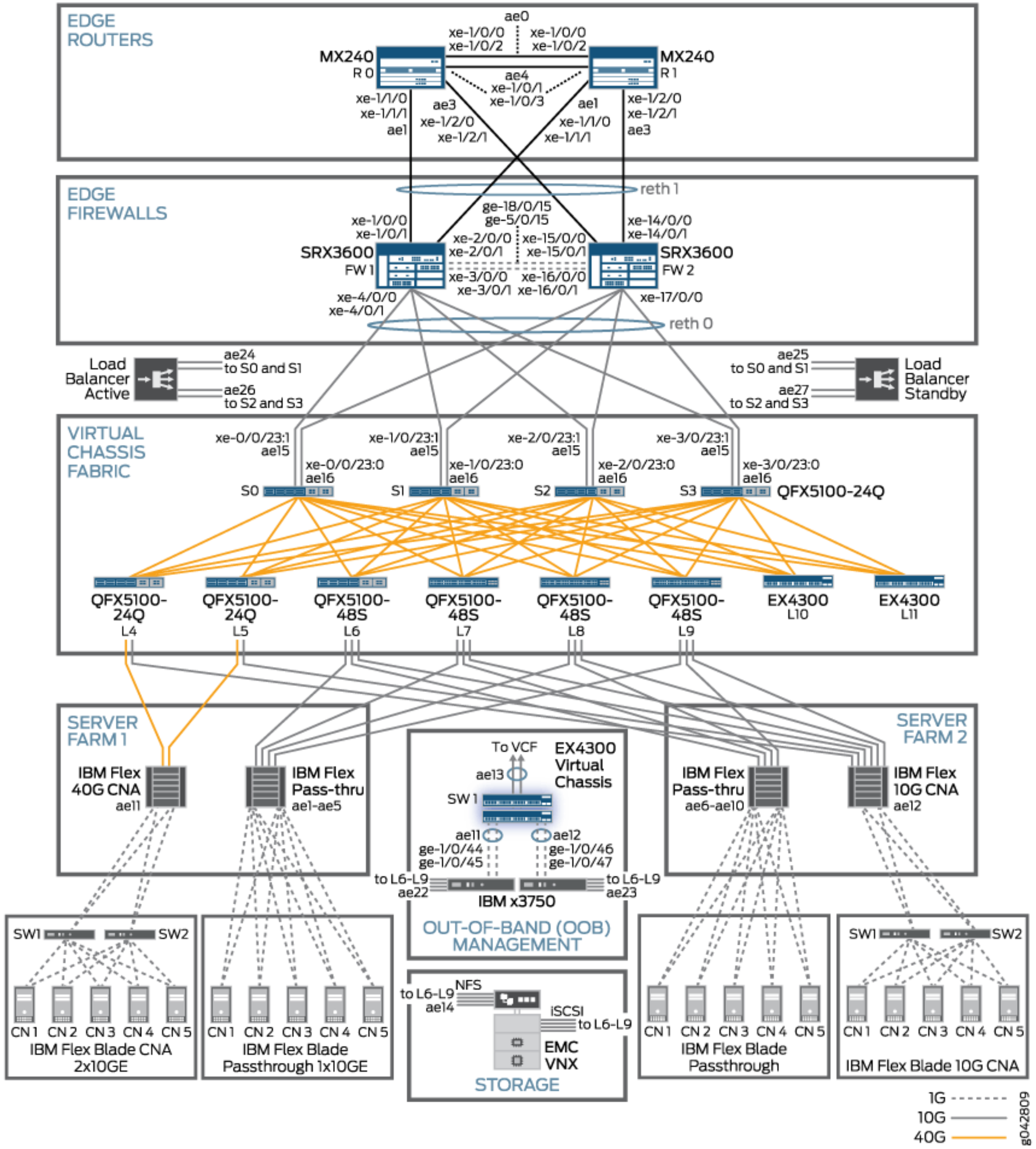
ACE

Aviatrix Certified Engineer

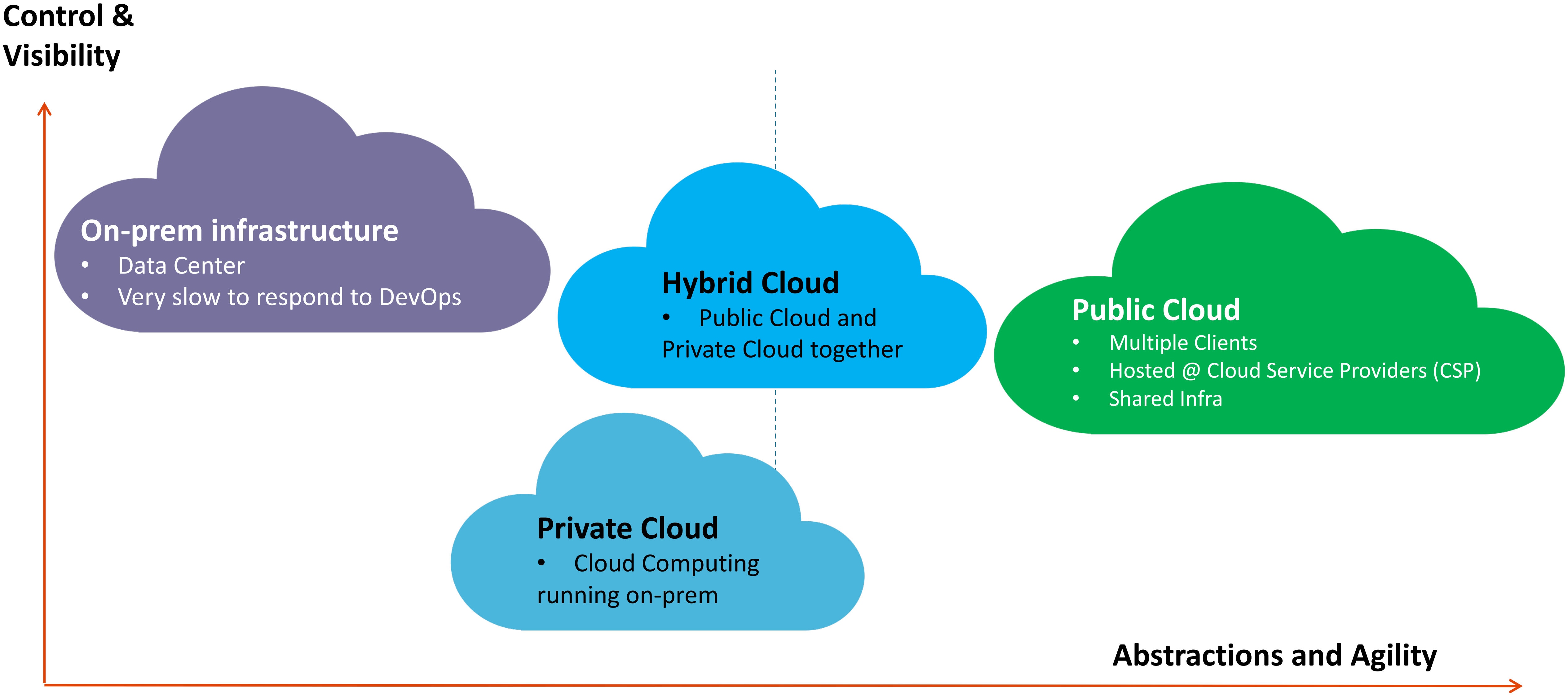
Introduction to Public Cloud Networking

FUNDAMENTALS

On-Prem Data Center Networks Control and Visibility



On-prem infra vs Hybrid Networking vs Private Cloud vs Public Cloud vs Hybrid Cloud



Control & Visibility

On-prem infrastructure

- Data Center
- Very slow to respond to DevOps

Hybrid Cloud

- Public Cloud and Private Cloud together

Public Cloud

- Multiple Clients
- Hosted @ Cloud Service Providers (CSP)
- Shared Infra

Private Cloud

- Cloud Computing running on-prem

Abstractions and Agility

Public Cloud Basics

Public Cloud is just some one else’s data center.
Your data center is/was not perfect and had issues.
Data Centers of Cloud Service Providers are no different.

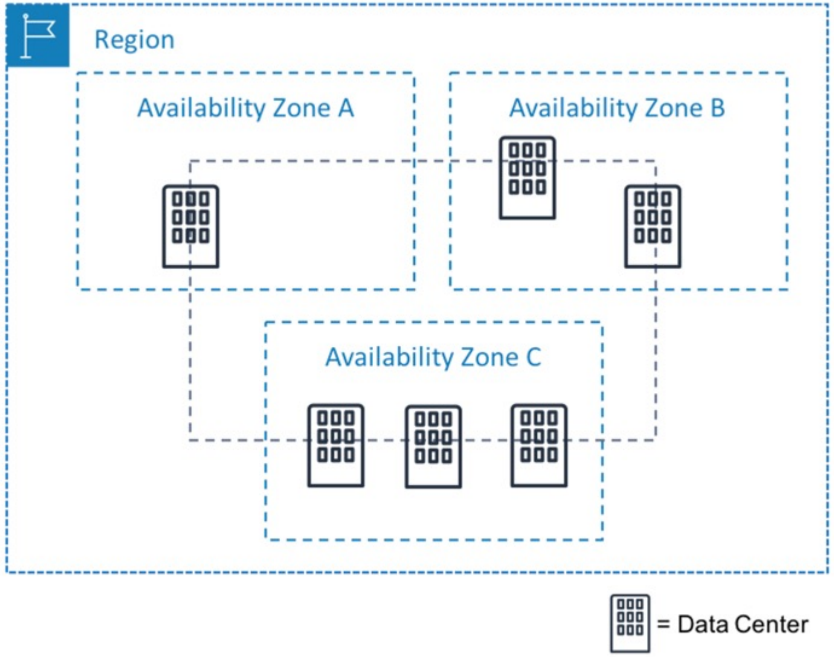
Except you have no visibility or control over it

Region

- Data Centers are grouped in geographic regions to provide **service** availability.
- Examples: US-West, US-East, Europe, Middle East, Australia etc.

Availability Zone (Data Center)

- Distinct locations within a region that are engineered to be isolated from failures
- Low-latency network connectivity to other Availability Zones in the same region
- Not all CSPs have regions with multiple Availability Zones
  - Fault Domains / Availability Domains offer multiple racks / power lines for redundancy
- AZs are randomized outside of an account



Important Services Common to Every CSP

Function	Comments
Identity and Access Management	Who can do What to Which resource
Service	Compute, Storage, Network, Database
Resource	Specific instances that you can create (aka *Constructs*)
Virtual Data Center	Collection of resources that you can create within a geography
Dedicated Connectivity	Private path connectivity from on-prem to CSP region

Networking Areas to Consider in Cloud

- Transit Networking
  - Hub-and-spoke Architecture
  - Intra-region, inter-region, inter-cloud
- Connecting to Data Center over private links
- Connecting to customers and one-off branches
- Connecting to fleet of branches
- Connecting to users
- Connecting resources to Internet
- Connecting to resources from Internet

Consistent routing, ensuring end-to-end network correctness

aviatrix

ACE

Aviatrix Certified Engineer

Next: AWS Networking 101

aviatrix

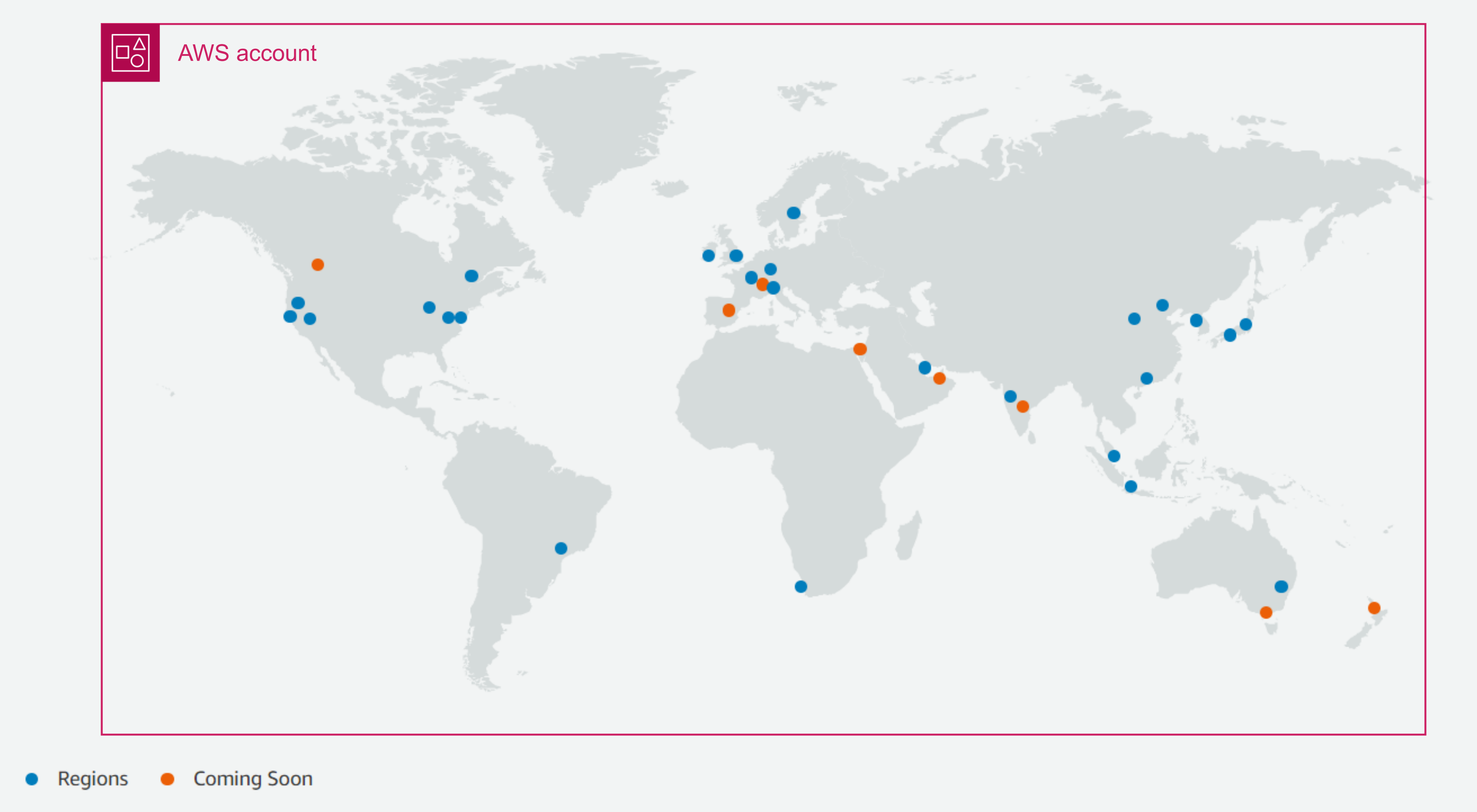
ACE

Aviatrix Certified Engineer

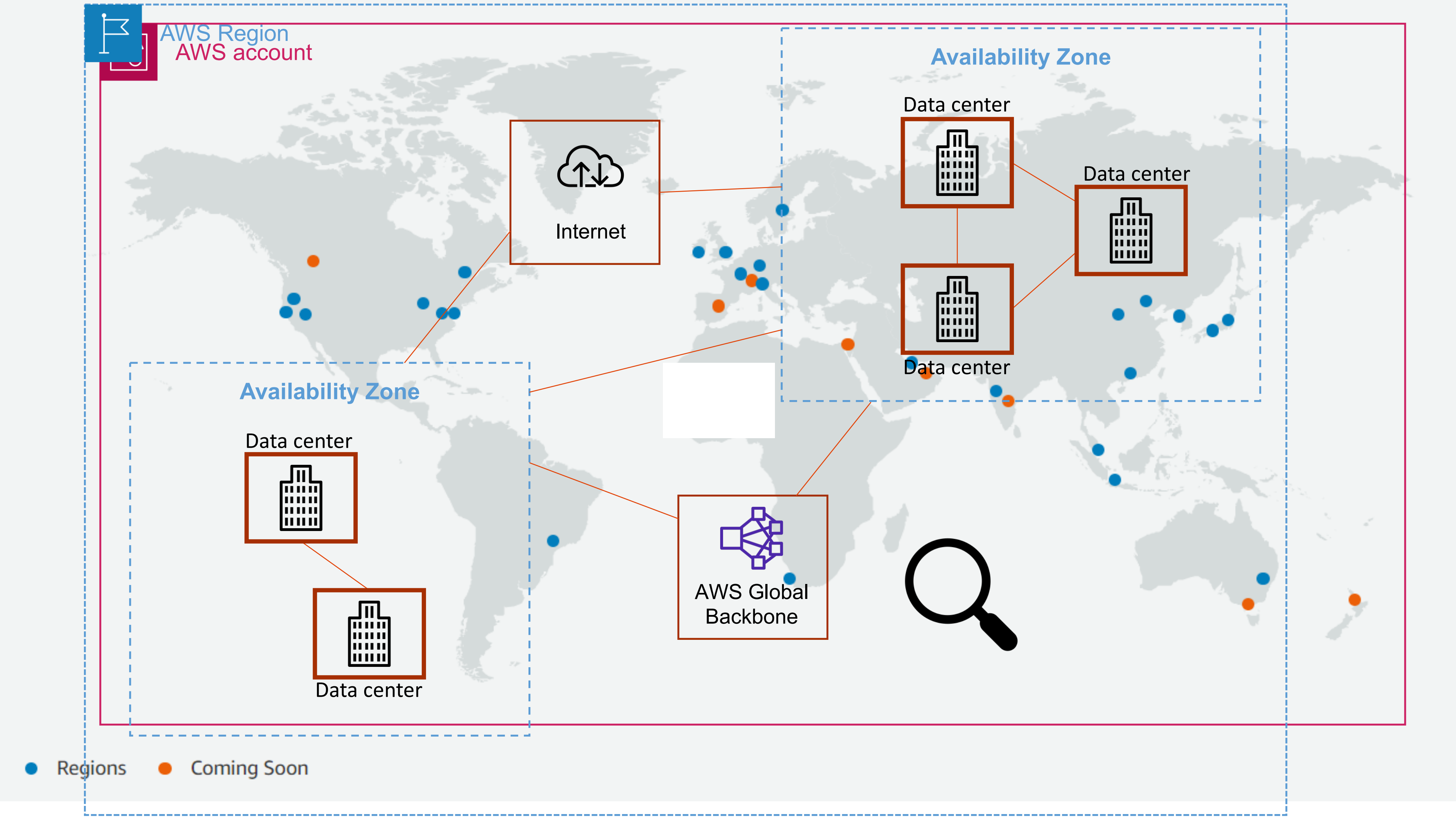
AWS Networking 101

FUNDAMENTALS

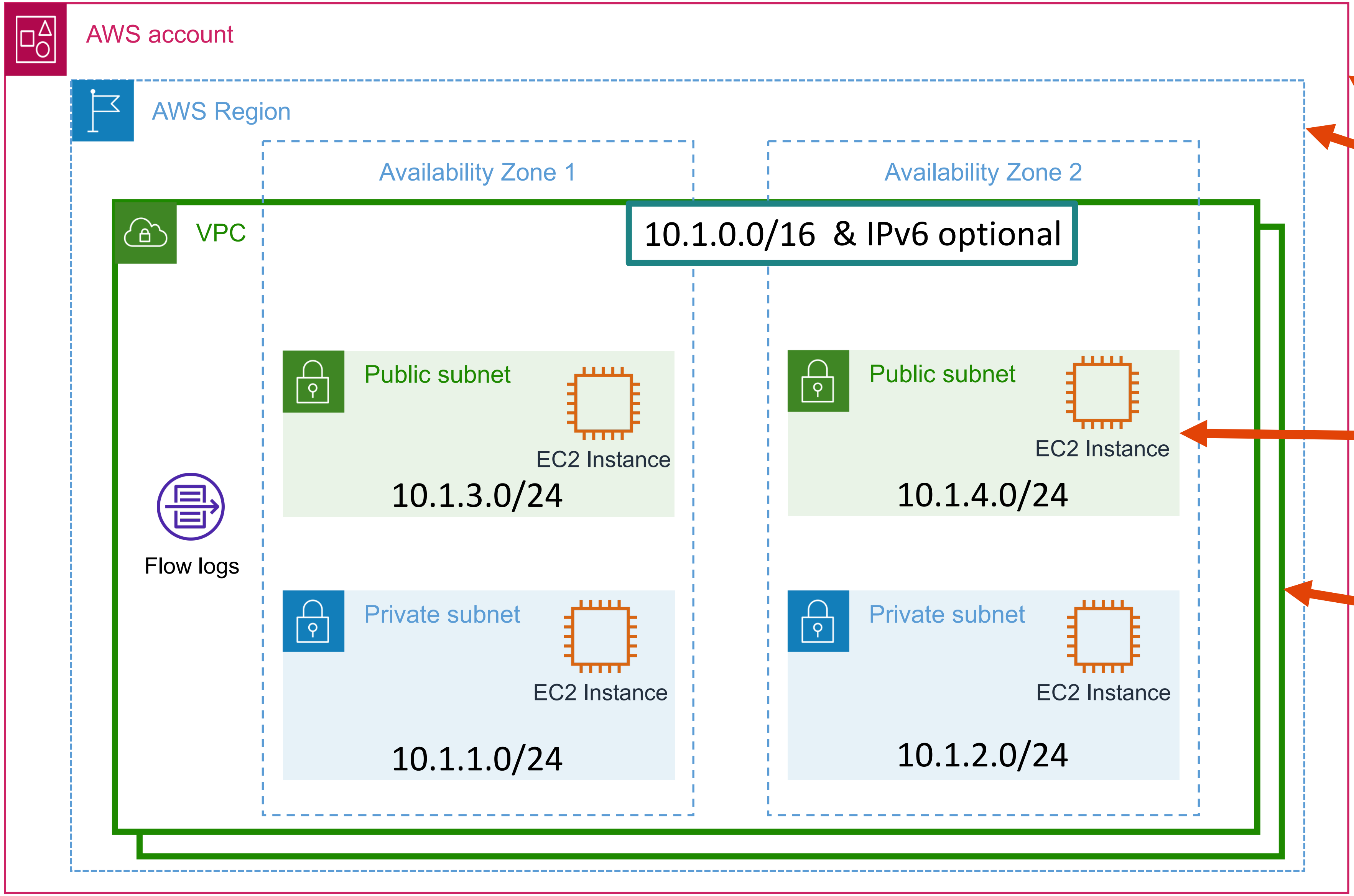
AWS Region



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

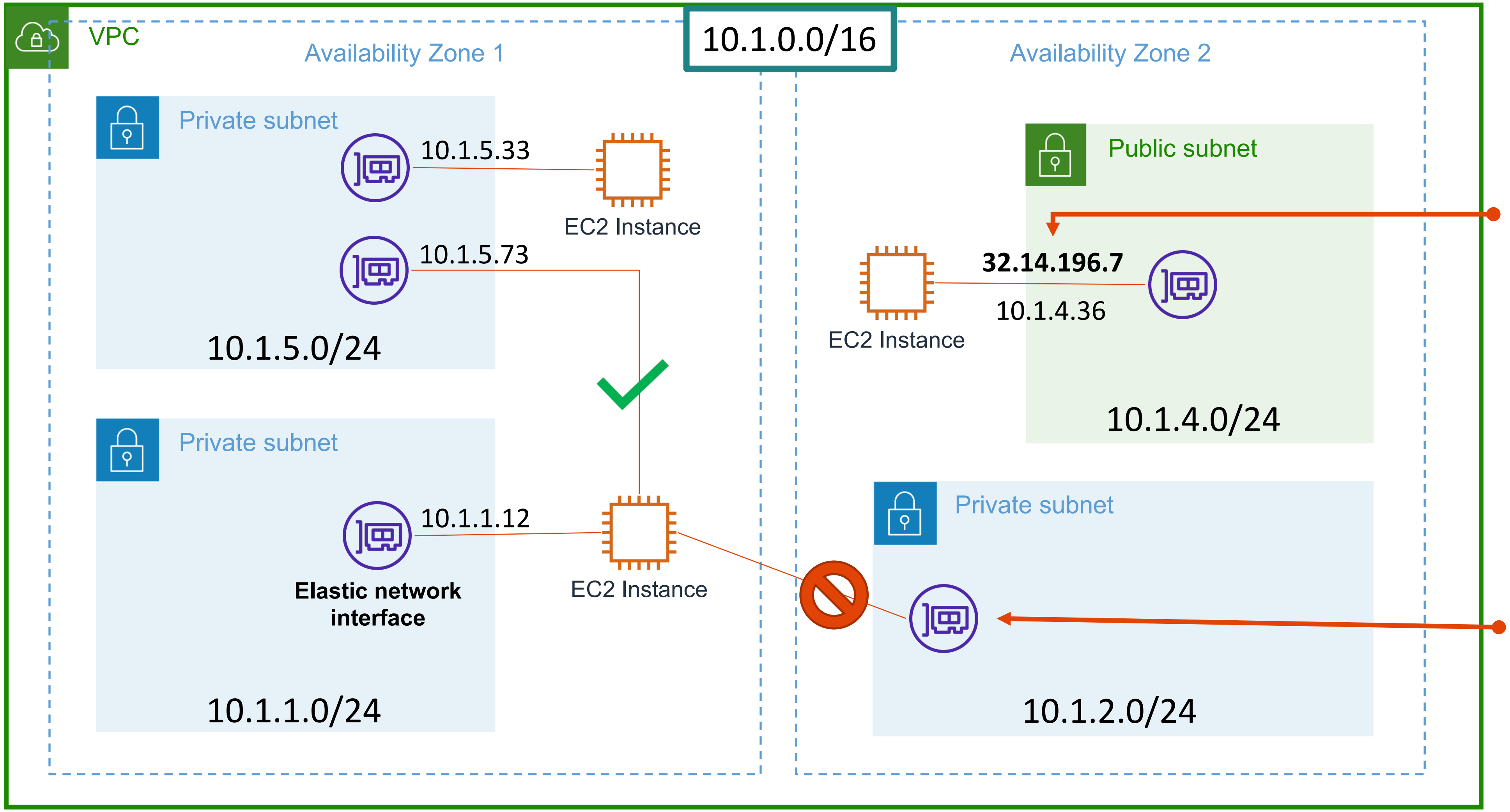
The VPC spans multiple availability zones in a region

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)

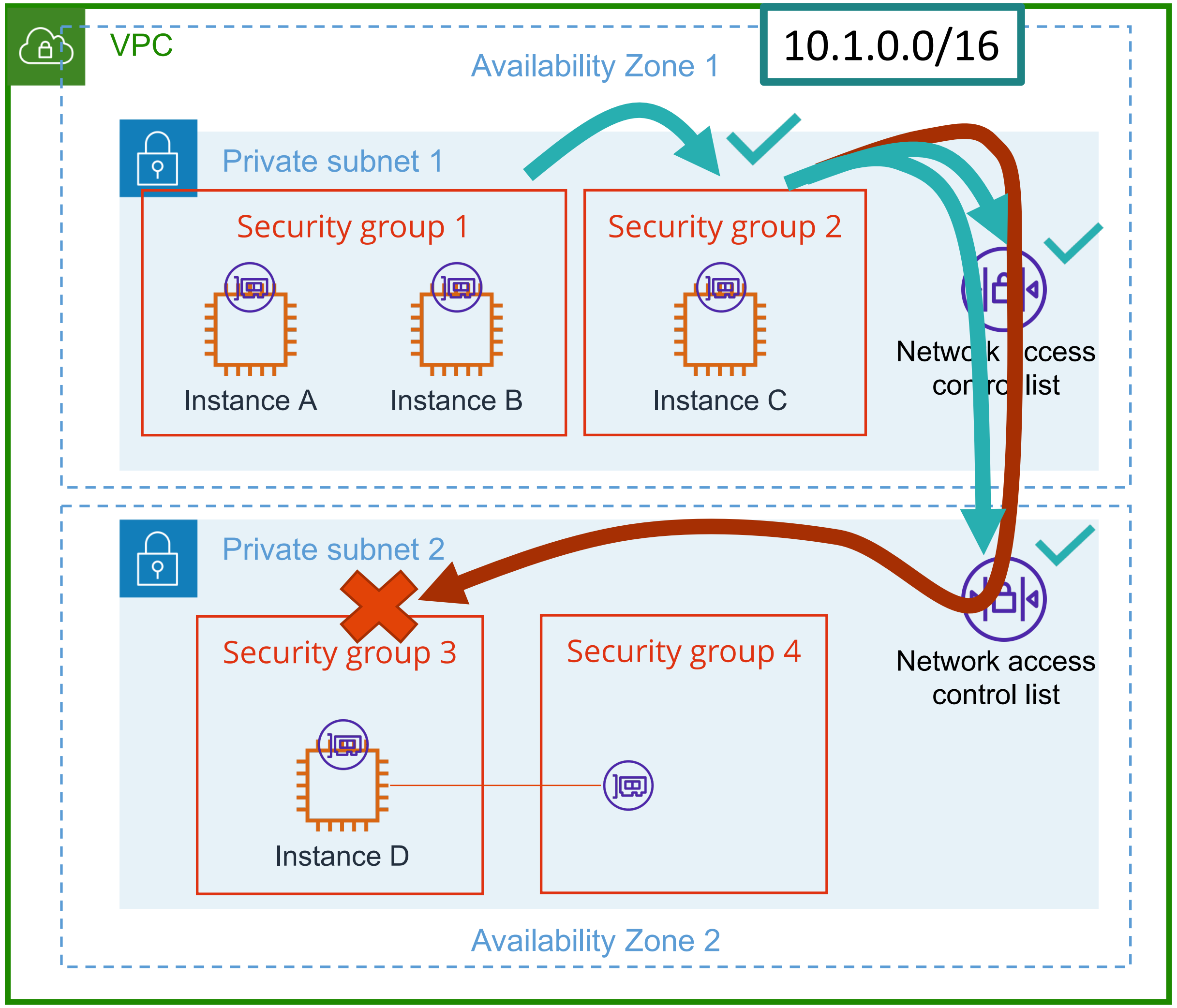


Elastic IP Address (EIP)

Can have multiple ENIs per EC2 instance

ENI and EC2 instance must be in the same availability zone

VPC Security Groups and NACLs



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

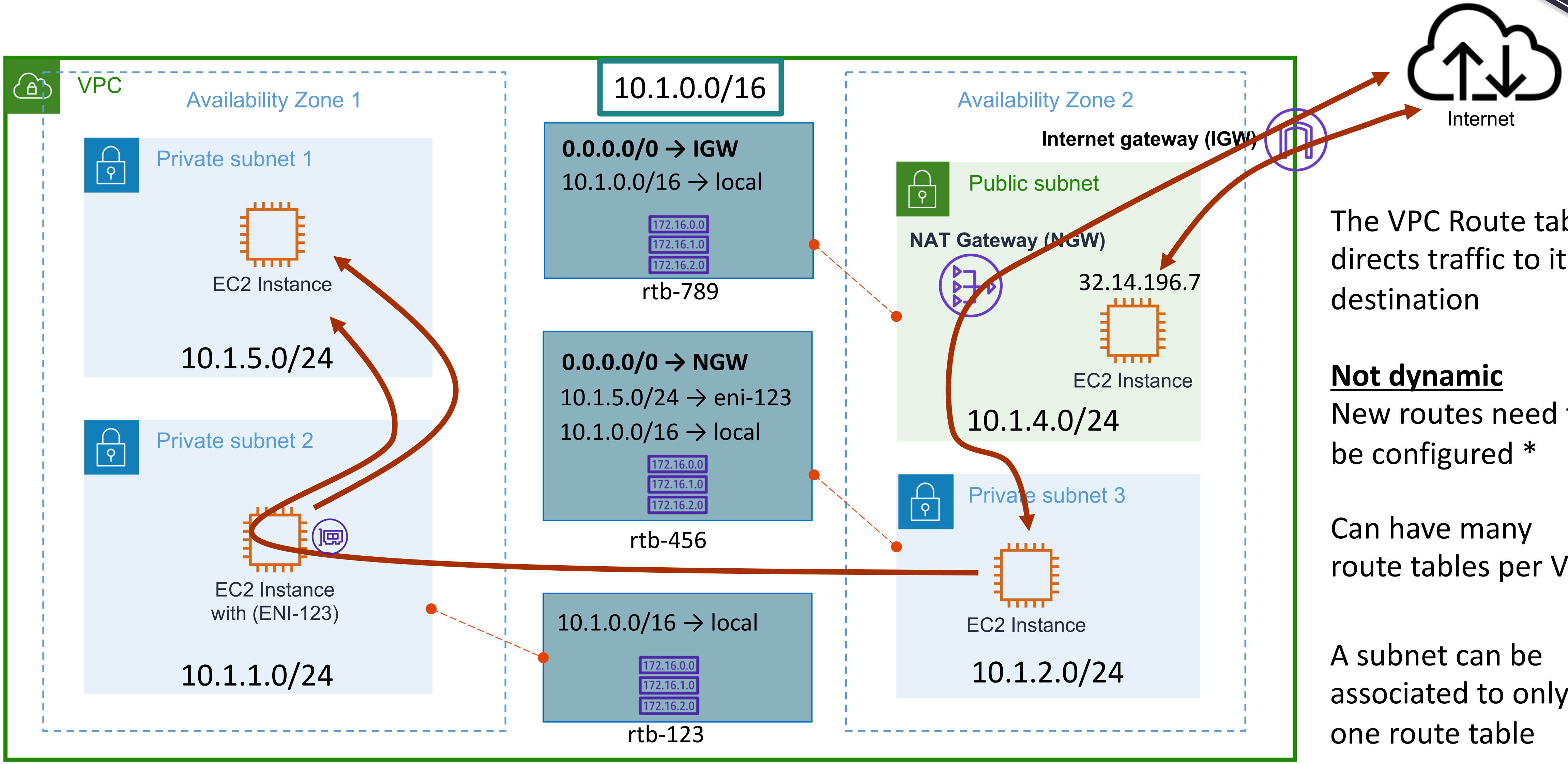
Security Groups

- 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

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



The VPC Route table directs traffic to its destination

Not dynamic

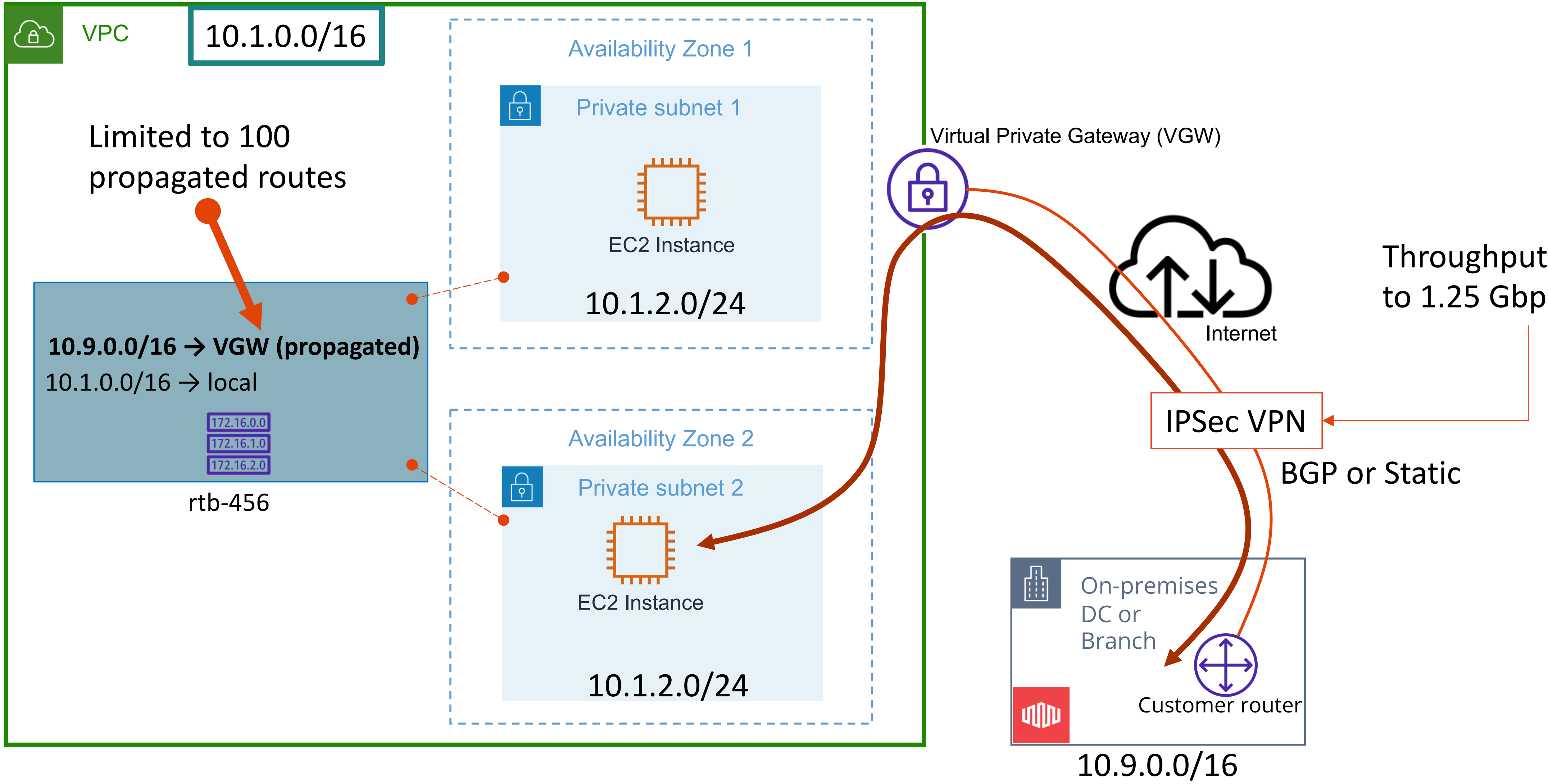
New routes need to be configured *

Can have many route tables per VPC

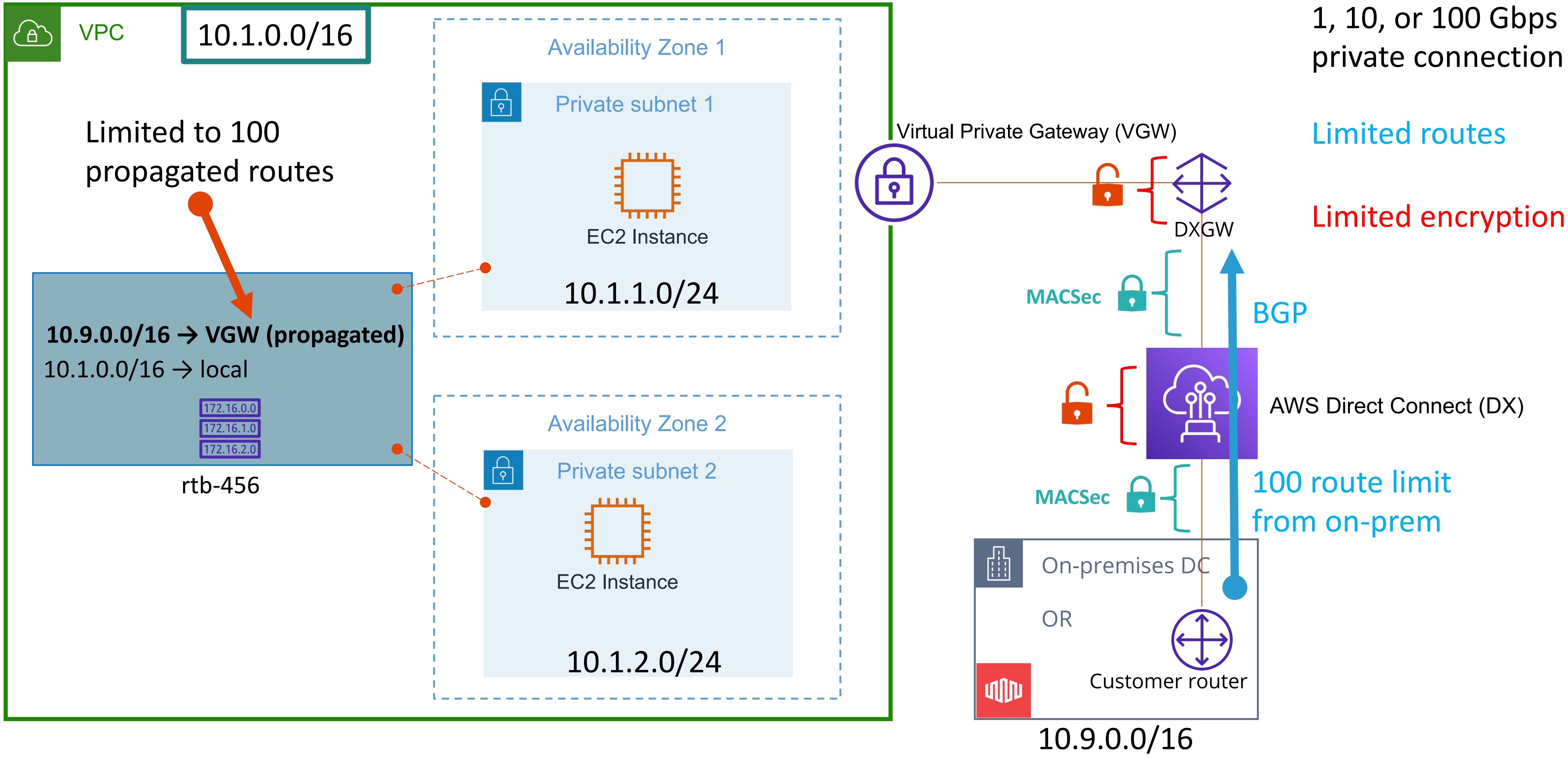
A subnet can be associated to only one route table

* Except for propagated routes from a VGW

Virtual Private Gateways (VGW)



AWS Direct Connect



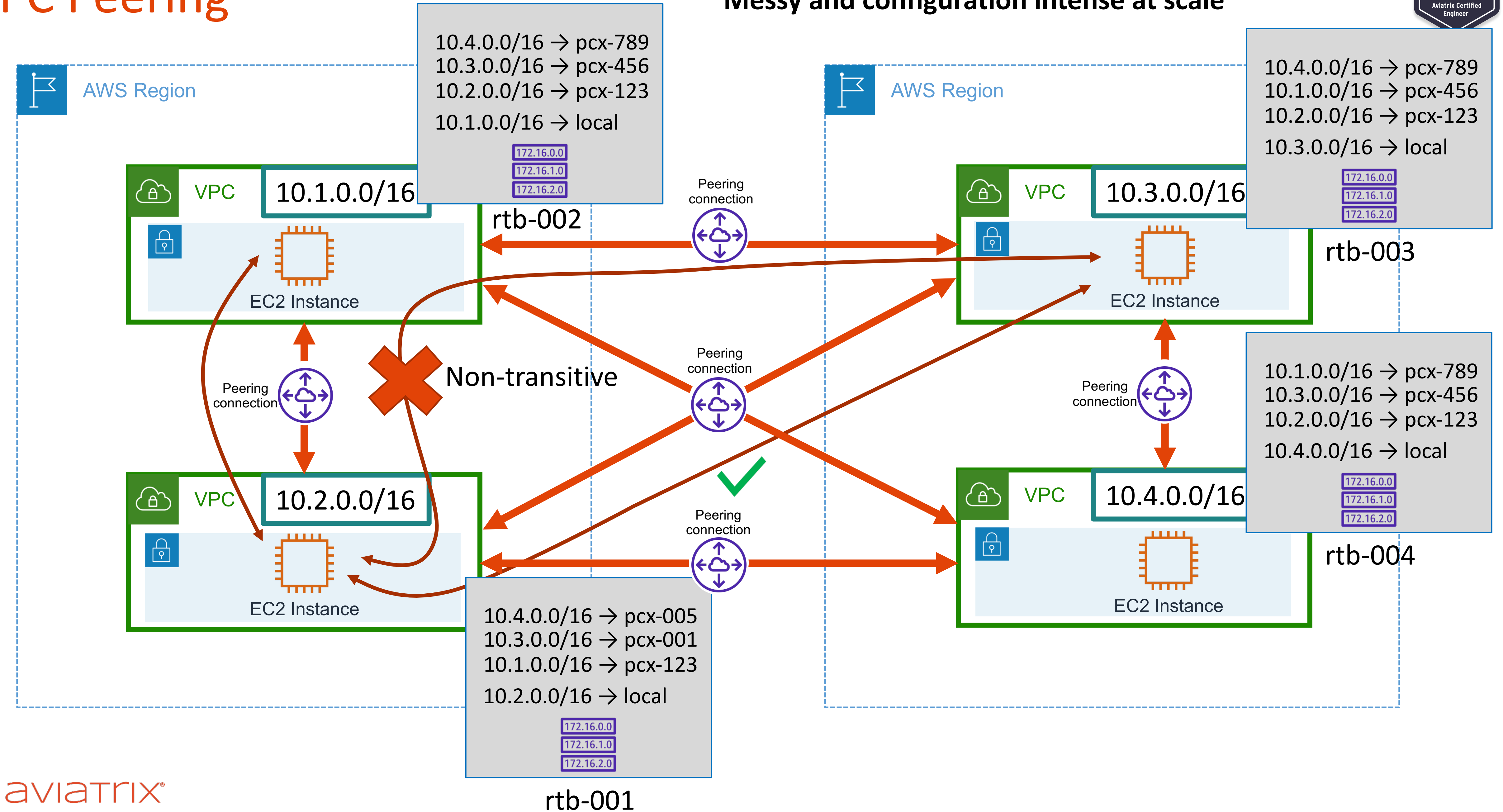
1, 10, or 100 Gbps private connection

Limited routes

Limited encryption

VPC Peering

Full mesh required
Messy and configuration intense at scale



rtb-002

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-003

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

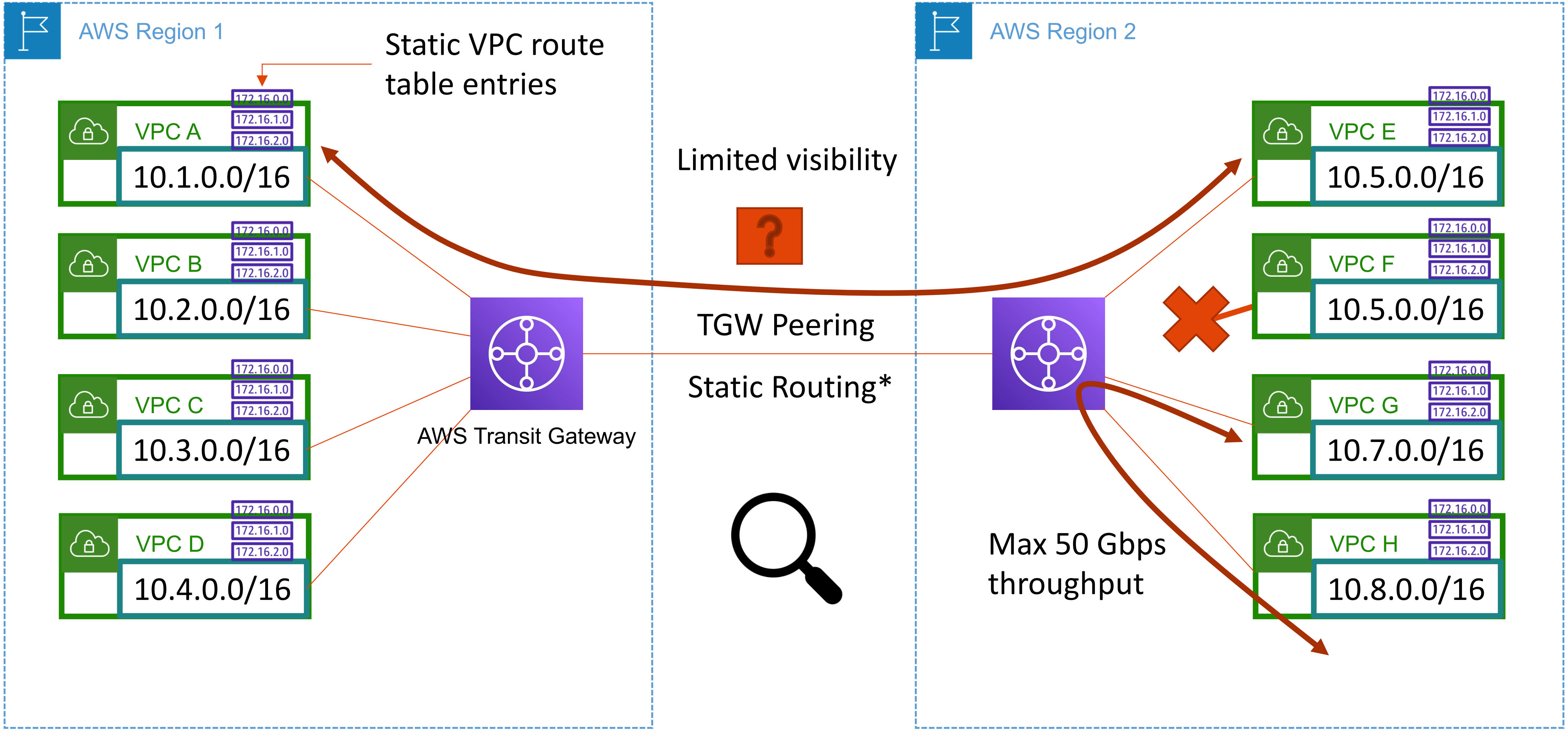
rtb-004

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

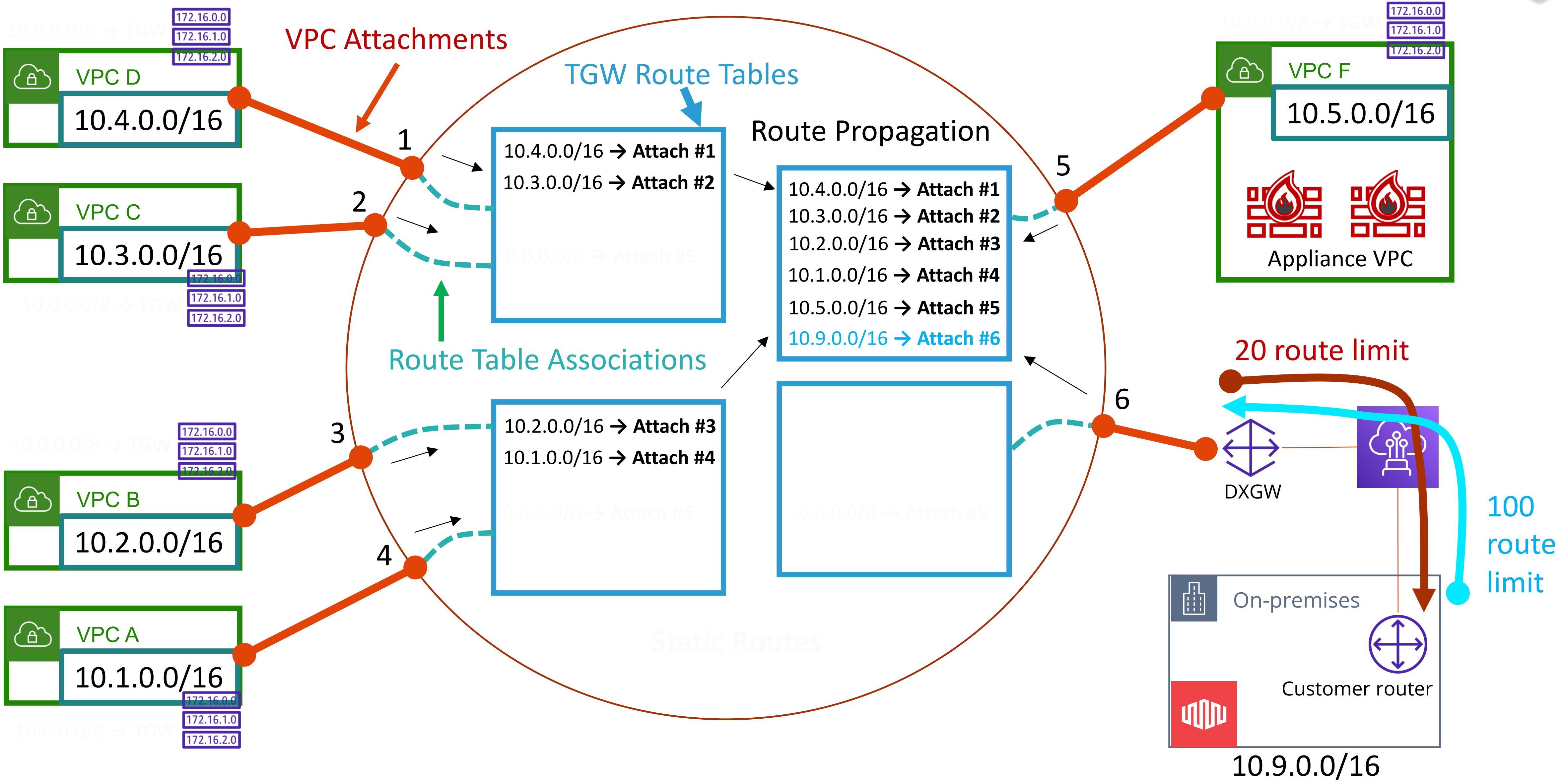
rtb-001

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

AWS Transit Gateway (TGW)



Inside the AWS Transit Gateway (TGW)



TGW Route Tables

Route table 1:
10.4.0.0/16 → Attach #1
10.3.0.0/16 → Attach #2
0.0.0.0/0 → Attach #5

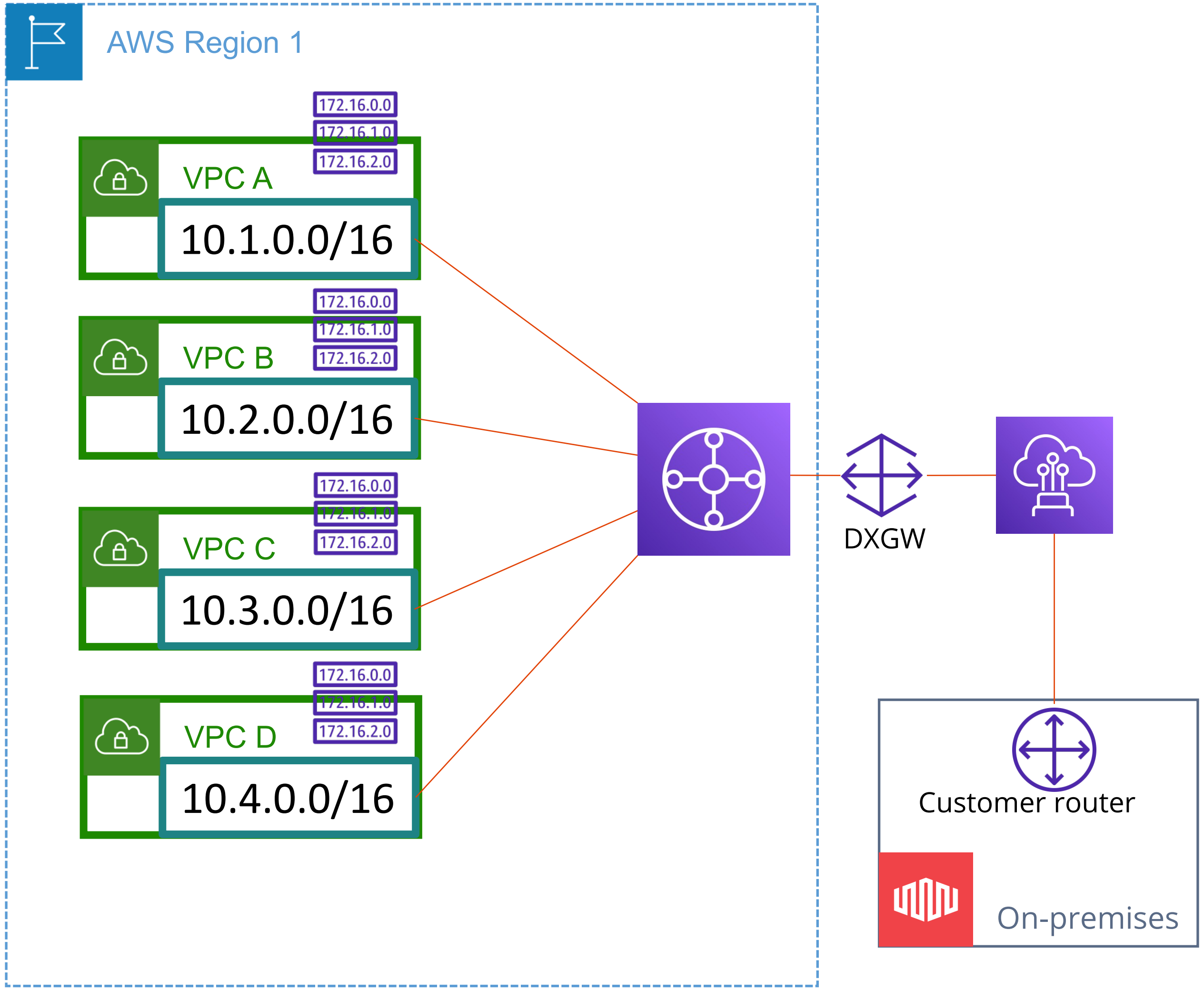
Route table 2:
10.2.0.0/16 → Attach #3
10.1.0.0/16 → Attach #4
0.0.0.0/0 → Attach #5

Route table 3:
10.4.0.0/16 → Attach #1
10.3.0.0/16 → Attach #2
10.2.0.0/16 → Attach #3
10.1.0.0/16 → Attach #4
10.5.0.0/16 → Attach #5
10.9.0.0/16 → Attach #6

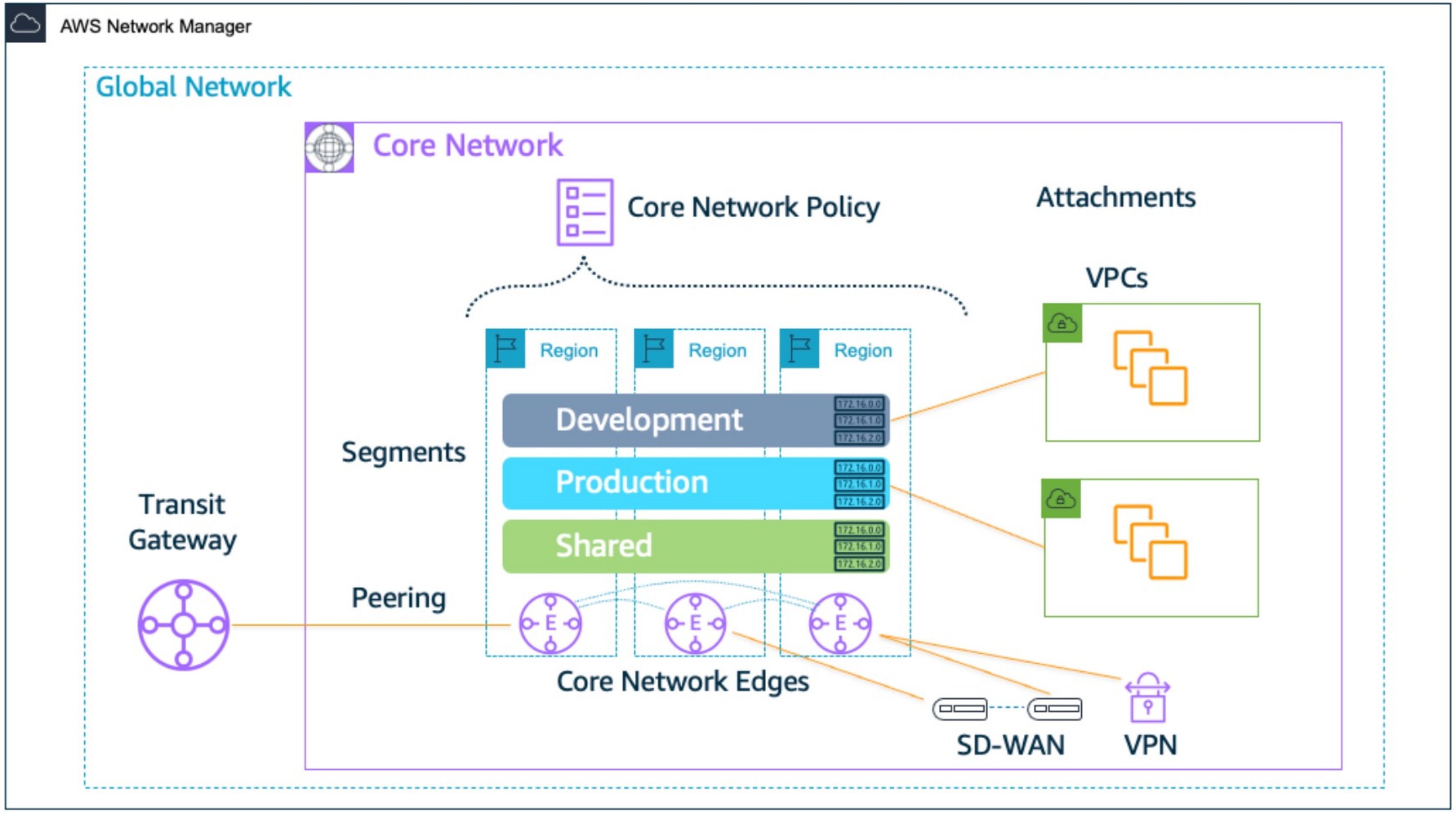
Route table 4:
0.0.0.0/0 → Attach #5

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



AWS Cloud WAN



Orchestrates VPC Segmentation and Isolation

Orchestrates multi region network peering

JSON Policy document defines Zones and Policies

AWS only

TGW under the hood, with the same limited troubleshooting and visibility

Not free
https://aws.amazon.com/cloud-wan/pricing/

Next: Azure Networking 101

aviatrix

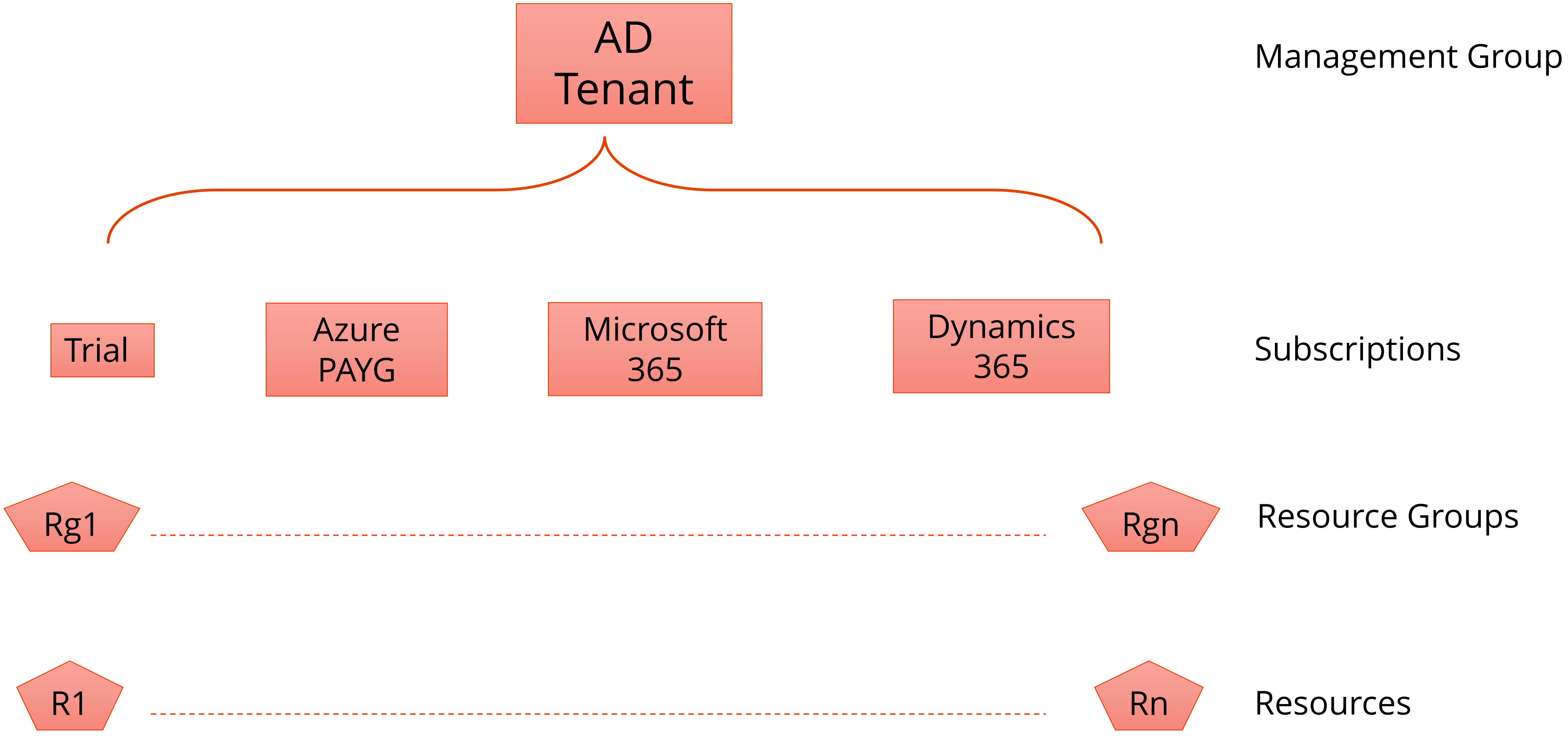
ACE

Aviatrix Certified Engineer

Azure Networking 101

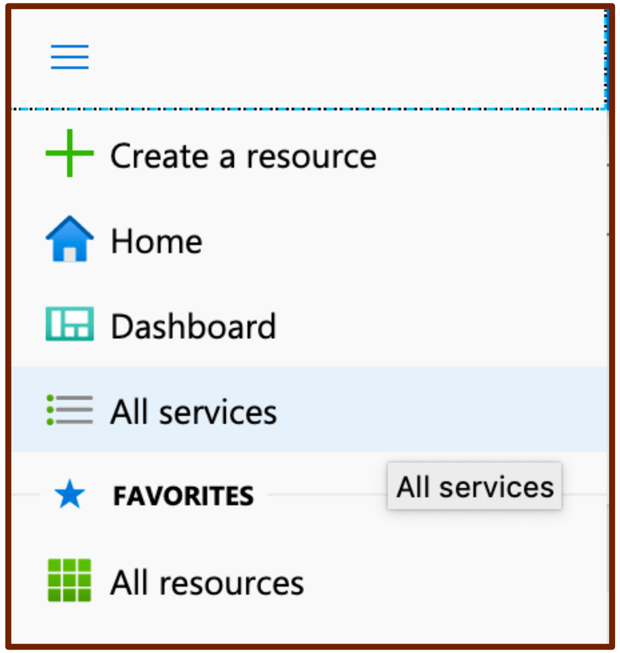
ACE Solutions Architecture Team

Azure Hierarchy



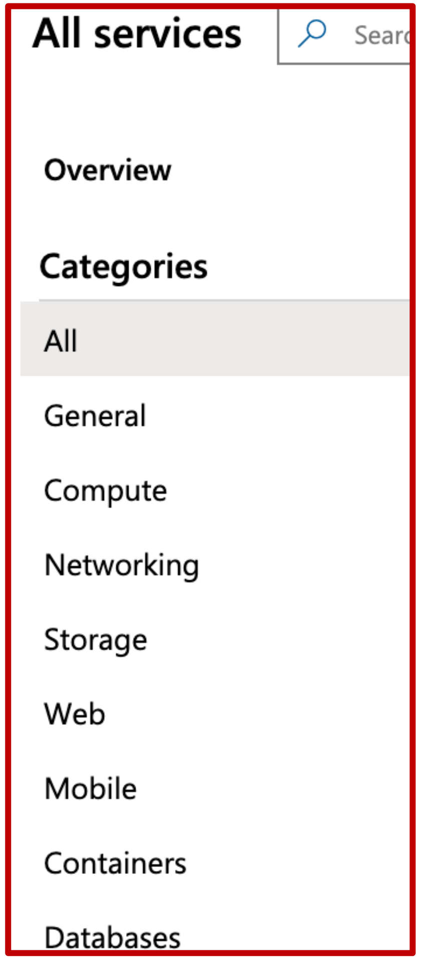
Microsoft Azure Service and Resource

Ability to See All Services



- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All services
- All resources

List of Service (categories)



All services

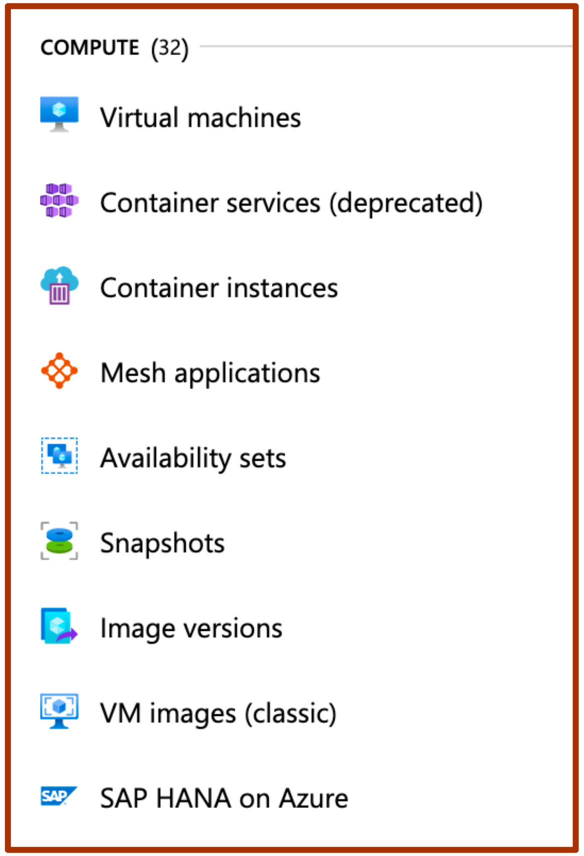
Sear

Overview

Categories

- All
- General
- Compute
- Networking
- Storage
- Web
- Mobile
- Containers
- Databases

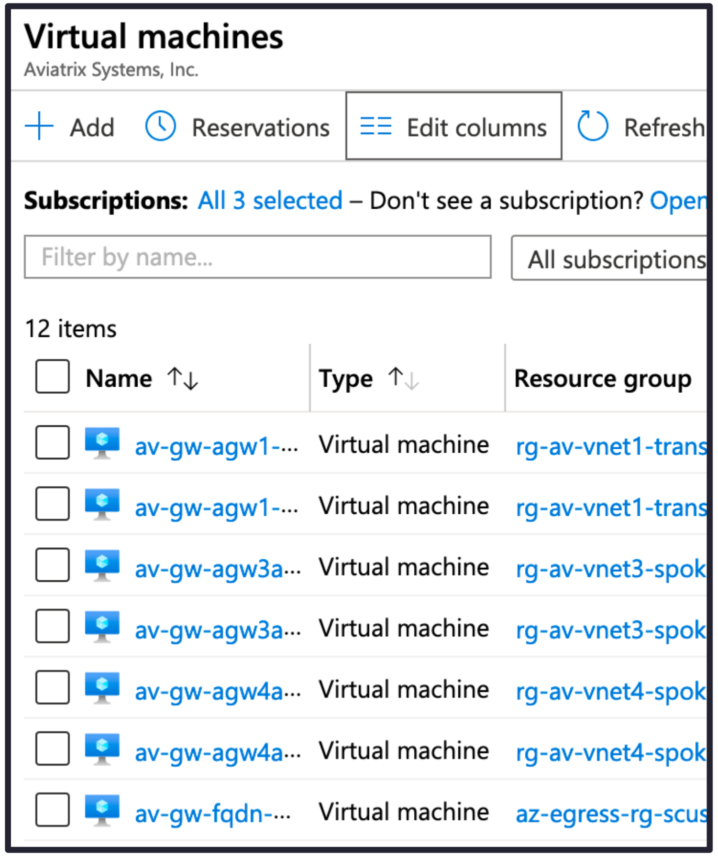
Resources are grouped inside each Service



COMPUTE (32)

- Virtual machines
- Container services (deprecated)
- Container instances
- Mesh applications
- Availability sets
- Snapshots
- Image versions
- VM images (classic)
- SAP HANA on Azure

Resource is an instance of a Service in a Resource Group



Virtual machines

Aviatrix Systems, Inc.

Subscriptions: All 3 selected – Don't see a subscription? Open

Filter by name...

All subscriptions

12 items

□	Name ↑↓	Type ↑↓	Resource group
□	av-gw-agw1-...	Virtual machine	rg-av-vnet1-trans
□	av-gw-agw1-...	Virtual machine	rg-av-vnet1-trans
□	av-gw-agw3a...	Virtual machine	rg-av-vnet3-spok
□	av-gw-agw3a...	Virtual machine	rg-av-vnet3-spok
□	av-gw-agw4a...	Virtual machine	rg-av-vnet4-spok
□	av-gw-agw4a...	Virtual machine	rg-av-vnet4-spok
□	av-gw-fqdn-...	Virtual machine	az-egress-rg-scus

Azure Service Categories

Category Name	Example Services
Compute	Virtual Machines, WebApps, Virtual Machine Scale Sets, Azure Virtual Desktop
Storage	Blob Storage, Disk Storage, Azure NetApp Files
Networking	Virtual Network, DNS, VPN Gateway, ExpressRoute, CDN
Databases	Azure SQL, Azure Cosmos DB, Azure Cache for Redis
Containers	Azure Kubernetes Service, Azure Red Hat OpenShift, Container Registry, Container Instances
Identity	Azure Active Directory
Security	Microsoft Defender for Cloud, Azure Sentinel, Azure Firewall, Web Application Firewall
AI + Machine Learning	Azure Databricks, Azure Cognitive Services

Azure Core Networking Services

Virtual Network

Address space can be one or more networks either public or private

- Isolated, logical network providing connectivity for virtual machines and some PaaS services

Subnets

Provides full Layer 3 semantics and partial Layer 2 semantics (DHCP, ARP, no broadcast/multicast)

- Networks within a VNet which can be used for more granular separation of virtual machines

Network Interface

Provides network services to virtual machines

- Up to 8 NICs supported on a VM depending on the SKU.
- All NICs must belong to the same Virtual Network

DNS

Provides name resolution services for resources deployed in Virtual Networks and the Internet

- All VMs in a VNet belong to the same internal DNS zone by default. It is possible to create custom public and private DNS Zones

Public IP Address

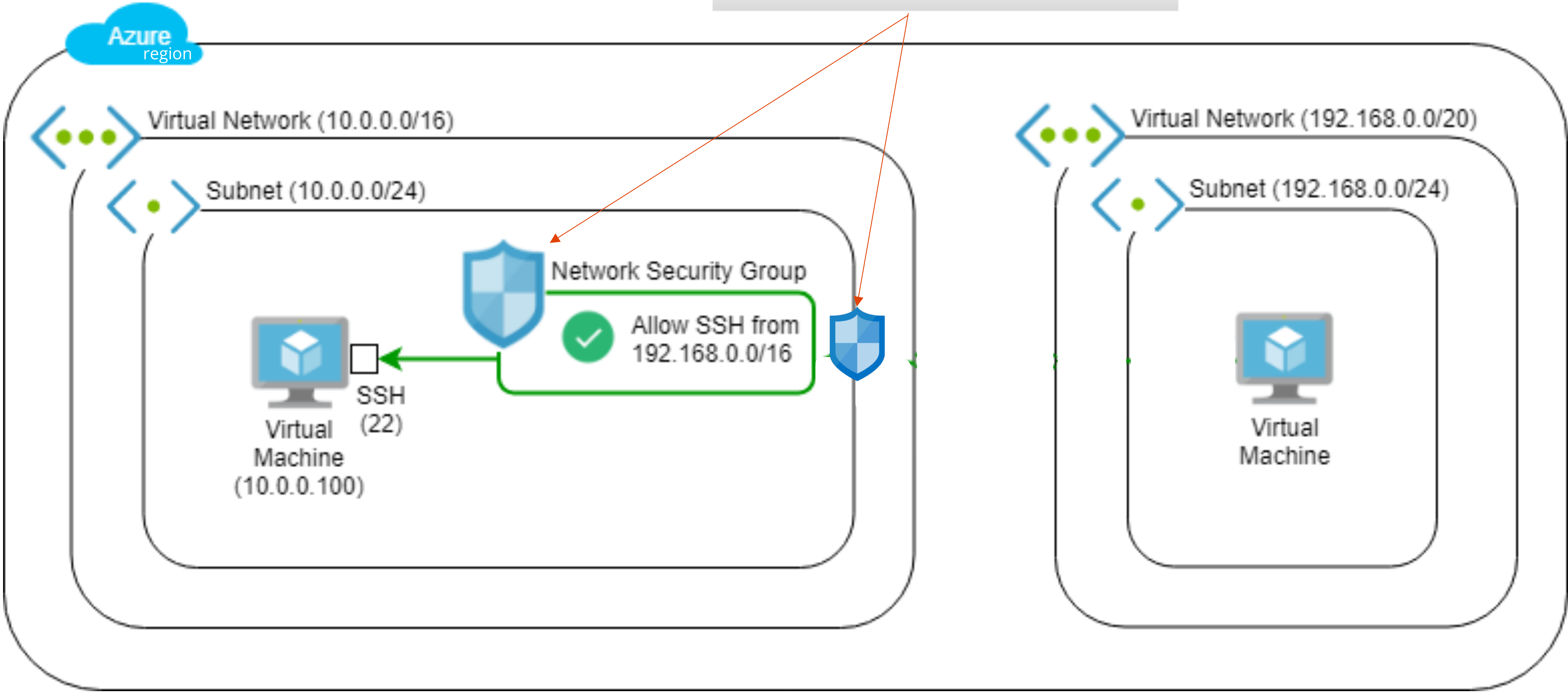
Provides communication from the Internet to services deployed in a Virtual Network

- Can be static or dynamic. Assigned by Microsoft
- Used for Internet inbound connectivity

NSG

NSG can be at Subnet level or NIC level

You can have NO NSG at all

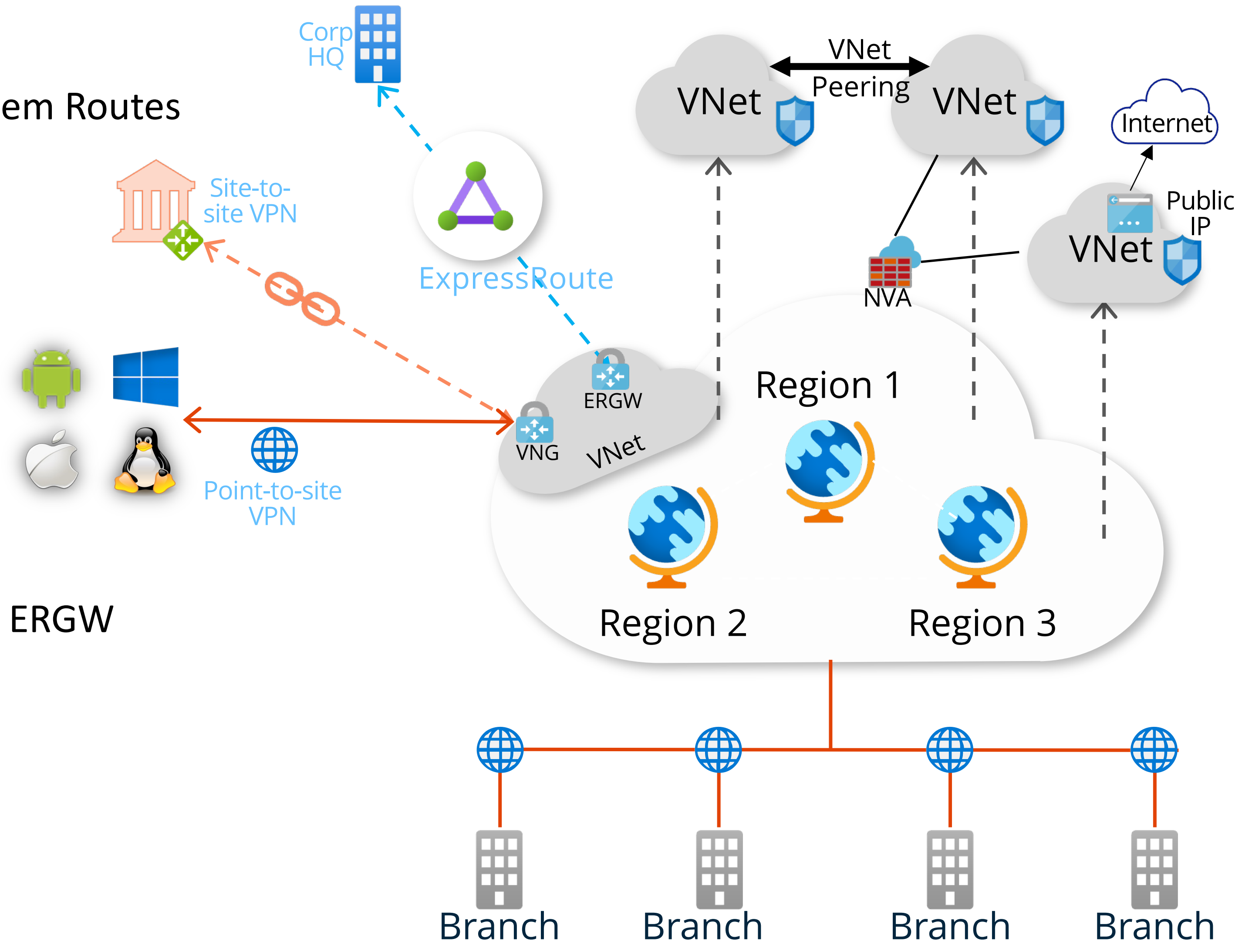


Azure region
Virtual Network (10.0.0.0/16)
Subnet (10.0.0.0/24)
Network Security Group
Allow SSH from 192.168.0.0/16
SSH (22)
Virtual Machine (10.0.0.100)
Virtual Network (192.168.0.0/20)
Subnet (192.168.0.0/24)
Virtual Machine

Azure Networking Components

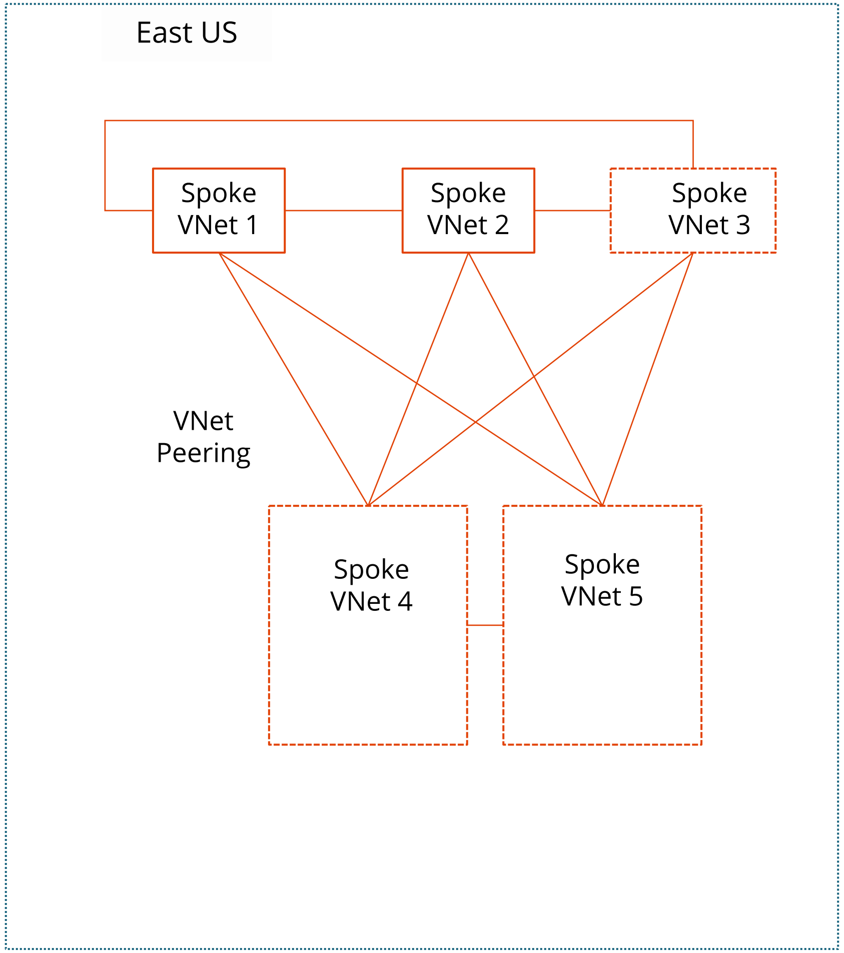
- VNet (Virtual Network)
- Routing: User-Defined Route (UDR), BGP and System Routes
- Availability Zones (not all regions)
- Network Security Group
- Virtual Network Gateways
  1. VPN Gateway (VNG)
     - S2S (max 30 tunnels) and P2S VPN
     - Local Network Gateway (on-prem entity)
  2. ExpressRoute Gateway (ERGW)

  Note: No communication path between VNG and ERGW
- Public and Private IP Address
- VNet Peering
- NVA (Network Virtual Appliance)



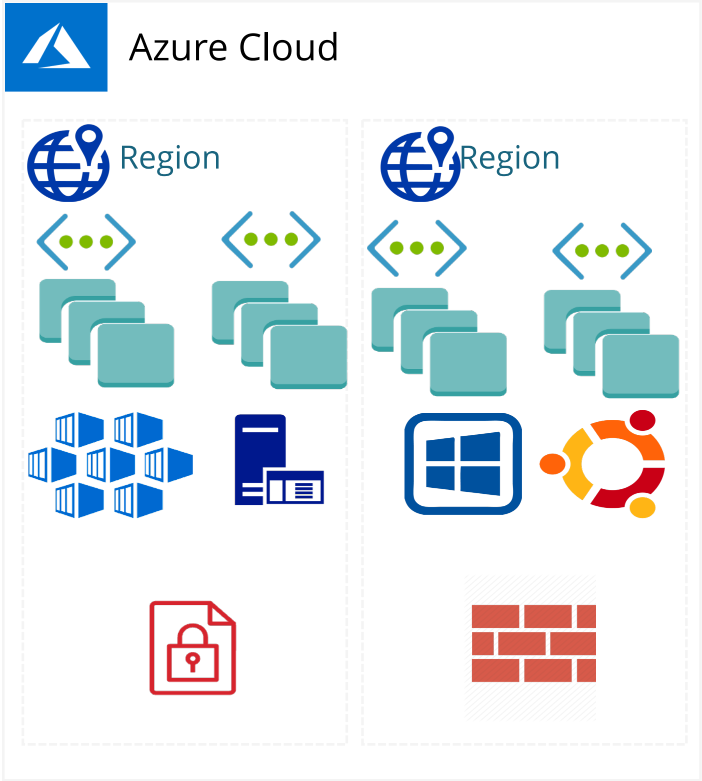
Azure VNet Peering

- Preferred Method by Microsoft Product Group for Transit in Azure
- No Real BW Limitation
- 1-to-1 Mapping
- Does not scale
- No easy way to insert FWs
- No granularity (all or none subnets)
- VNet peering data charges for ingress and egress in both directions
- Inter-region supported (Global VNet peering)

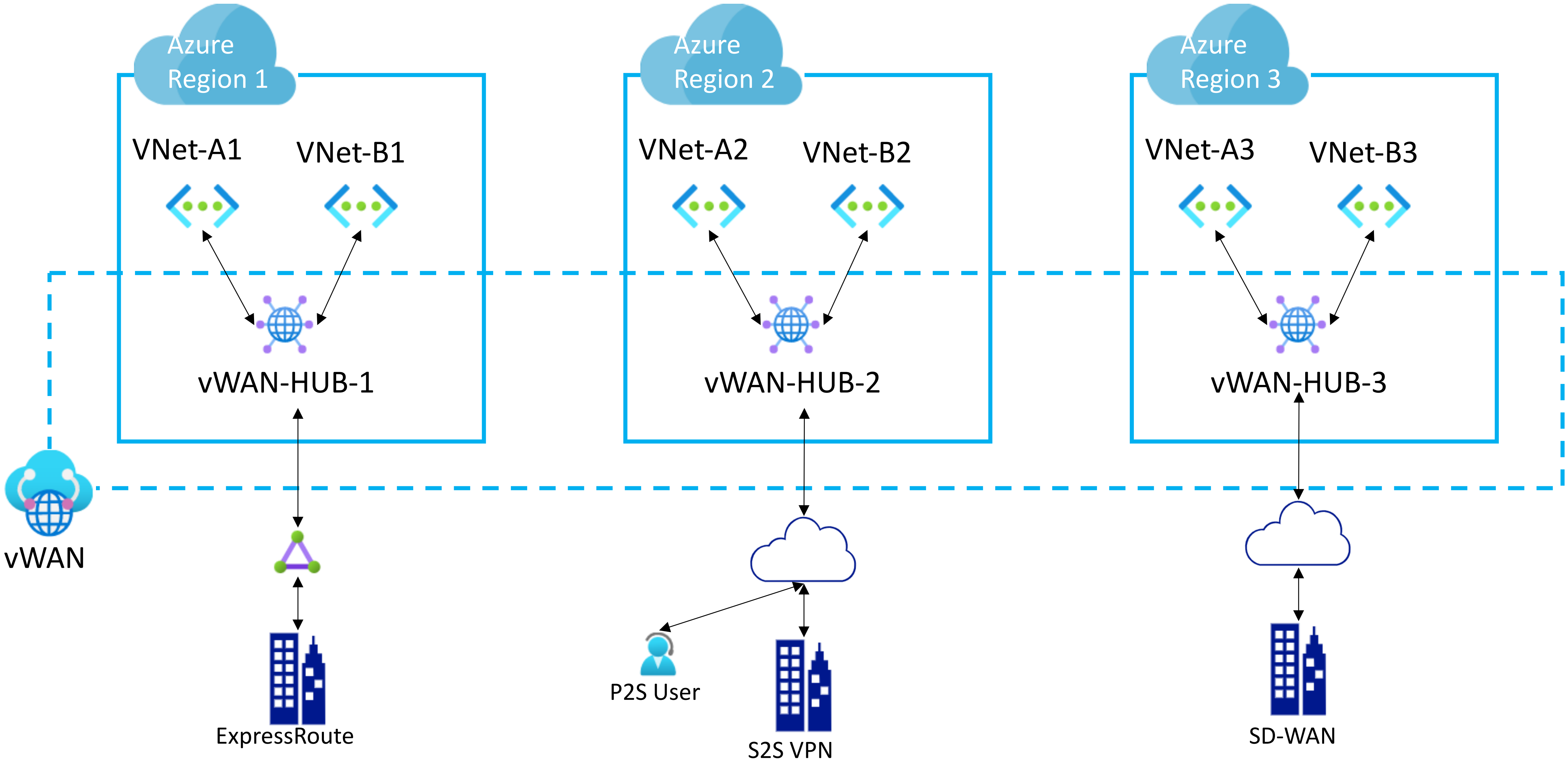


Transit in Azure

- Transit is the most important part of any cloud network
  - Transit is responsible for scale out way of interconnecting VNets
  - It connects VNets within a region, across-regions, and with
    VNet equivalents (VPC, VNC, etc.) in other clouds
  - Azure official documentation recommends to use Transit VNet using VNet Peering
- Transit with HUB VNet using VNet Peering is provided by the following Deployment models:
  1. via ExpressRoute Edge routers
  2. via Network Virtual Appliance in Transit/Hub VNet



Azure Virtual WAN



aviatrix

ACE

Aviatrix Certified Engineer

Next: GCP Networking 101