Evolution of networking in the cloud

FROM SIMPLE SDNS TO MULTI-CLOUD NETWORK SOFTWARE (MCNS)

Evgeny Vaganov

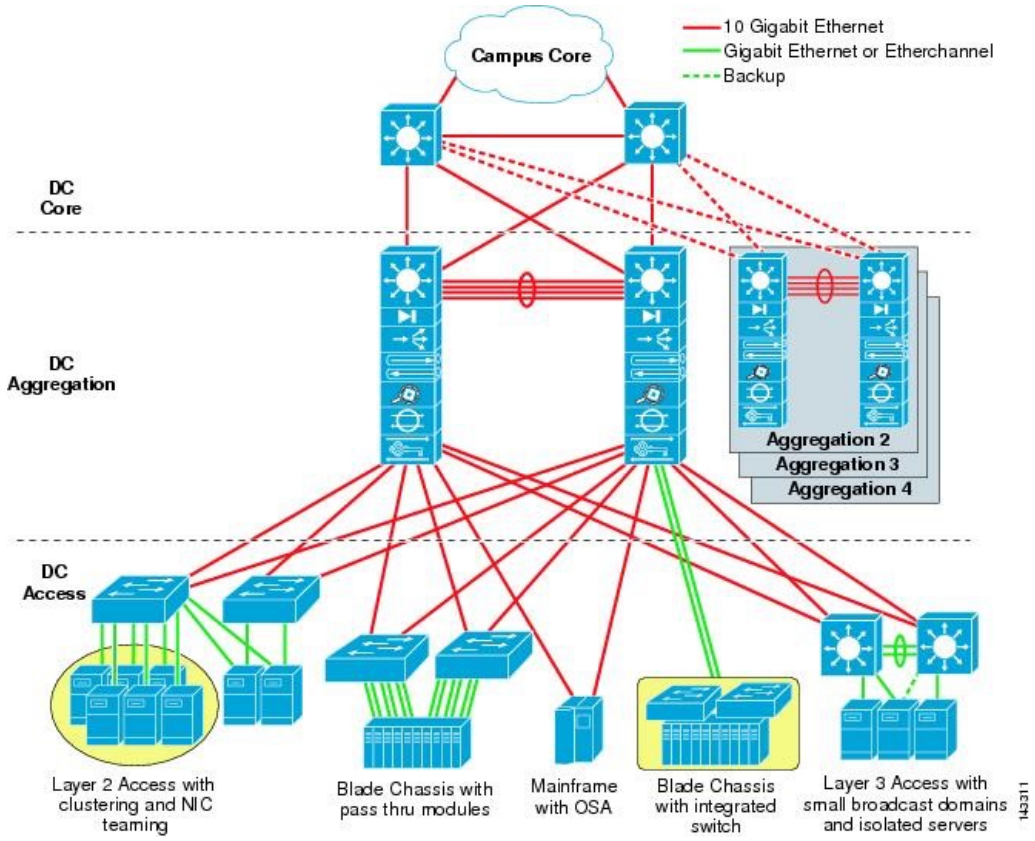
VP, Solutions Architecture, APAC, Aviatrix

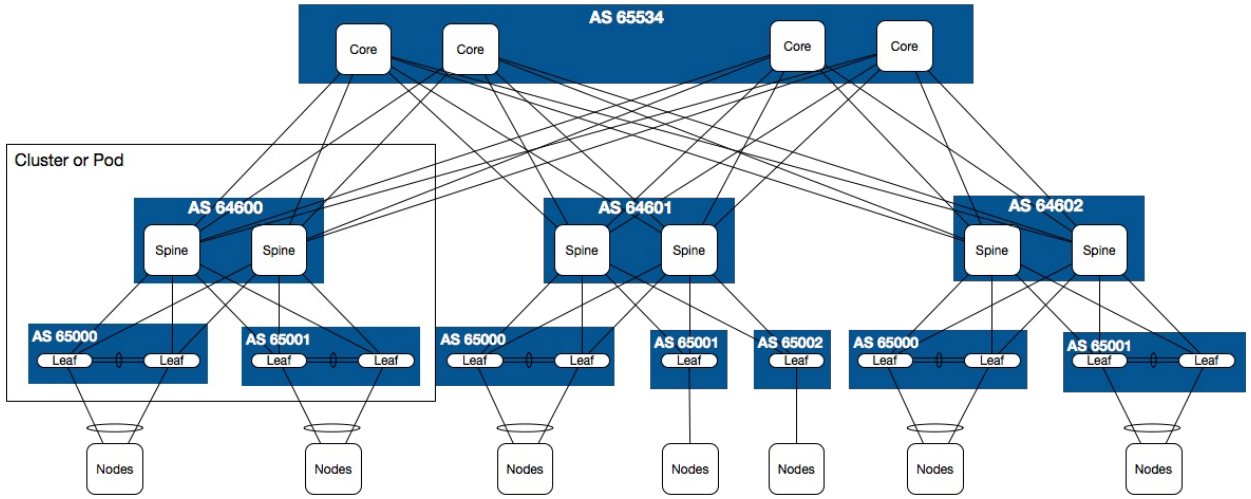
evgeny@aviatrix.com

www.linkedin.com/in/evgeny-vaganov

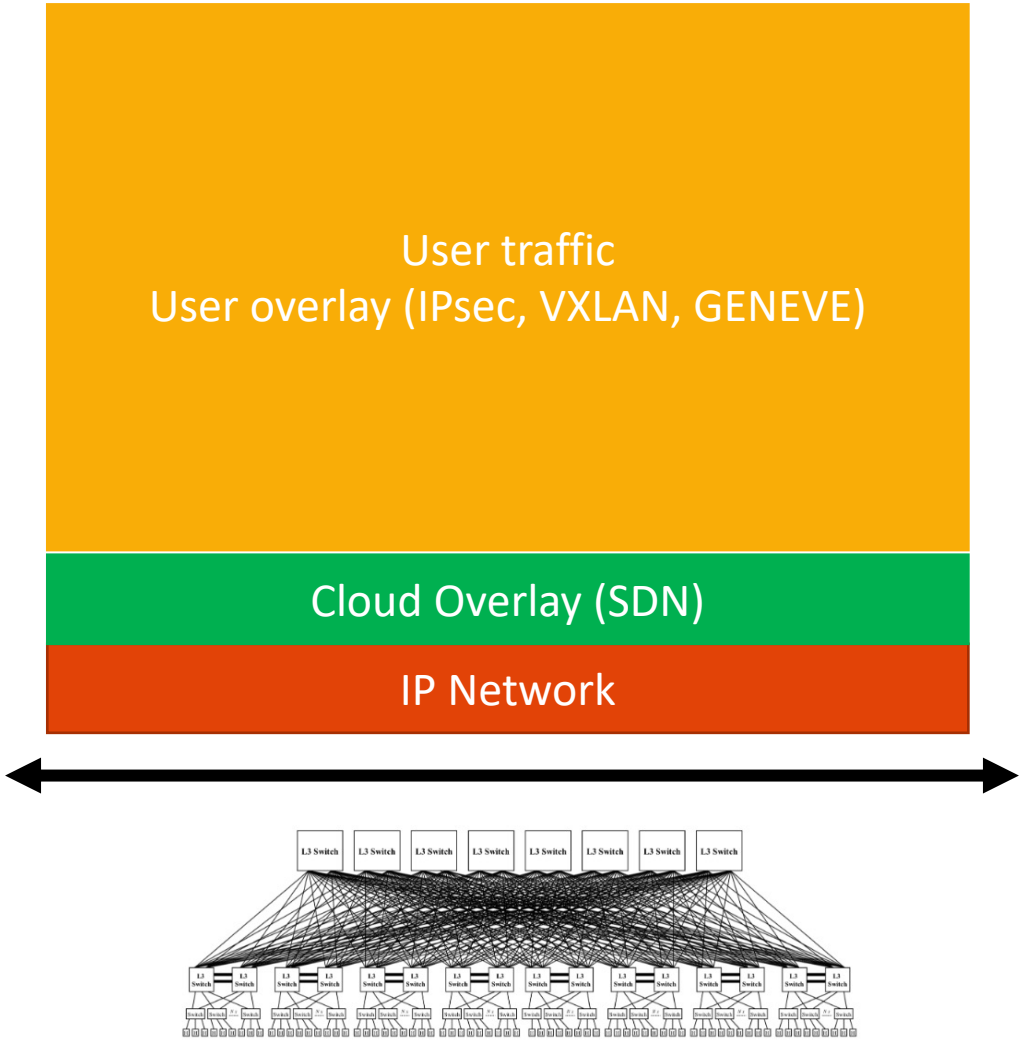
Prequel

Reference architectures in on-premises networks



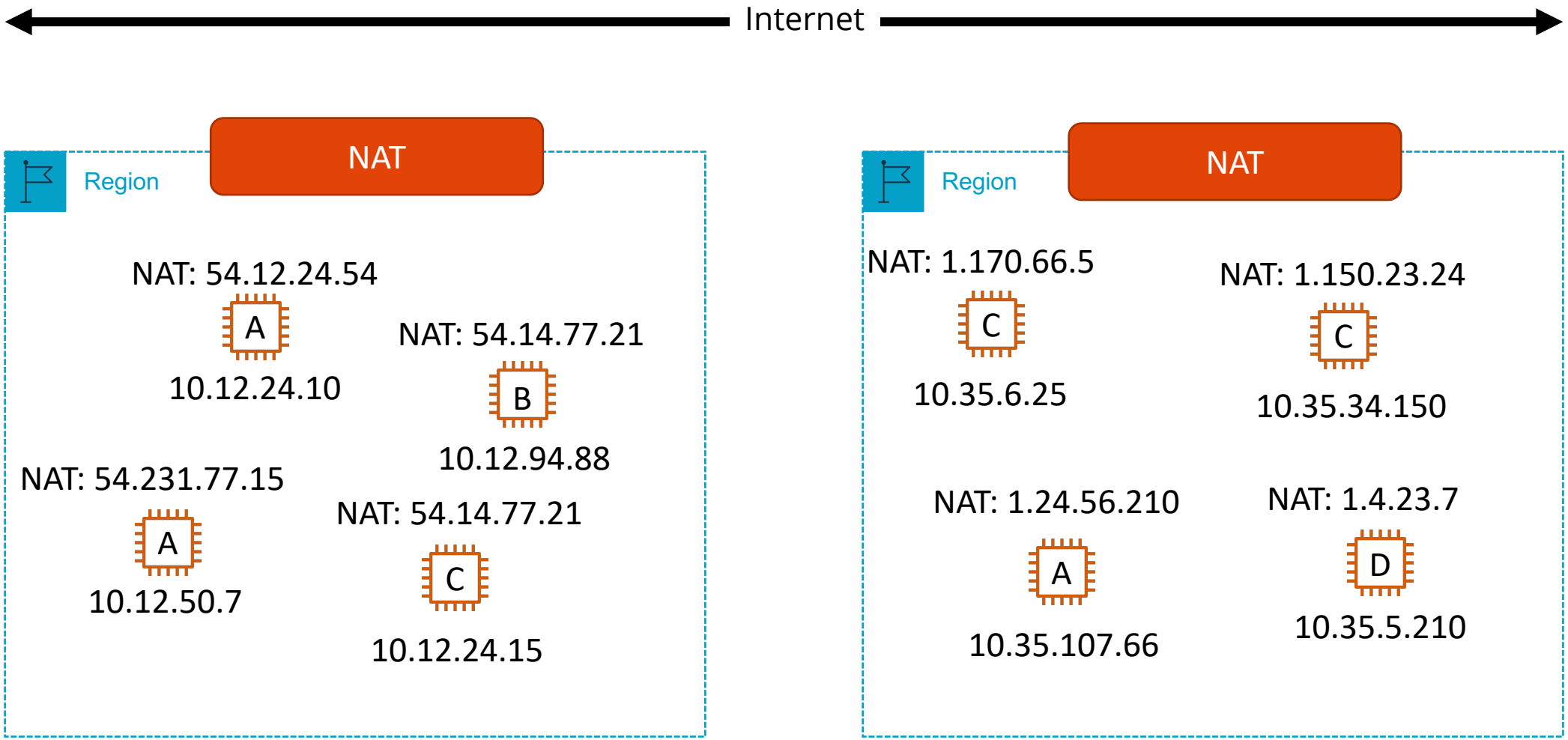


Overlay vs underlay



The age of cloud computing
1st gen cloud networking

EC2 Classic


Internet
Region
NAT
NAT: 54.12.24.54
A
10.12.24.10
NAT: 54.14.77.21
B
10.12.94.88
NAT: 54.231.77.15
A
10.12.50.7
NAT: 54.14.77.21
C
10.12.24.15
Region
NAT
NAT: 1.170.66.5
C
10.35.6.25
NAT: 1.150.23.24
C
10.35.34.150
NAT: 1.24.56.210
A
10.35.107.66
NAT: 1.4.23.7
D
10.35.5.210

Farewell

AWS News Blog

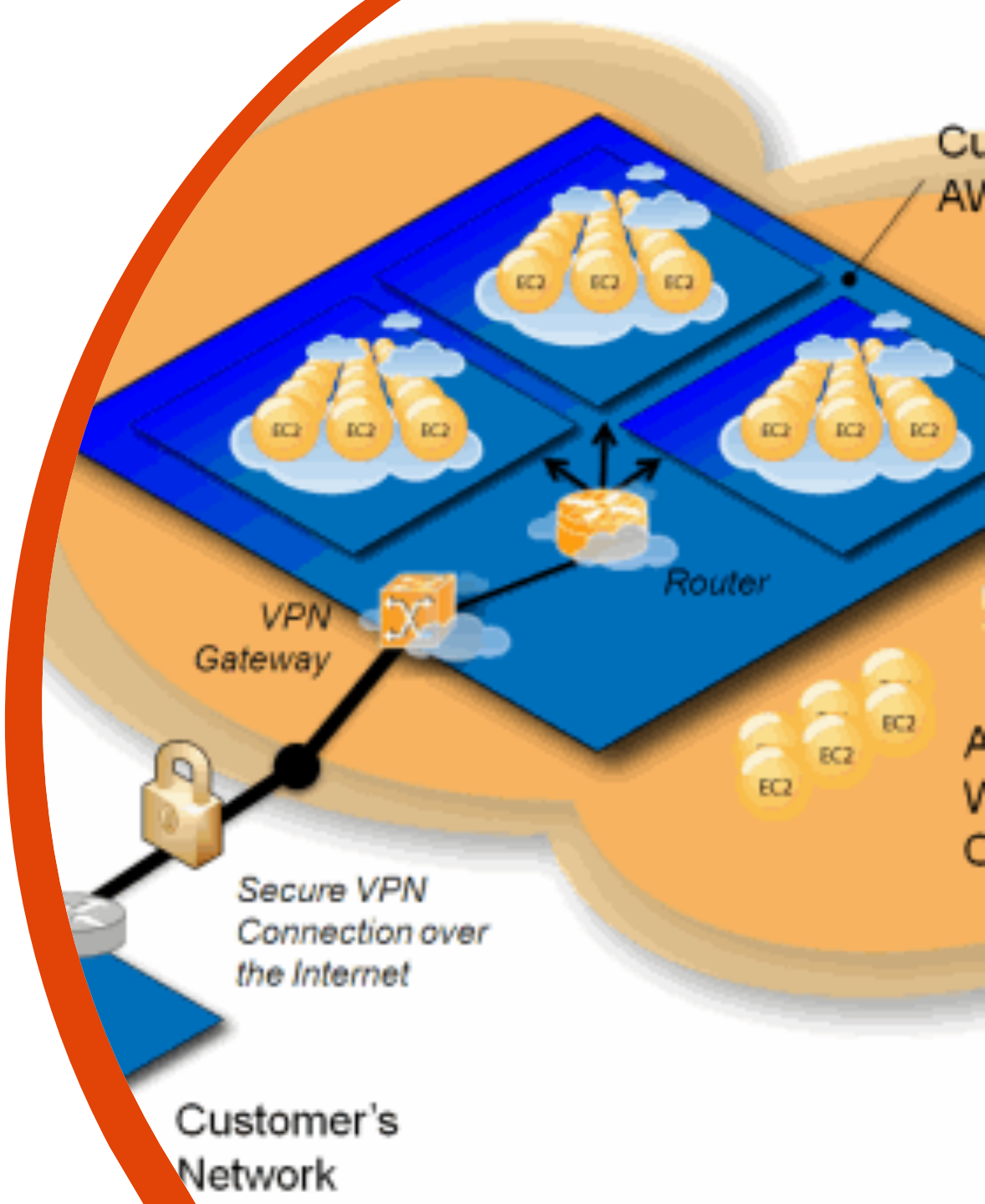
EC2-Classic Networking is Retiring – Here's How to Prepare

by Jeff Barr | on 28 JUL 2021 | in Amazon EC2, Deprecation, Launch, News | Permalink | Share

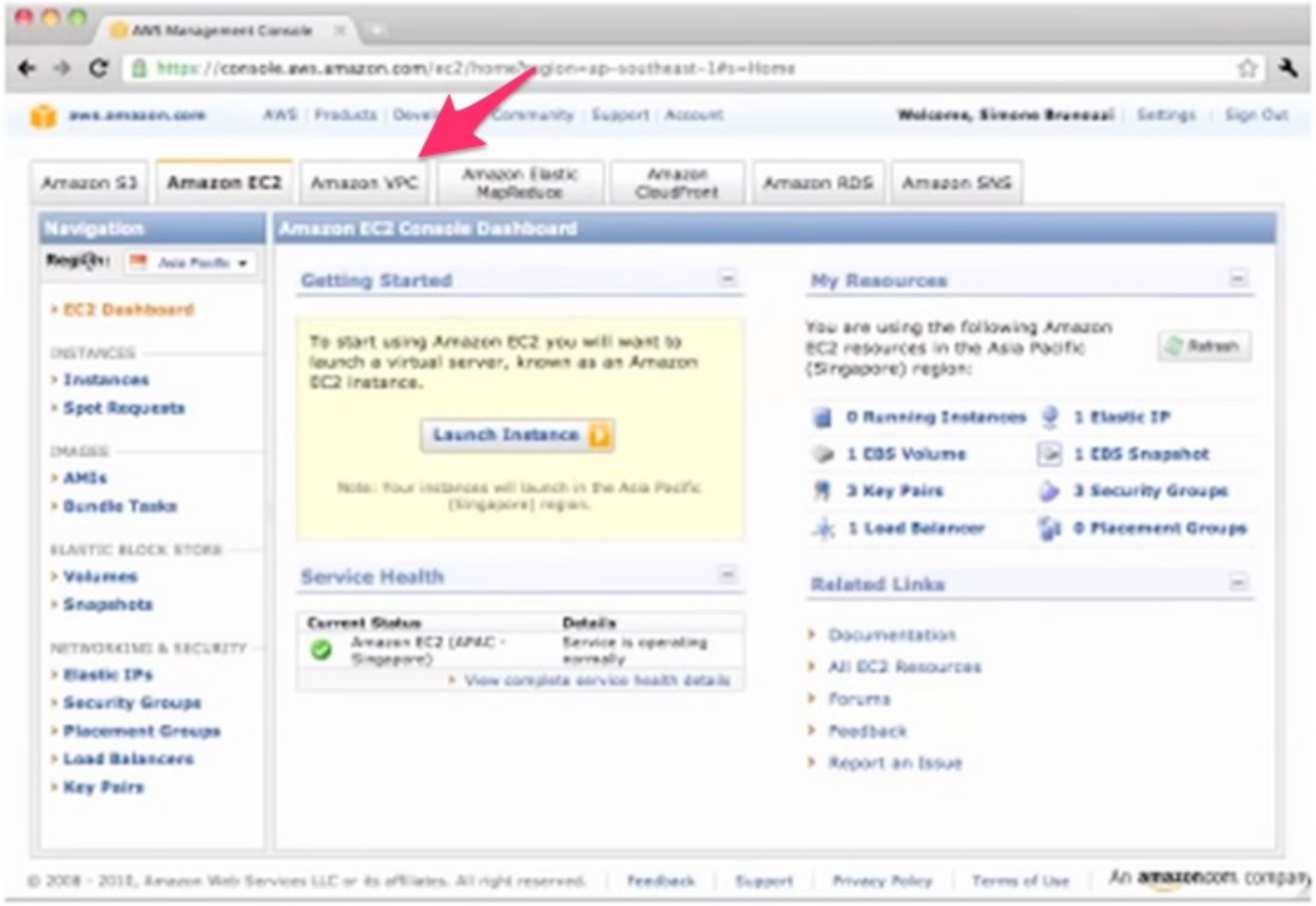
- **On October 30, 2021** we will disable EC2-Classic in Regions for AWS accounts that have no active EC2-Classic resources in the Region, as listed below. We will also stop selling 1-year and 3-year Reserved Instances for EC2-Classic.
- On **August 15, 2022** we expect all migrations to be complete, with no remaining EC2-Classic resources present in any AWS account.

https://aws.amazon.com/blogs/aws/ec2-classic-is-retiring-heres-how-to-prepare/

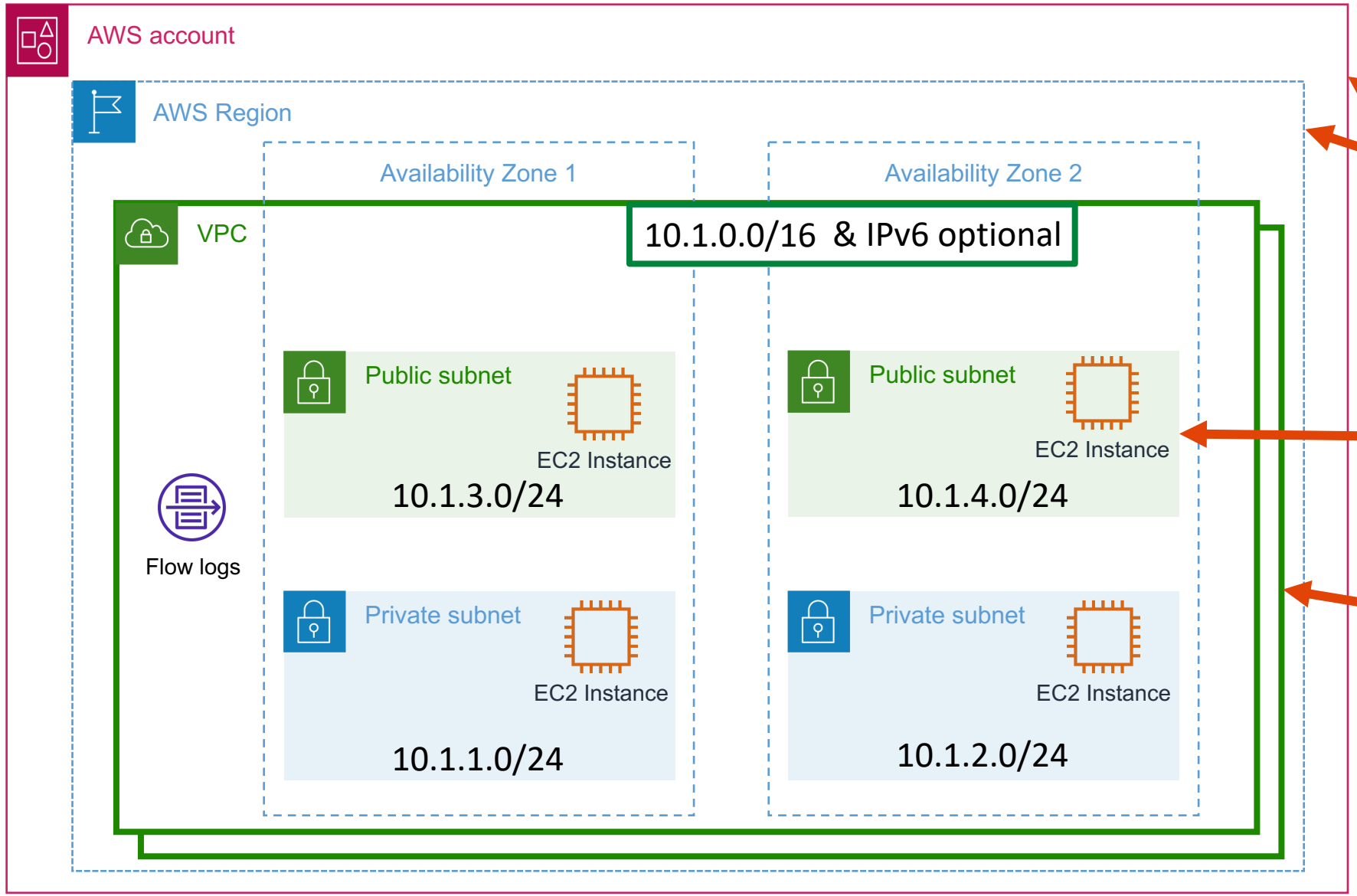
VPCs everywhere
2nd gen cloud networking



Virtual Private Cloud



Amazon VPC example



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

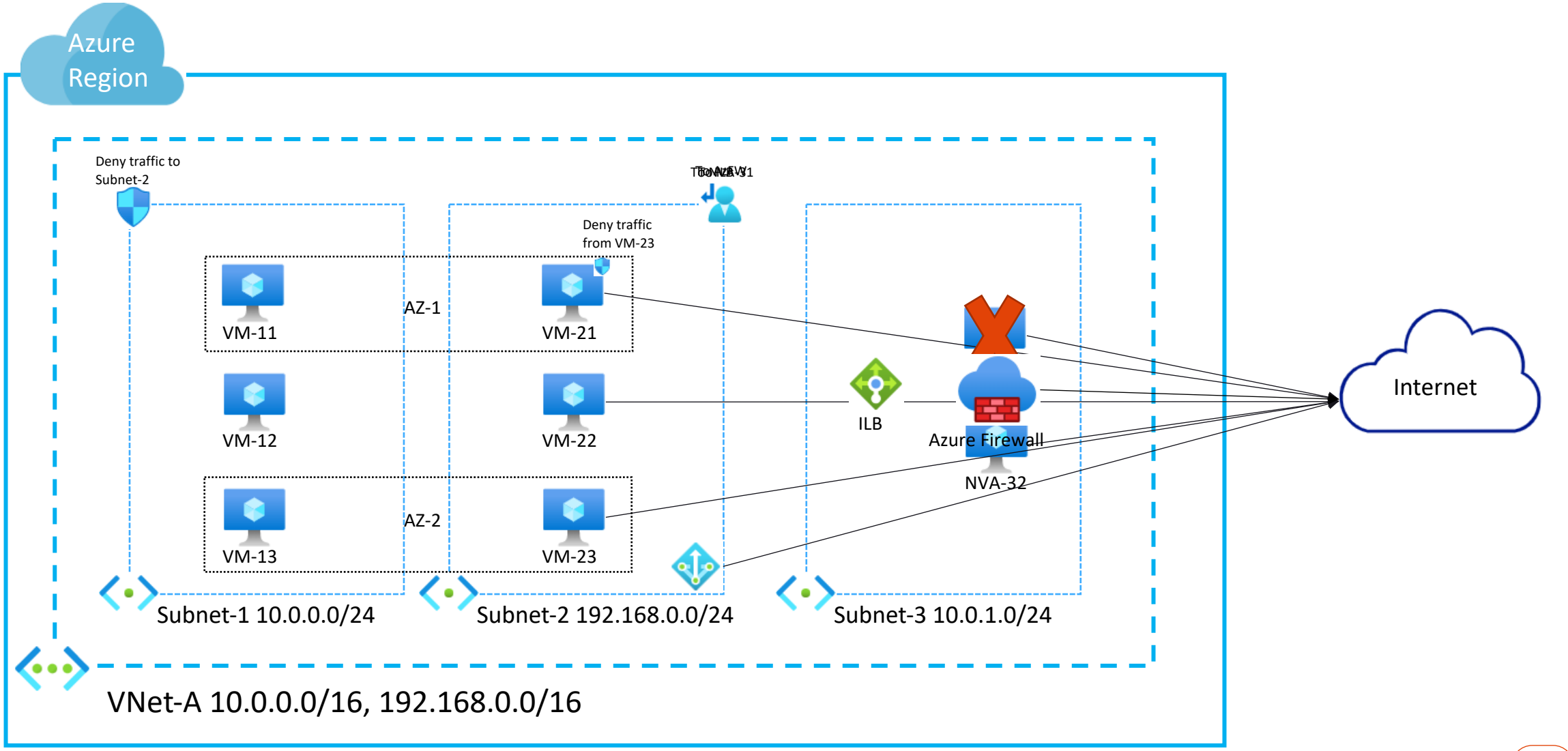
Can enable VPC Flow logs for traffic flow data

Building upon success

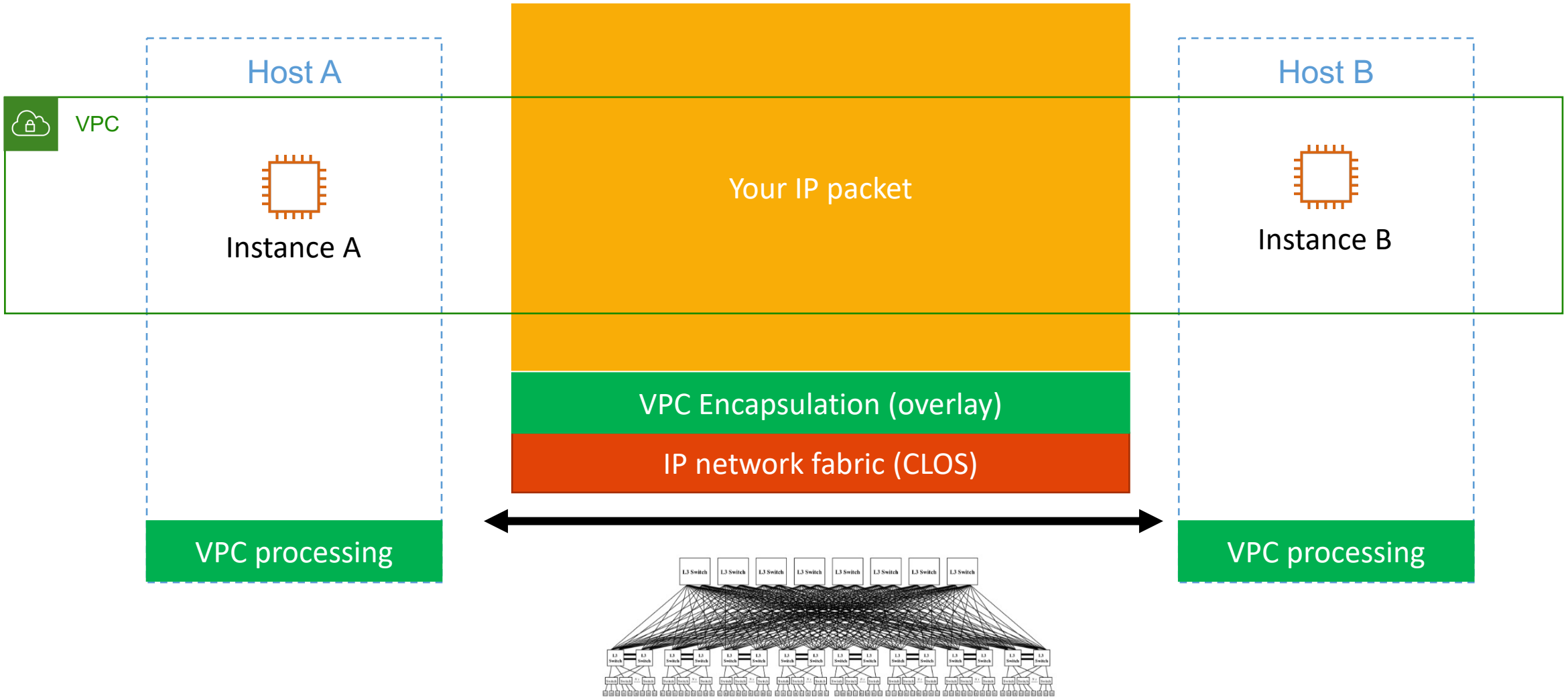
EC2 Classic and EC2 VPC Differences

EC2 Classic	EC2 VPC
EIP is disassociated when instance stopped	EIP remains associated when instance stopped
Unlimited number of security groups	Up to 5 security groups
Can't change the SGs of a running instance	Can change the SGs of a running instance
SG rules for inbound traffic only	SG rules for inbound and outbound traffic.
Instance can access the Internet by default	Requires IGW and route to IGW
DNS hostnames are enabled by default	DNS hostnames are disabled in default VPC
Runs on shared hardware only	Shared hardware or single-tenant hardware

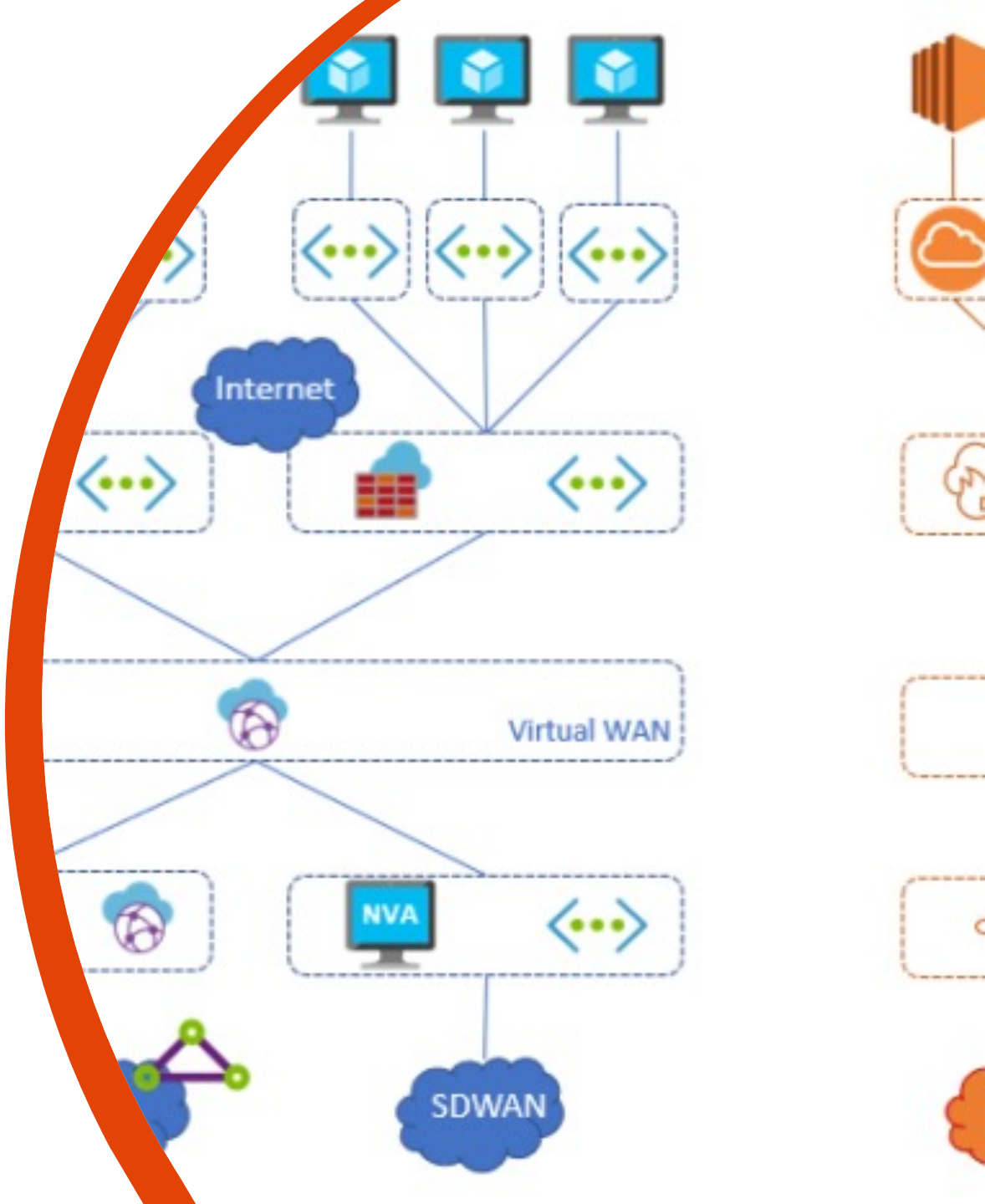
Azure VNet


Azure Region
Deny traffic to Subnet-2
Deny traffic from VM-23
AZ-1
AZ-2
VM-11
VM-12
VM-13
VM-21
VM-22
VM-23
ILB
Azure Firewall
NVA-32
Internet
Subnet-1 10.0.0.0/24
Subnet-2 192.168.0.0/24
Subnet-3 10.0.1.0/24
VNet-A 10.0.0.0/16, 192.168.0.0/16

VPC on the wire

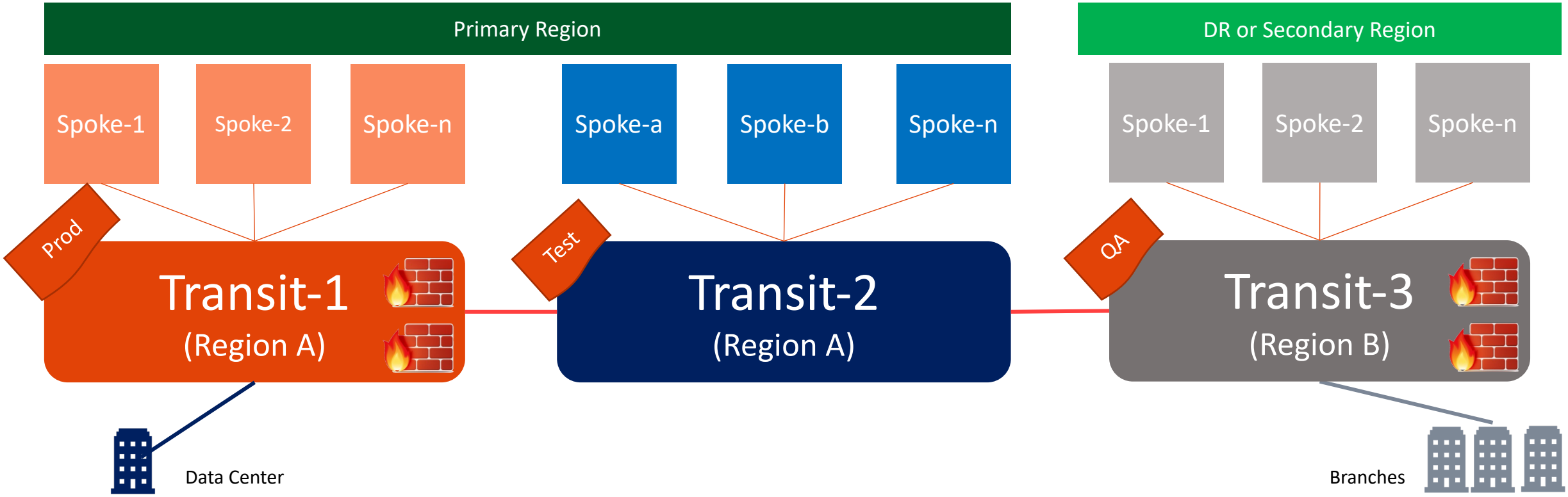


Hub and Spoke
3rd gen cloud networking

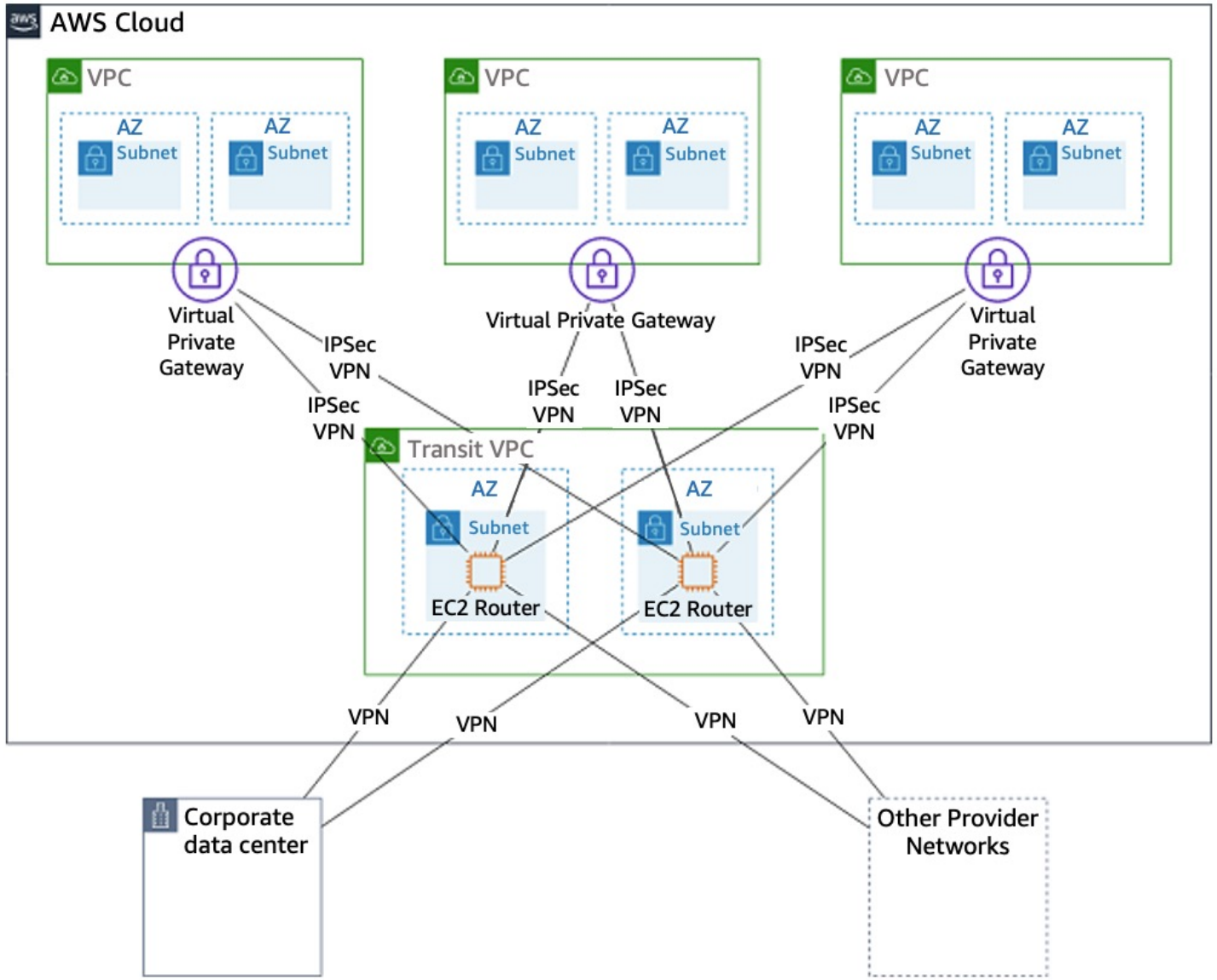


Purpose of Transit in Cloud Networking

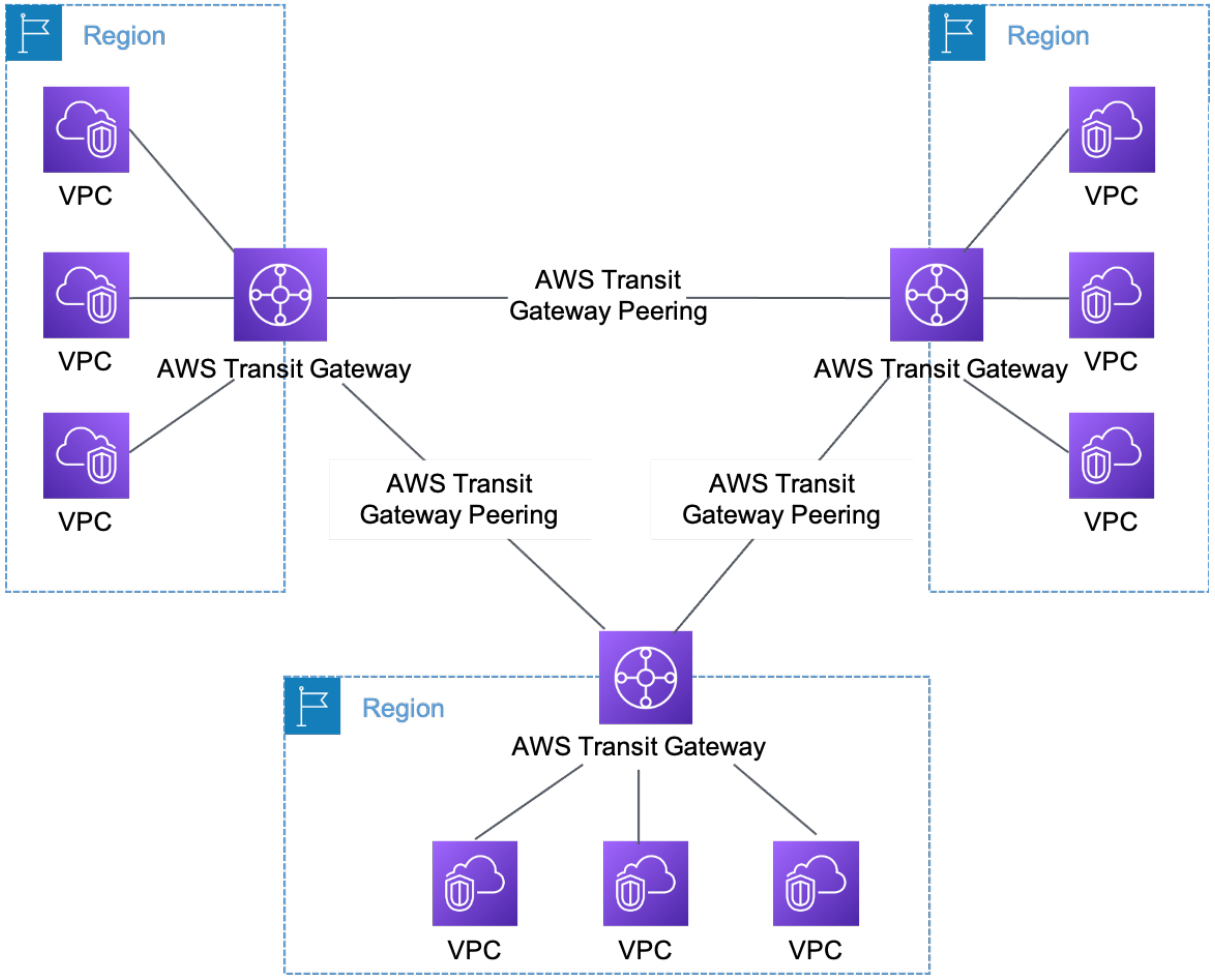
- Hub and Spoke Architecture for Cloud
  - Provides connectivity for intra-VPCs/VNets/VCNs
  - Works inside a region
  - May need one or many transits in a single region
- Connects multiple cloud regions
- Point of insertion for rich services (FWs)
- Connects to on-prem locations

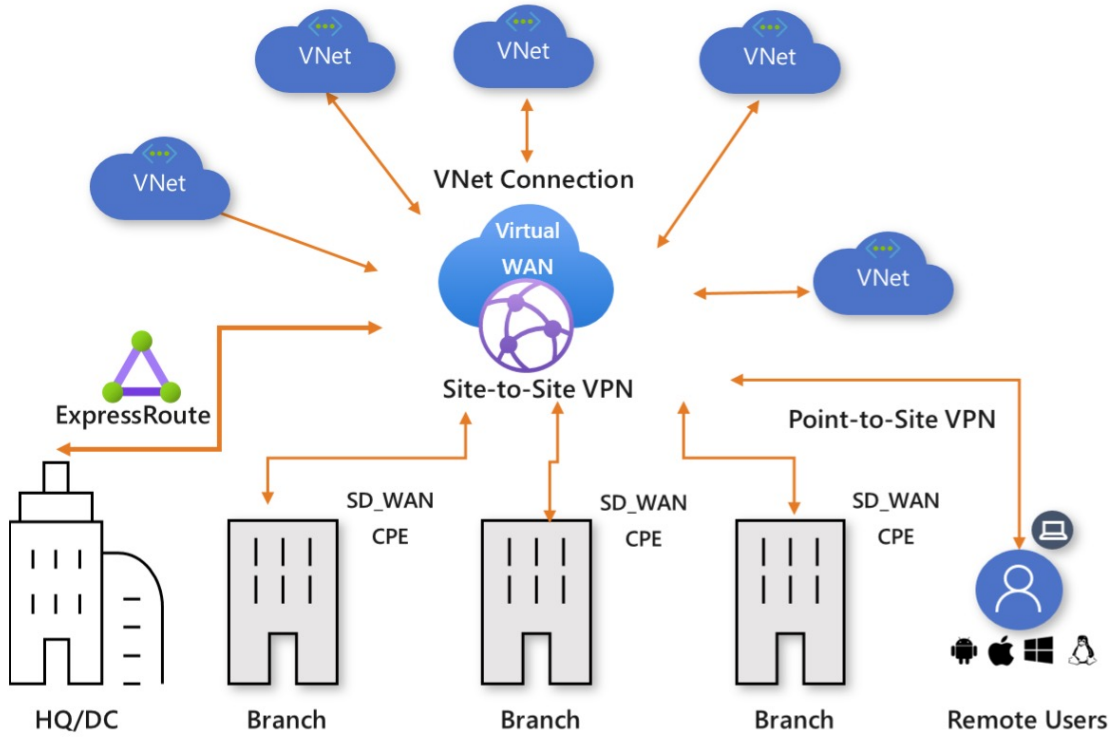


Transit VPC

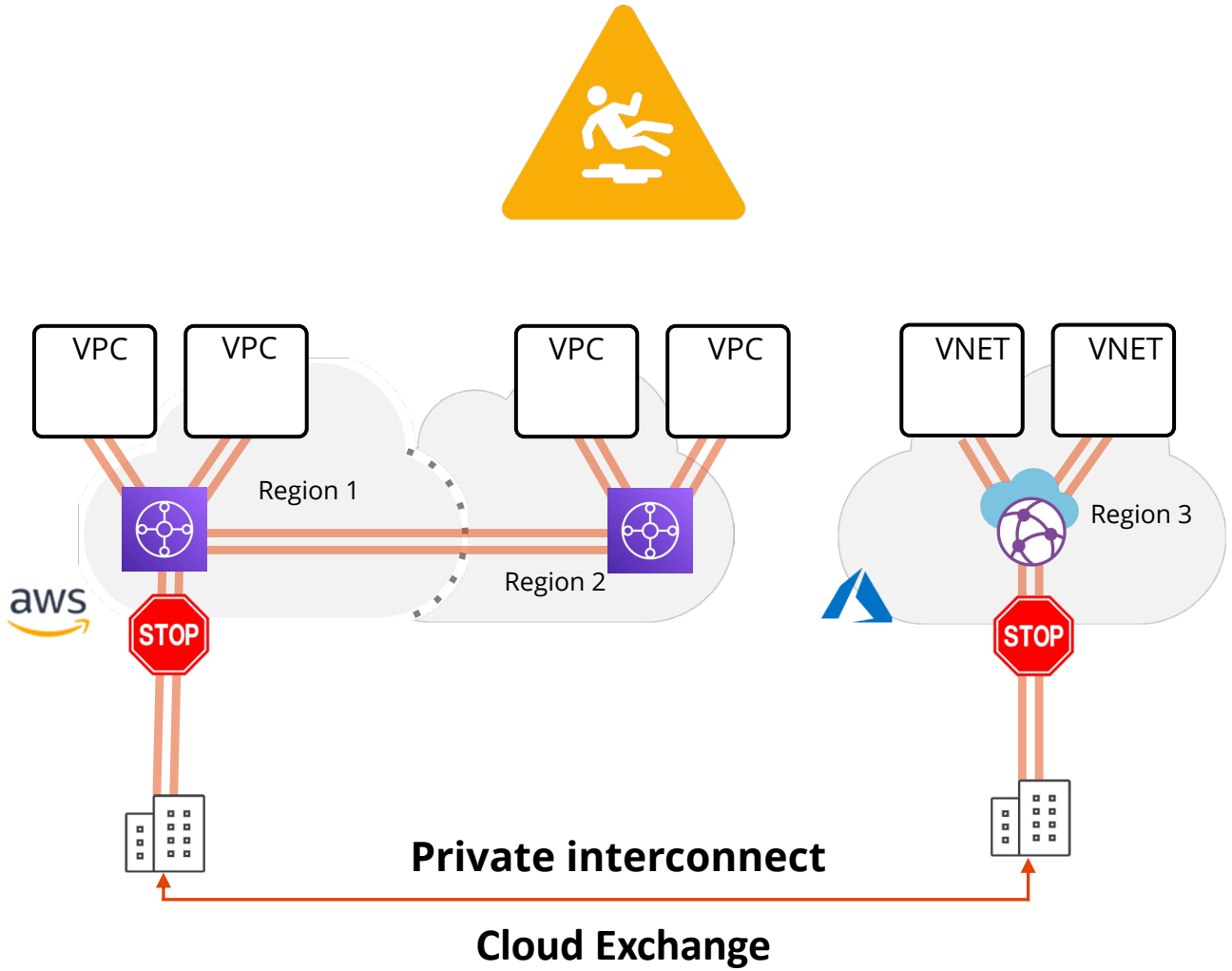

AWS Cloud
VPC
AZ
Subnet
AZ
Subnet
VPC
AZ
Subnet
AZ
Subnet
VPC
AZ
Subnet
AZ
Subnet
Virtual Private Gateway
Virtual Private Gateway
Virtual Private Gateway
IPSec VPN
IPSec VPN
IPSec VPN
IPSec VPN
IPSec VPN
IPSec VPN
Transit VPC
AZ
Subnet
EC2 Router
AZ
Subnet
EC2 Router
VPN
VPN
VPN
VPN
Corporate data center
Other Provider Networks

Managed network services

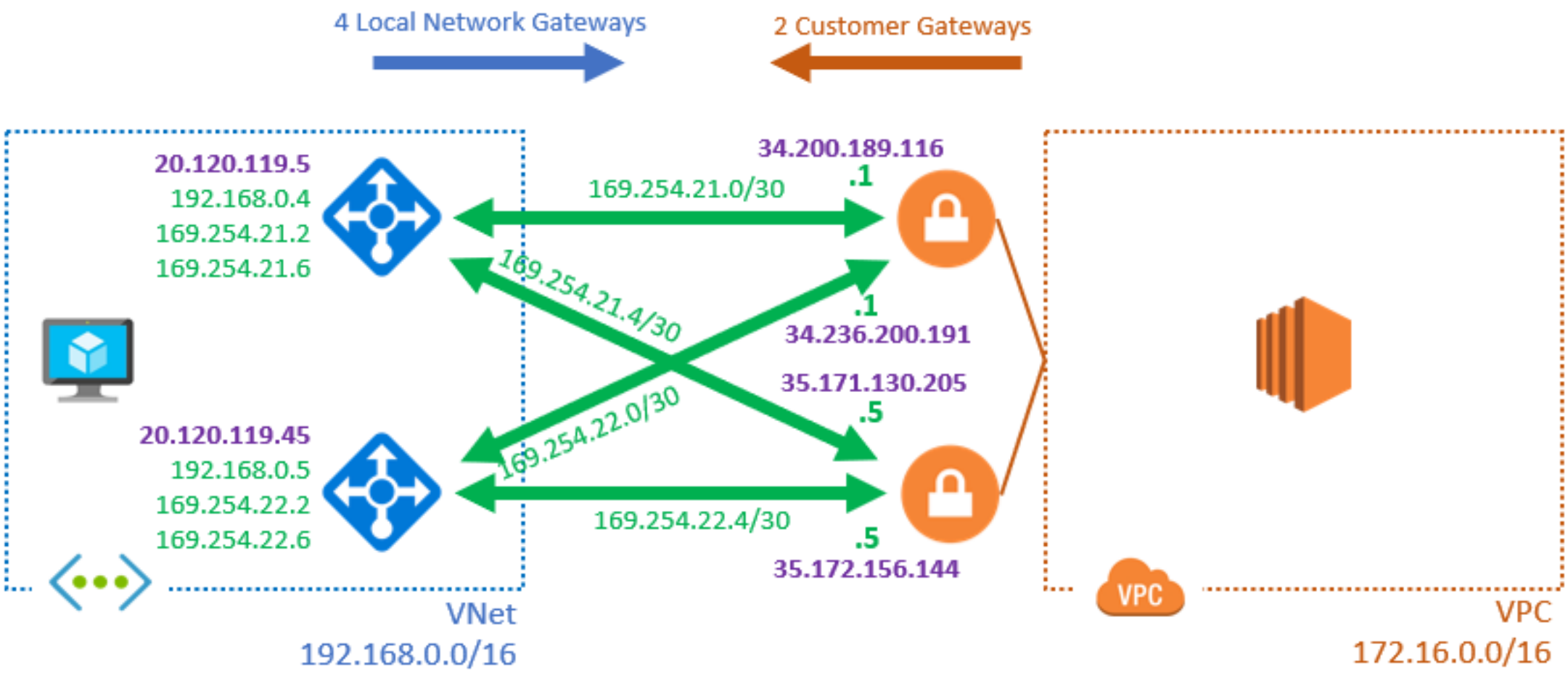




Multi-cloud?

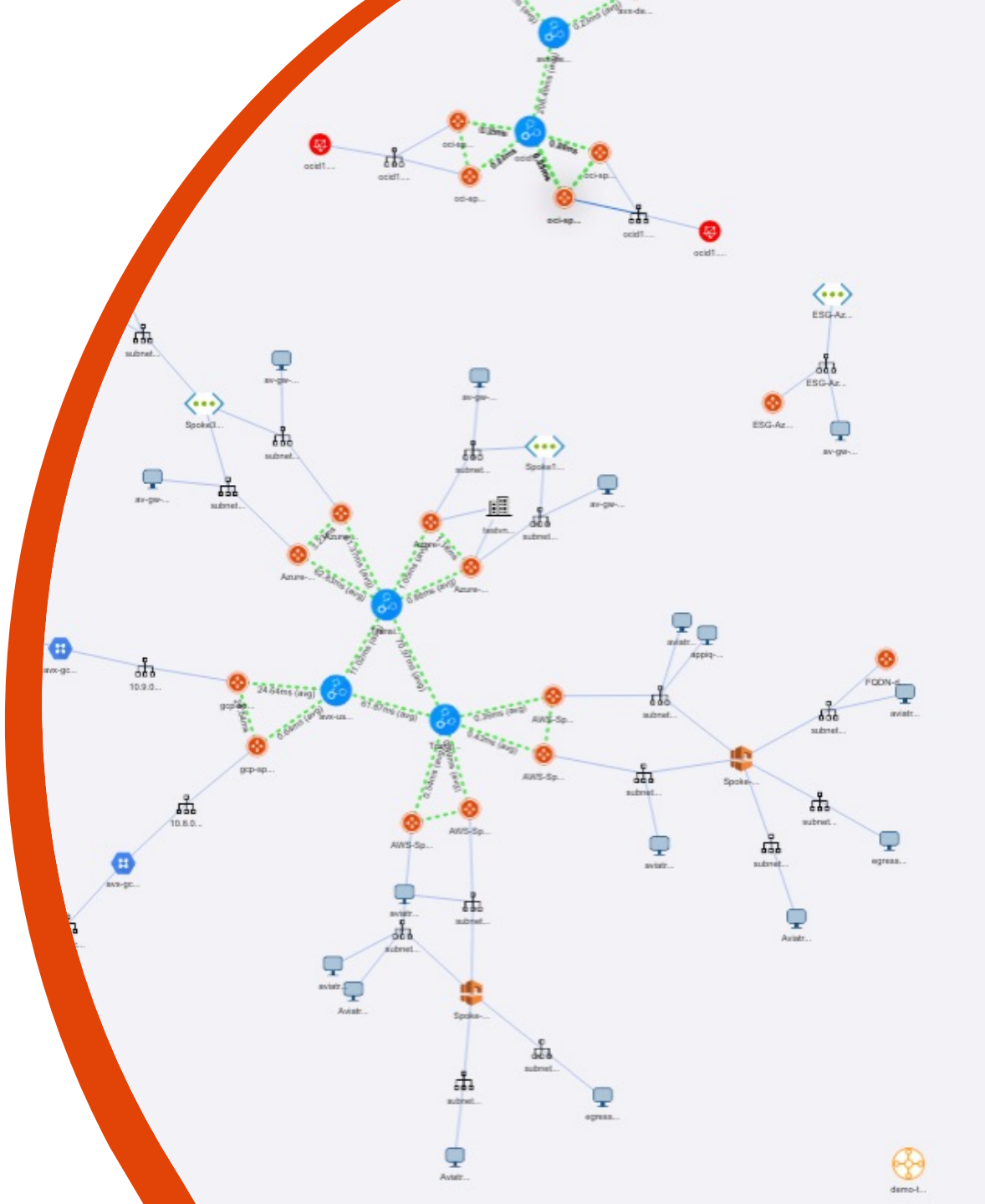

VPC
VPC
VPC
VPC
VNET
VNET
Region 1
Region 2
Region 3
aws
STOP
STOP
Private interconnect
Cloud Exchange

Going with native



https://blog.cloudtrooper.net/2022/04/11/tunnels-between-clouds/

Multi-cloud networking software (MCNS)
4th gen cloud networking



Networking challenges in multi/poly/super cloud

Network and Security Complexity

- Single or Multi-Cloud
- Consistency Across Clouds
- Available security features

Skills Gap

- Different Native Constructs
- Lack of Automation across clouds
- Keeping up with new features

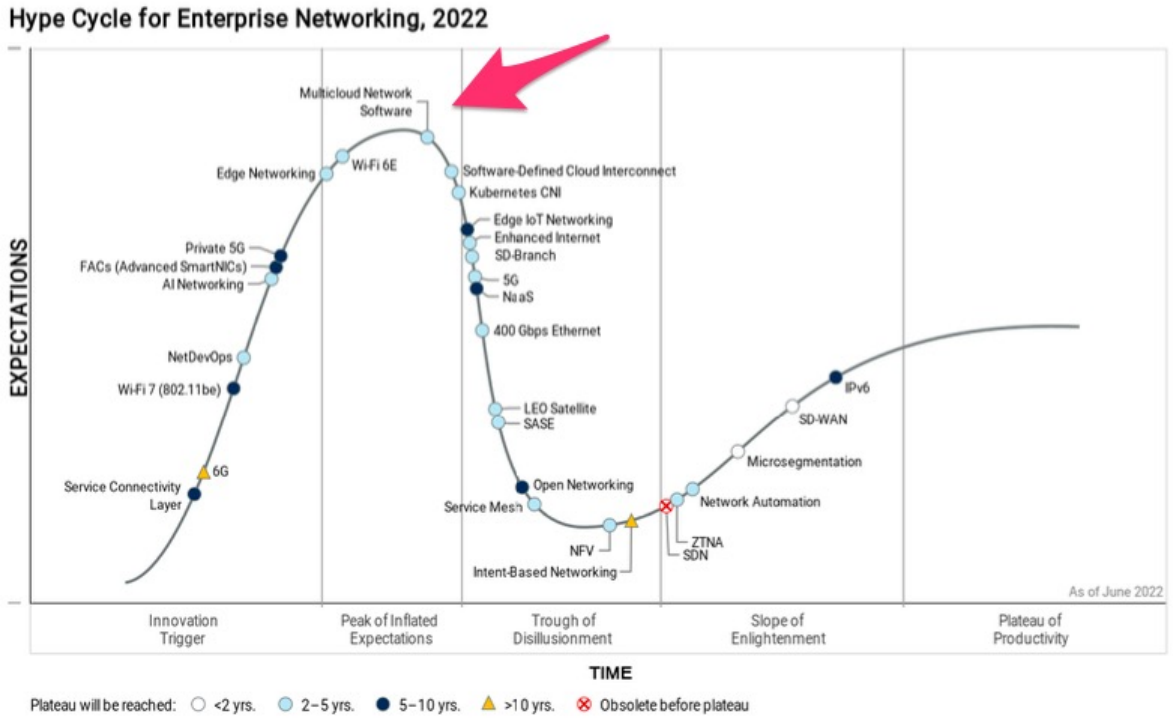
Explosion of Cloud Connectivity Options

- Connectivity to the cloud
- SD-WAN
- Encryption

Observability and Troubleshooting

- Different and limited across clouds
- Multi-Cloud Visibility
- Flying Blind across clouds

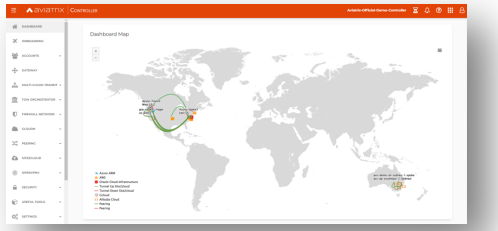
Gartner Hype Cycle for Enterprise Networking, 2022

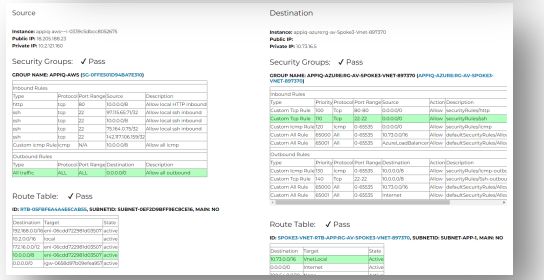


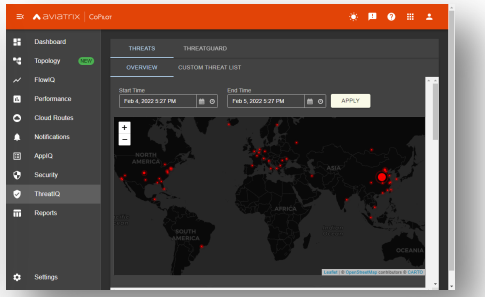
Source: Gartner (June 2022)

"MCNS enables the design, deployment and operation of a network in multiple public cloud environments. MCNS products enable consistent networking policy, network security, governance and network visibility across multiple cloud environments via a single point of management."
Reference: https://blogs.gartner.com/andrew-lerner/2022/04/21/multicloud-networking-software-mcns/

Common use cases for MCNS

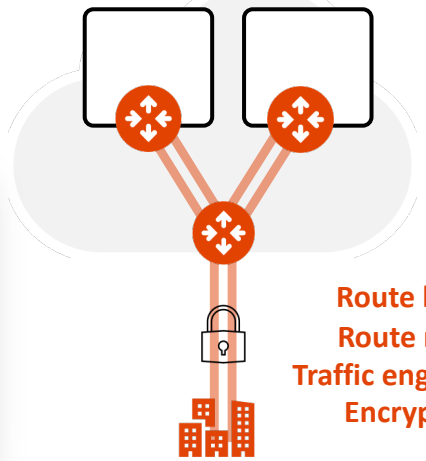






Visibility & Operations

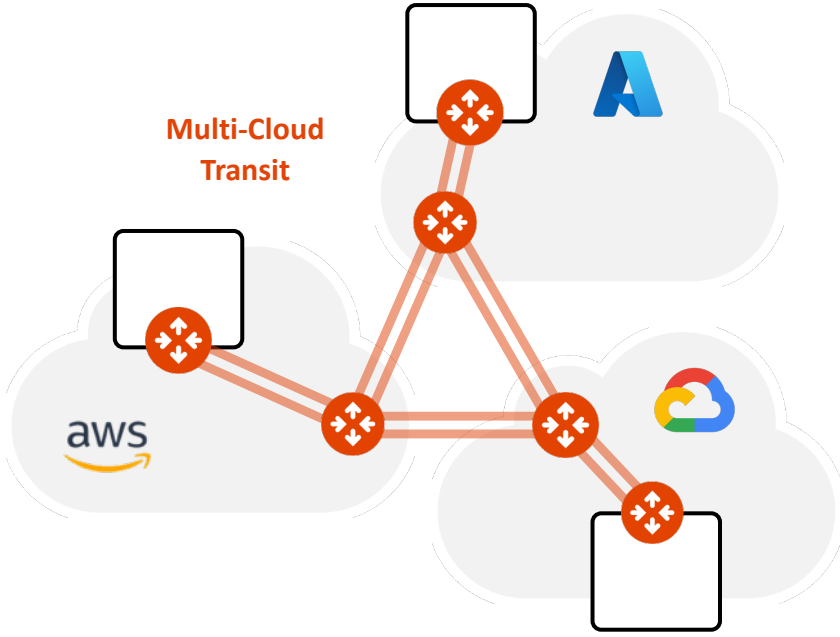
High-Availability
Hub-n-Spoke

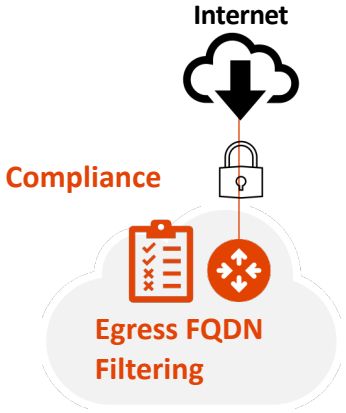


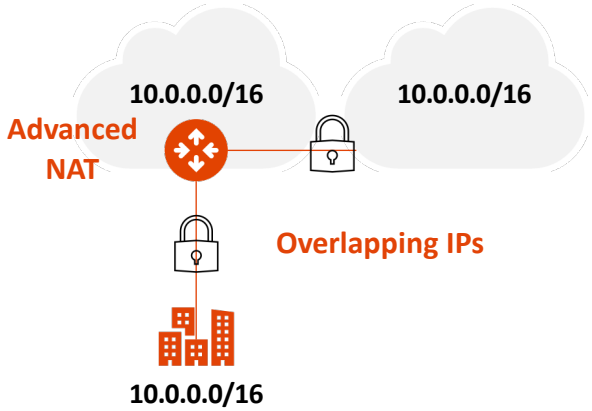
Route limits
Route maps
Traffic engineering
Encryption

Data Center-to-Cloud

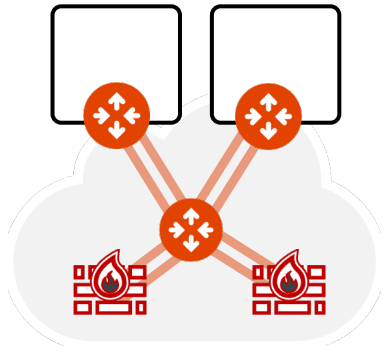
Multi-Cloud
Transit



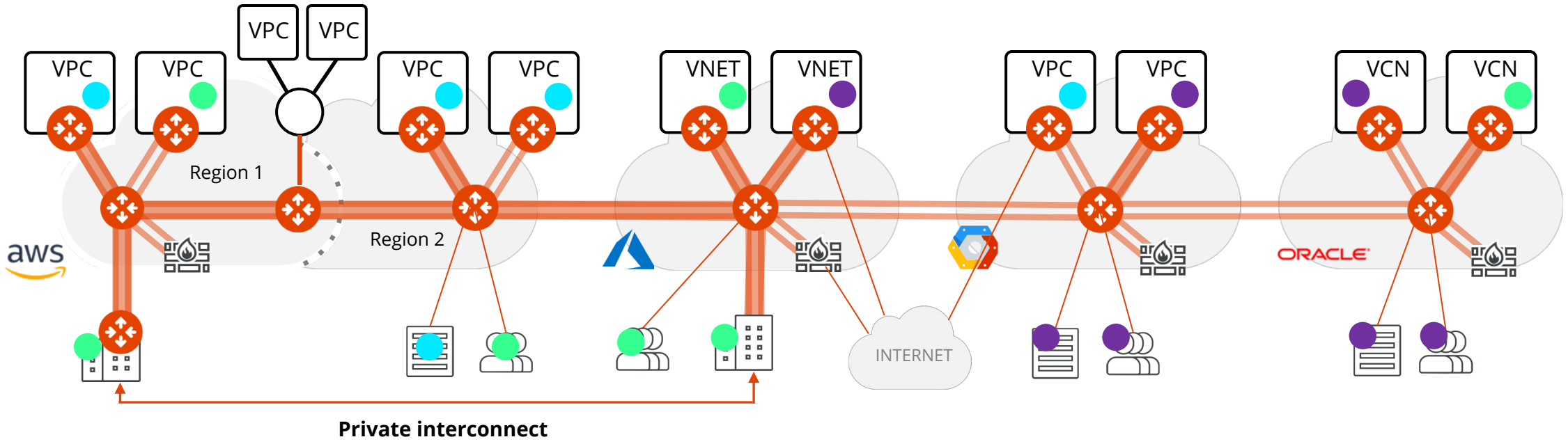




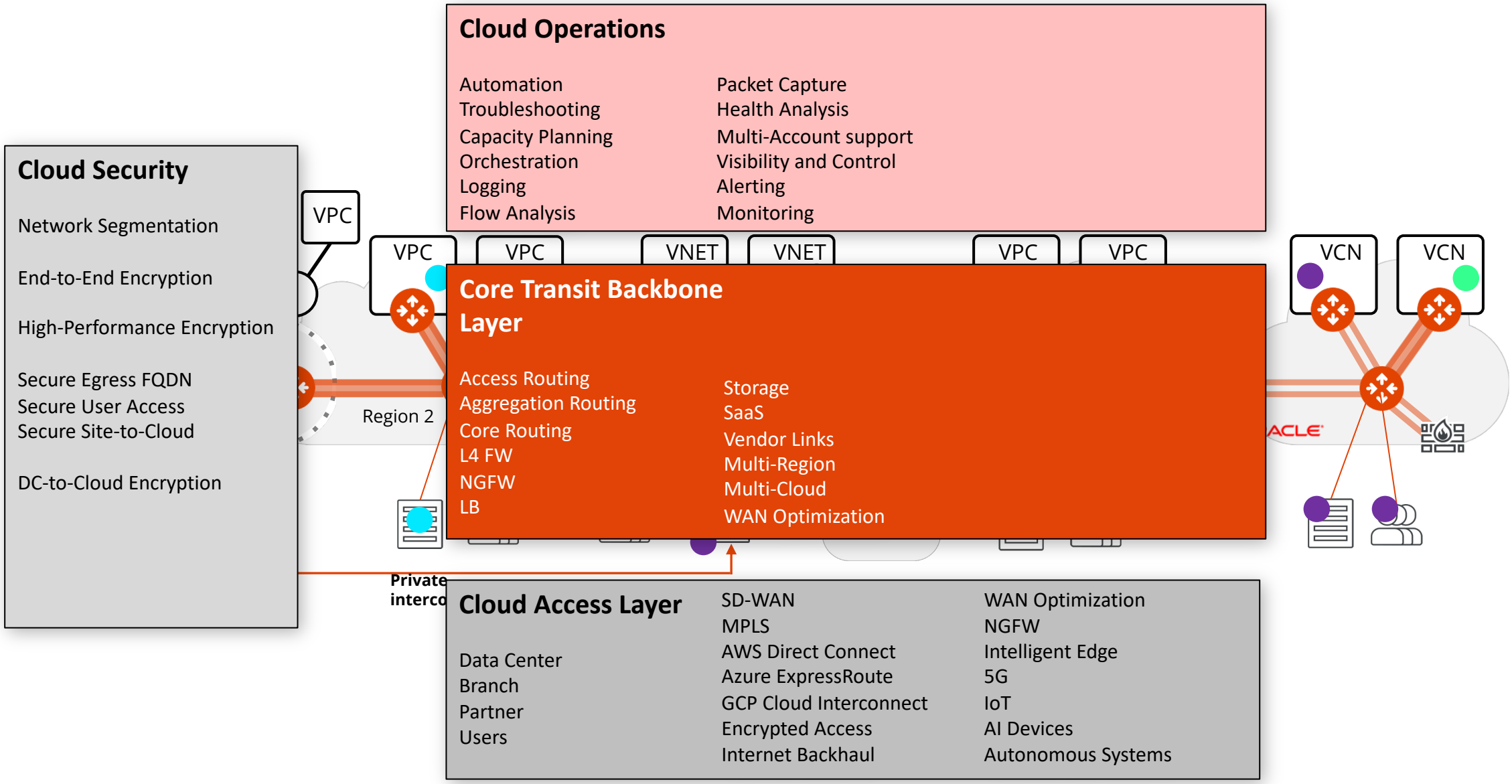
Consistent
Service Insertion
(NGFW)



Multi-Cloud Networking and Security



Multi-Cloud Networking and Security



Key take aways

- Cloud networking is continuously evolving
- Major cloud providers don’t make multi-cloud connectivity easy
- Service providers and MCNS are saving the day
- Cloud hub and spoke is the new spine-leaf repeatable architecture

Thank you!

Evgeny Vaganov
VP, Solutions Architecture, APAC, Aviatrix
evgeny@aviatrix.com
www.linkedin.com/in/evgeny-vaganov