

# 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](mailto:evgeny@aviatrix.com)



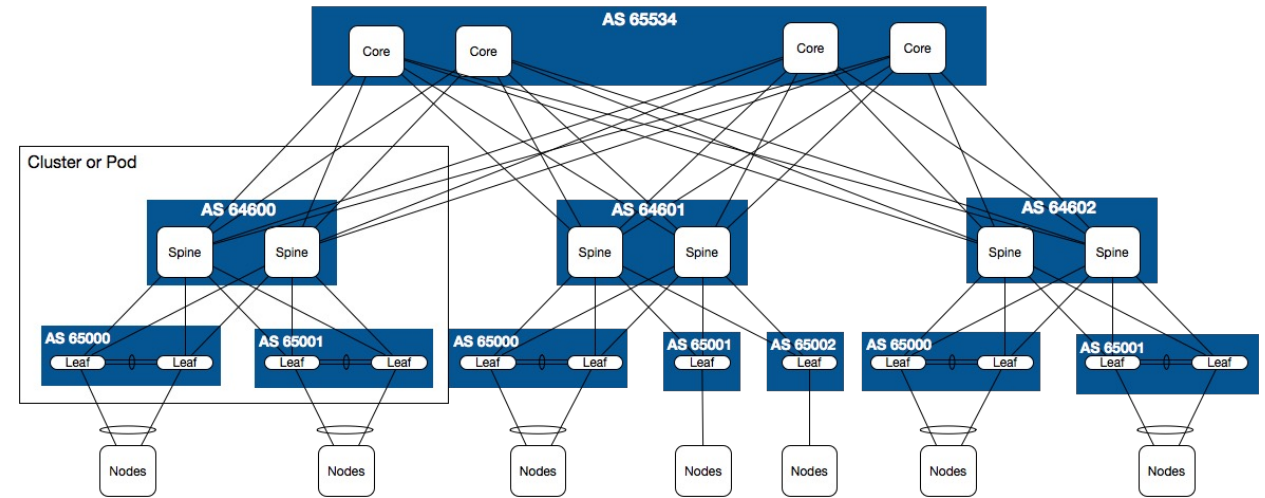
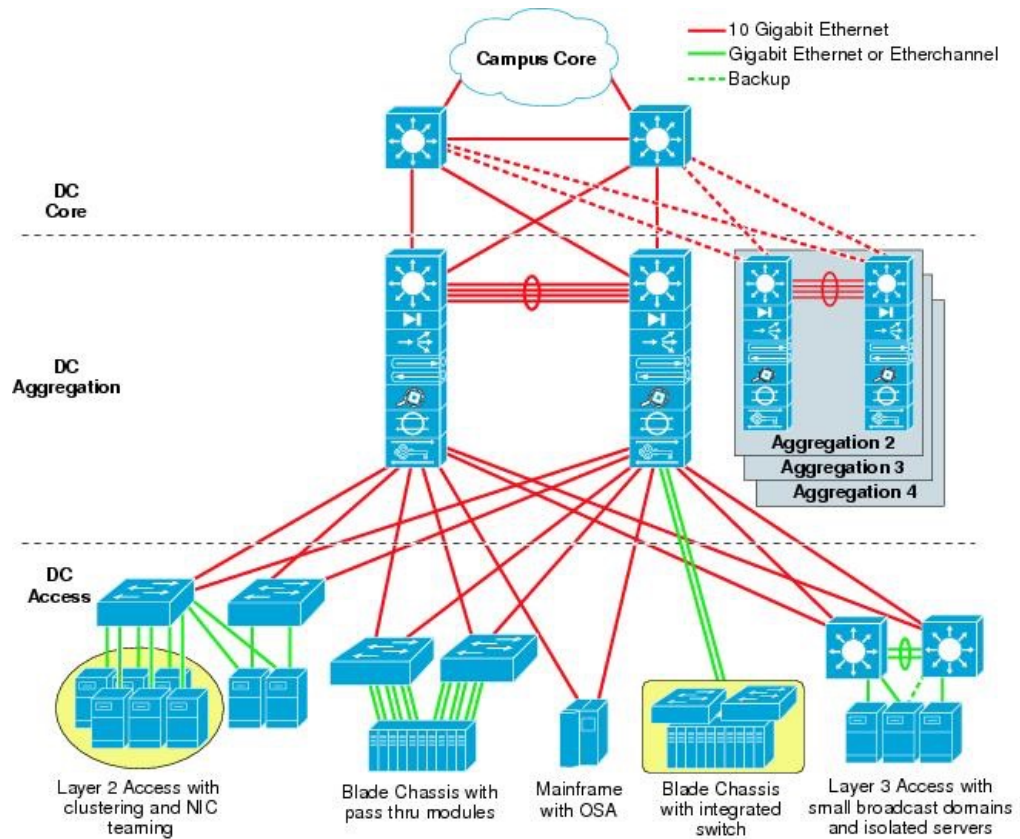
[www.linkedin.com/in/evgeny-vaganov](https://www.linkedin.com/in/evgeny-vaganov)



Prequel

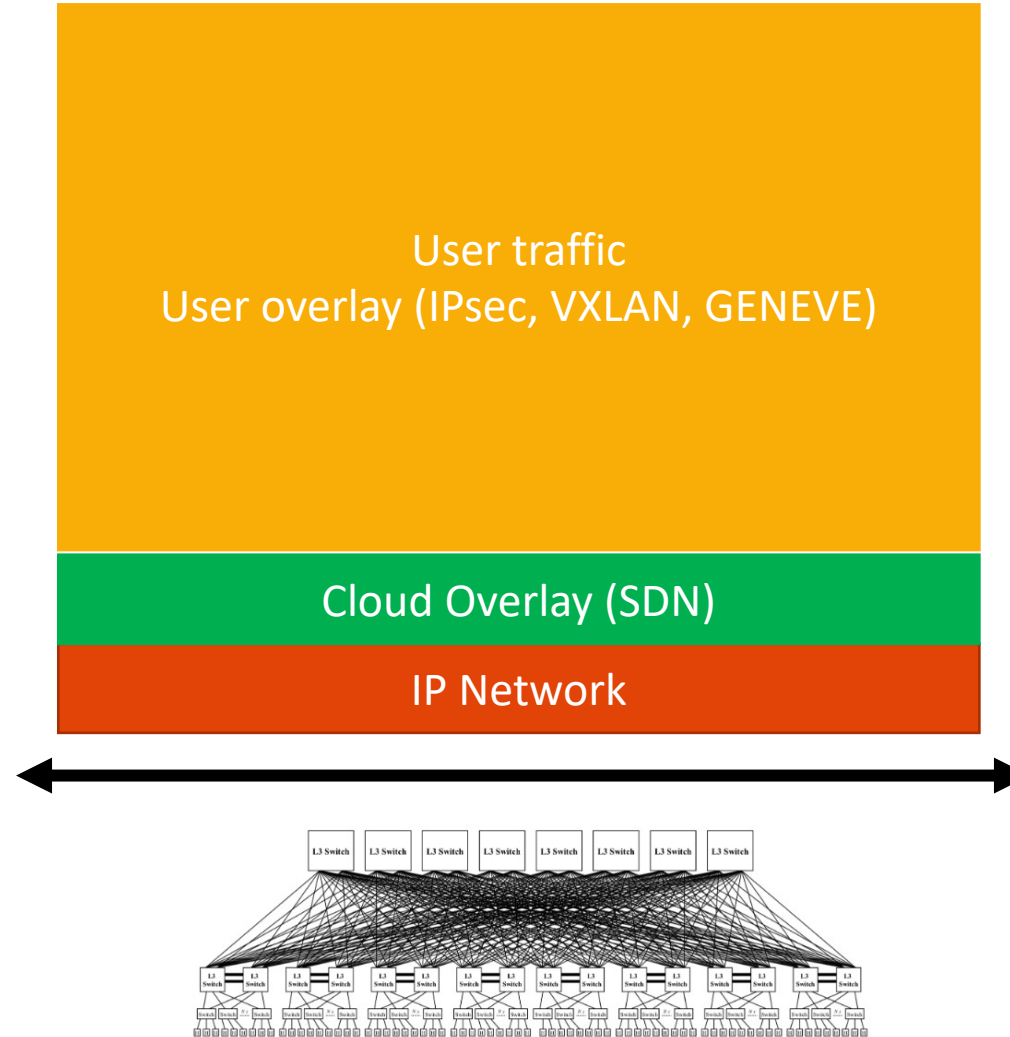


# Reference architectures in on-premises networks



# Overlay vs underlay

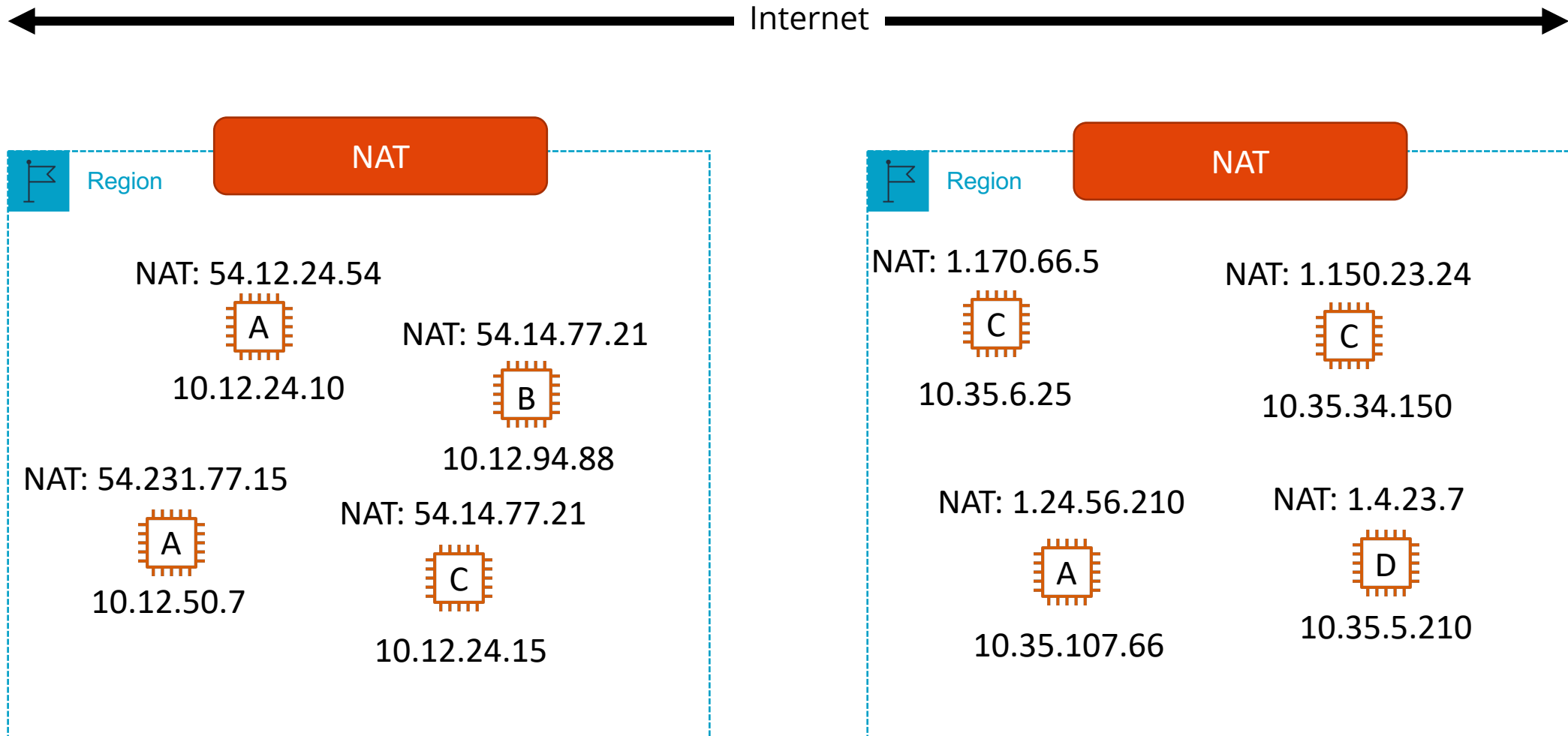
---



The age of cloud computing  
1st gen cloud networking



# EC2 Classic



**AWS News Blog**

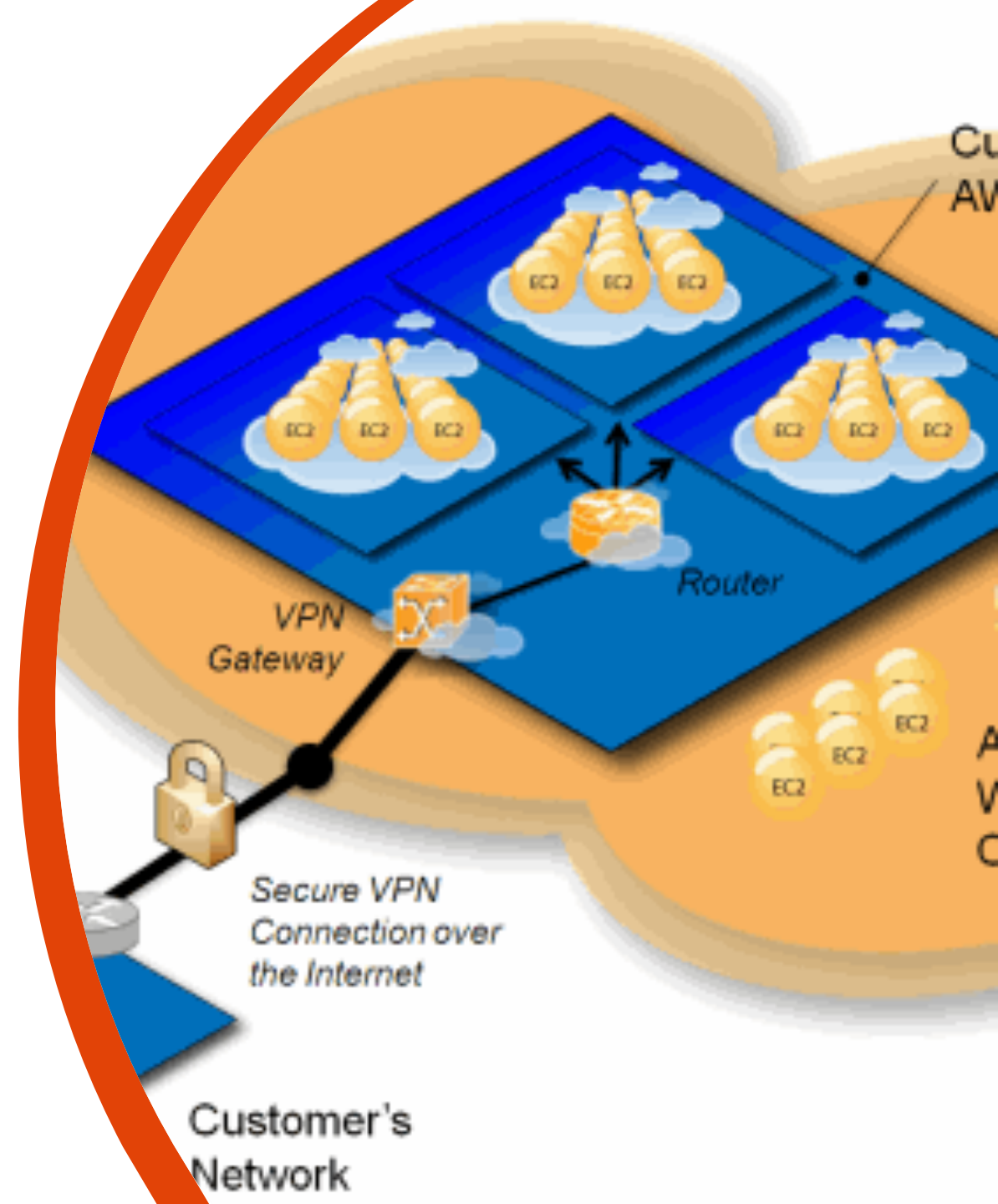
## **EC2-Classic Networking is Retiring – Here's How to Prepare**

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.

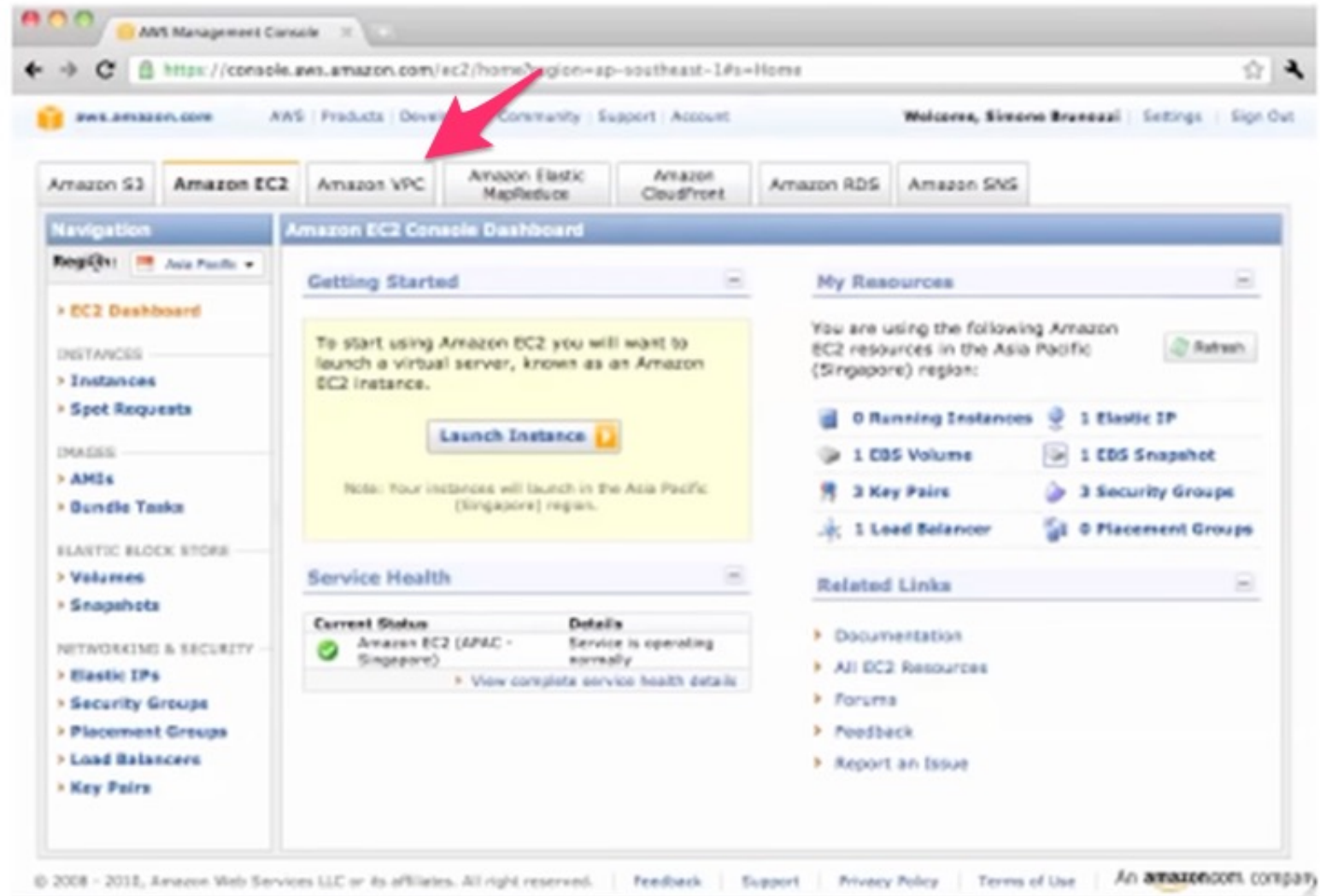
<https://aws.amazon.com/blogs/aws/ec2-classic-is-retiring-heres-how-to-prepare/>

# VPCs everywhere 2nd gen cloud networking





# Virtual Private Cloud

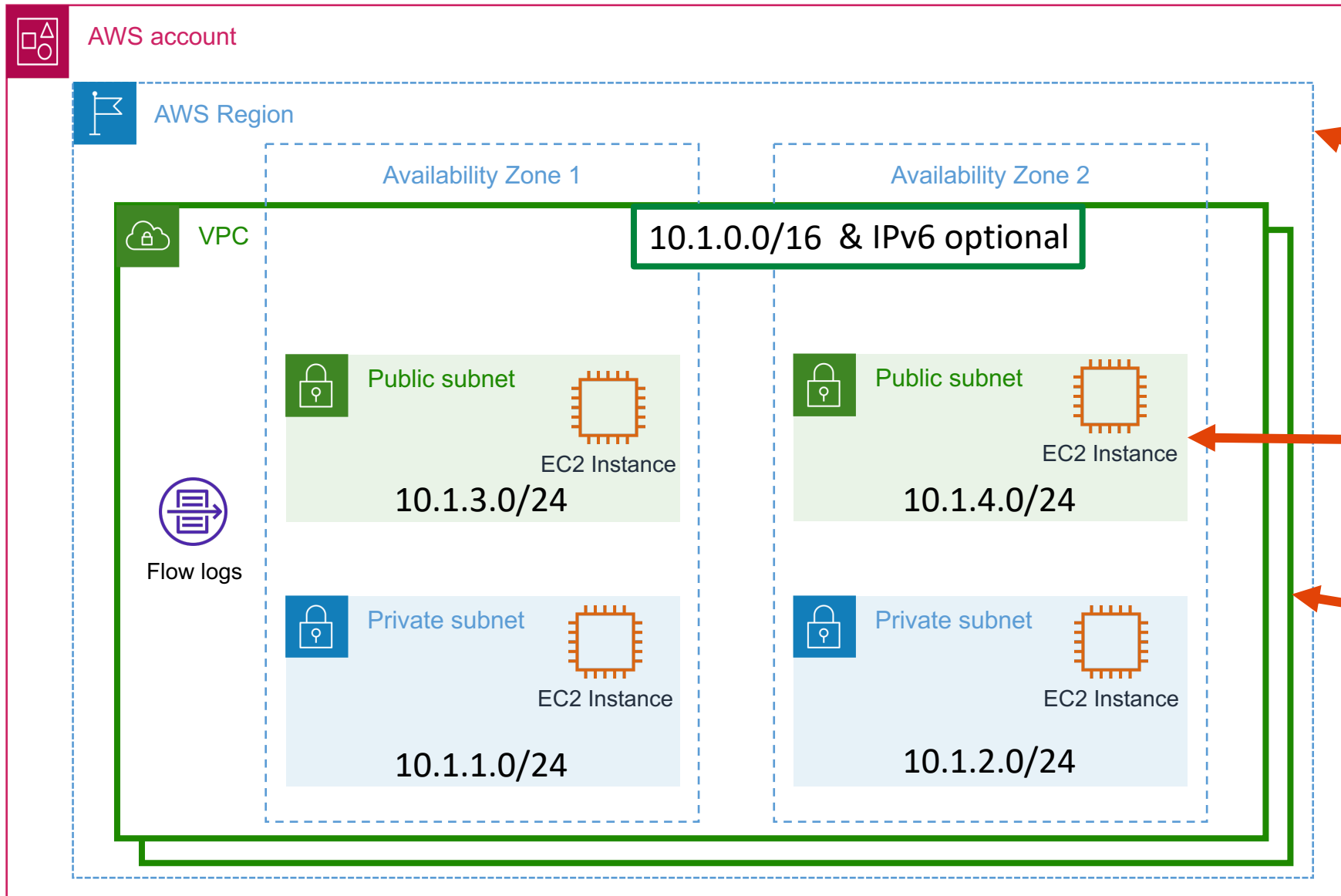


The screenshot displays the AWS Management Console interface. At the top, the browser address bar shows the URL `https://console.aws.amazon.com/ec2/home?region=ap-southeast-1#p=Home`. The navigation bar includes links for AWS, Products, Developer, Community, Support, and Account, along with the user name 'Welcome, Simone Brazzoli' and options for Settings and Sign Out. Below the navigation bar, a row of service tabs is visible: Amazon S3, Amazon EC2 (highlighted with a red arrow), Amazon VPC, Amazon Elastic MapReduce, Amazon CloudFront, Amazon RDS, and Amazon SNS. The main content area is titled 'Amazon EC2 Console Dashboard' and is divided into several sections:

- Getting Started:** A yellow box with the text 'To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.' and a prominent 'Launch Instance' button. A note below states: 'Note: Your instances will launch in the Asia Pacific (Singapore) region.'
- My Resources:** A summary of resources in the Asia Pacific (Singapore) region, including:
  - 0 Running Instances
  - 1 Elastic IP
  - 1 EBS Volume
  - 1 EBS Snapshot
  - 3 Key Pairs
  - 3 Security Groups
  - 1 Load Balancer
  - 0 Placement Groups
- Service Health:** A table showing the current status of the Amazon EC2 (APAC - Singapore) service, which is 'operating normally'. A link is provided to 'View complete service health details'.
- Related Links:** A list of links including Documentation, All EC2 Resources, Forums, Feedback, and Report an Issue.

The footer of the console contains copyright information: '© 2008 - 2013, Amazon Web Services LLC or its affiliates. All rights reserved.' and links for Feedback, Support, Privacy Policy, and Terms of Use, along with the Amazon logo and the text 'An Amazon.com company'.

# 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

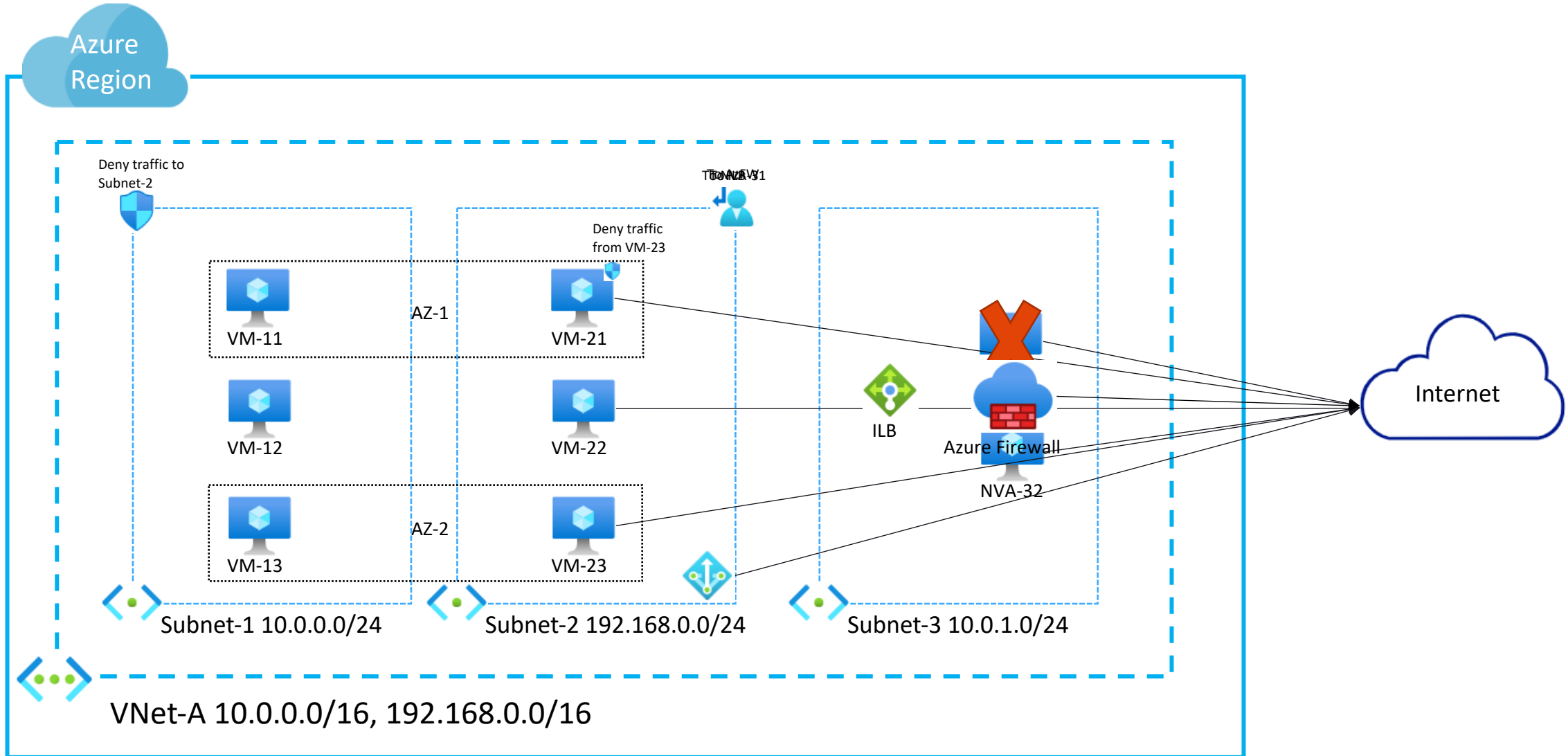
Can enable VPC Flow logs for traffic flow data

## EC2 Classic and EC2 VPC Differences

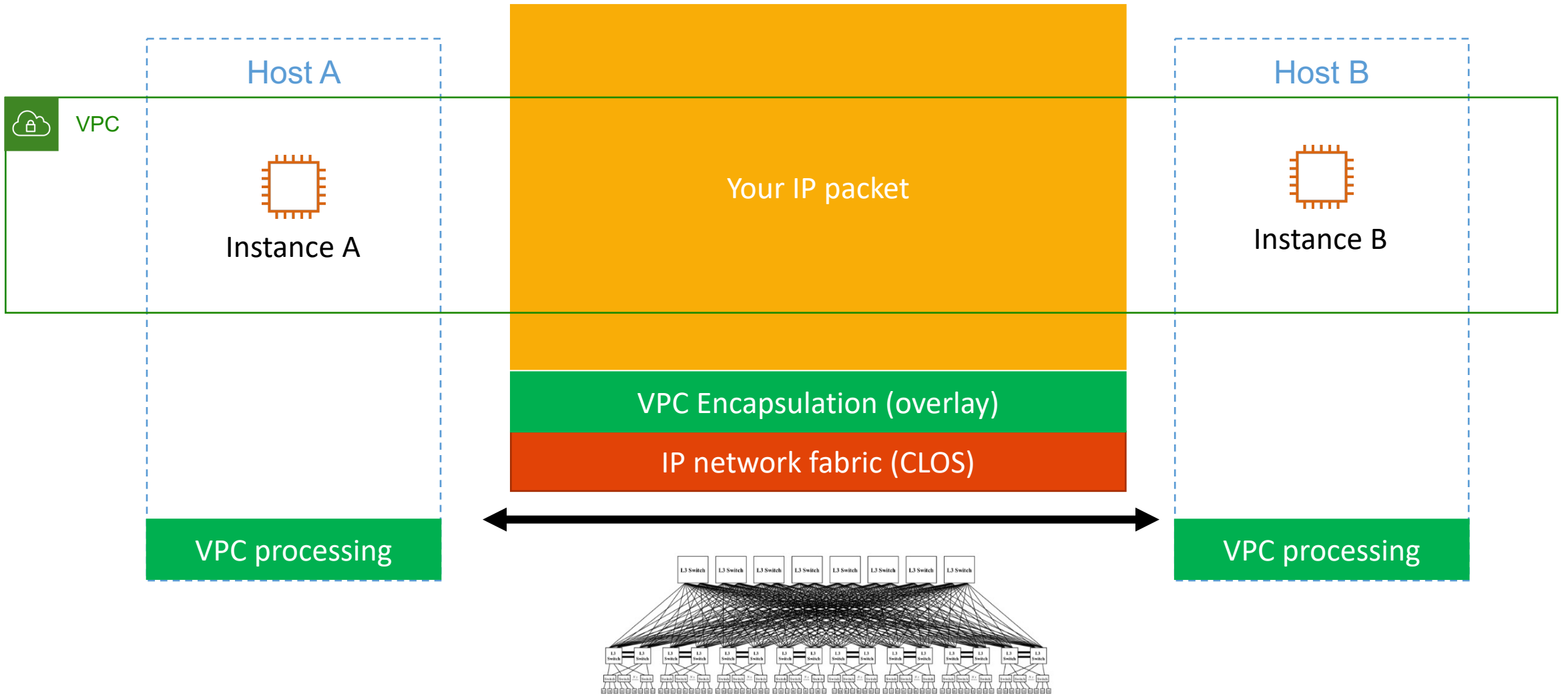


EC2 Classic	EC2 VPC
EIP is disassociated when instance stopped	EIP remains associated when instance stopped
Unlimited number of security groups	Up to 5 security groups
Can't change the SGs of a running instance	Can change the SGs of a running instance
SG rules for inbound traffic only	SG rules for inbound 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

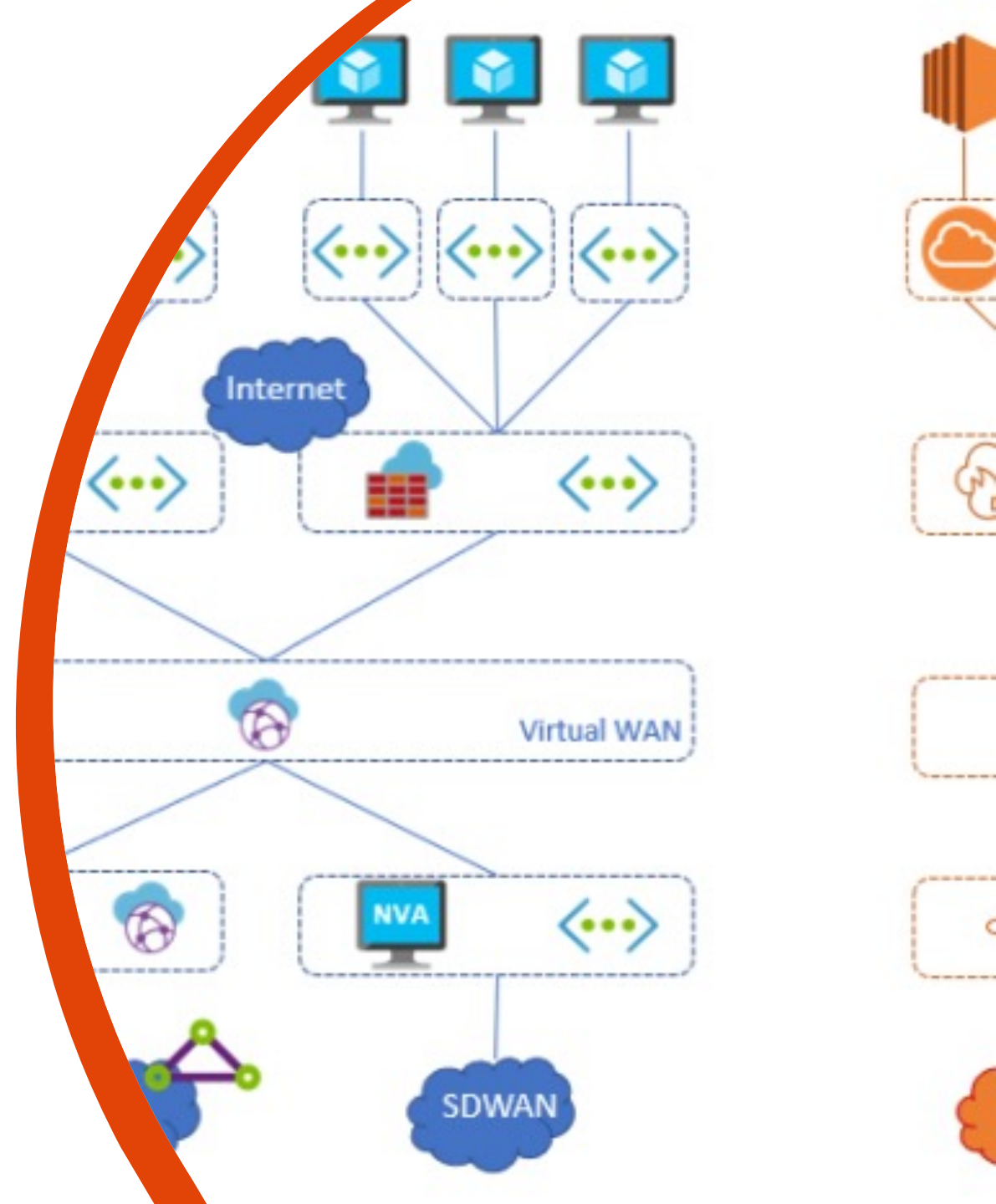
# Azure VNet



# VPC on the wire

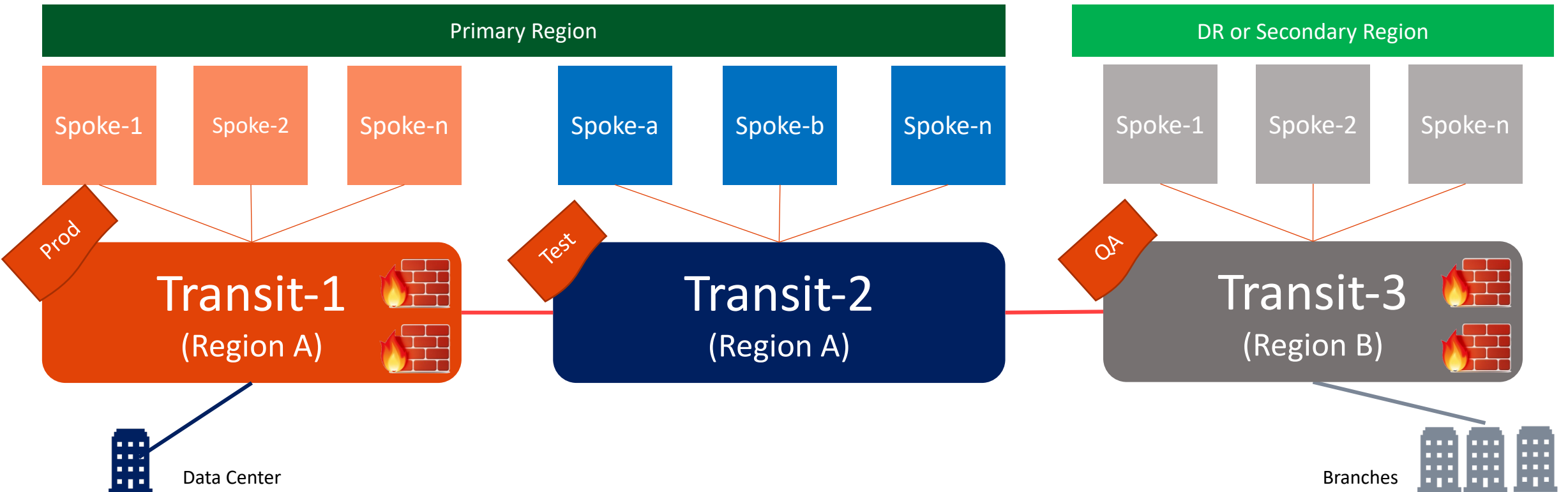


# Hub and Spoke 3rd gen cloud networking

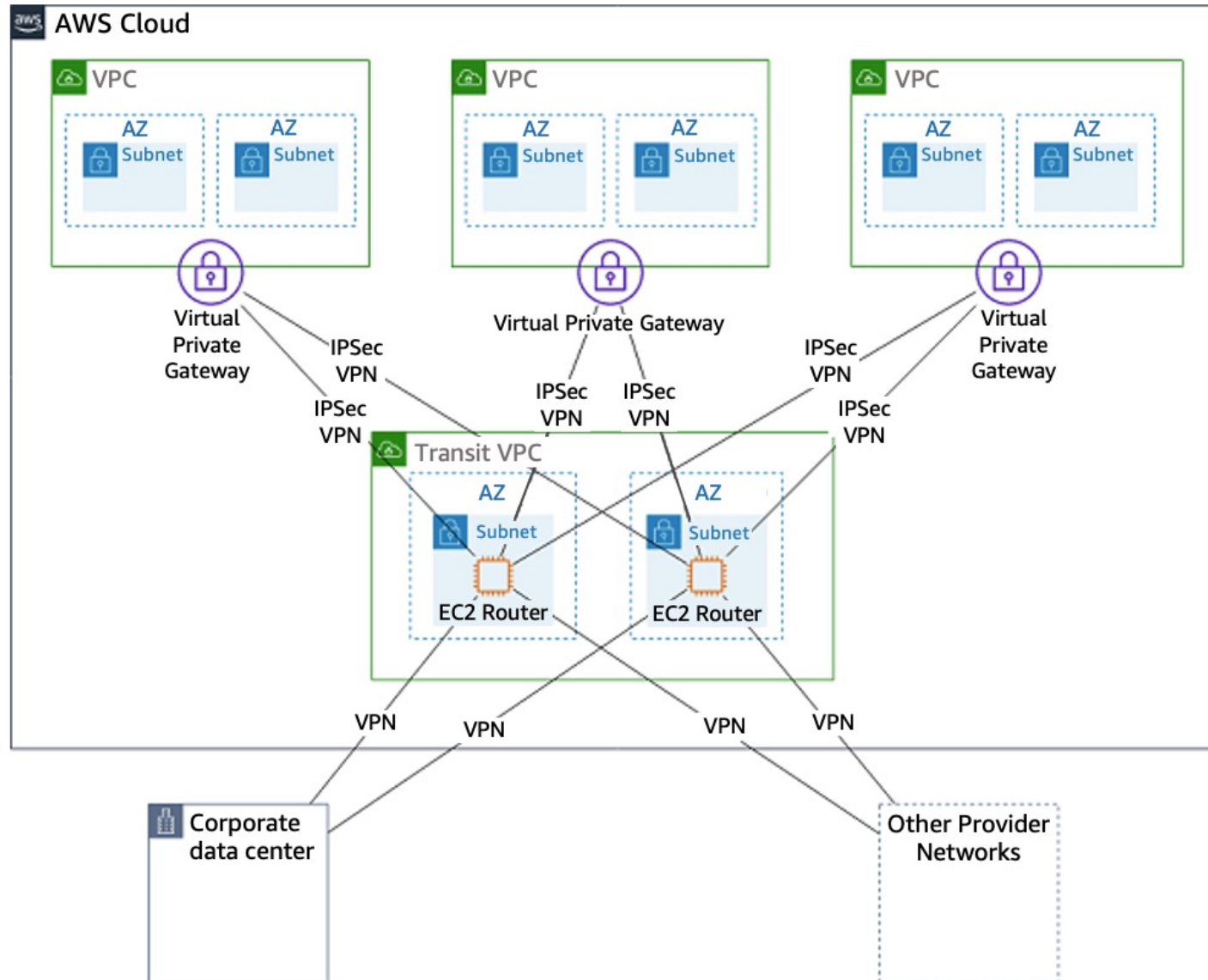


# Purpose of Transit in Cloud Networking

- 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

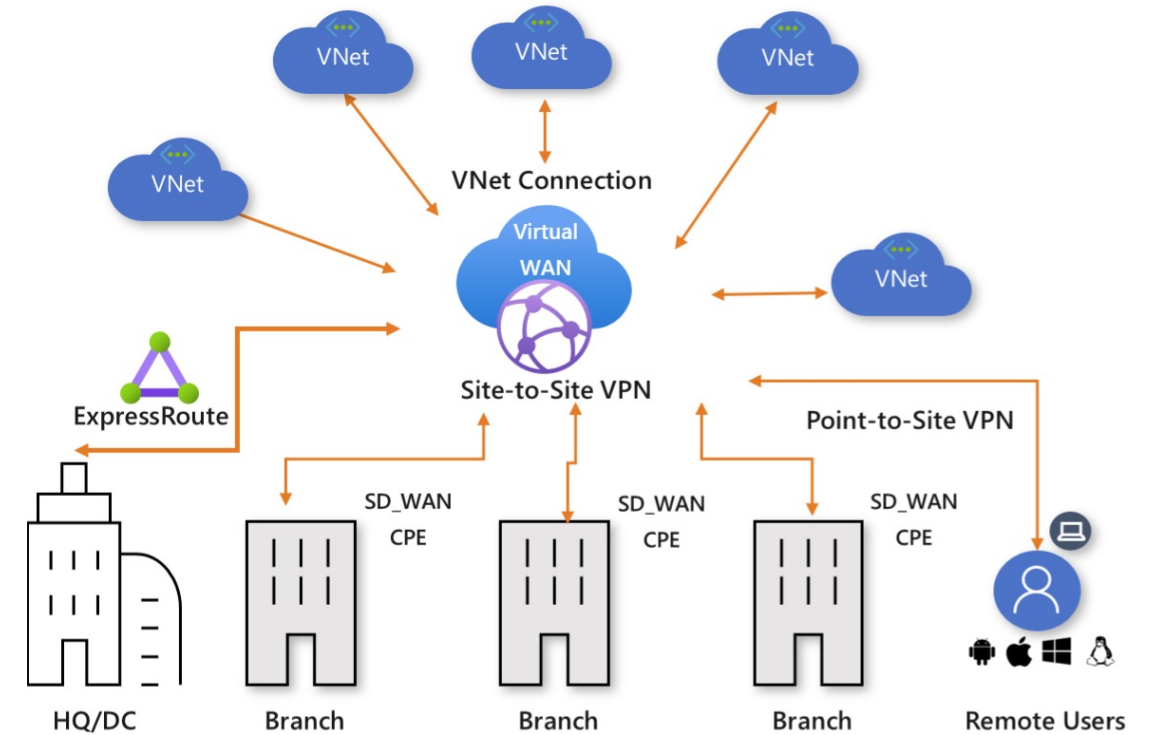
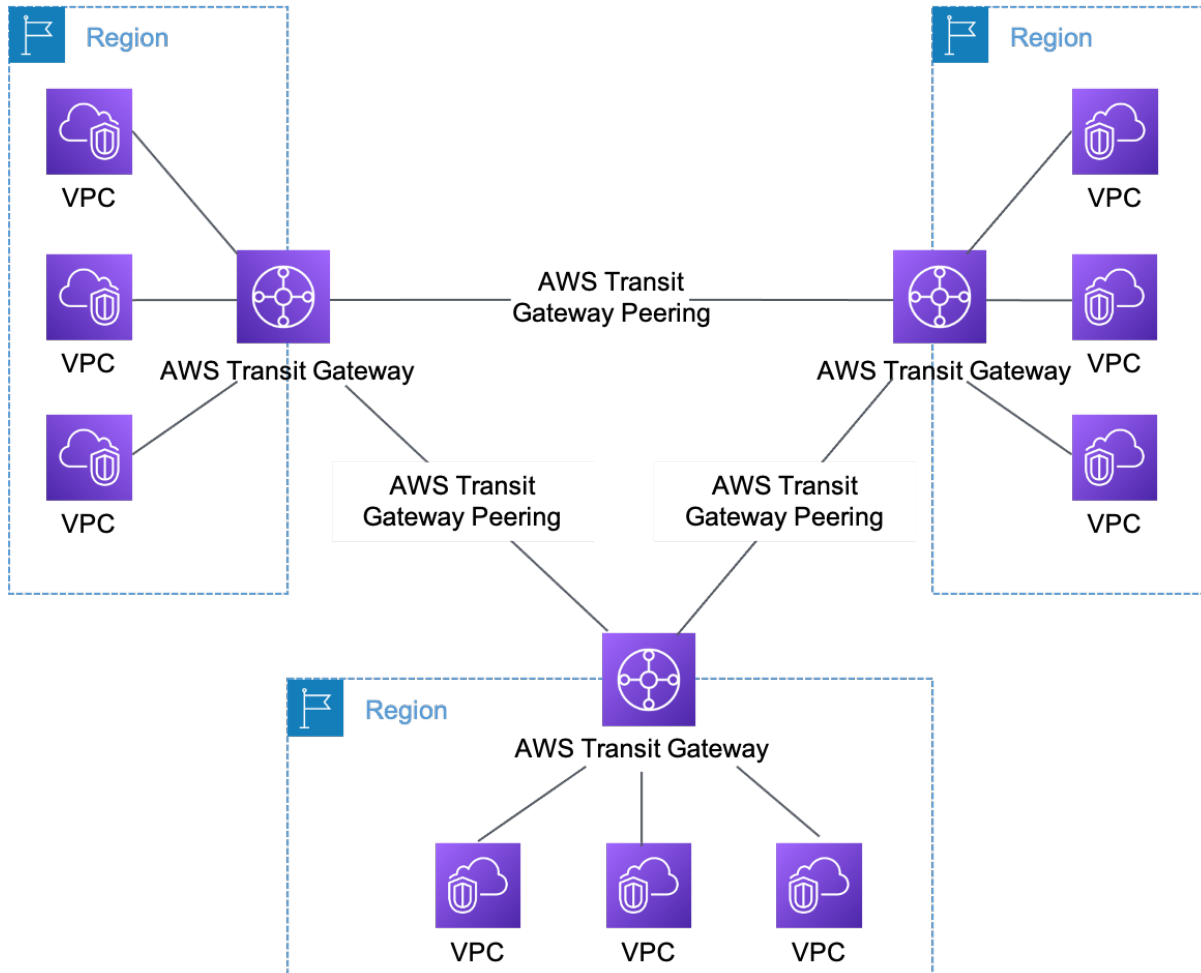


# Transit VPC

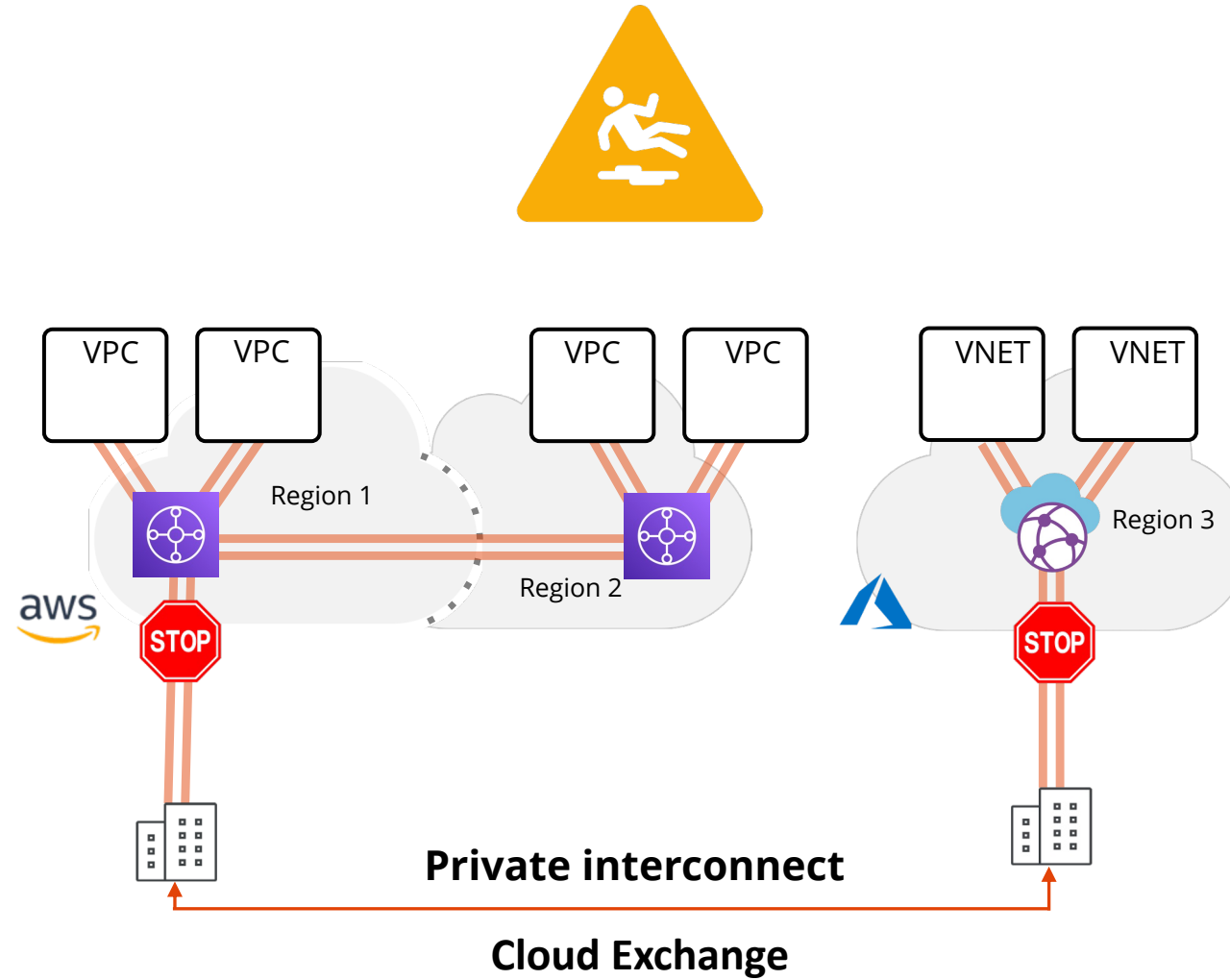




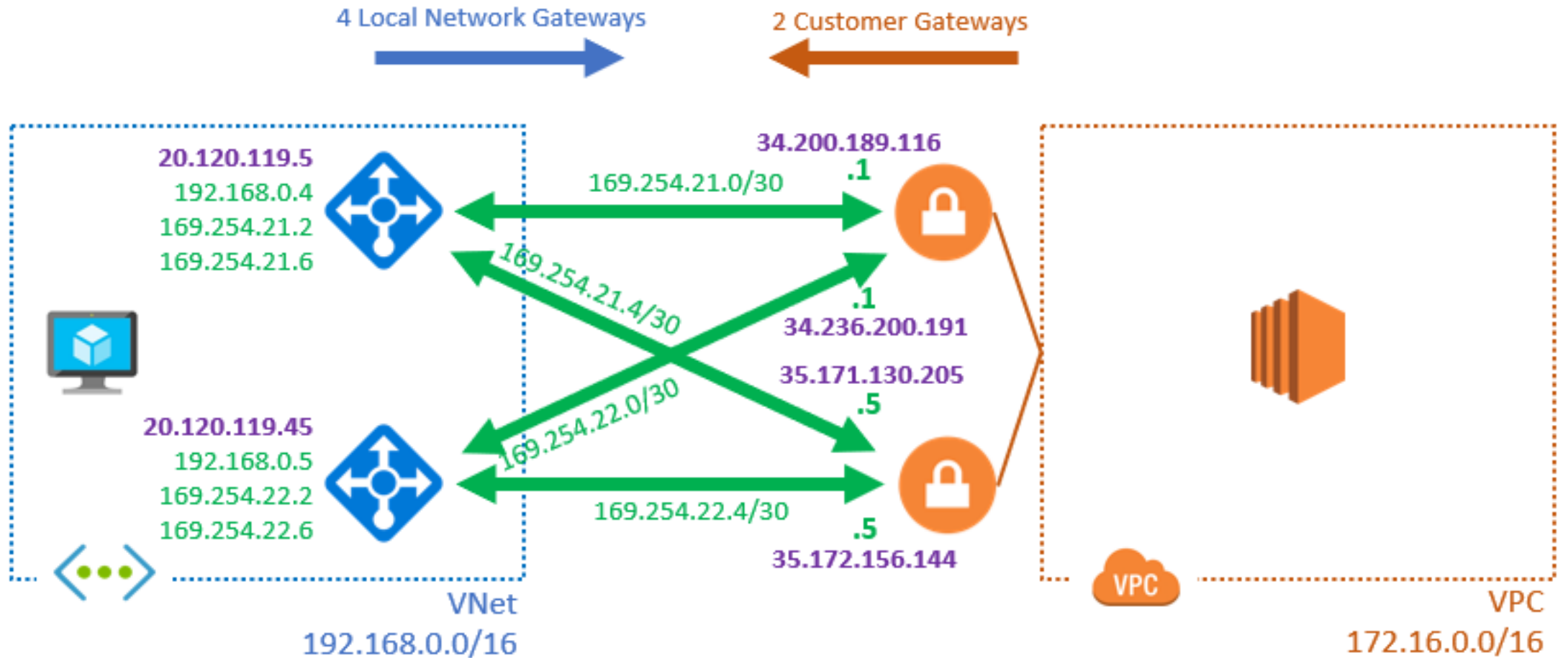
# Managed network services



# Multi-cloud?

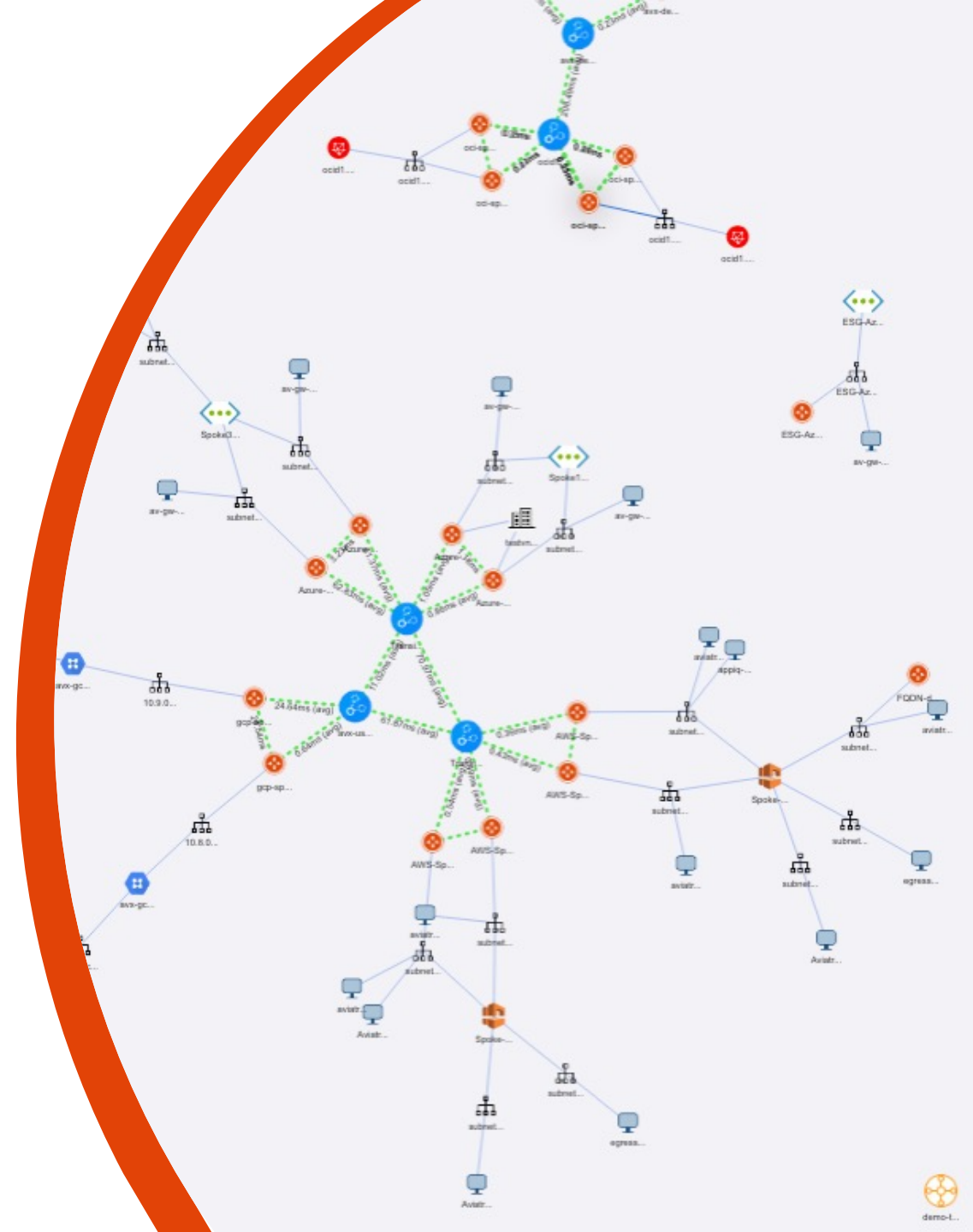


# Going with native



<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

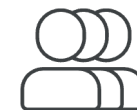
- Different and limited across clouds
- Multi-Cloud Visibility
- Flying Blind across clouds



Data  
Centers



Branch  
Offices

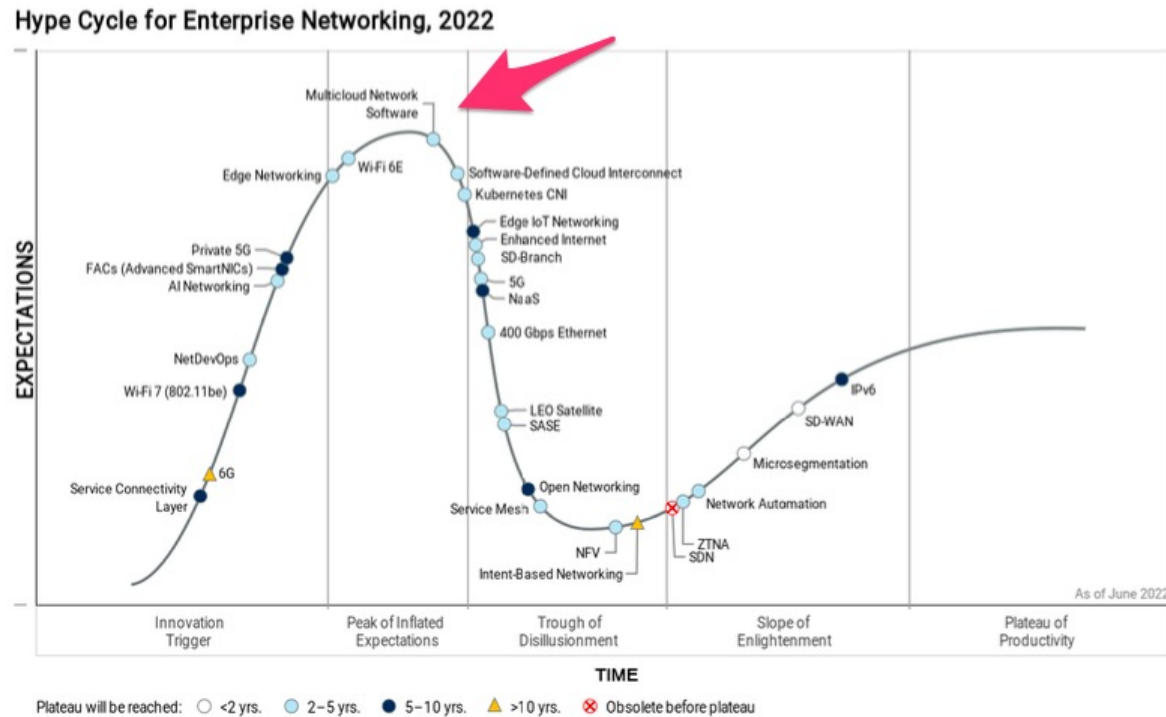


Remote  
Users



Partners &  
Customers

# Gartner Hype Cycle for Enterprise Networking, 2022



Gartner

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

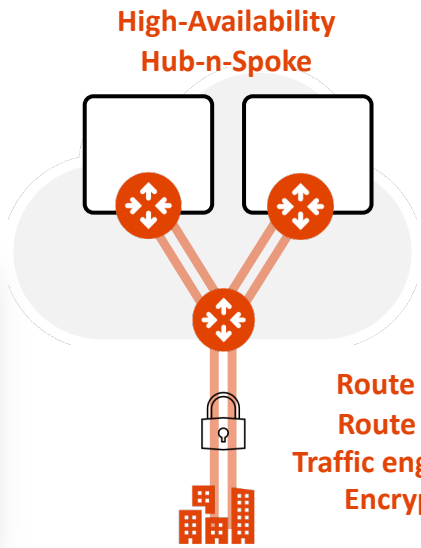
The screenshot displays the Panorama configuration interface. At the top, there's a 'Dashboard Map' showing a world map with a highlighted region. Below it are two configuration tables:

Security Groups: ✓ Pass			
Group Name	App/Service	ICMP	HTTP/S
...	...	...	...

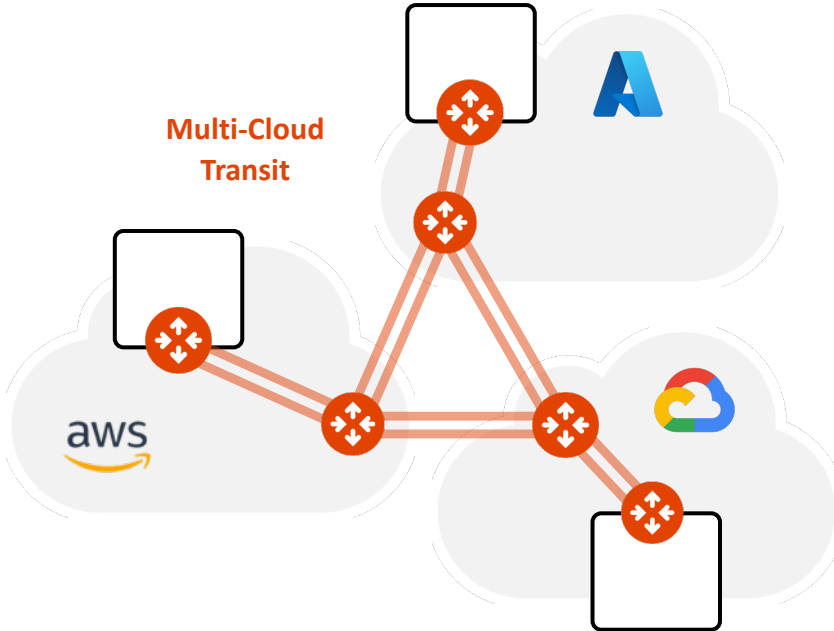
Route Table: ✓ Pass			
ID	IPsec	Summit	...
...	...	...	...

Visibility & Operations

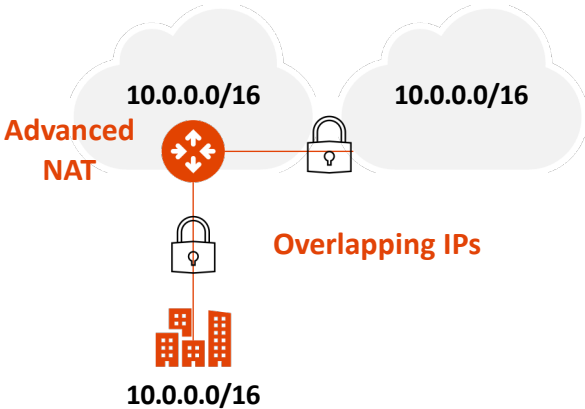
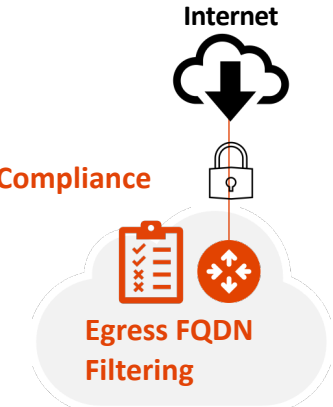


Data Center-to-Cloud

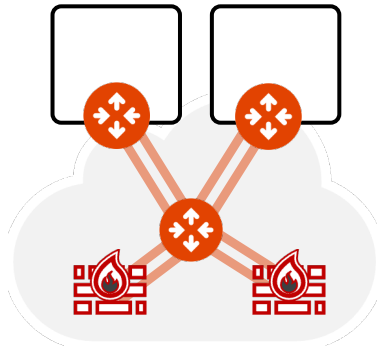
Route limits  
Route maps  
Traffic engineering  
Encryption



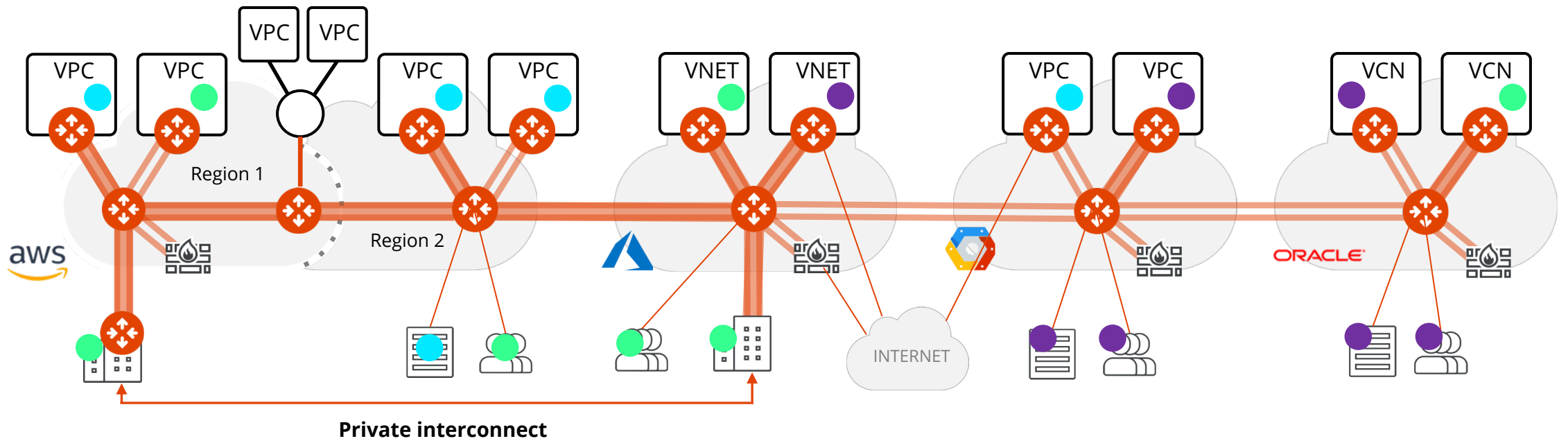
Multi-Cloud Transit



Consistent Service Insertion (NGFW)

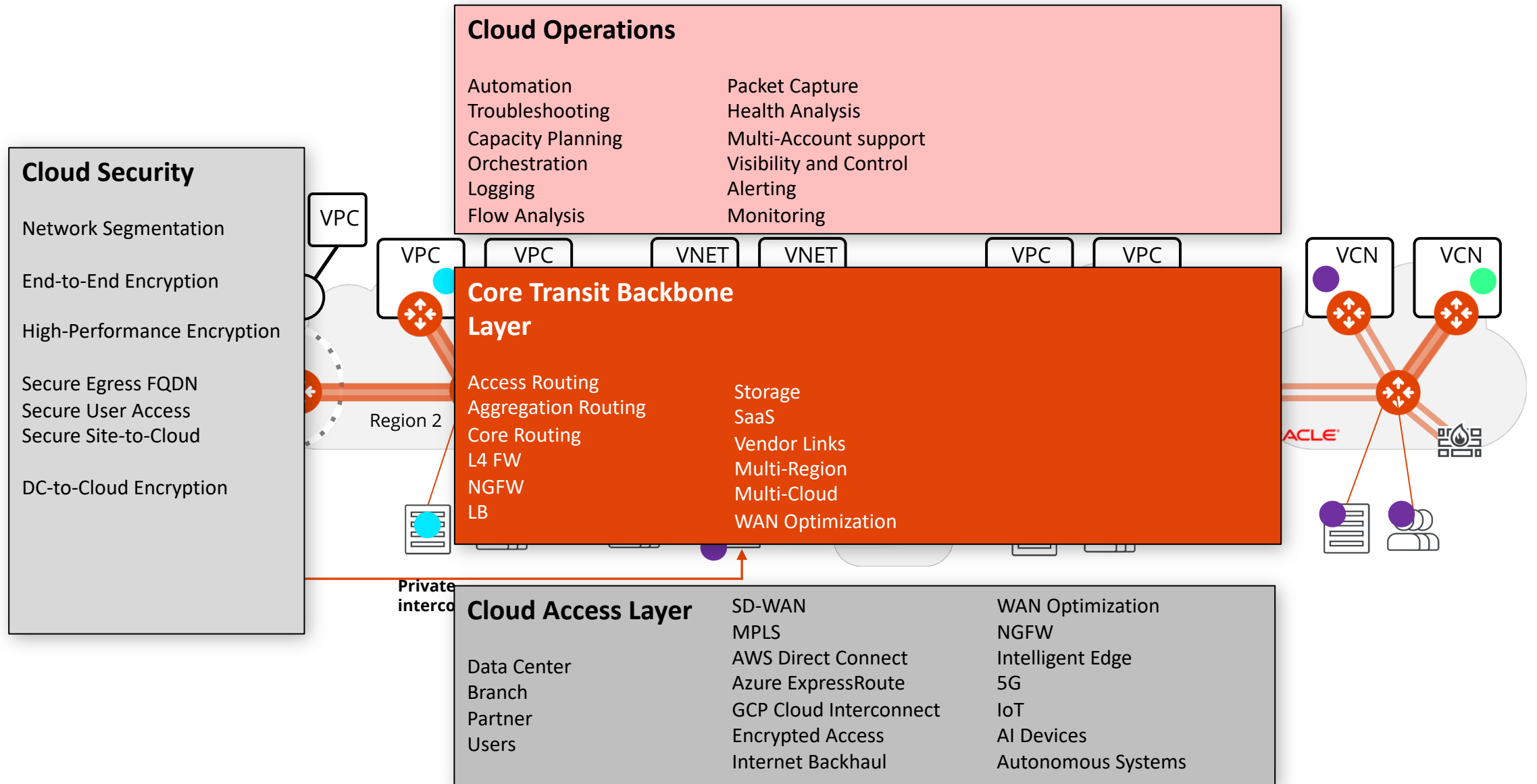


# Multi-Cloud Networking and Security





# 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](mailto:evgeny@aviatrix.com)



[www.linkedin.com/in/evgeny-vaganov](https://www.linkedin.com/in/evgeny-vaganov)