AWS
User Groups
Bulgaria

Networking design concepts in AWS

Nikolay Bunev

AWS Community Day Bulgaria 2023

Who am I

- Father of 2 great kids
- Mechanical engineer by education
- IT engineer/consultant by choice
- Doing cloudy things in AWS in the last 7 years
- Currently leading a team of AWS ProServ experts @ SoftwareOne
- AWS Community Builder in the Security & Identity category since 2020

AWS community builder

aws certified Solutions Architect PROFESSIONAL

aws certified DevOps Engineer PROFESSIONAL

”A robust network architecture is the foundation of both performance and security in the cloud.”


SO MANY CHOICES.
I KNOW, RIGHT?

“What are you optimizing for?”

James Hamilton,
SVP & Distinguished Engineer,
Amazon Web Services

I’ve asked ChatGPT What is VPC?

A Virtual Private Cloud (VPC) is a virtual network environment provided by cloud service providers like Amazon Web Services (AWS) that allows you to create a logically isolated section of the cloud where you can deploy and manage your cloud resources.

”Multi-VPC or Multi-account is a better isolation strategy?”

It Depends.


TOO MANY CHOICES...
FALSE.
memes.com

New workloads on AWS

Migrations to AWS

Traffic Inspection in AWS

Single VPC

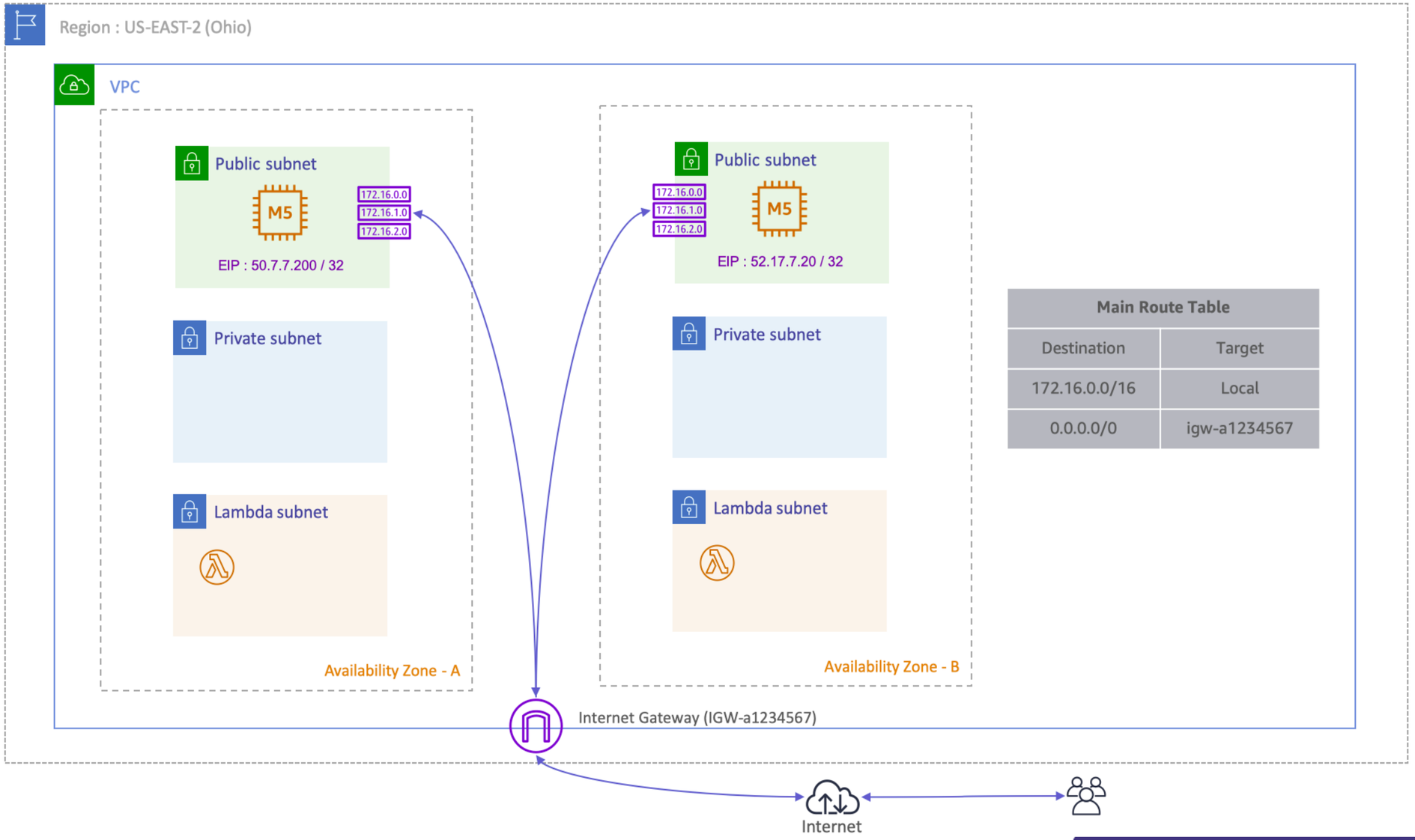
Multi-VPC / Multi-Account

Hybrid Connectivity

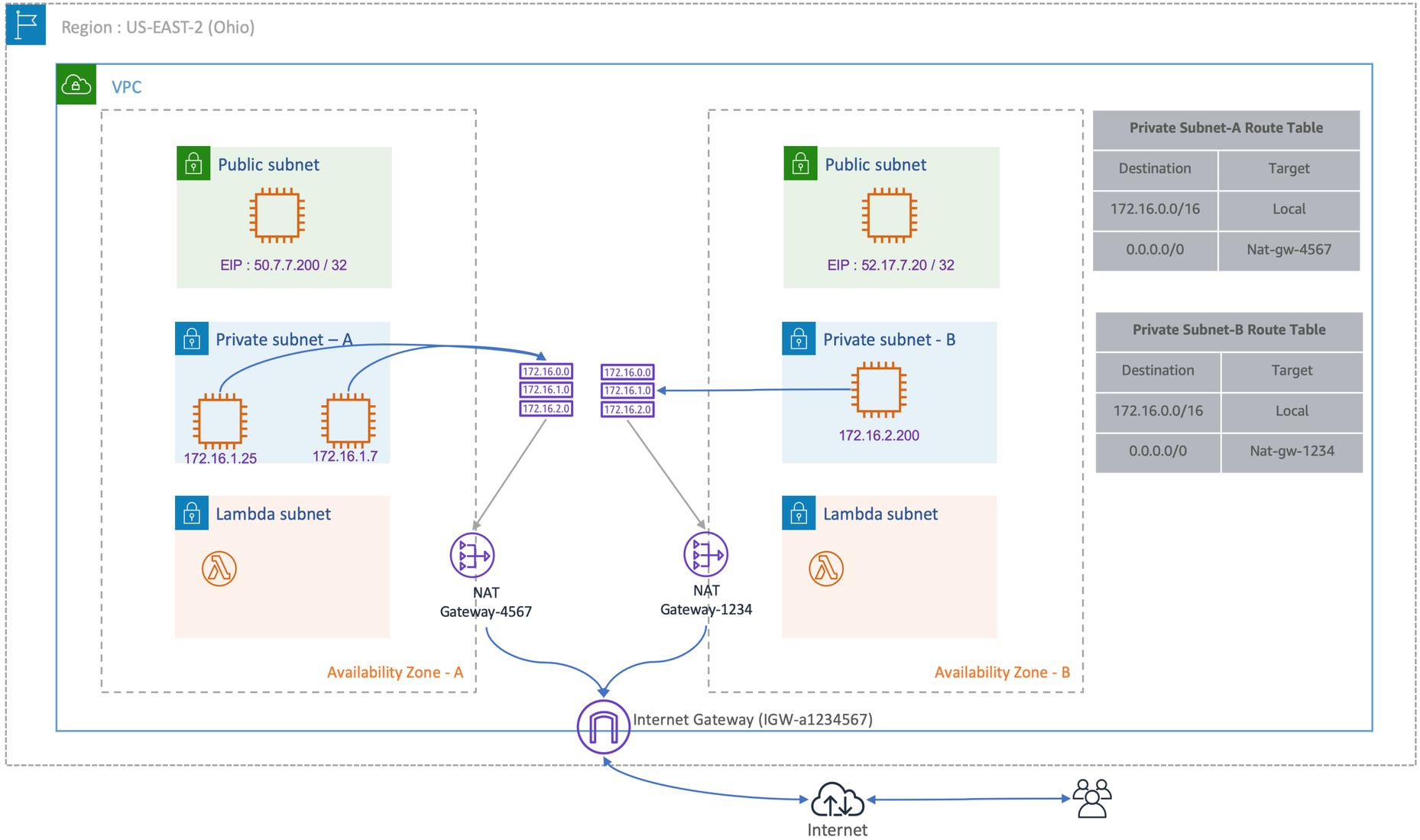
Traffic Inspection in AWS

Single VPC

Single VPC


Region : US-EAST-2 (Ohio)
VPC
Public subnet
M5
172.16.0.0
172.16.1.0
172.16.2.0
EIP : 50.7.7.200 / 32
Private subnet
Lambda subnet
Availability Zone - A
Public subnet
172.16.0.0
172.16.1.0
172.16.2.0
M5
EIP : 52.17.7.20 / 32
Private subnet
Lambda subnet
Availability Zone - B
Main Route Table
Destination
Target
172.16.0.0/16
Local
0.0.0.0/0
igw-a1234567
Internet Gateway (IGW-a1234567)
Internet

Single VPC

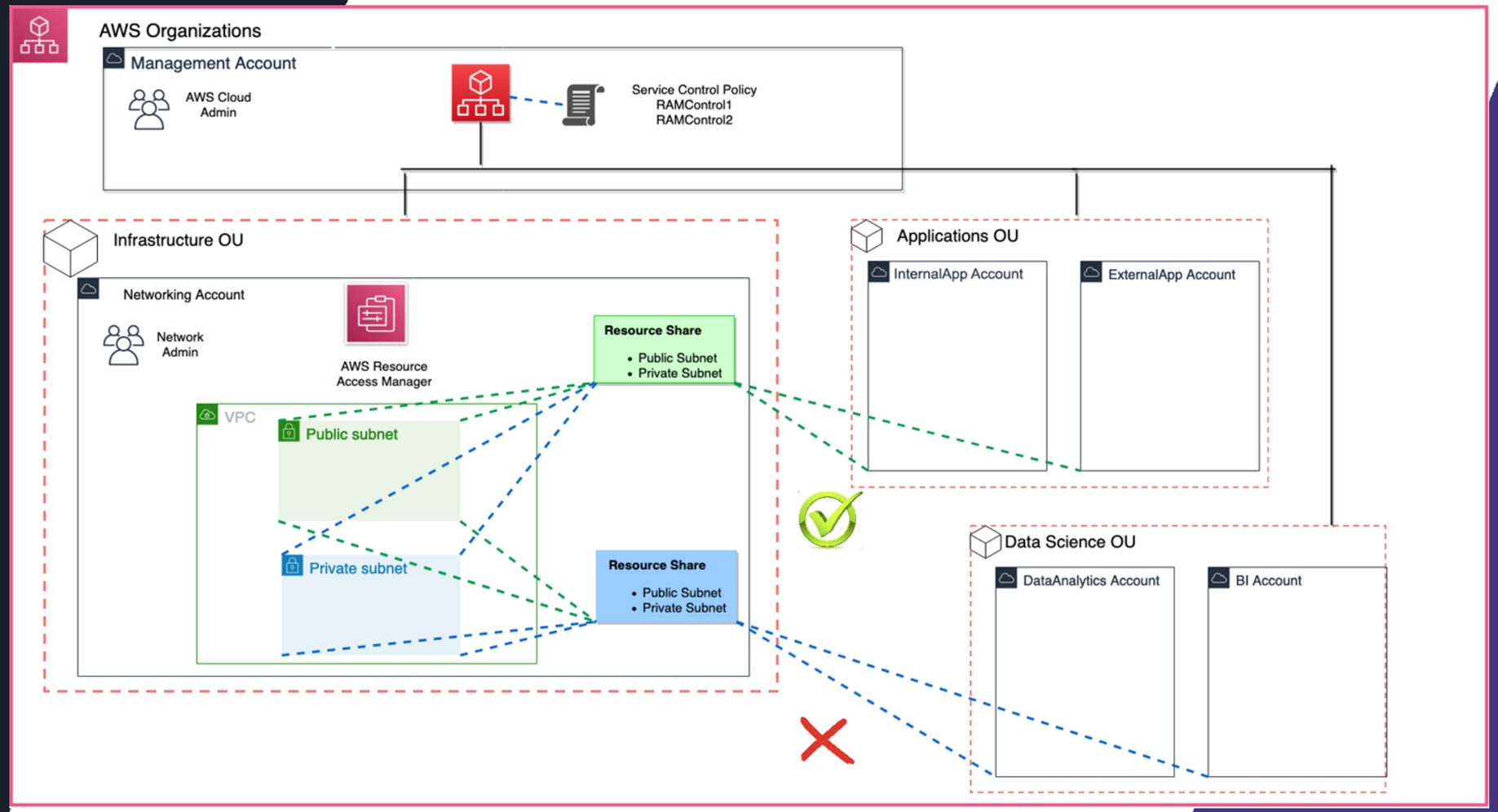


Private Subnet-A Route Table	
Destination	Target
172.16.0.0/16	Local
0.0.0.0/0	Nat-gw-4567

Private Subnet-B Route Table	
Destination	Target
172.16.0.0/16	Local
0.0.0.0/0	Nat-gw-1234

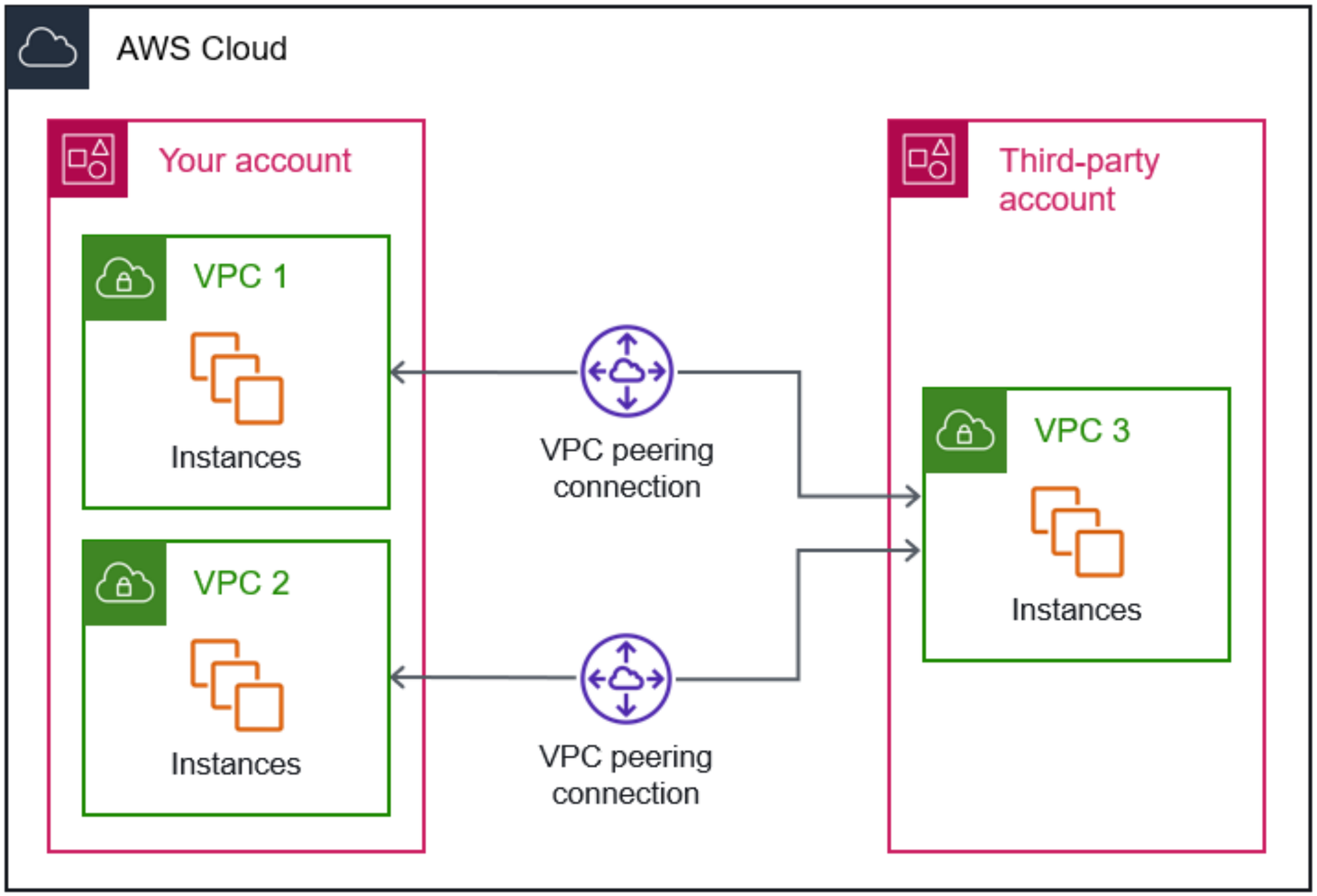
Single VPC / Multi-Account

Multi-Account / Shared VPC

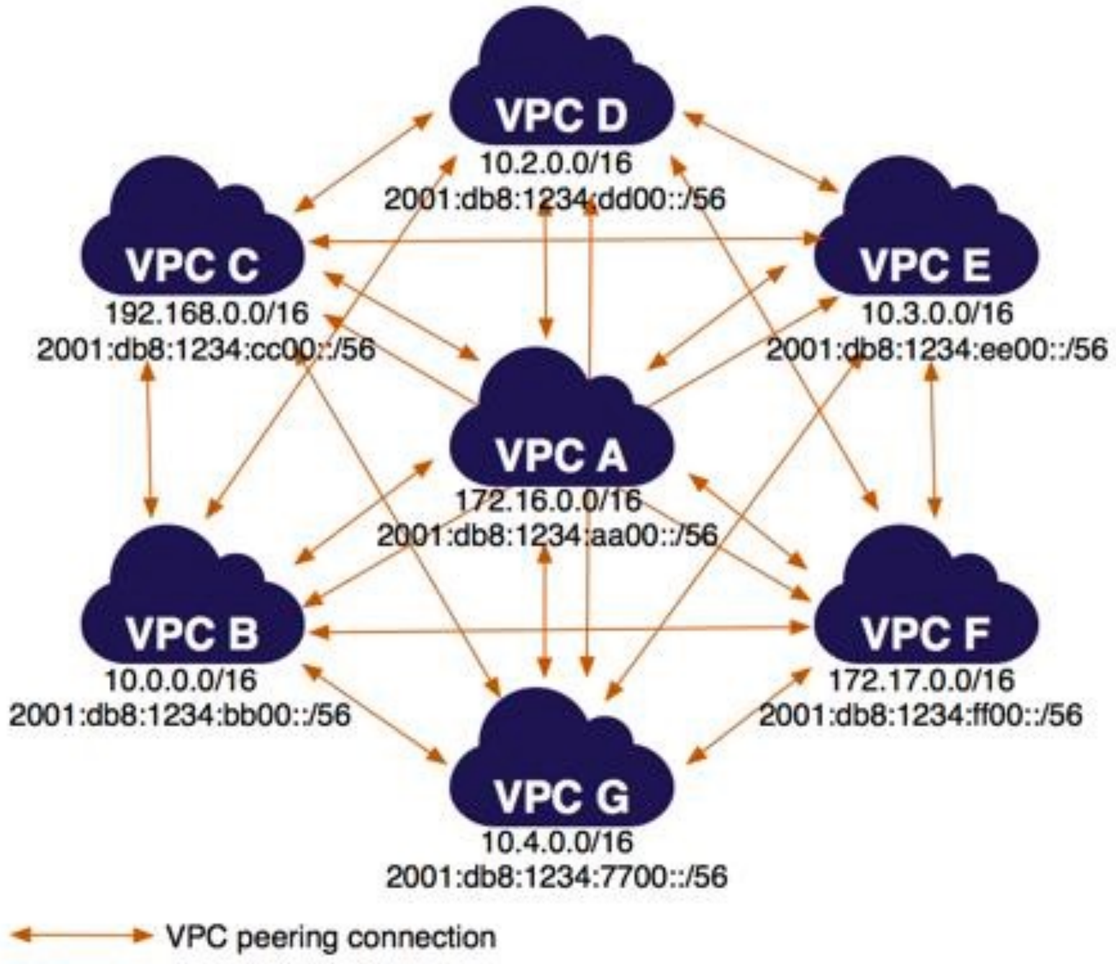


Multi VPC / Multi-Account

VPC Peering

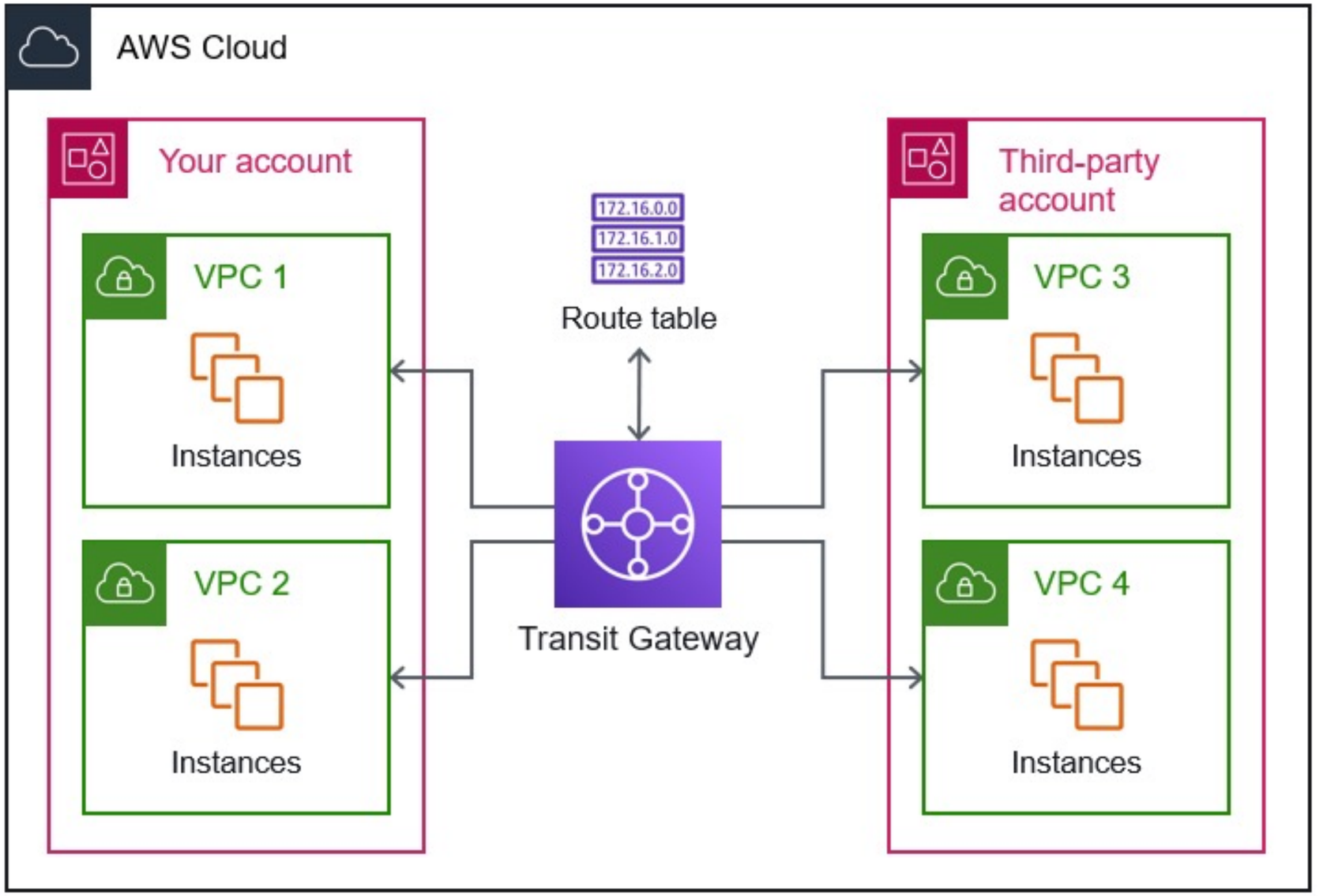

AWS Cloud
Your account
VPC 1
Instances
VPC 2
Instances
VPC peering connection
VPC peering connection
Third-party account
VPC 3
Instances

VPC Peering



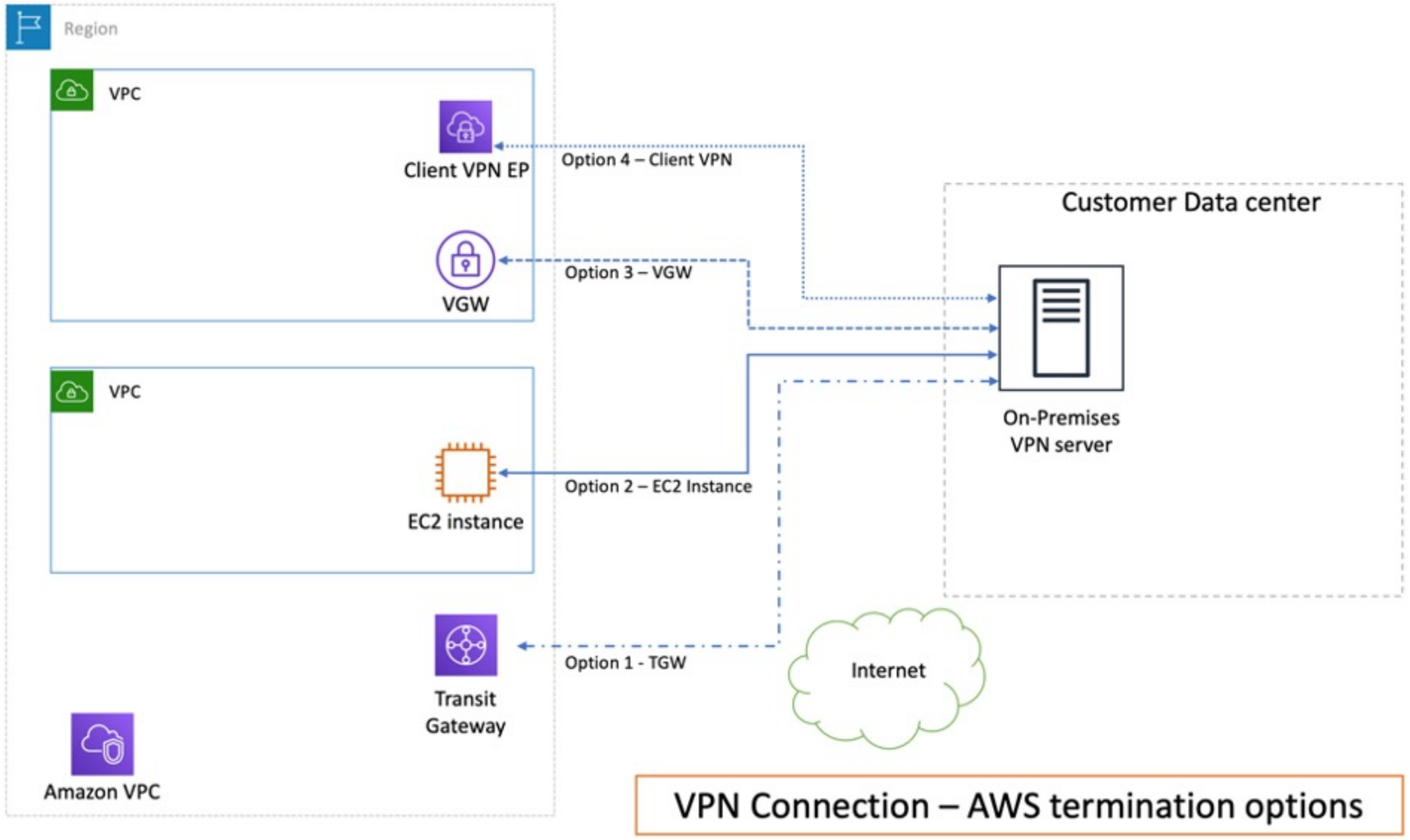
- Good for one-to-one or one-to-two
- One-to-many is achievable but it’s hard to manage when the number of VPC grows
- Many to many is hard to achieve as peering is not transitive

Transit Gateway



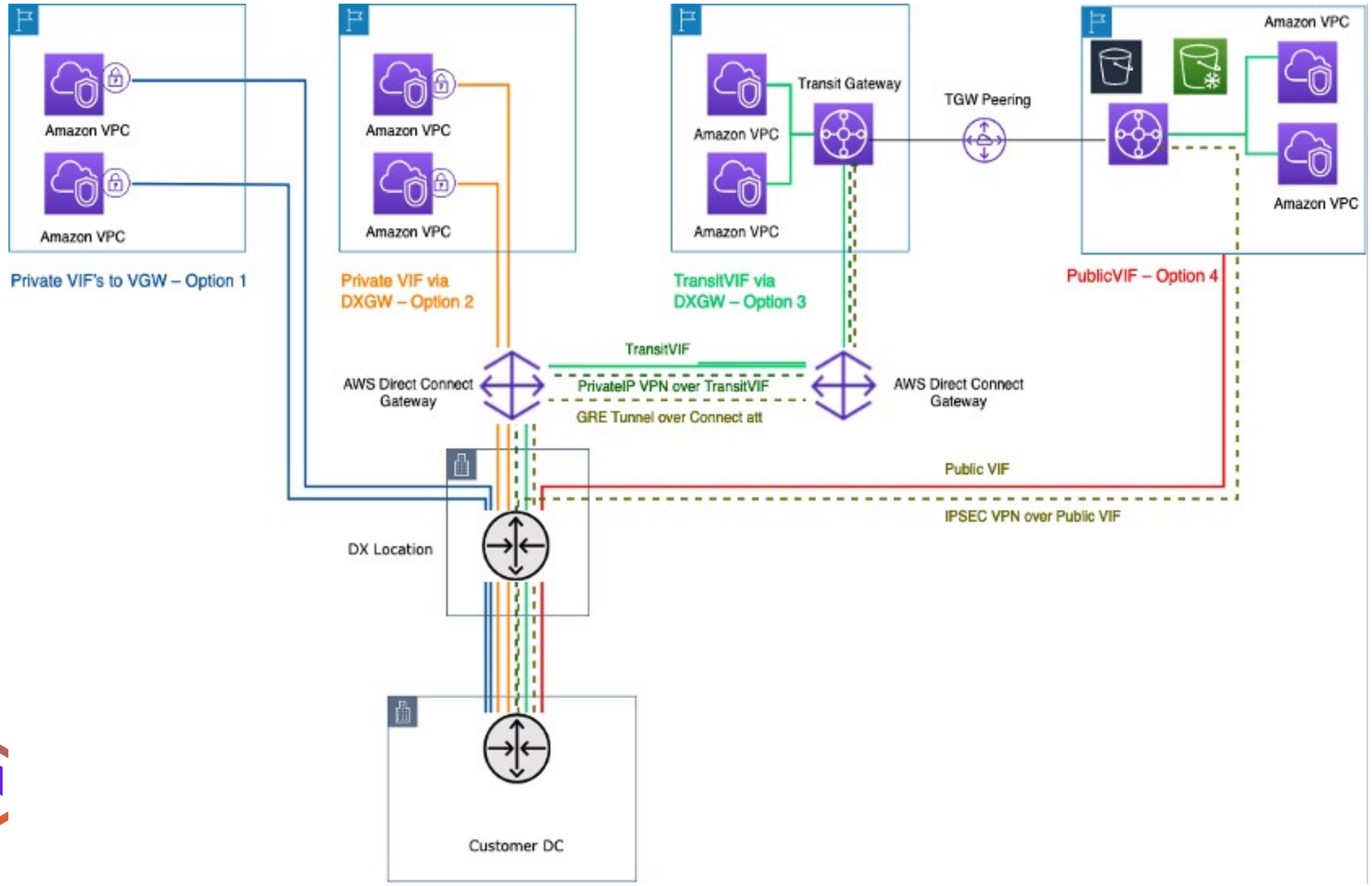
Hybrid Connectivity

Hybrid Connectivity – site-to-site VPN



VPN Connection – AWS termination options

Hybrid Connectivity – Direct Connect



Traffic Inspection

Inbound inspection - AWS WAF

AWS WAF

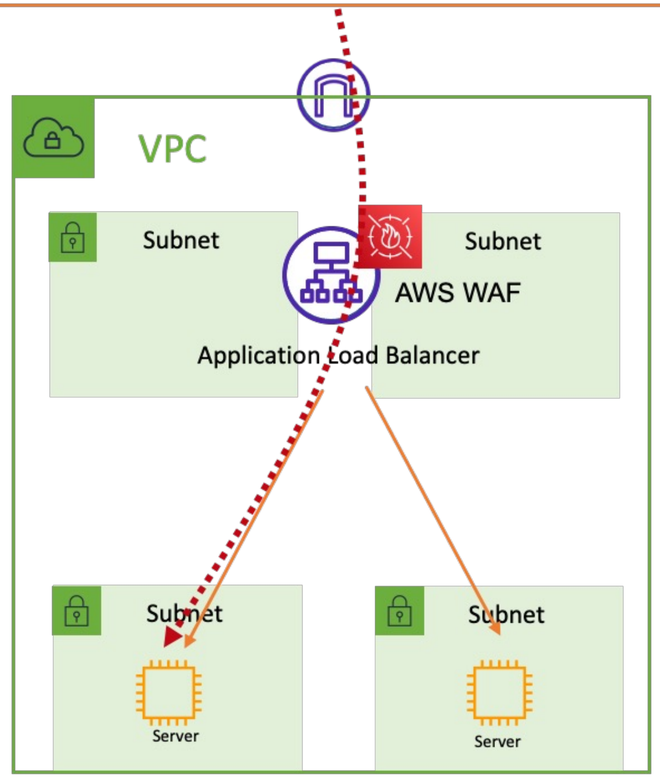
Supported app:
HTTP(S)

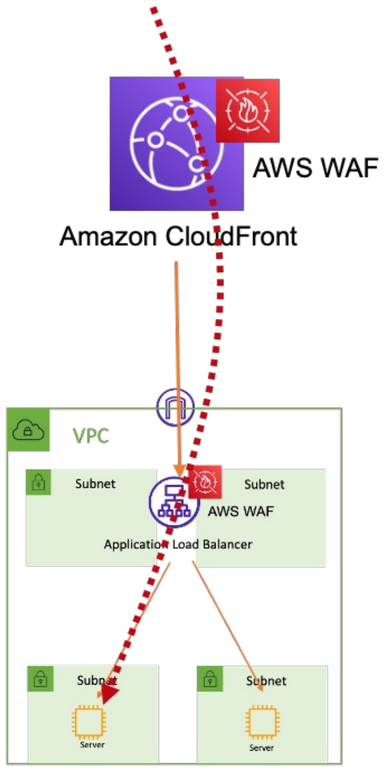
TLS decryption:
True

Inspection depth:
Application layer

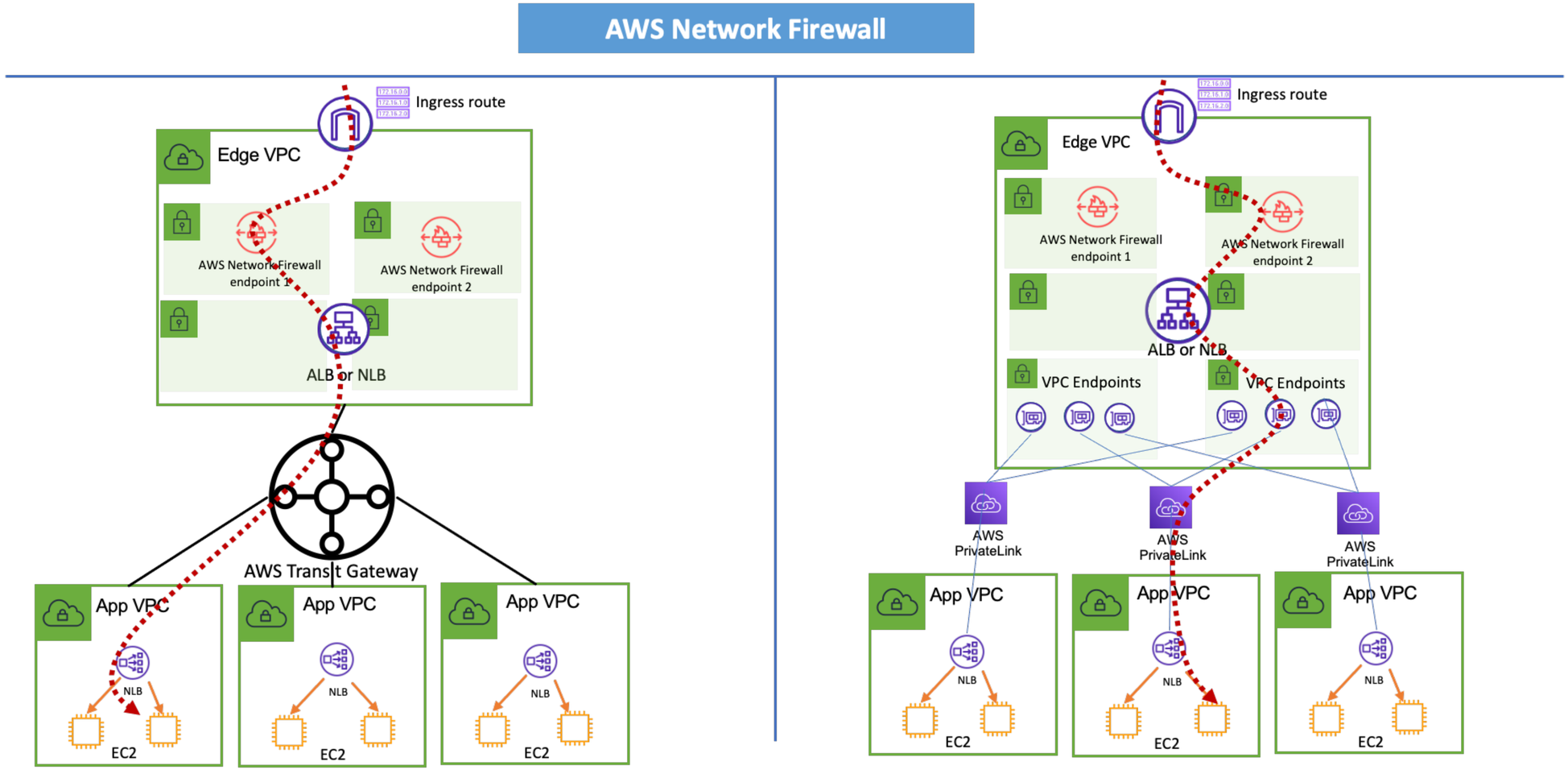
Data plane:
Distributed

Management:
Centralized via FMS

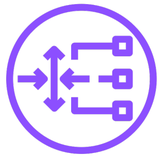




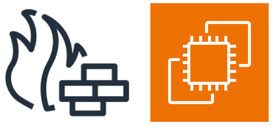
Inbound inspection - AWS Network Firewall



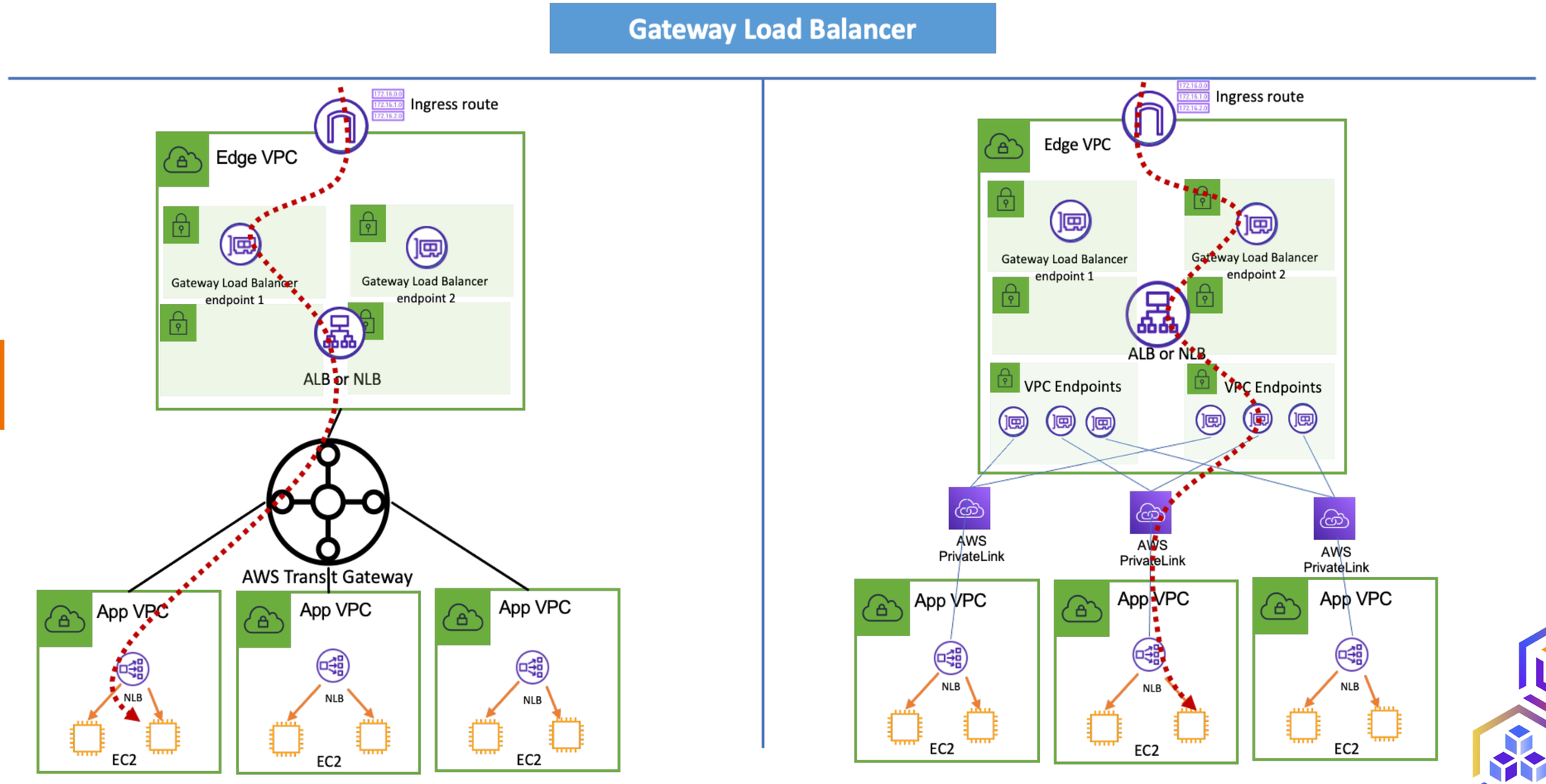
Inbound inspection - AWS GWLB



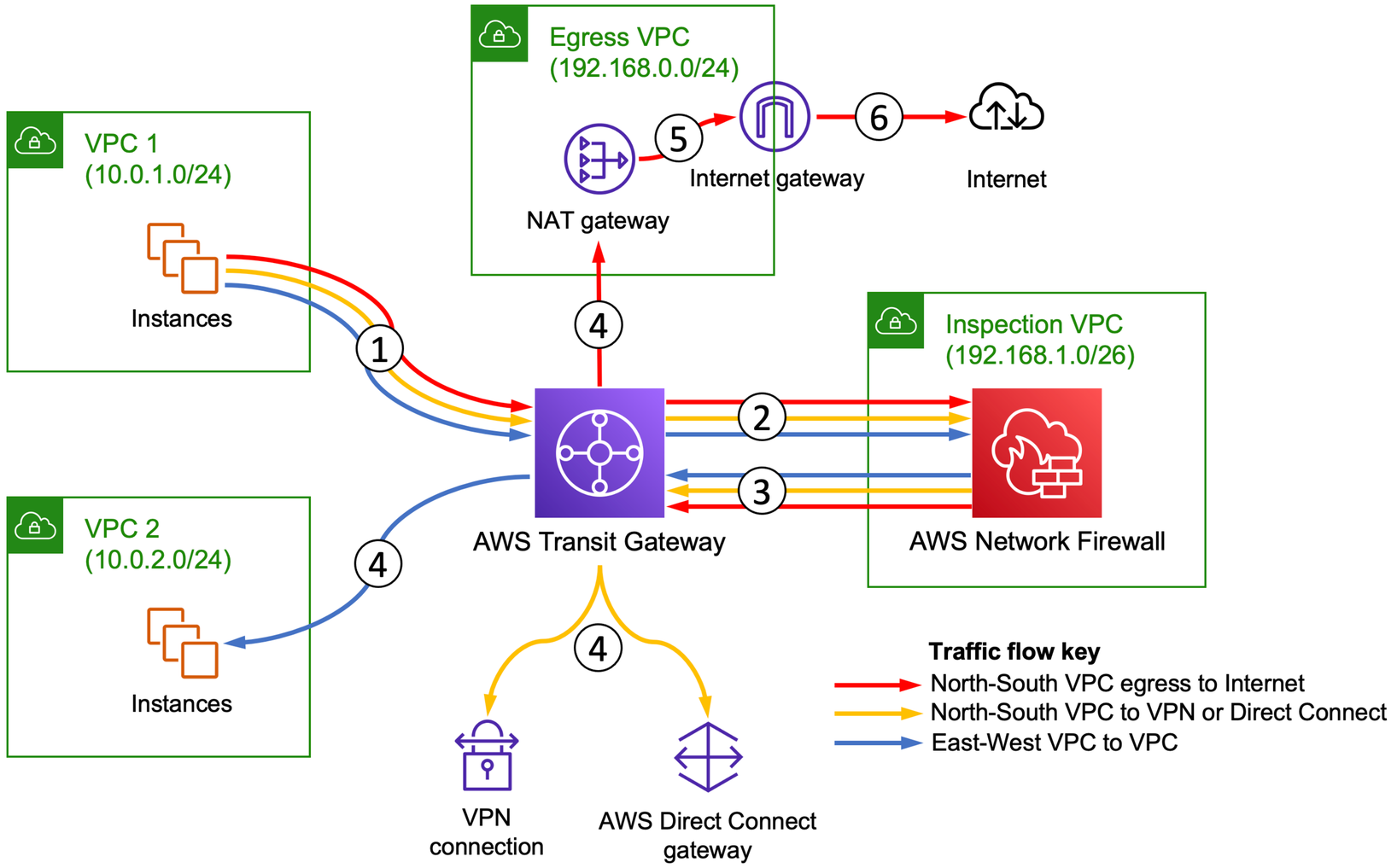
Gateway Load Balancer



Firewall Appliance

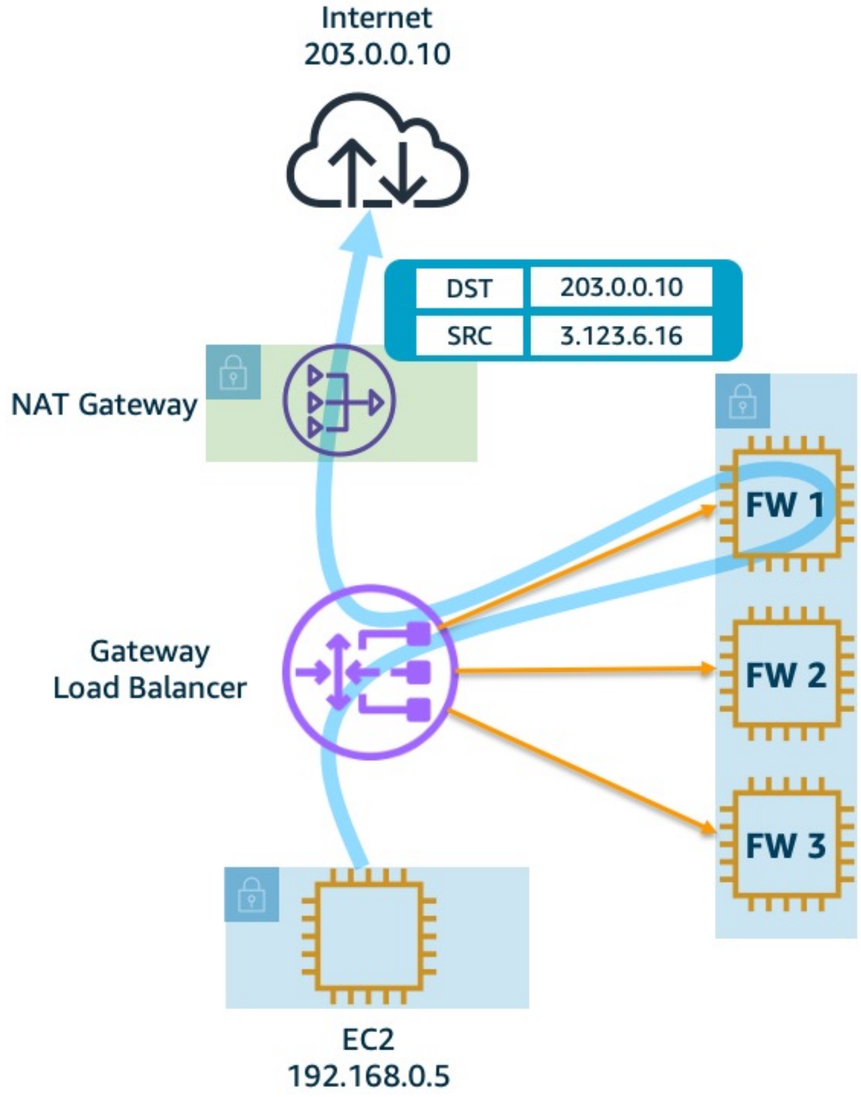


Traffic inspection - AWS Network Firewall

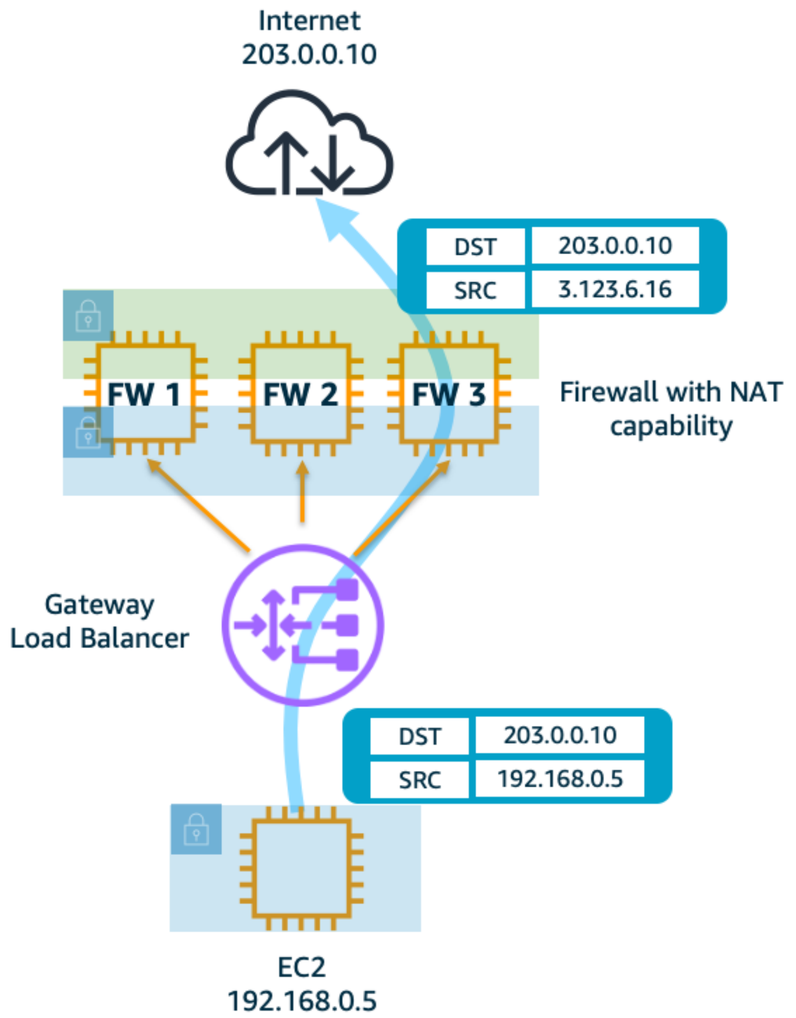


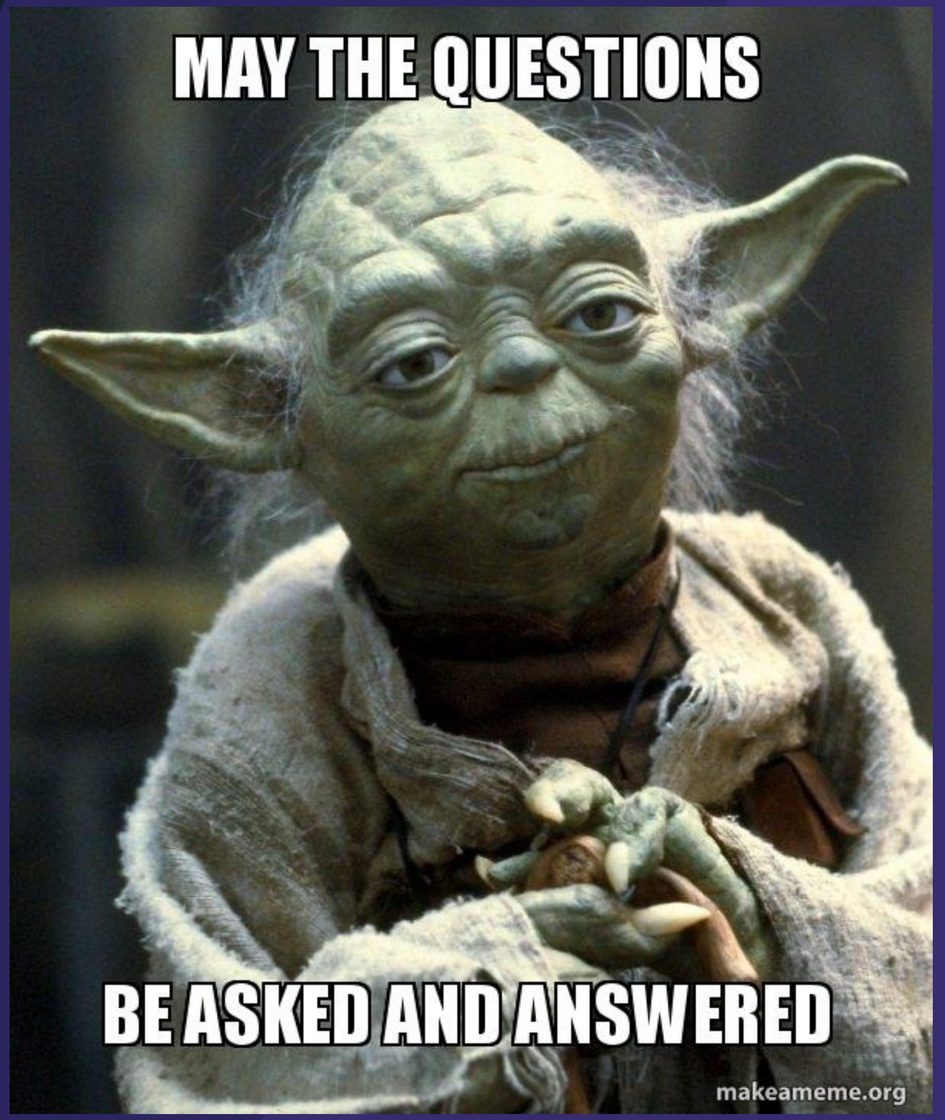
Traffic inspection - GWLB

One-Arm



Two-Arm




MAY THE QUESTIONS
BE ASKED AND ANSWERED
makeameme.org

Thank You

Where to find me:

- https://nickonaws.bunev.net
- https://twitter.com/just4nick
- https://www.linkedin.com/in/nbunev/

References

- https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/welcome.html
- https://docs.aws.amazon.com/prescriptive-guidance/latest/integrate-third-party-services/welcome.html
- https://aws.amazon.com/blogs/architecture/one-to-many-evolving-vpc-design/
- https://aws.amazon.com/blogs/architecture/field-notes-how-to-scale-your-networks-on-amazon-web-services/
- https://aws.amazon.com/blogs/networking-and-content-delivery/design-your-firewall-deployment-for-internet-ingress-traffic-flows/