VPC Lattice – Smarter Alternative to Transit Gateway and VPC Peering

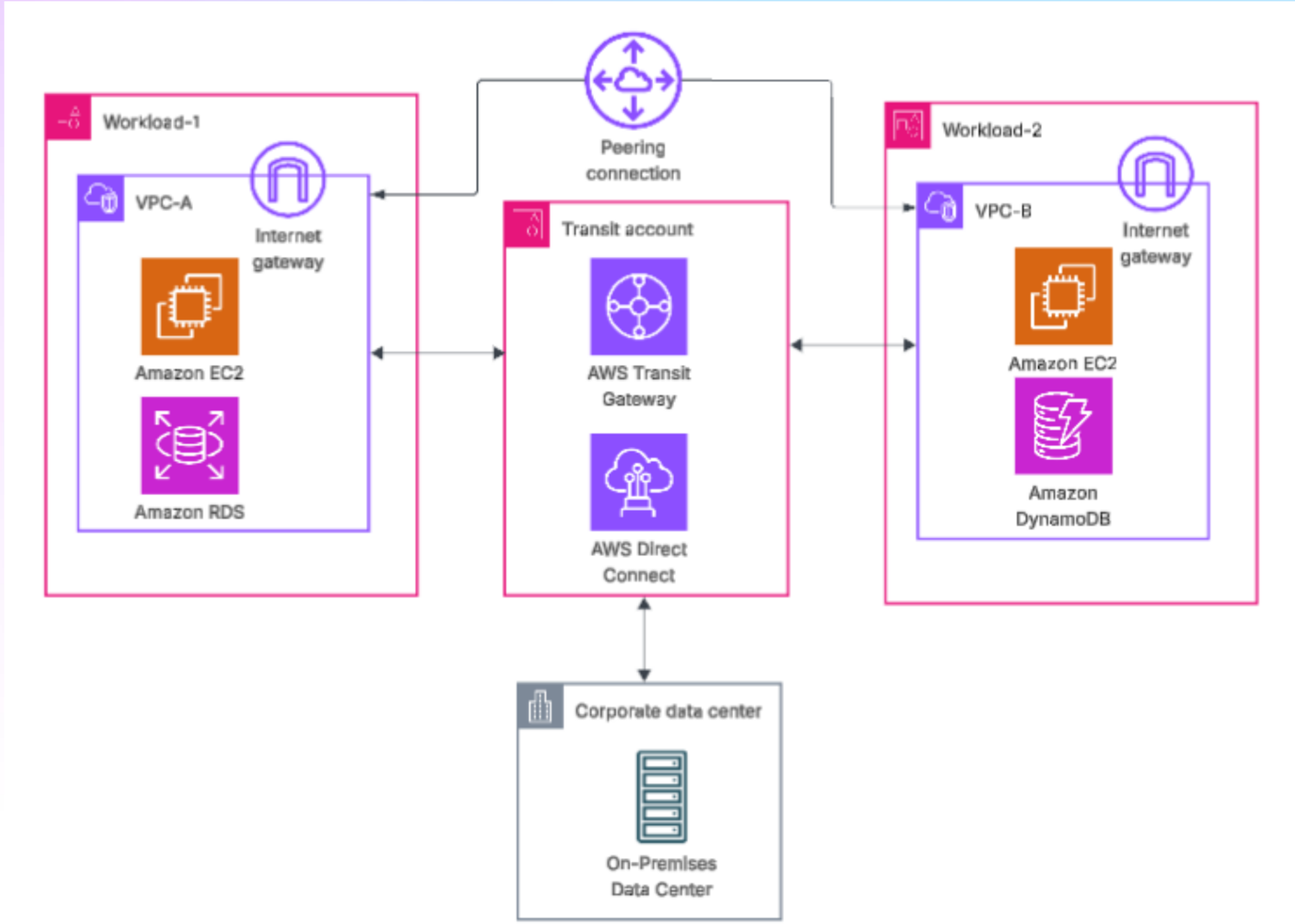
Srinivasan
Cloud Architect - PwC

Overview:

- Networking Foundation
- Network Segmentation
- VPC Lattice – Composition
- Use case – Demo
- Governance
- Switching over to VPC Lattice
- VPC Lattice Pricing
- Key Takeaways
- Q & A

Networking Foundation:

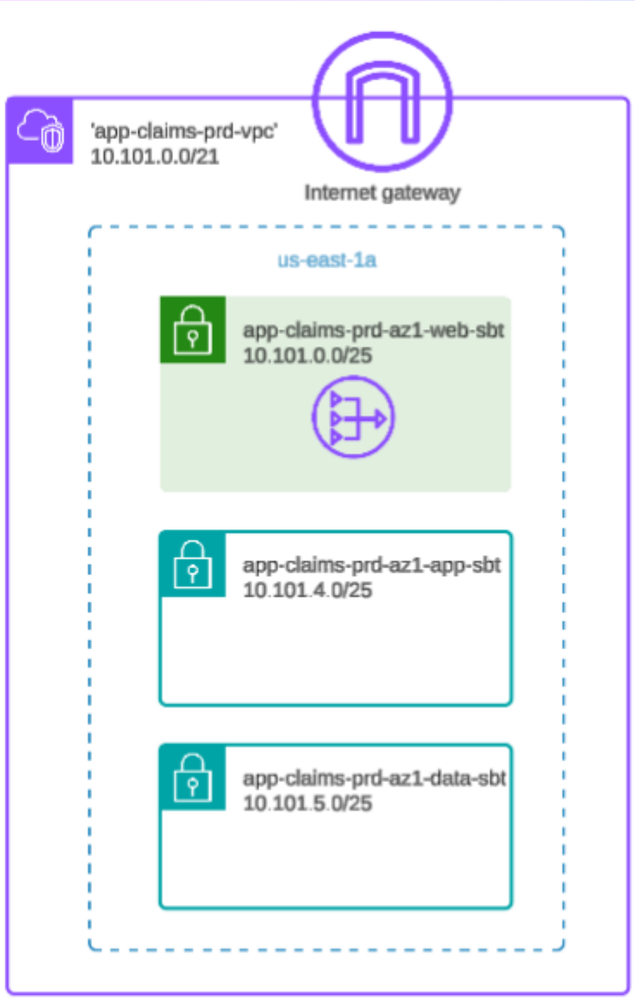
- **Account:** Logical boundary within AWS
- **VPC:** Isolated environment to host workloads
- **Internet Gateway:** Connects VPC to internet
- **VPC Peering:** Connect 2 VPC’s privately
- **Transit Gateway:** Network router that interconnects VPCs, On-premises networks
- **Direct Connect:** low-latency connection between AWS and on-premise network



Network Segmentation

- **Subnets:** Smaller segments within VPC CIDR range
- **Route table:** Defines network path for the given subnet
- **NAT Gateway:** Provides internet access to private subnet resources
- **NACLs:** Stateless; Controls traffic at subnet level
- **Security groups:** Stateful; controls traffic at ENI level

SG's is the only protection layer



Route table: rtb-0b3ad334820bea6a9 / app-claims-prd-vpc-rtb-public

Routes (4)

Filter routes

Destination	Target
10.101.0.0/21	local
0.0.0.0/0	igw-0c968b909ef46bc62

Route table: rtb-007188a1920bb3704 / app-claims-prd-vpc-rtb-private1-us-east-1a

Routes (5)

Filter routes

Destination	Target
10.101.0.0/21	local
0.0.0.0/0	nat-08f84c12988d7b05a
pl-63a5400a	vpce-01011f0b6ef8940fa

acl-0a58cfa0ea668d300

Details | Inbound rules | Outbound rules | Subnet associations | Tags

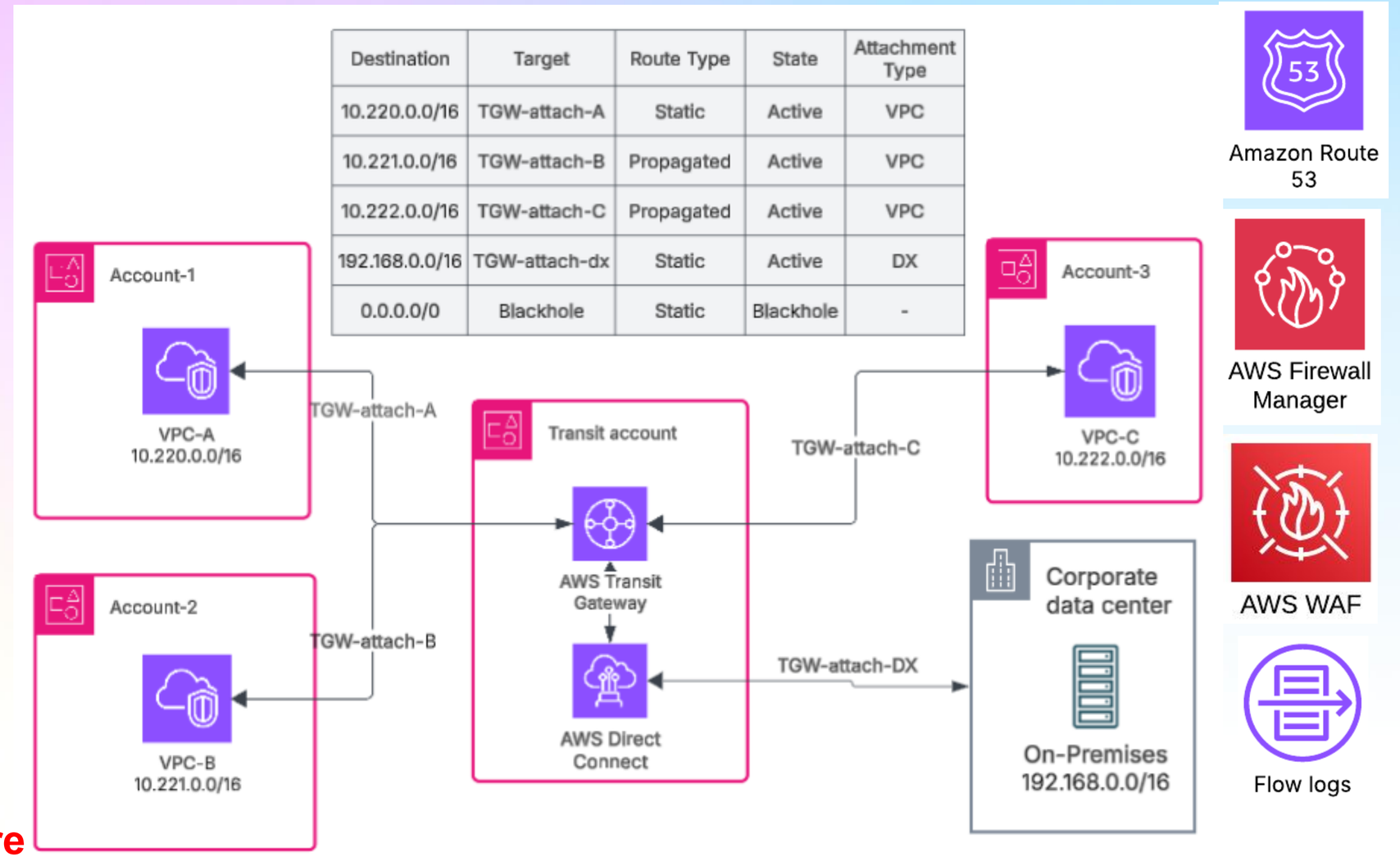
Inbound rules (2)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

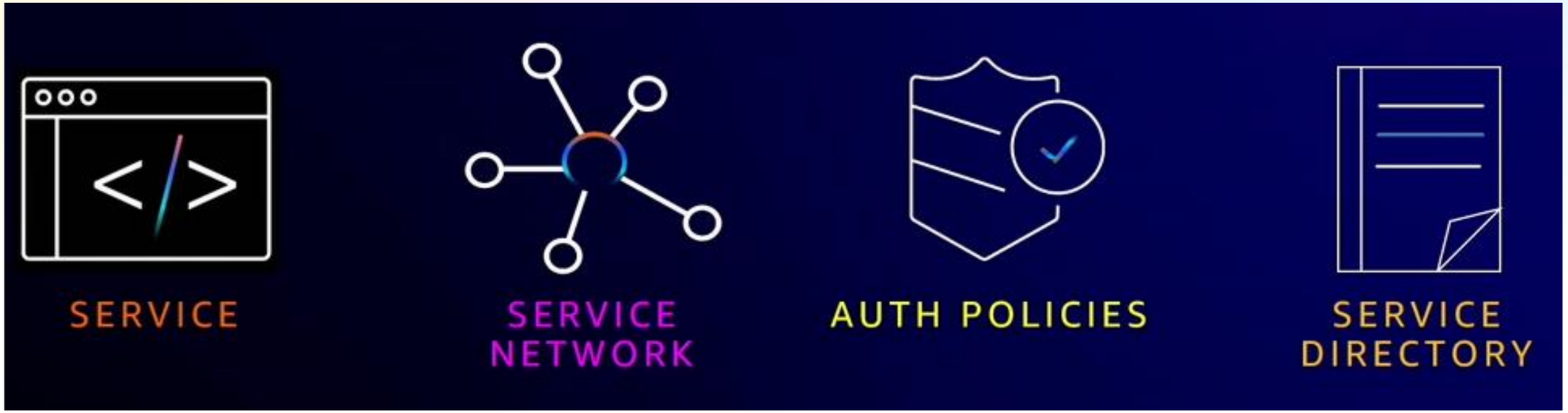
Network Segmentation(At-Scale)

- **TGW RT:** Enables segmented routing between VPC's, DC
- **Route 53:** DNS resolution for associated VPC's
- **Firewall Manager:** Traffic Inspection of Egress/Ingress
- **WAF:** Protective shield for web applications from common attacks
- **Flow-logs:** Captures detailed information at VPC & ENI level
- **Overheads in maintenance of TGW RT entries to limit exposure**



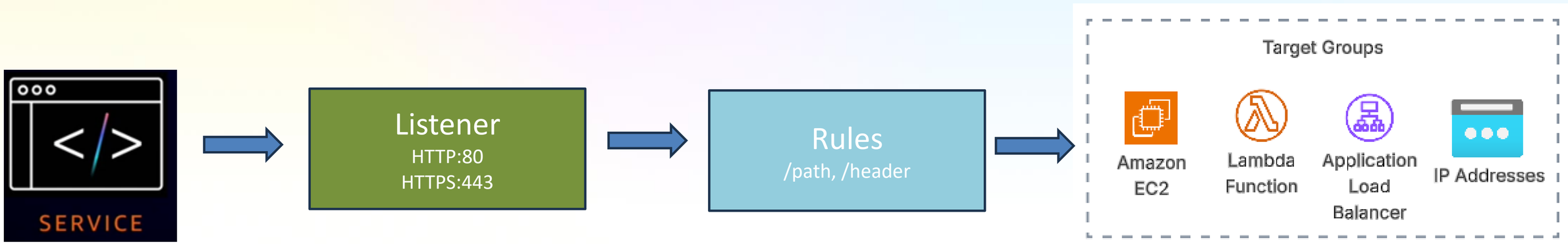
What is VPC Lattice?

- Managed Application layer networking service
- Simplified Networking and connectivity
- Leverages Zero Trust Network Architecture principles



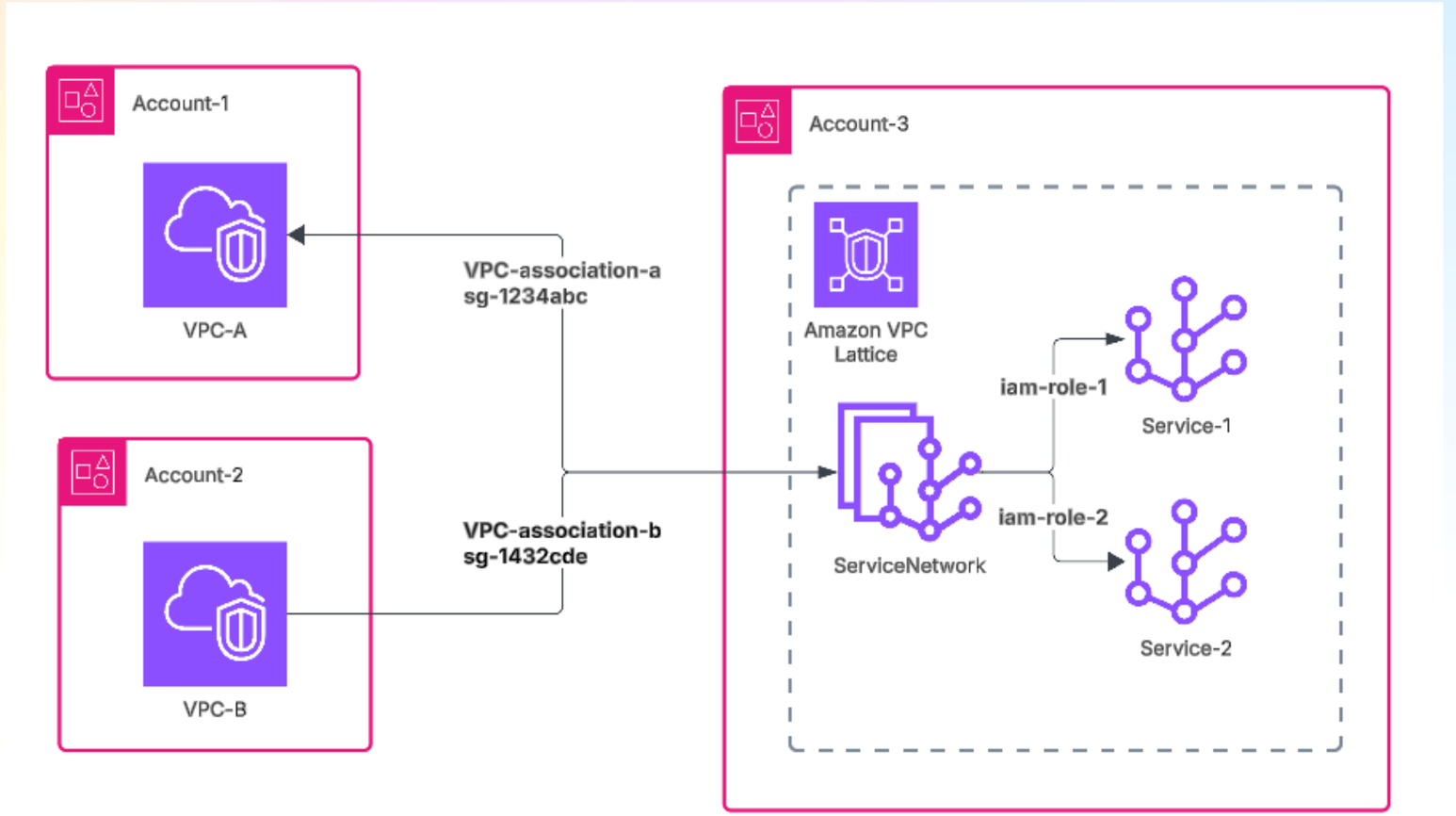
VPC Lattice Service:

- Logical abstraction in front of your application
- Workloads shall be hosted on instances, containers and serverless.
- Consists of listeners, rules and target groups



Service Network:

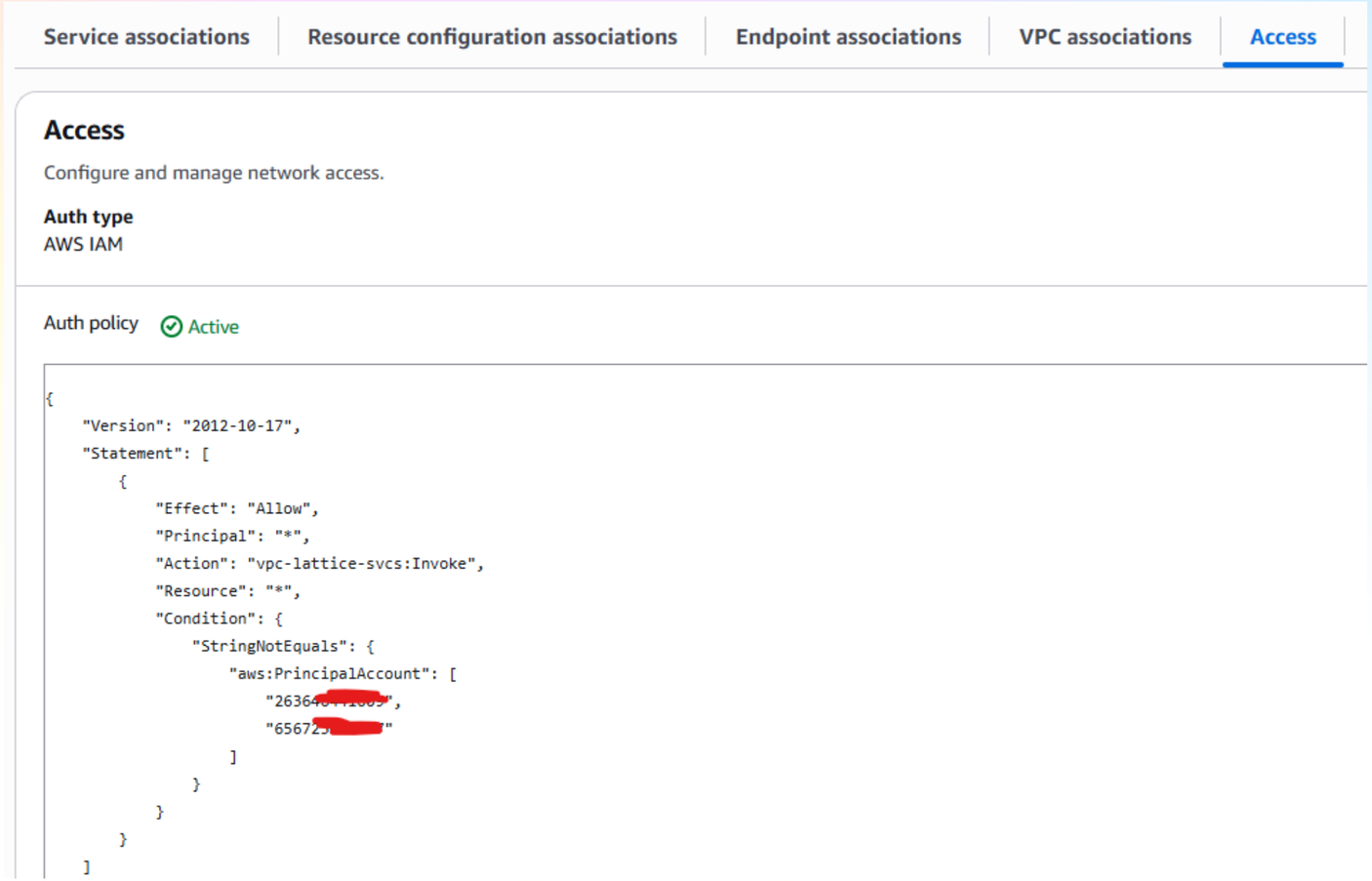
- Enables connectivity and common authorization controls to collection of Services
- Share service network with Resource Access Manager(RAM)



AWS Resource Access Manager

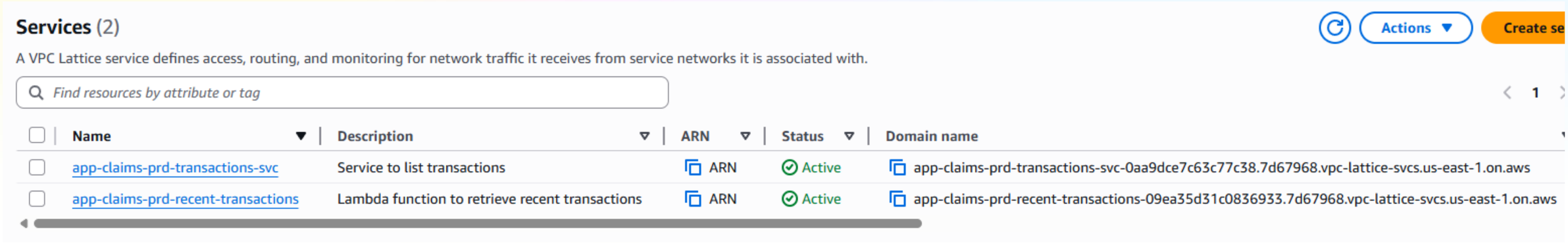
Auth Policies:

- **IAM resource policies can be associated with Service Network and Individual services to support request level authentication and context specific authorization**



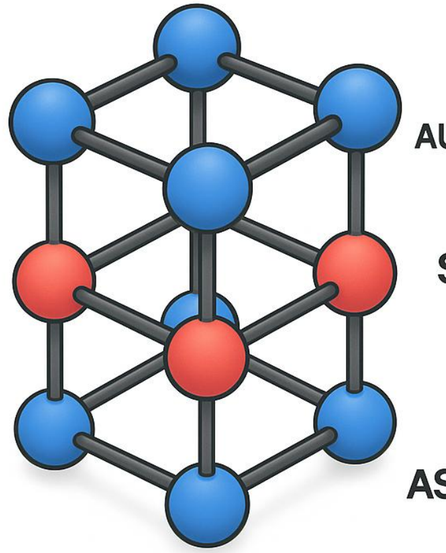
Service Discovery:

- Centralized view of the services that you own or that have been shared with you through AWS Resource Access Manager(RAM)
- Every service is assigned a unique Fully Qualified Domain Name (FQDN) generated by VPC Lattice
- Custom Domain name with PHZ in Route53 is supported



Layered Network Security:

- Routing handled by prefix lists
- Network defense in multiple layers
- ZTNA : Never Trust, Always verify
- VPC Lattice is fully TLS encrypted



rtb-007188a1920bb3704 / app-claims-prd-vpc-rtb-private1-us-east-1a

Details | Routes | Subnet associations | Edge associations | Route propagation

Routes (5)

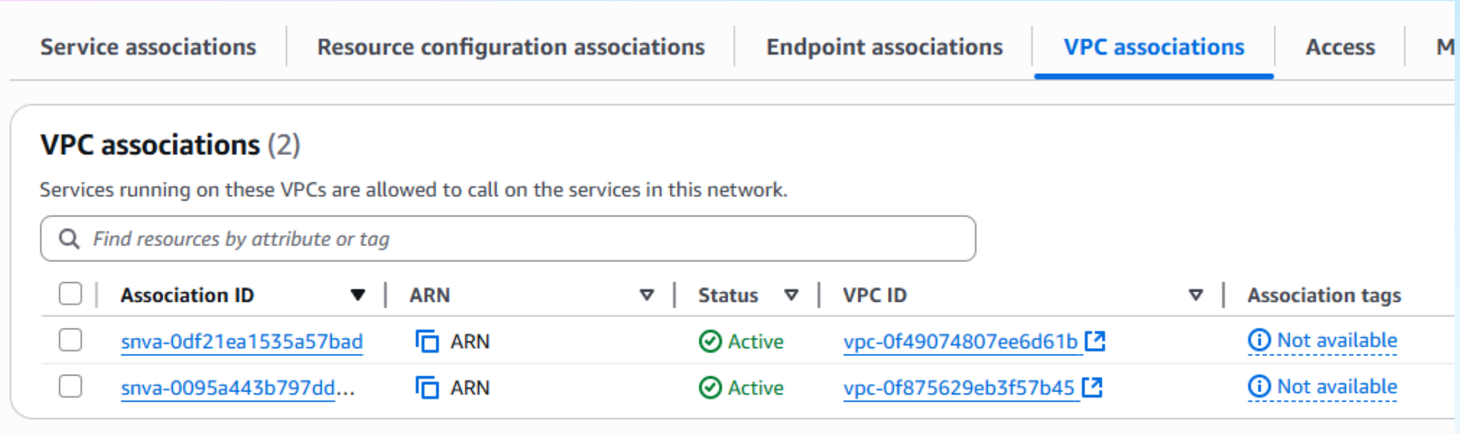
Filter routes

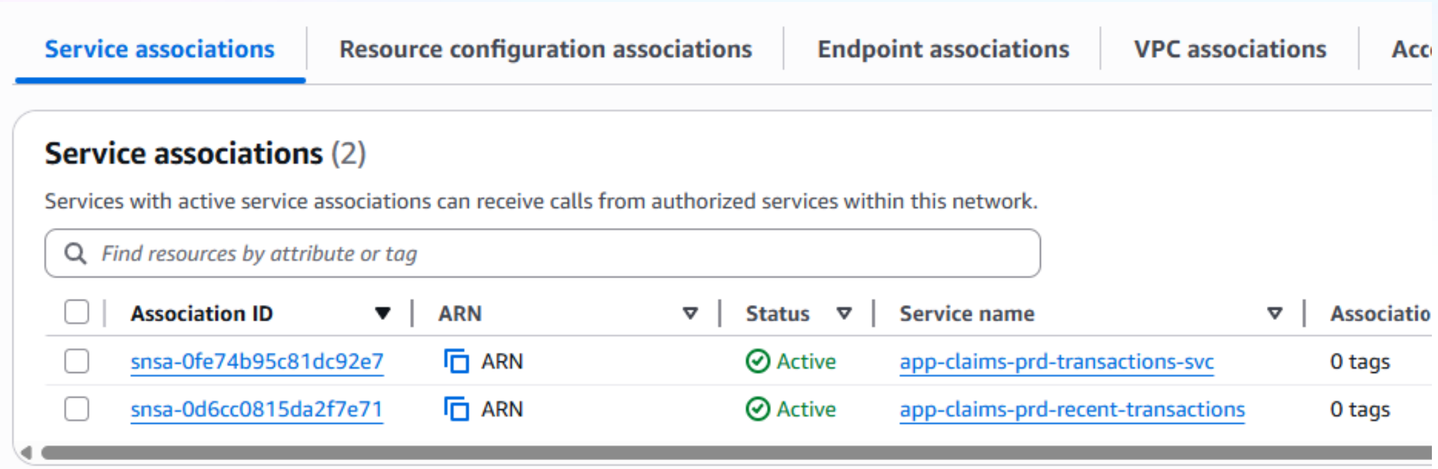
Destination	Target	Status
fd00:ec2:80::/64	VpcLattice	Active
169.254.171.0/24	VpcLattice	Active

Demo

Governance:

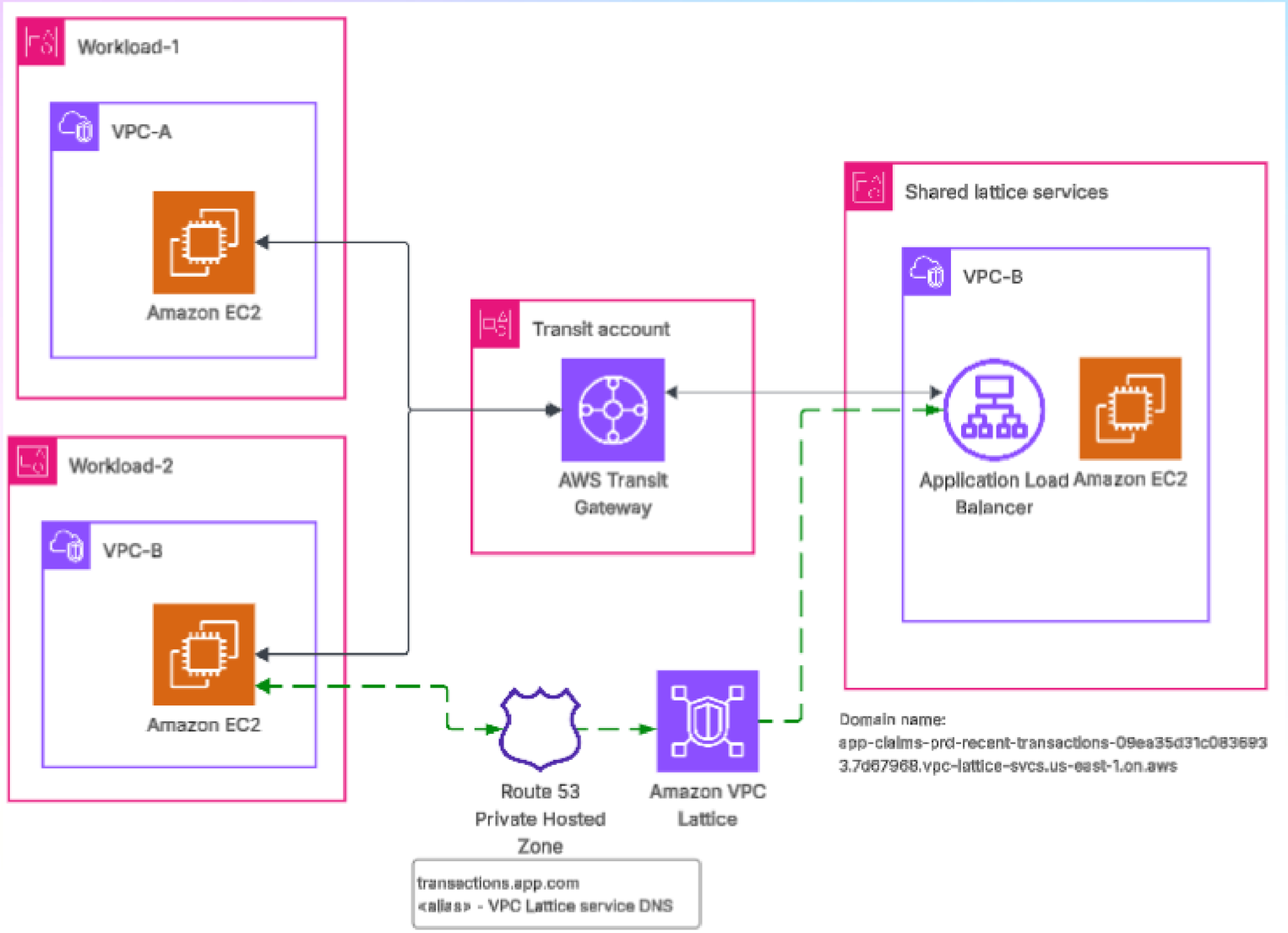
1. Network Administrators:
    - Create Service Networks
    - Define access controls
    - VPC Associations
2. Developers/Application team:
    - Create services
    - Defines traffic-management and authorization
    - Associate services to service networks





Switching over to VPC Lattice:

1. Setup Target group to expose selected workload as VPC Lattice service to obtain DNS name
2. Setup Service Network and VPC association
3. In R53 Private Hosted Zone, add a ‘Alias’ record to the above DNS name



Pricing:

1. **Transit Gateway:**
   - Transit Gateway attachment (~ $0.05 per attachment)
   - Data processing charges per attachment (~ $0.02/GB of data processed)

2. **VPC Lattice:**
   - Number of services provisioned (~ $0.025/hour per service)
   - Data processing charges per each service (~ $0.025/GB of data processed)
   - Number of requests ($0.10 per 1 million requests/connections)

Outliers:

1. VPC association is free
2. Multiple path behind a DNS name → still counted as one service

Key Takeaways:

1. VPC Lattice is an application layer networking service
2. Expose workloads as a lattice service, get a DNS name
3. Map lattice service into service networks as per the requirements
4. VPC Lattice is not just dedicated for Microservices
5. Comparing with service-mesh..? Similar, but implemented differently
6. Everything behind is still just IP and Port; Managed Prefix lists

Q & A

THANK YOU FOR ATTENDING!

Linkedin