
aws
COMMUNITY DAY
AOTEAROA

aws
COMMUNITY DAY
AOTEAROA

Amazon VPC Lattice: When to Use It and When to Skip It

John Ajera | **18th Sep 2025**

Platform Engineer

Earth Sciences New Zealand

Session Resources

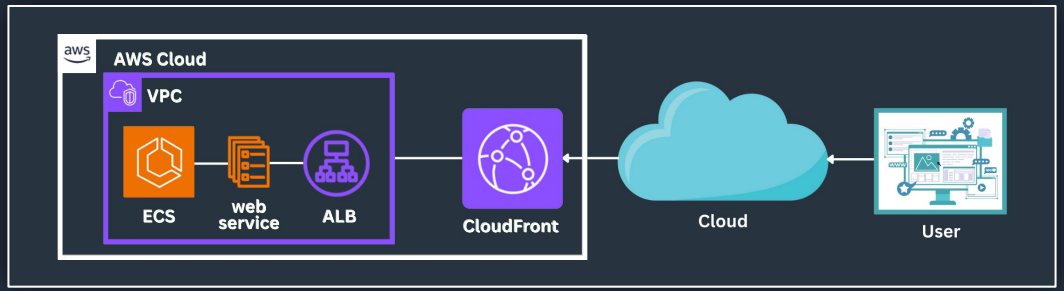
Agenda

- Introduction
- Overview
- How VPC Lattice Works
- When to Use It and When to Skip it
- Demo

Introduction

What is an Amazon VPC?

VPC is the foundational network environment for your AWS resources.



Common Inter VPC Connectivity

VPC Peering

Transit Gateway

PrivateLink

Overview

VPC Lattice Overview

No sidecar proxies required

Fully managed control plane with no proxies to deploy and maintain

Works across all compute options

Amazon EC2, Amazon EKS, Amazon ECS, and AWS Lambda

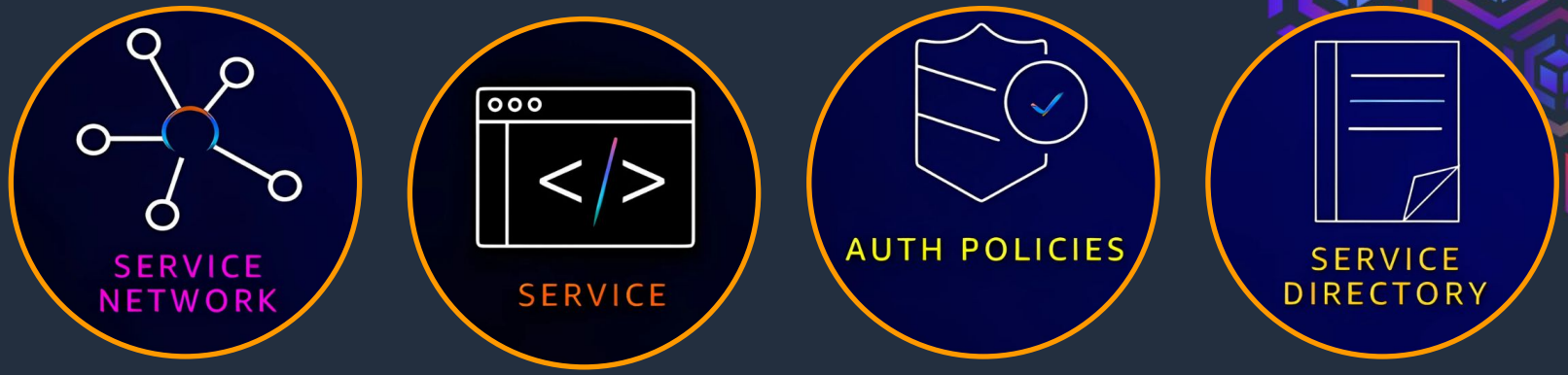
Unified traffic and access controls

Improved security posture and rich traffic controls and segmentation

Integrates with existing network connectivity

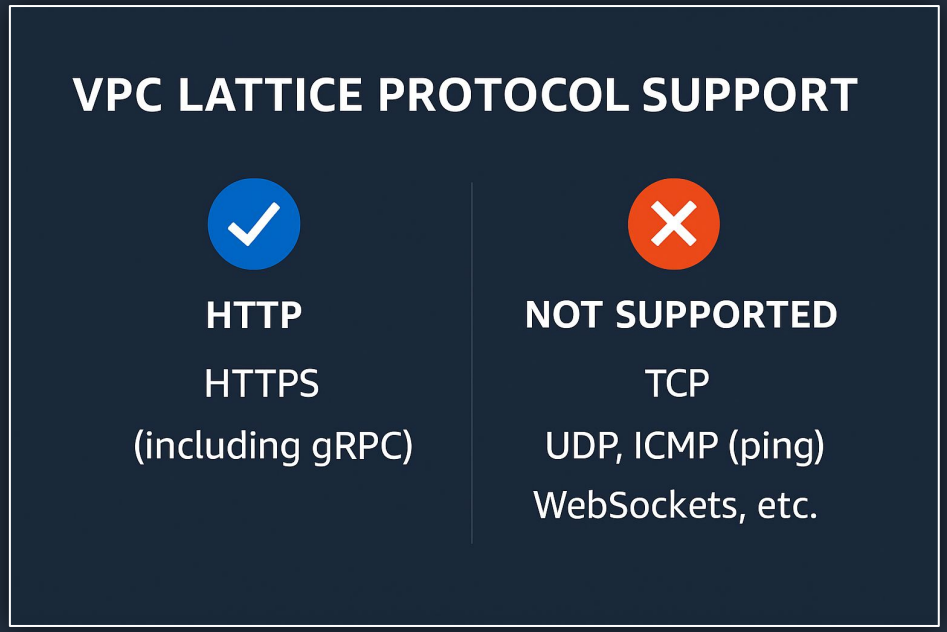
You can choose what services are accessible through VPC Lattice

Four Main Components of VPC Lattice



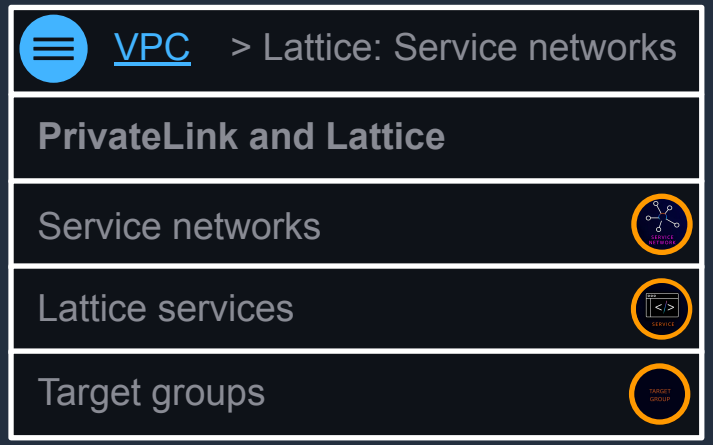
Protocol Support

Amazon VPC Lattice is an application-level (Layer 7) service networking solution.

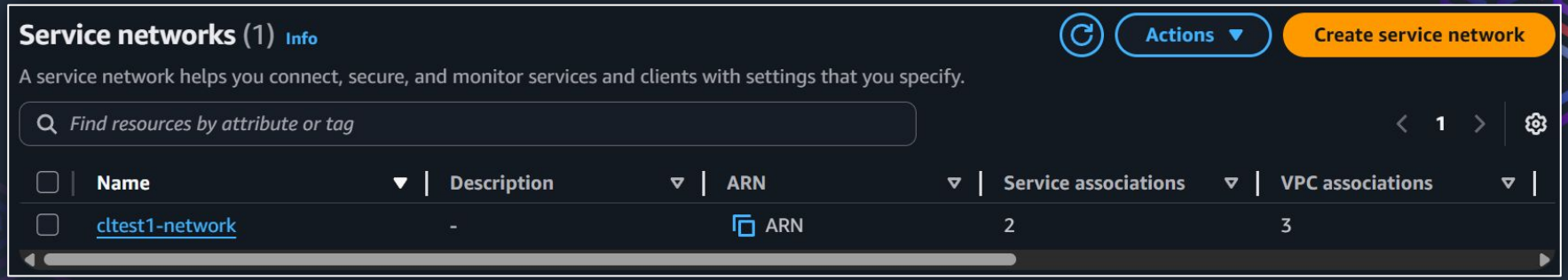


How to Access VPC Lattice

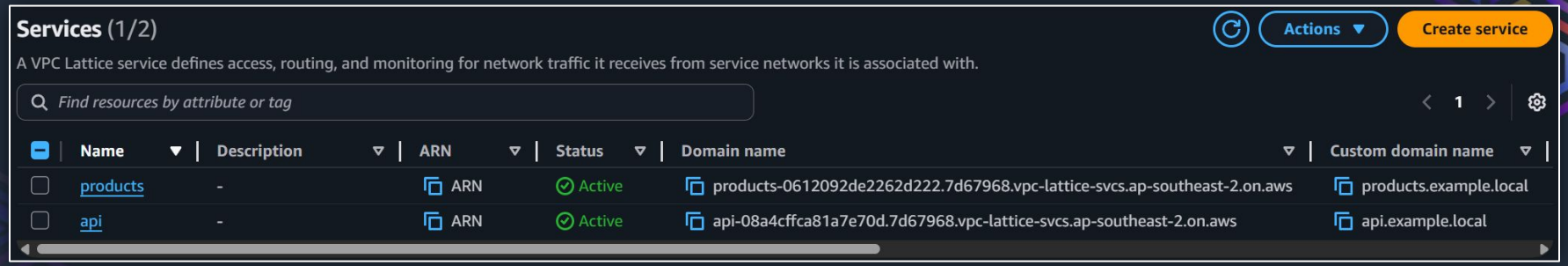
Virtual private cloud (VPC)



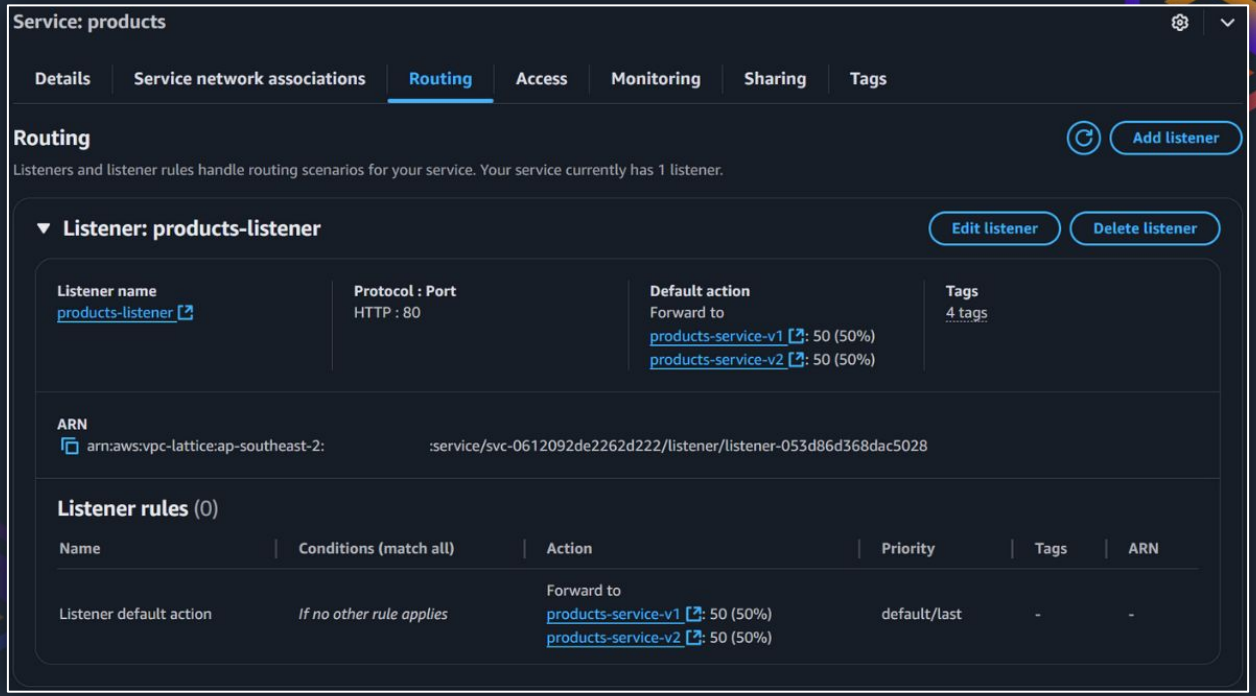
How to Access VPC Lattice – Service Networks



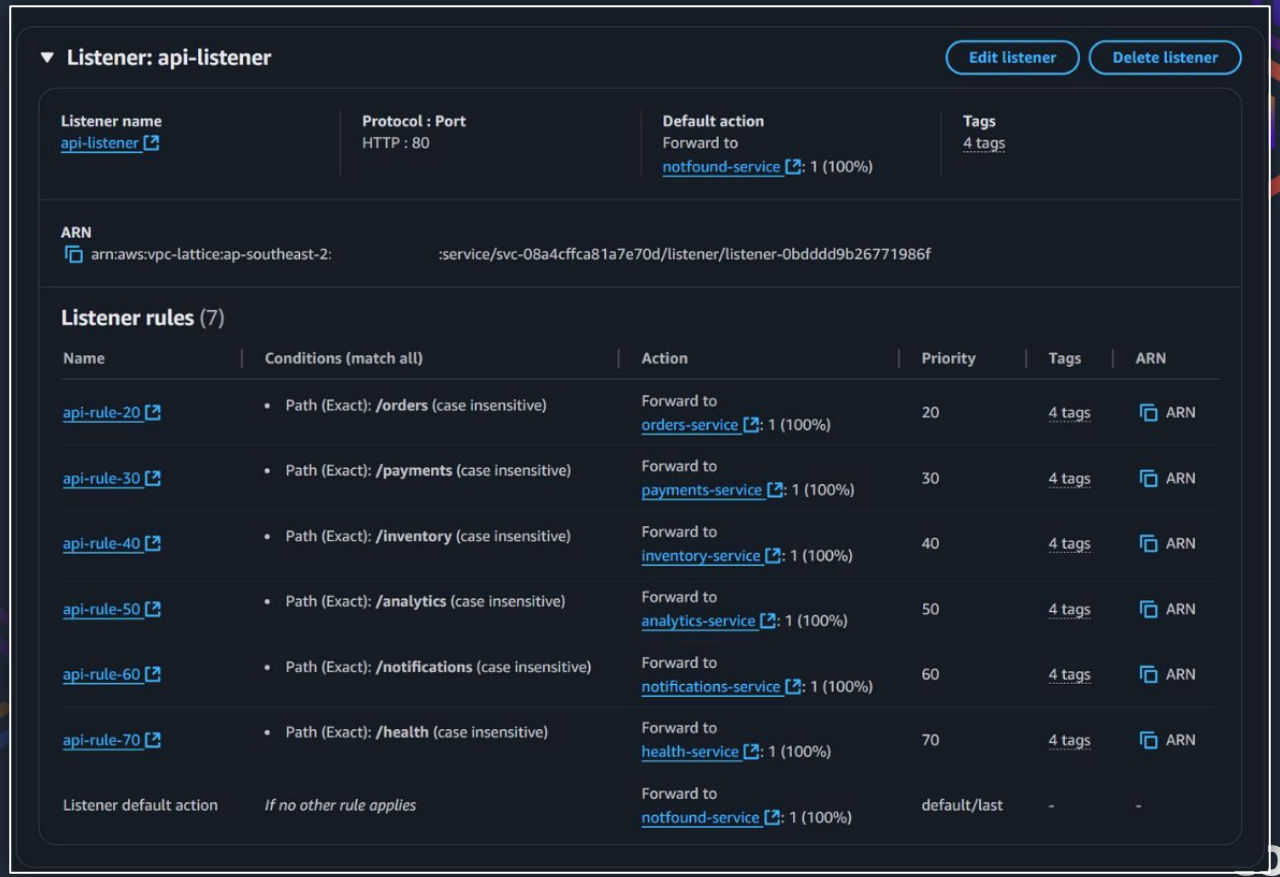
How to Access VPC Lattice – Services



How to Access VPC Lattice – Service Routing



How to Access VPC Lattice – Service Routing



▼ **Listener: api-listener**

Edit listener | Delete listener

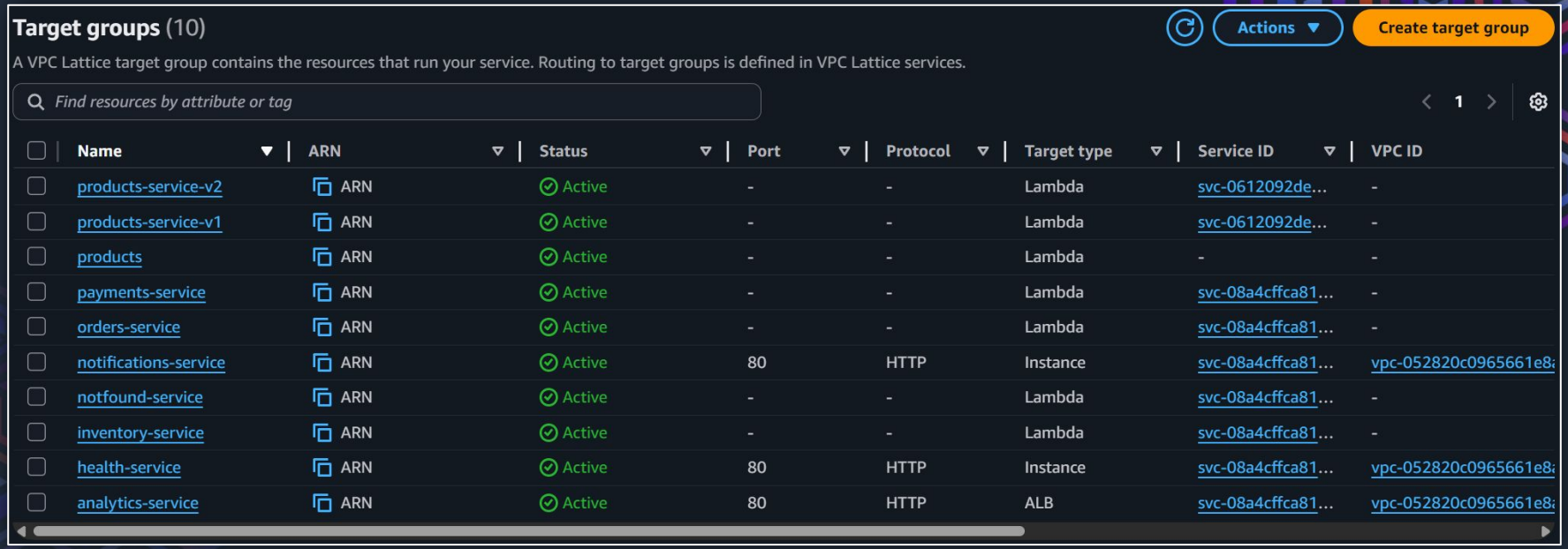
Listener name	Protocol : Port	Default action	Tags
api-listener	HTTP : 80	Forward to notfound-service: 1 (100%)	4 tags

ARN
arn:aws:vpc-lattice:ap-southeast-2: :service/svc-08a4cffca81a7e70d/listener/listener-0bdddd9b26771986f

Listener rules (7)

Name	Conditions (match all)	Action	Priority	Tags	ARN
api-rule-20	• Path (Exact): **/orders** (case insensitive)	Forward to orders-service: 1 (100%)	20	4 tags	ARN
api-rule-30	• Path (Exact): **/payments** (case insensitive)	Forward to payments-service: 1 (100%)	30	4 tags	ARN
api-rule-40	• Path (Exact): **/inventory** (case insensitive)	Forward to inventory-service: 1 (100%)	40	4 tags	ARN
api-rule-50	• Path (Exact): **/analytics** (case insensitive)	Forward to analytics-service: 1 (100%)	50	4 tags	ARN
api-rule-60	• Path (Exact): **/notifications** (case insensitive)	Forward to notifications-service: 1 (100%)	60	4 tags	ARN
api-rule-70	• Path (Exact): **/health** (case insensitive)	Forward to health-service: 1 (100%)	70	4 tags	ARN
Listener default action	*If no other rule applies*	Forward to notfound-service: 1 (100%)	default/last	-	-

How to Access VPC Lattice – Target Groups



Target groups (10)

Actions ▼ | Create target group

A VPC Lattice target group contains the resources that run your service. Routing to target groups is defined in VPC Lattice services.

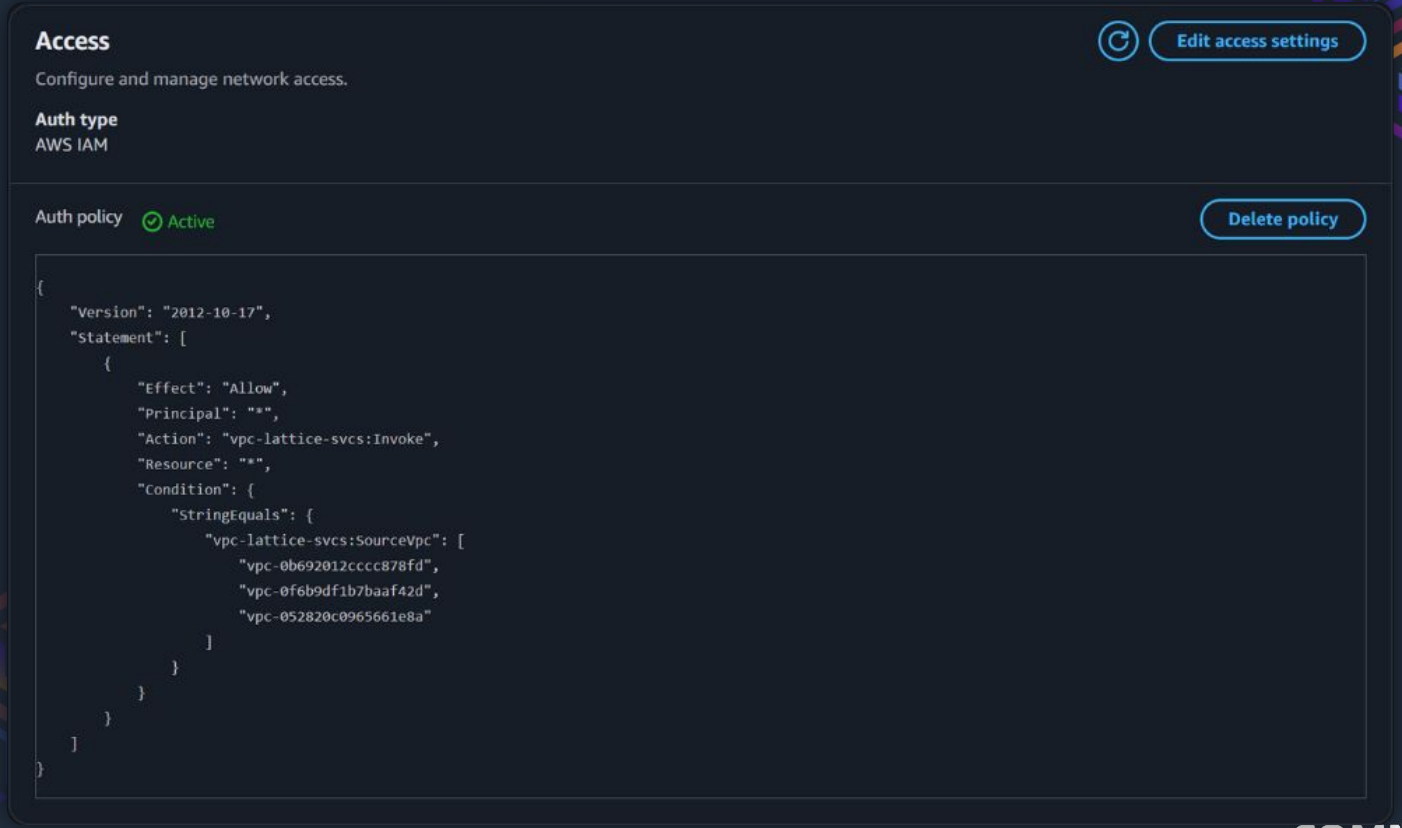
Find resources by attribute or tag

< 1 >

Name	ARN	Status	Port	Protocol	Target type	Service ID	VPC ID
products-service-v2	ARN	Active	-	-	Lambda	svc-0612092de...	-
products-service-v1	ARN	Active	-	-	Lambda	svc-0612092de...	-
products	ARN	Active	-	-	Lambda	-	-
payments-service	ARN	Active	-	-	Lambda	svc-08a4cffca81...	-
orders-service	ARN	Active	-	-	Lambda	svc-08a4cffca81...	-
notifications-service	ARN	Active	80	HTTP	Instance	svc-08a4cffca81...	vpc-052820c0965661e8
notfound-service	ARN	Active	-	-	Lambda	svc-08a4cffca81...	-
inventory-service	ARN	Active	-	-	Lambda	svc-08a4cffca81...	-
health-service	ARN	Active	80	HTTP	Instance	svc-08a4cffca81...	vpc-052820c0965661e8
analytics-service	ARN	Active	80	HTTP	ALB	svc-08a4cffca81...	vpc-052820c0965661e8

aws COMMUNITY DAY AOTEAROA

How to Access VPC Lattice – Access



How VPC Lattice Works

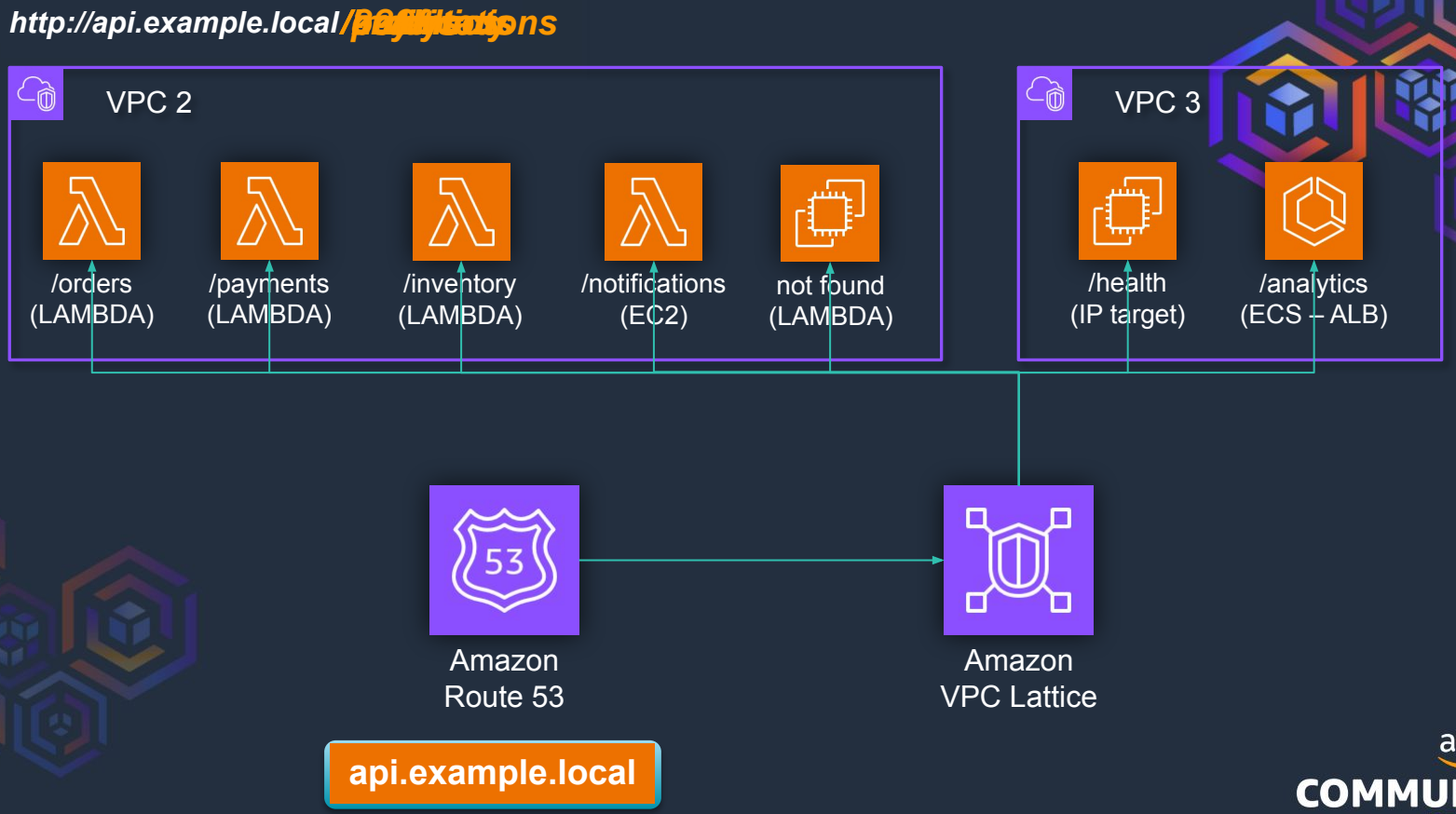
Service Network Creation

Service network name	Service associations	Network access	VPC associations
cltest1-network	SERVICE <= 500	None (Default) Security Group OR IAM	VPC VPC <= 500

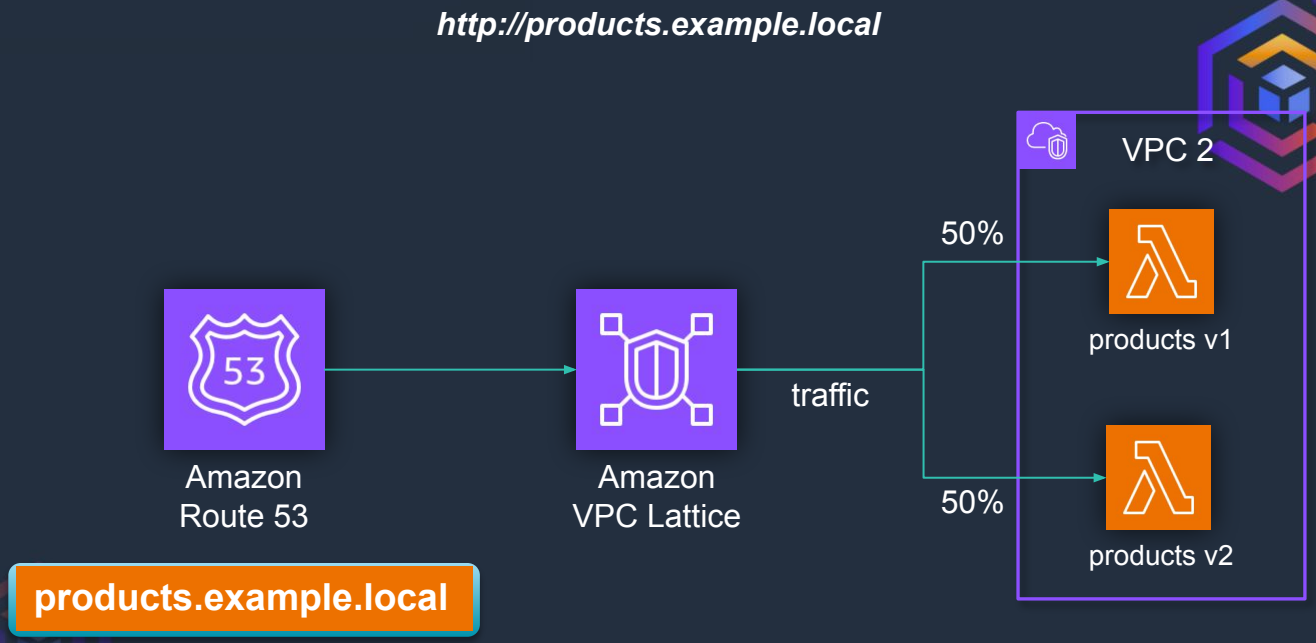
Lattice Service Creation

Service name	api
Domain configuration	api-094c8bf788085afc8.7d67968.vpc-lattice-svcs.ap-southeast-2.on.aws
Custom domain name	api.example.local Route53
Service access	Security Group; None (Default); OR; IAM

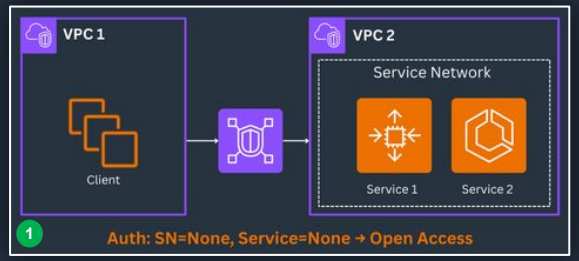
Example: api.example.local

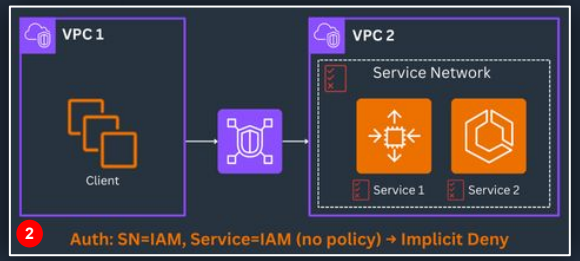


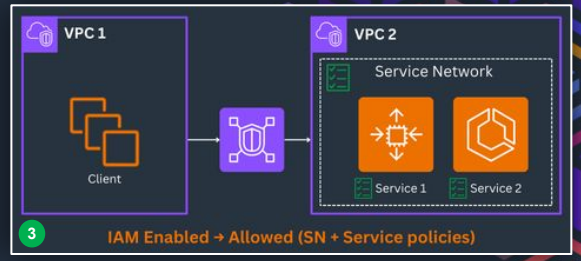
Example: products.example.local

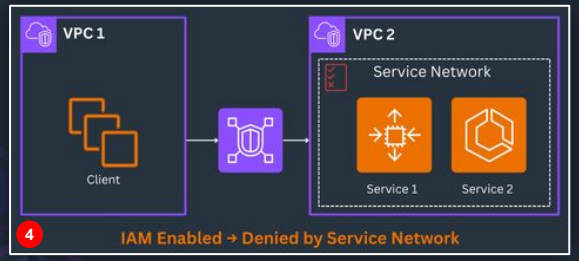


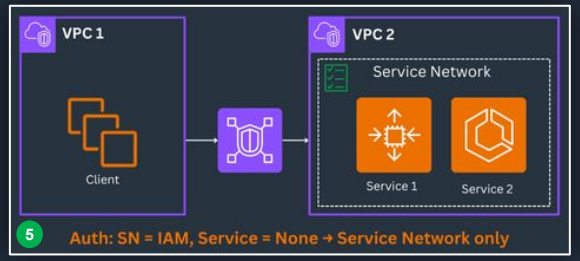
Amazon VPC Lattice – Auth & Policy Outcomes

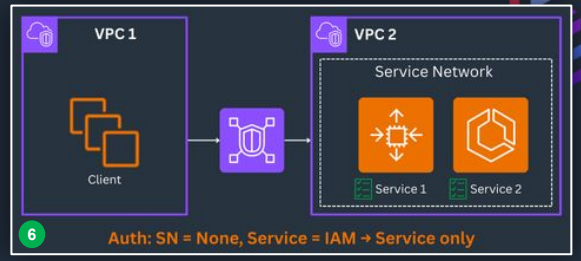


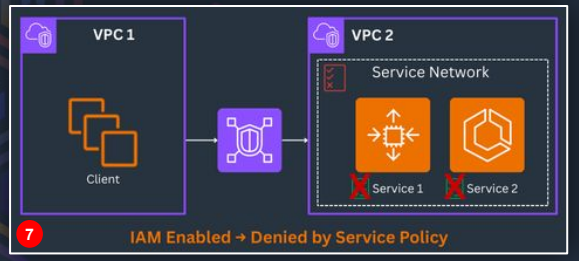


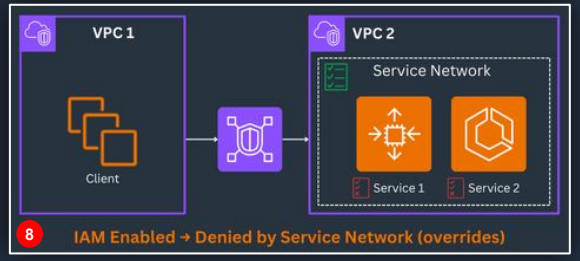






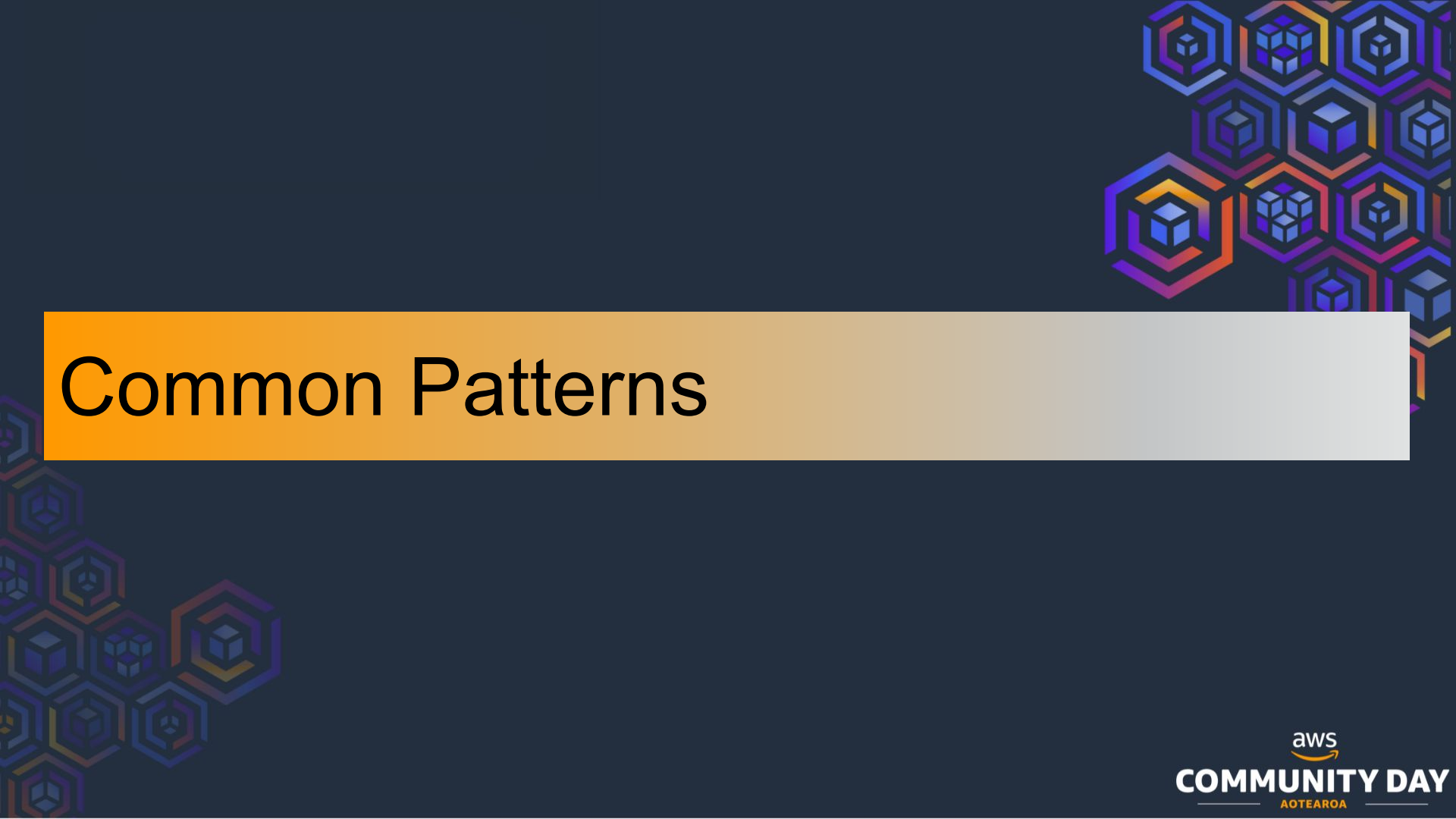






aws
COMMUNITY DAY
AOTEAROA

Common Patterns

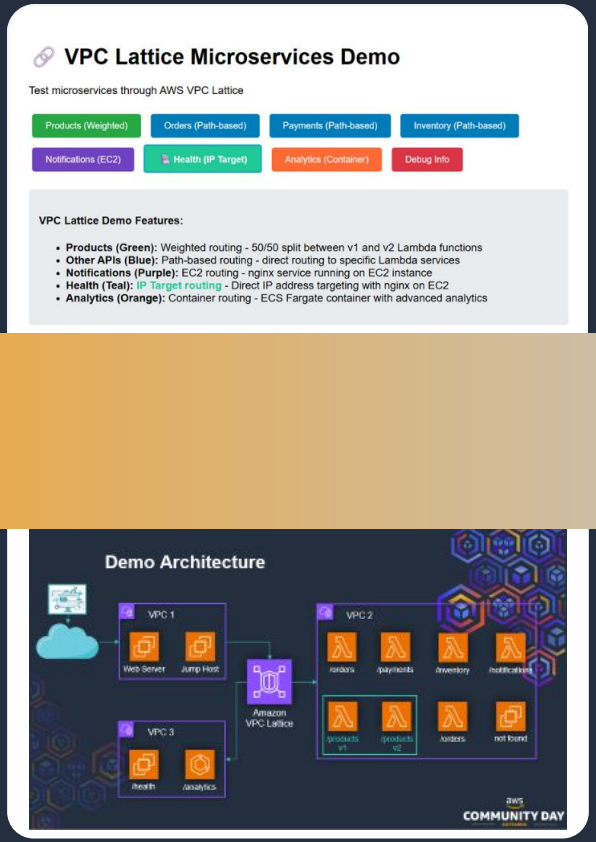


When to Use VPC Lattice

1. **Multiple VPCs / Accounts** – Need secure, consistent connectivity without VPC peering or TGW complexity.
2. **Application-Layer Routing** – Need to route by **path/hostname** (like /api, /orders) — similar to ALB or API Gateway, **but across multiple VPCs/accounts** without extra networking setup.
3. **Mixed Target Types** – Combine **Lambda, EC2, ECS, ALB/NLB** into a single logical service (no separate LBs per target type).
4. **Centralized Auth & Policies** – Use **IAM + fine-grained policies** to control *who* can call *what* at request level — built-in, no custom auth layer needed.
5. **Service-to-Service Discovery** – Simplify internal DNS and cross-VPC name resolution.
6. **Private Connectivity** – Services stay **inside the AWS network** — no public IPs or IGWs required.

When to Skip VPC Lattice

1. **Single VPC & Simple Routing** – Use ALB/NLB directly — Lattice adds unnecessary complexity here.
2. **East-West IP Traffic Only** – Lattice supports HTTP/HTTPS only — use TGW/peering for raw TCP/UDP.
3. **Ultra-Low Latency / High Throughput** – Adds a few ms of L7 overhead — not ideal for HPC or µs-sensitive apps.
4. **Public-Facing APIs** – Lattice is private-only; API Gateway/CloudFront are better for internet-exposed APIs.
5. **Cost-Sensitive Bulk Transfer** – Lattice charges per request + GB processed; TGW is cheaper for heavy L3 traffic.



Demo

aws COMMUNITY DAY AOTEAROA

Examples

Terraform module:

https://registry.terraform.io/modules/tfstack/vpc-lattice/aws/latest

Demo:

https://github.com/jajera/aws-community-day-aotearoa-2025-vpclattice-talk

Feedback

Go to

pigeonhole.at

Enter passcode

AWSCDNZ25

aws COMMUNITY DAY AOTEAROA

aws
COMMUNITY DAY
AOTEAROA

Appendix

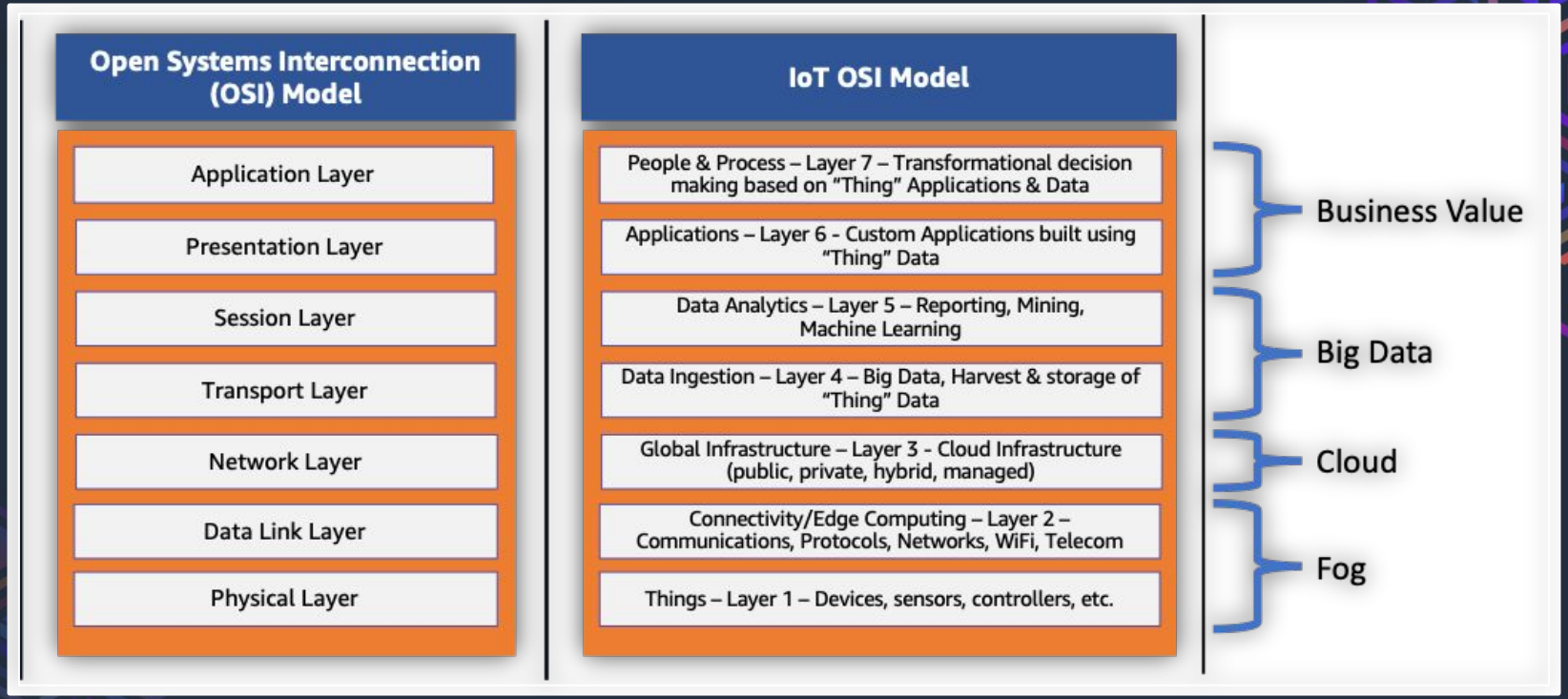
VPC Lattice Components

Component	Purpose
*** Service Network**	Logical boundary for a collection of services and resource configurations
*** Service**	Independently deployable unit of software that delivers a specific task or function
- Listener	Process that checks for connection requests and routes them to targets
- Rule	Component of a listener that forwards requests to targets based on conditions
- Target Group	Collection of resources (targets) that run your application or service
Resource	Entity such as RDS database, EC2 instance, application endpoint, domain-name target, or IP address
Resource Gateway	Point of ingress into the VPC where resources reside
Resource Configuration	Logical object representing single resource or group of resources
*** Service Directory**	Central registry of all VPC Lattice services owned or shared via AWS Resource Access Manager (RAM)
*** Auth Policies**	Fine-grained authorization policies for service access control

Amazon VPC Lattice Reference Architectures

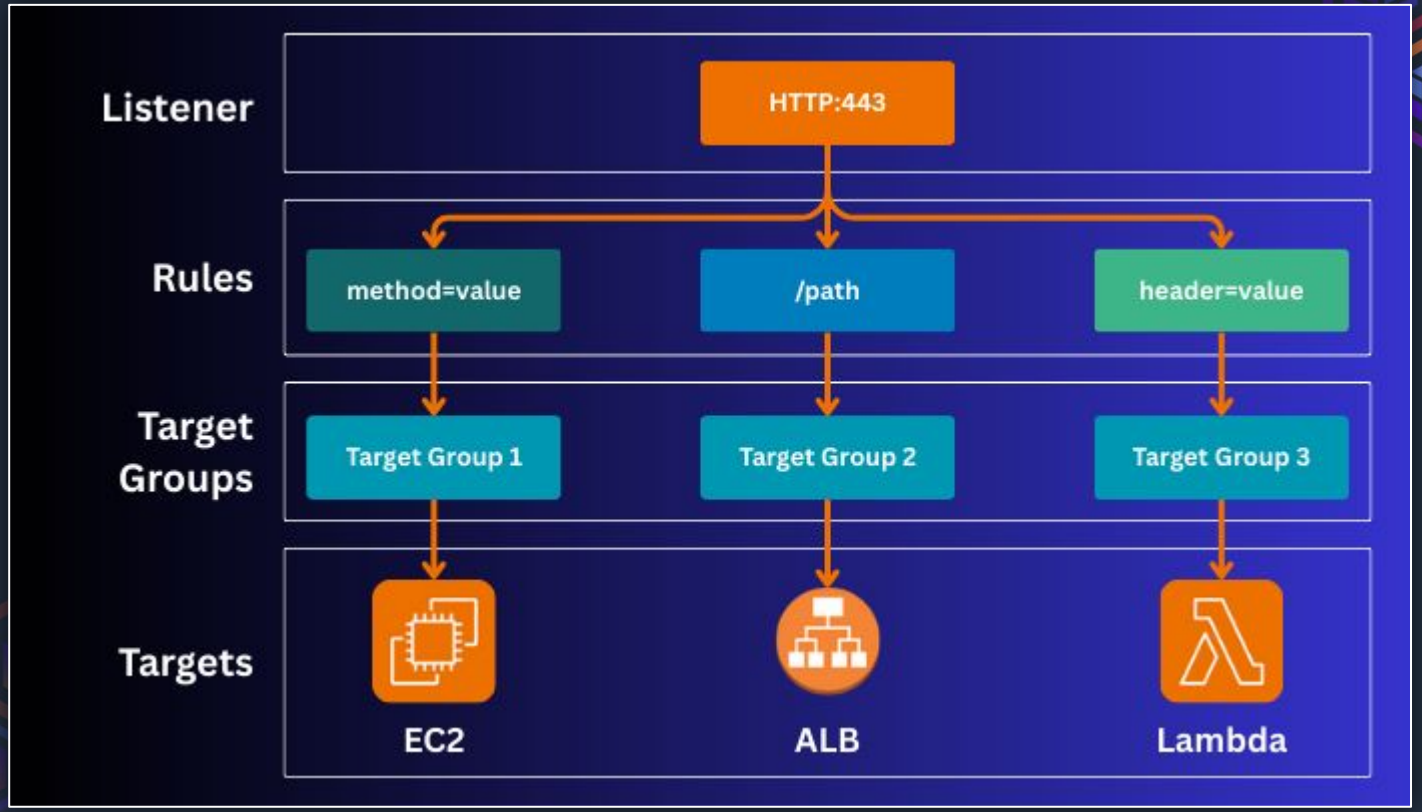
https://docs.aws.amazon.com/architecture-diagrams/latest/amazon-vpc-lattice-use-cases/amazon-vpc-lattice-use-cases.html

OSI Model



https://aws.amazon.com/what-is/osi-model/

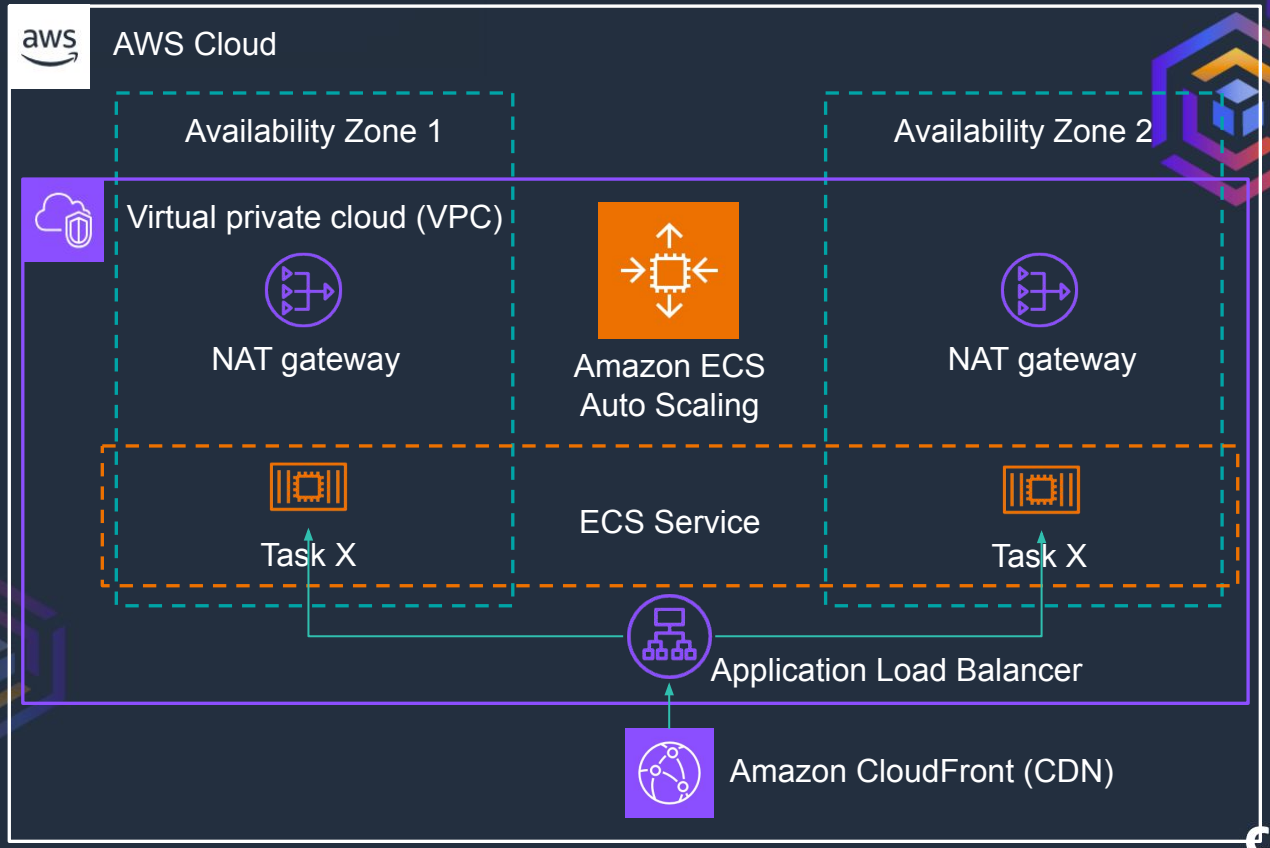
VPC Lattice: Service Components



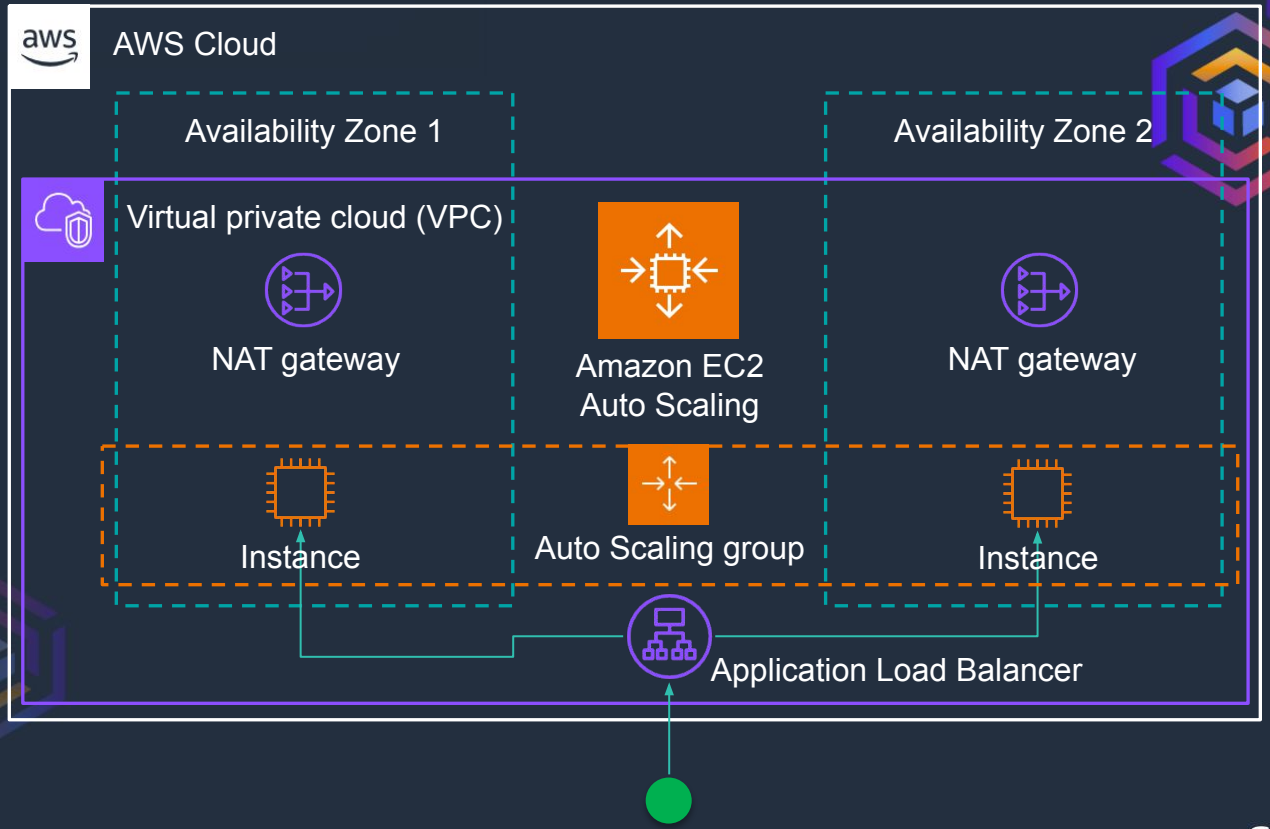
aws
COMMUNITY DAY
AOTEAROA

Zoom Slides

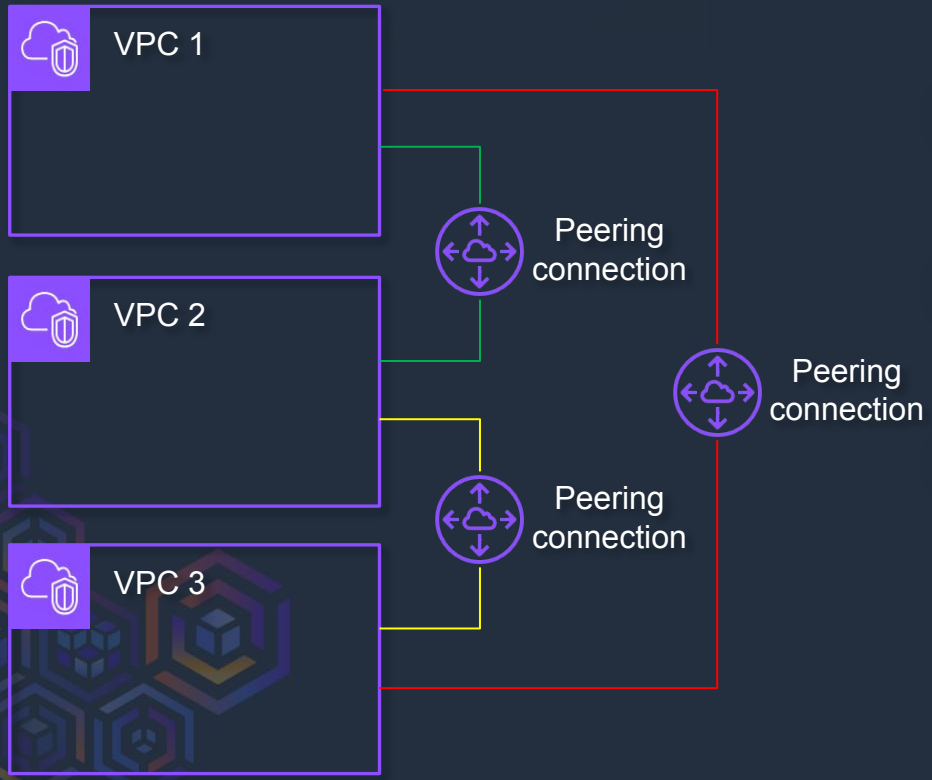
Web Service on Amazon ECS



Web Service on Amazon EC2

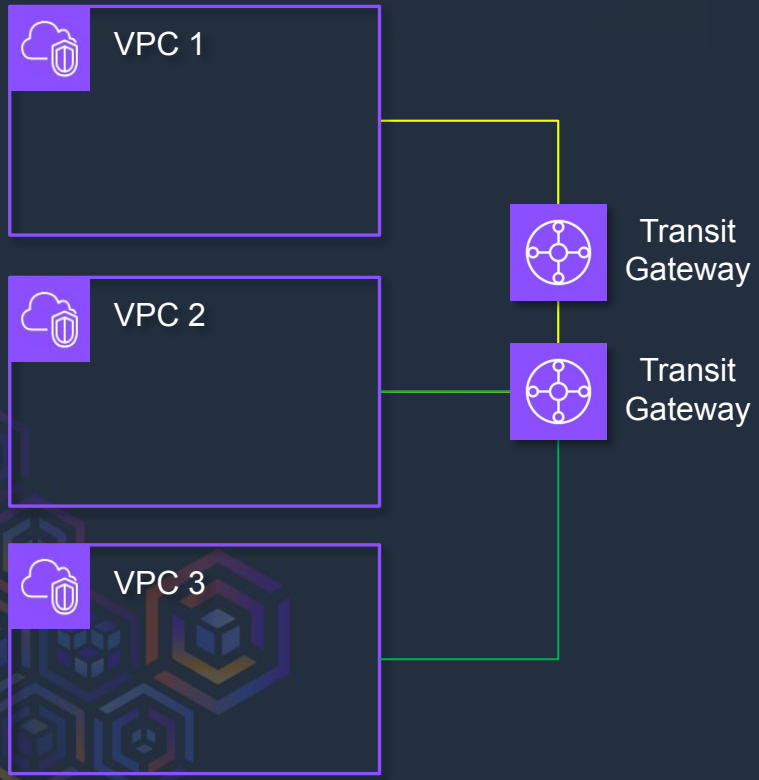


VPC Peering



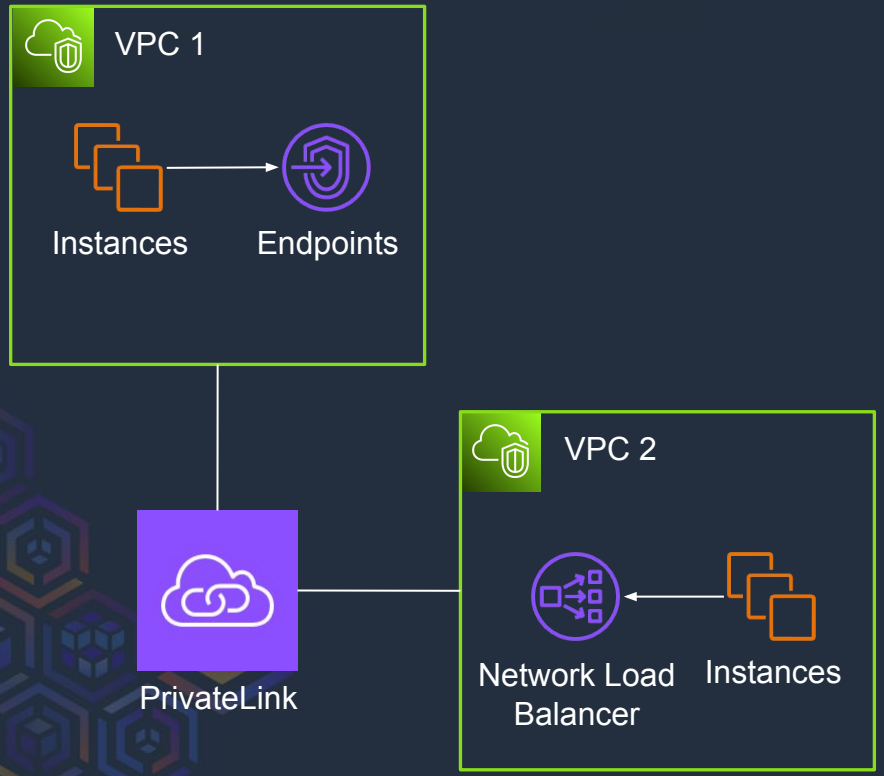
- Direct, one-to-one connection between two VPCs.
- Simple and low-cost, but no transitive routing.
- Works at layer 3 (network/ip) layer.

AWS Transit Gateway



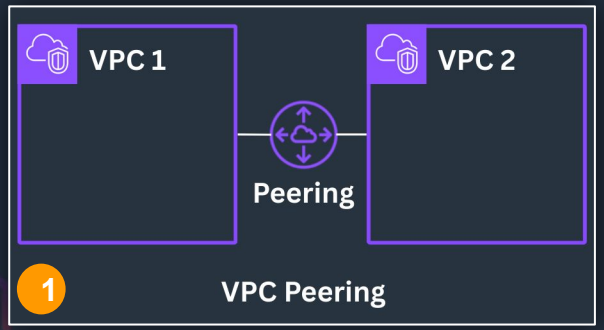
- Connects multiple VPCs through a single gateway.
- Scales better, supports transitive routing, but adds cost.
- Centralized hub-and-spoke model for many VPCs.
- Works at layer 3 (network/ip) layer.

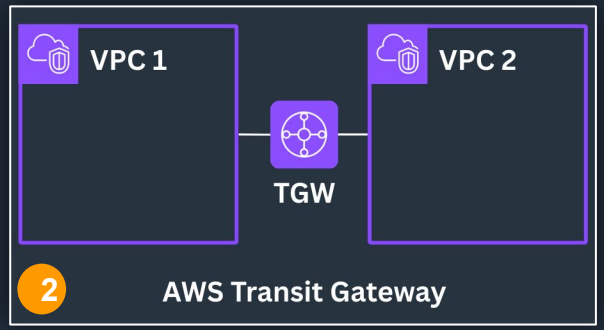
AWS PrivateLink

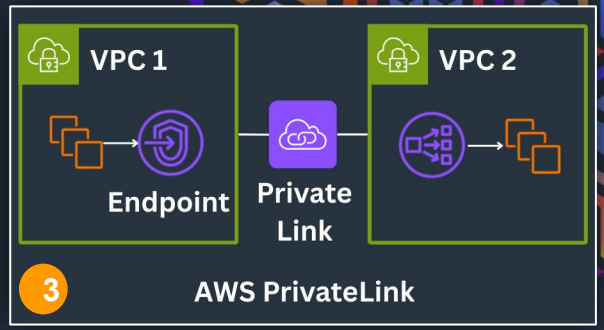


- Secure, service-level connectivity between VPCs.
- Exposes only specific services (via endpoints), not the entire VPC network.
- Works at layer 4 (transport) layer.

Common Inter VPC Connectivity







VPC Peering

- Direct, one-to-one connection between two VPCs.
- Simple and low-cost, but no transitive routing.

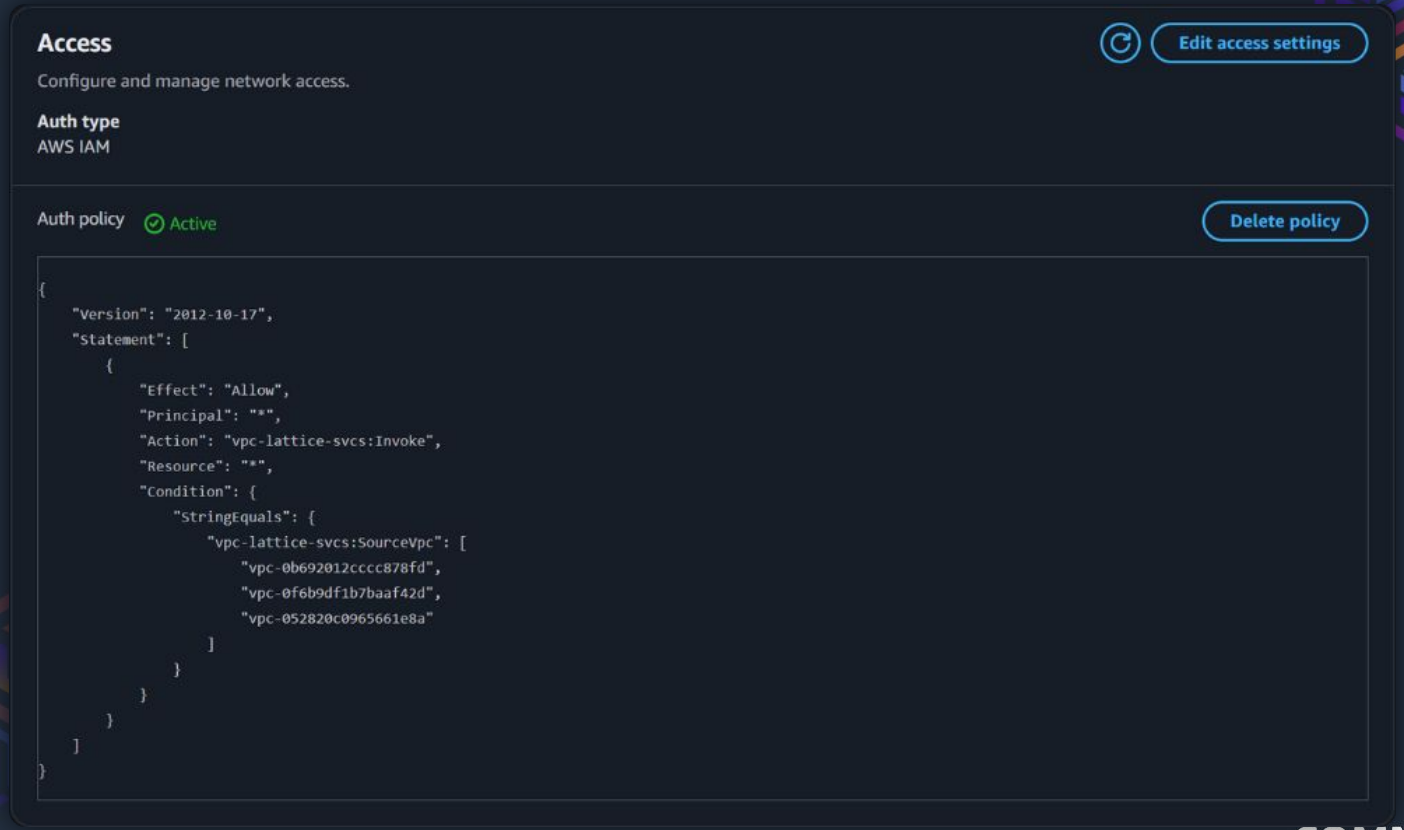
AWS Transit Gateway

- Centralized hub-and-spoke model for connecting many VPCs.
- Scales better, supports transitive routing, but adds cost.

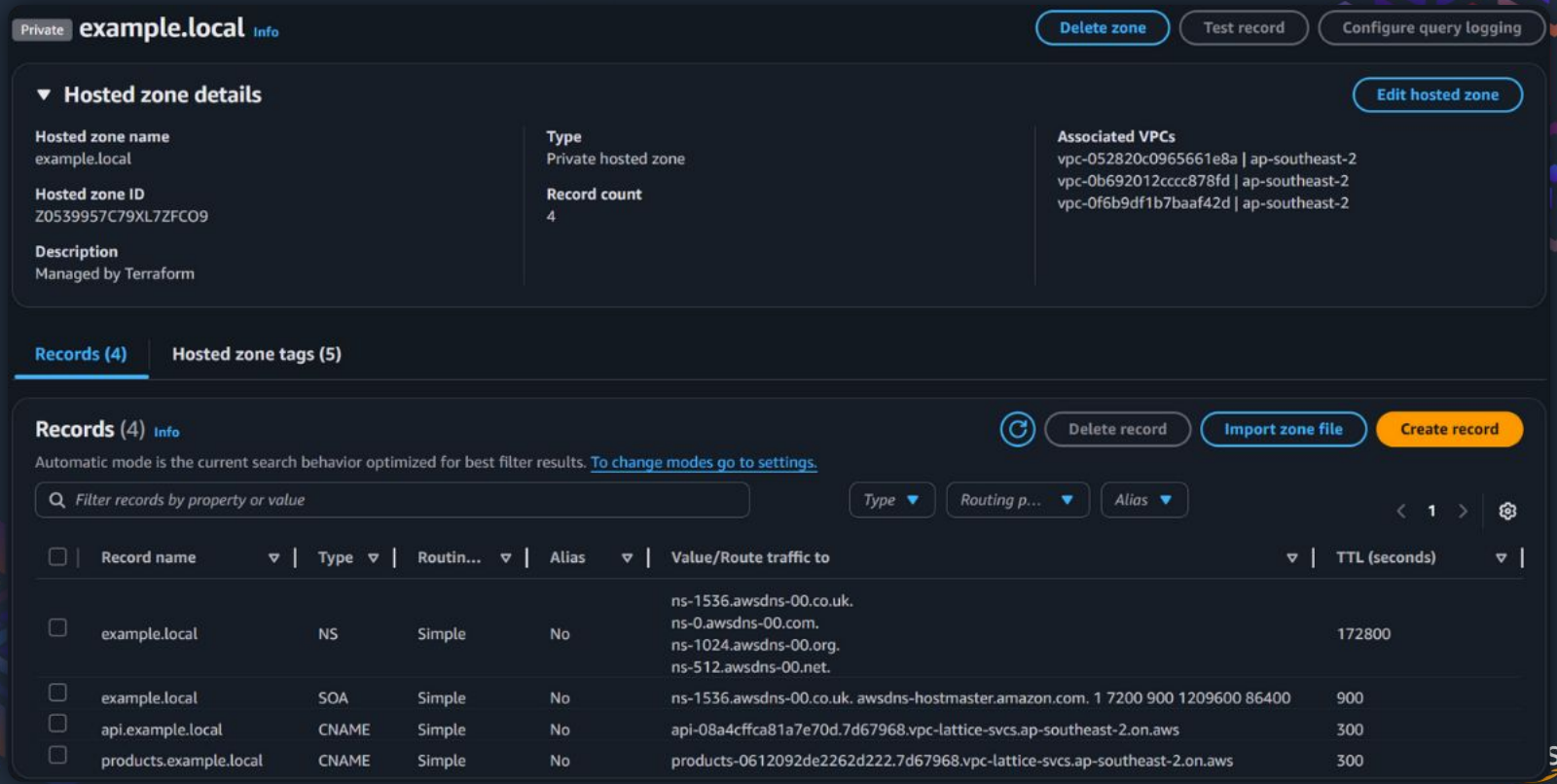
AWS PrivateLink

- Secure, service-level connectivity between VPCs.
- Exposes only specific services (via endpoints), not the entire VPC network.

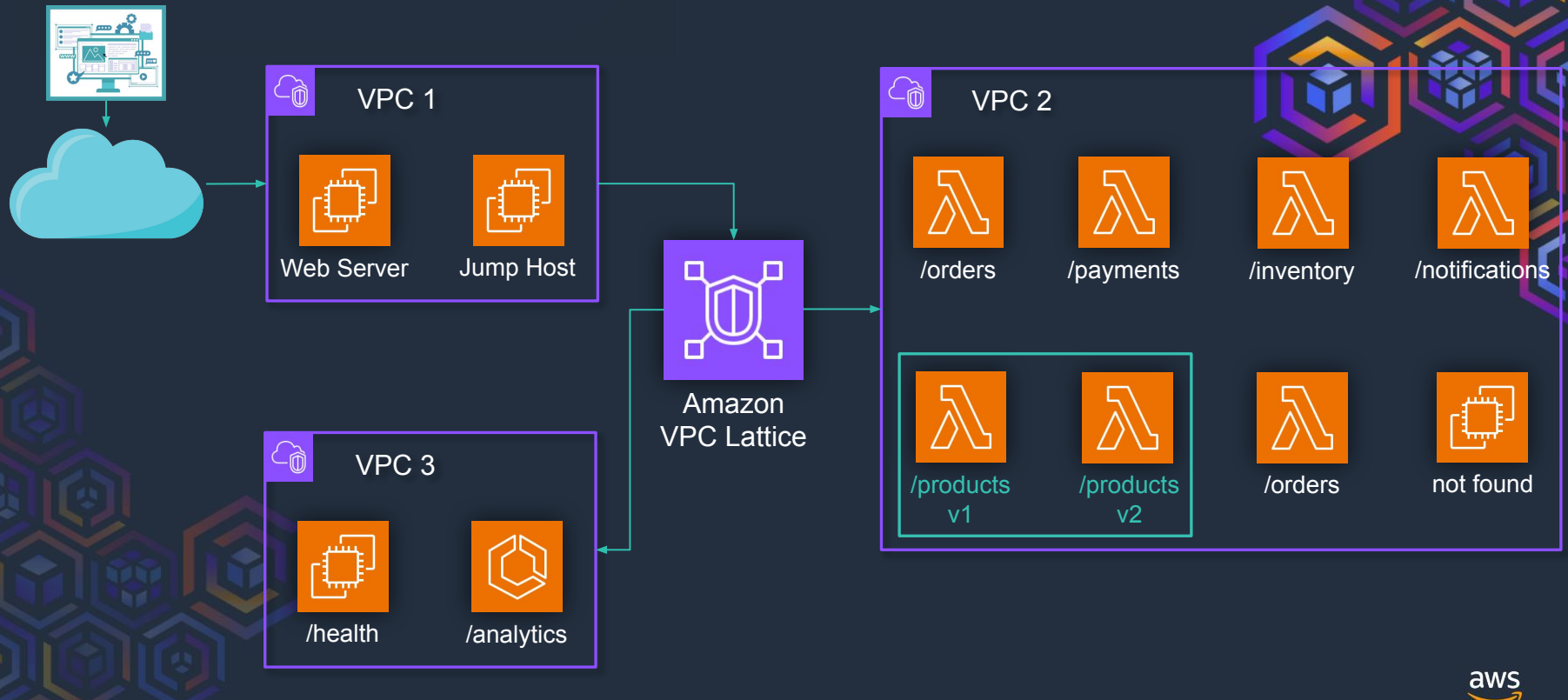
IAM Permission Example



Route 53 Record Example



Demo Architecture




aws
COMMUNITY DAY
AOTEAROA