# GCC 2.0 Tech Talks

- AWS GA since **4th May 2022**.
- If and when we talk about Native Services, we will probably cite **AWS only**.
- Information on Azure will be shared in coming months (to recap, Azure GA will be by Q3 2022).
- All slides will be shared and most of the documentation will also be translated to either Developers Portal (accessible by everyone) or Docs Portal (only accessible by for TechPass account holders).
- All the slides can be shared with existing contractors who are required to manage Projects on GCC as deemed fit by Agencies.
- The series of "Brown Bag" lunch time tech talk is arranged so as to ensure more people can join us in view that some will clash with your meetings. Please feel free to have your lunch while you join us.

## For Your Info

- You will be put on mute by default.
- Video should be turned off.

## Q&A Segment

- Type in message box when you want to ask a question.
- Wait to be acknowledged by the presenter before speaking.
- Unmute your microphone and state your name and agency clearly.

## Session Recording

- Please note that the series of GCC 2.0 Tech Talks will be recorded.
- The video recordings will be made available (in SharePoint).

# Let Us Know Your Feedback!

https://form.gov.sg/625cbdaa5ea46200123d92c5

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg

# How to resolve GCC FQDNs and WOG FQDNs | VPC Endpoints | ELB(ALB/NLB) and Gateway LB

Name: - Cherng Wei & AWS Solutions Architects
Department :- CODEX-GCC & AWS

Date :- 6th May 2022(Friday)
Ver 1.0

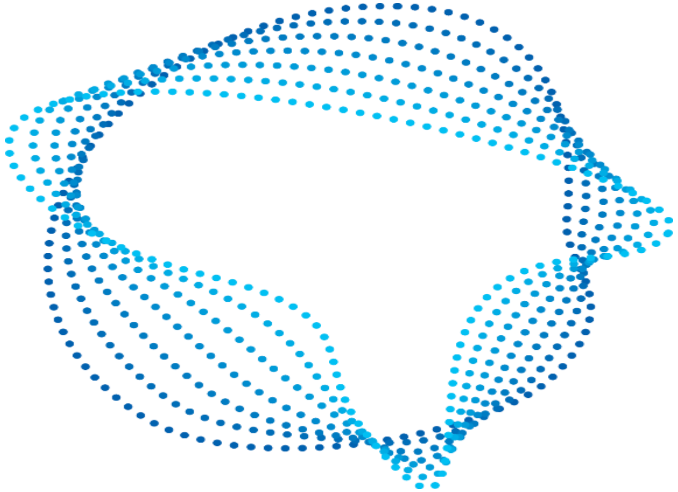
# TABLE OF CONTENTS

1. DNS Resolver(Route 53) for GCC 2.0

2. Virtual Private Cloud (VPC) Endpoints

3. Elastic Load Balancers(ALB/NLB) & Gateway Load Balancer

DNS Resolver for GCC 2.0



# Use of AWS Route 53 in GCC 2.0

# DNS Resolver for GCC 2.0( GEN Routable[INTRANET] )

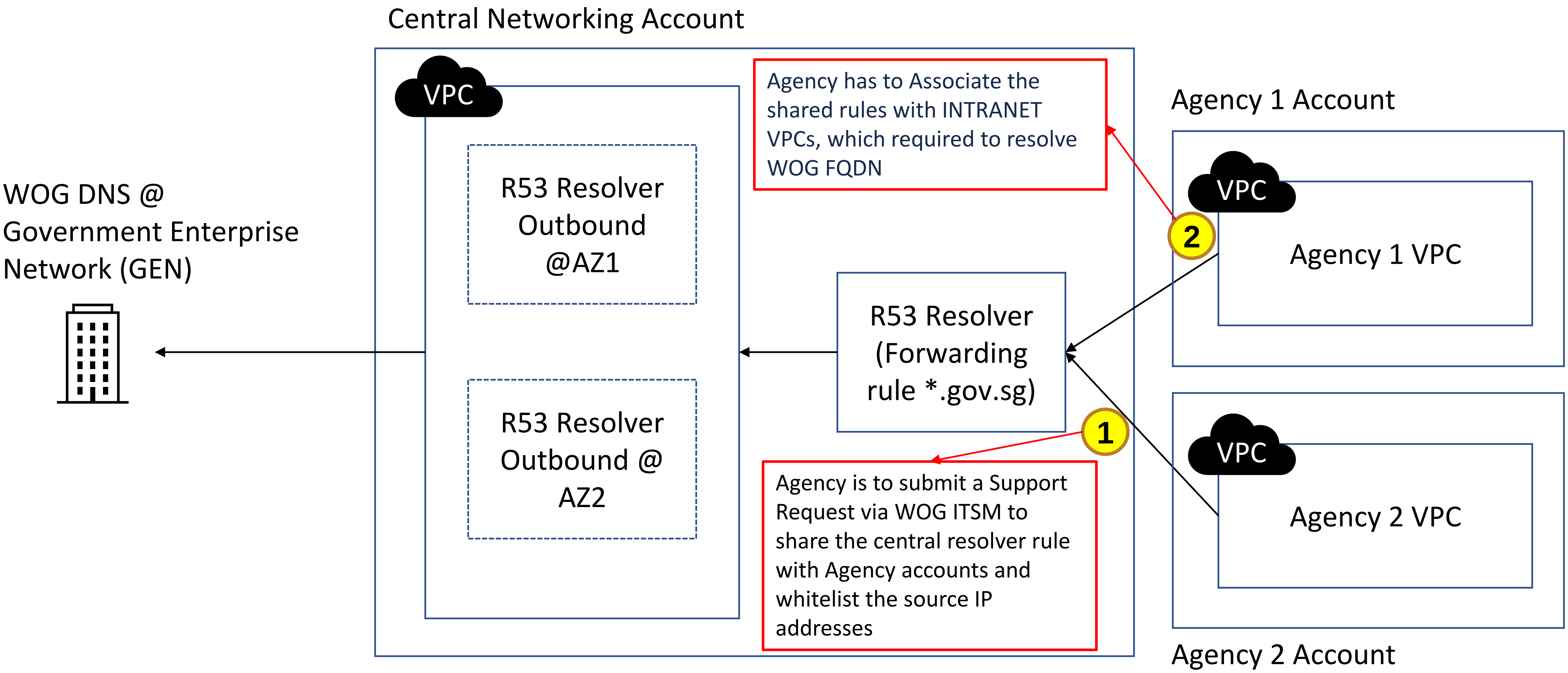
*What is new about this in GCC 2.0 as compared to GCC 1.0?*

- GCC 2.0 uses Cloud Native Service AWS Route 53 Resolver endpoints with conditional forwarding to resolve WOG DNS and GCC AWS domains(FQDNs)

- To resolve WOG DNS domains, the outbound resolver rules will be shared to Agencies' AWS Accounts using RAM(Resource Access Manager) when Agency raises a request to Central team to share the GCC DNS service and whitelist the Agencies source IP address at security group of outbound ENIs

- To resolve GCC AWS domains from WOG, similar to GCC 1.0, we leverage on Cloud Native Service Route 53 Resolver Inbound endpoints to query GCC AWS FQDNs from GEN (Government Enterprise Network) via WOG DNS Conditional Forwarding

# GCC DNS Lookup for INTRANET Systems (GCC to GEN)


Central Networking Account
VPC
R53 Resolver Outbound @AZ1
R53 Resolver Outbound @ AZ2
R53 Resolver (Forwarding rule *.gov.sg)
WOG DNS @ Government Enterprise Network (GEN)
Agency 1 Account
VPC
Agency 1 VPC
VPC
Agency 2 VPC
Agency 2 Account
1
2

Agency has to Associate the shared rules with INTRANET VPCs, which required to resolve WOG FQDN

Agency is to submit a Support Request via WOG ITSM to share the central resolver rule with Agency accounts and whitelist the source IP addresses

# DNS Resolver for GCC 2.0 (GEN to GCC)

2

Submit a Support Request at WOG ITSM to associate the new CNAME with AWS FQDN

AWS Private Zone Records

| FQDN | Value |
|---|---|
| app1-xxx.aws-resolve.gcc.gov.sg | Internal-alb-app1-xxx-xxxx.ap-southeast-1.elb.amazonaws.com |
| app2-xxx.aws-resolve.gcc.gov.sg | Internal-alb-app2-xxx-xxxx.ap-southeast-1.elb.amazonaws.com |

WOG DNS @ Government Enterprise Network (GEN)

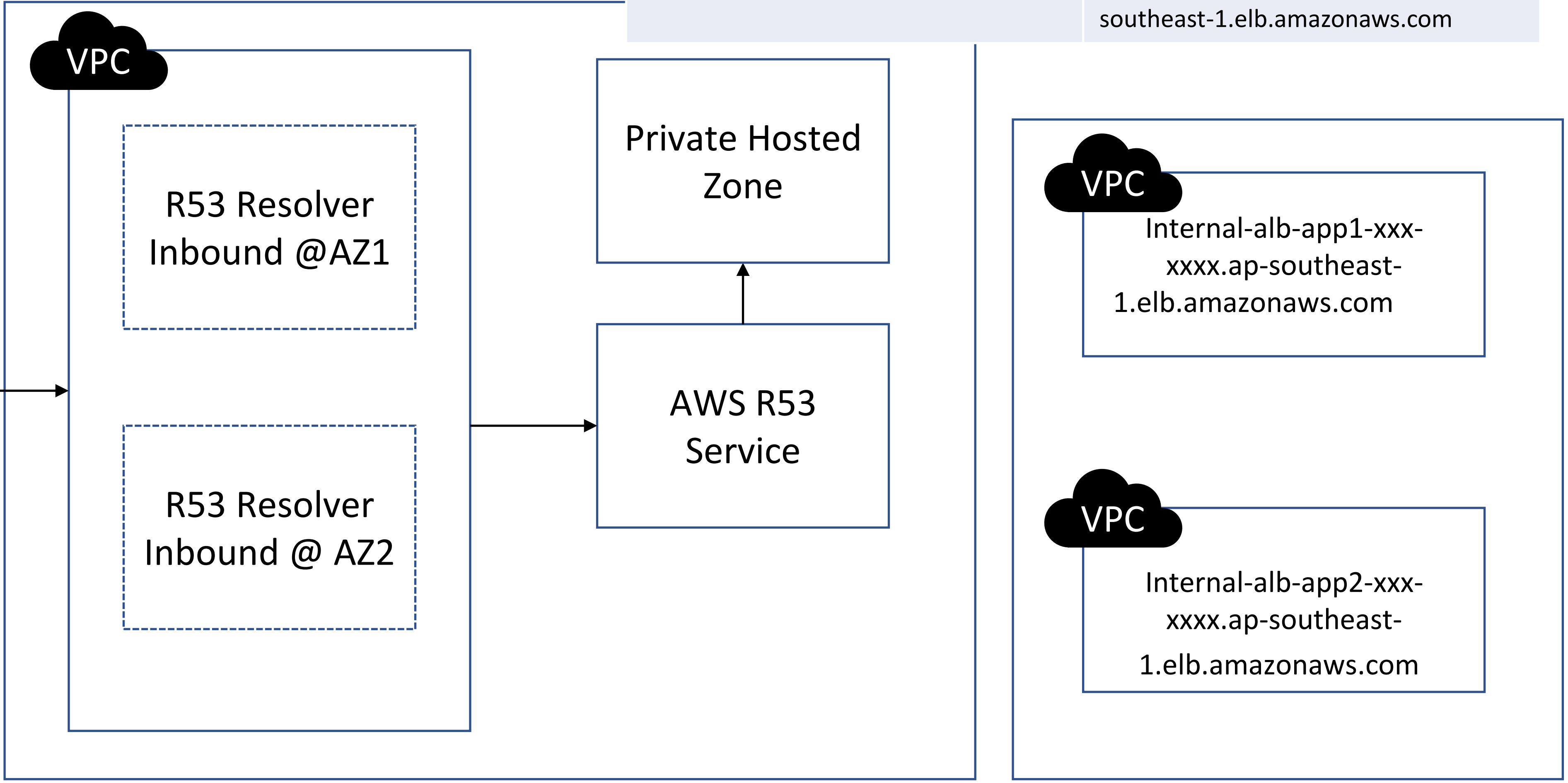
| FQDN | Value |
|---|---|
| App1.Agency.gov.sg | app1-xxx.aws-resolve.gcc.gov.sg |
| App2.Agency.gov.sg | app2-xxx.aws-resolve.gcc.gov.sg |

WOG DNS Records

1

Agency uses the WOG DNS Management Portal to configure the CNAME. Add a new CNAME as per the example.
app1.agency.gov.sg → app1-xxx.aws-resolve.gcc.gov.sg (CNAME)

Central Networking Account



VPC
R53 Resolver Inbound @AZ1
R53 Resolver Inbound @ AZ2
Private Hosted Zone
AWS R53 Service
VPC
Internal-alb-app1-xxx-xxxx.ap-southeast-1.elb.amazonaws.com
VPC
Internal-alb-app2-xxx-xxxx.ap-southeast-1.elb.amazonaws.com

# FAQs

- What about Non-Gen Routable[Internet] Compartments( with & without Common Services ) for DNS resolution ?

  Agency are able to use any Public DNS servers for their DNS resolutions of Internet FQDNs.
  E.g. Google Public DNS → 8.8.8.8 or 8.8.4.4 | Cloudflare Public DNS 1.1.1.1 or 1.0.0.1

- What about GCC 1.0 **migrated** compartments for their DNS resolution for WOG FQDNs ?

  Agencies can choose to have the existing DNS setup(remain) using Project DNS servers method( no change required ). Or Agency can choose to use the Route 53 DNS resolver Endpoints which will be made available.

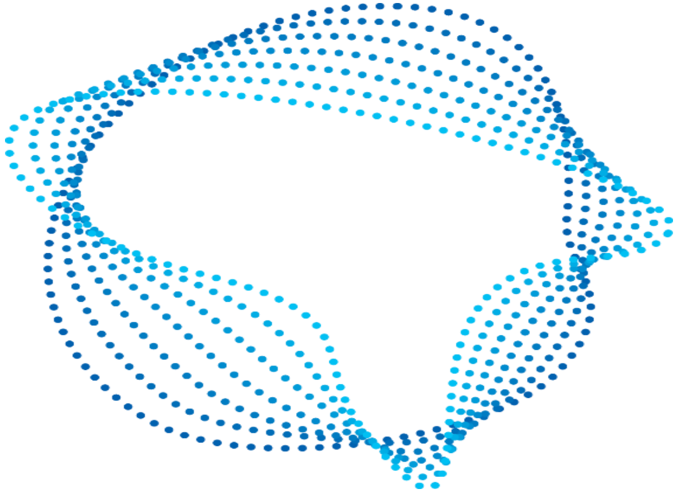
- Is conditional Forwarding of *.sgnet.gov.sg still required ?

  No, it is no longer required as the authoritative zone been migrated to WOG DNS servers instead of previously it was with WOG AD DNS servers.

- Can Agency choose to use their own unique 4th level domain(e.g 4thlevel.agency.gov.sg ) instead of **aws-resolve**.gcc.gov.sg ?

  Yes, it is possible but Agency needs to have proper DNS knowledge and understanding how it should be setup + configured on WOG DNS portal.

DNS Resolver for GCC 2.0



# Route 53
# AWS DNS Service

# Route 53 – At a Glance

- Domain Name Registration (DNS) Services
  - Register new domains
  - Transfer existing domains

- DNS resolution within and among AWS VPCs
  - Uses Anycast network of DNS servers
  - Highly Available

- **Route 53 Availability SLA - 100%**

# Route 53 Common Record Types

- ALIAS – Similar to a CNAME without the 2x lookup penalty; free of charge.  References another record

- A Record – Routes traffic to an IPv4 Address
- AAAA Record – Routes traffic to an IPv6 Address
- CNAME Record – Routes traffic to another name
- MX Record – Specified Mail Servers
- NS Record – Specified Name Servers for a Hosted Zone
- DS Records – Used to specify DNSSEC Delegation Records

# Route 53 Public vs Private DNS

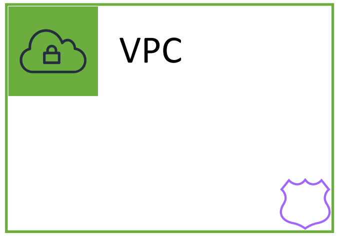
## Public Hosted Zones

- Route to Internet facing resources
- Resolve from the Internet
- Global Routing Policies

Internet

## Private Hosted Zones

- Route to VPC resources
- Resolve from inside the VPC
- Integrate with on-premises private zones using forwarding rules and endpoints



# Route 53 Resolver ( 2nd IP of CIDR in the VPC )

- When a VPC is created, the Route 53 Resolver that is created by default is mapped to a DNS server that runs on a reserved IP address for the VPC network range, it is the 2nd IP of the Primary CIDR of the VPC.

- For example, the DNS server on a 11.0.0.0/16 network is located at 11.0.0.2.

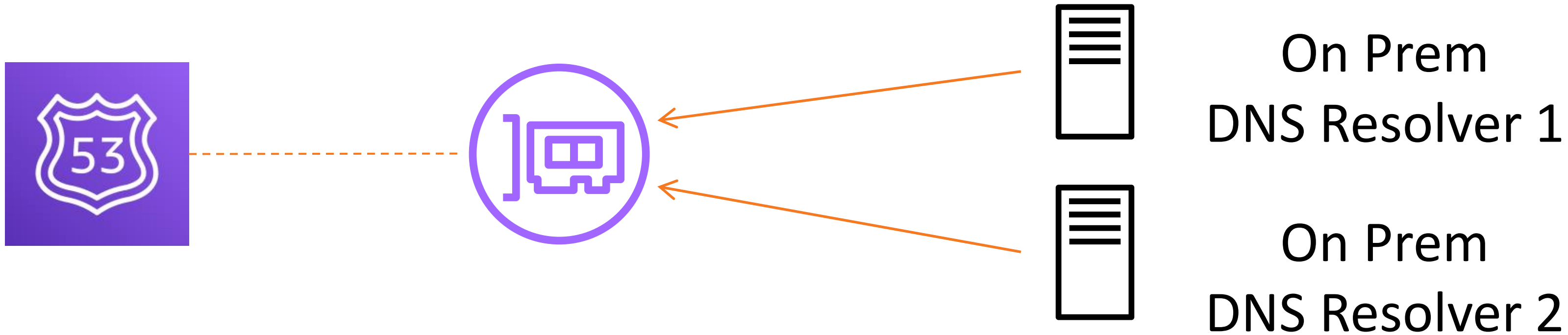
- For VPCs with multiple CIDR blocks, the DNS server IP address is located in the primary CIDR block.

# Route 53 Inbound Resolvers

Allow on-premises resolvers query Route 53 Resolver

Creates routable ENIs in VPC reachable over DX or VPN

Limit: 10,000 QPS per ENI



Best Practices:

Use multiple ENIs in separate AZs for high availability

Use a retrying DNS resolver on-premises

Specify your IPs

CloudWatch alarms on QPS

EC2 Instances use VPC+2 Resolver not Inbound Endpoints

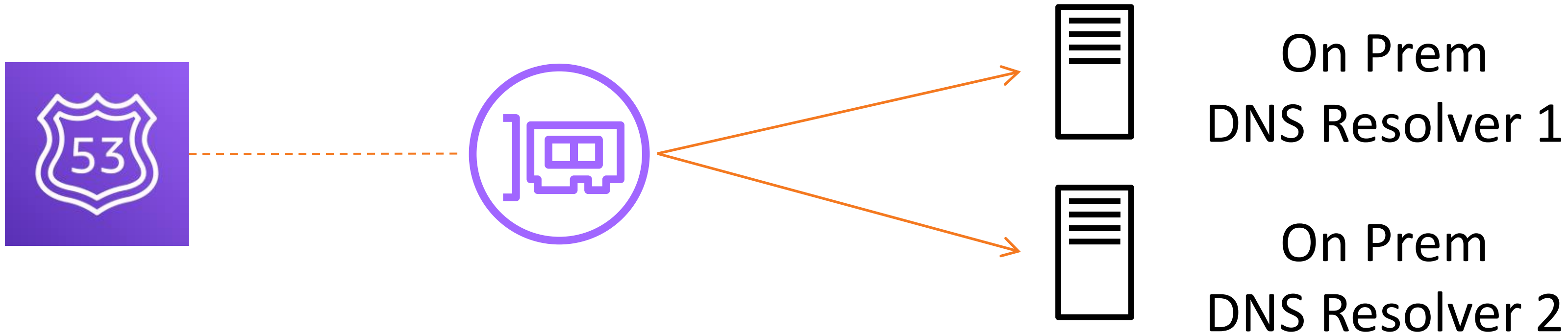
# Route 53 Outbound Resolvers

Path for the Route 53 Resolver to query your DNS Resolvers

Creates source ENIs in your VPC

Usable by many VPCs

Limit: 10,000 QPS per ENI



Best Practices:

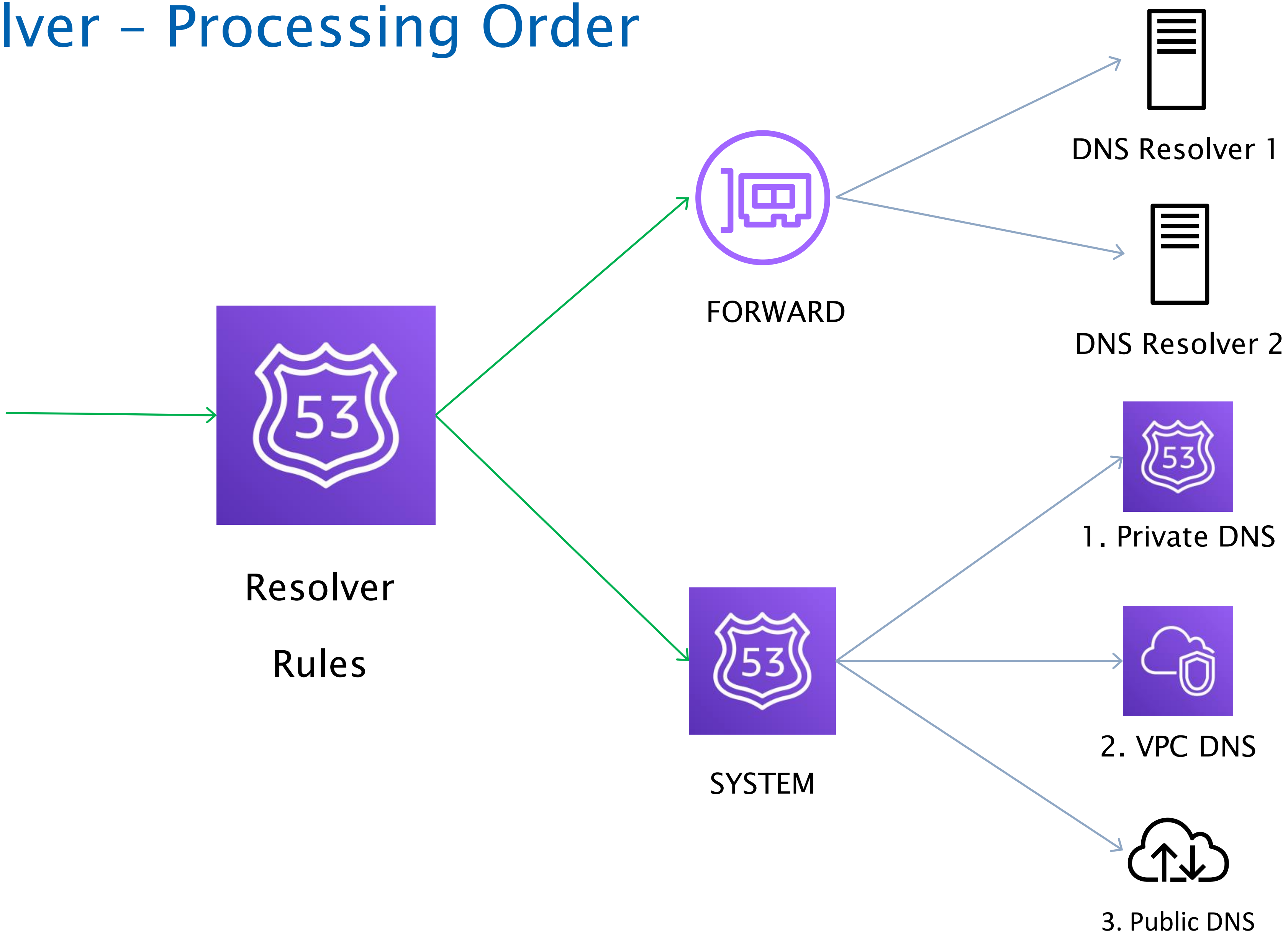
Use multiple ENIs in separate AZs for high availability

Use forwarding sparingly

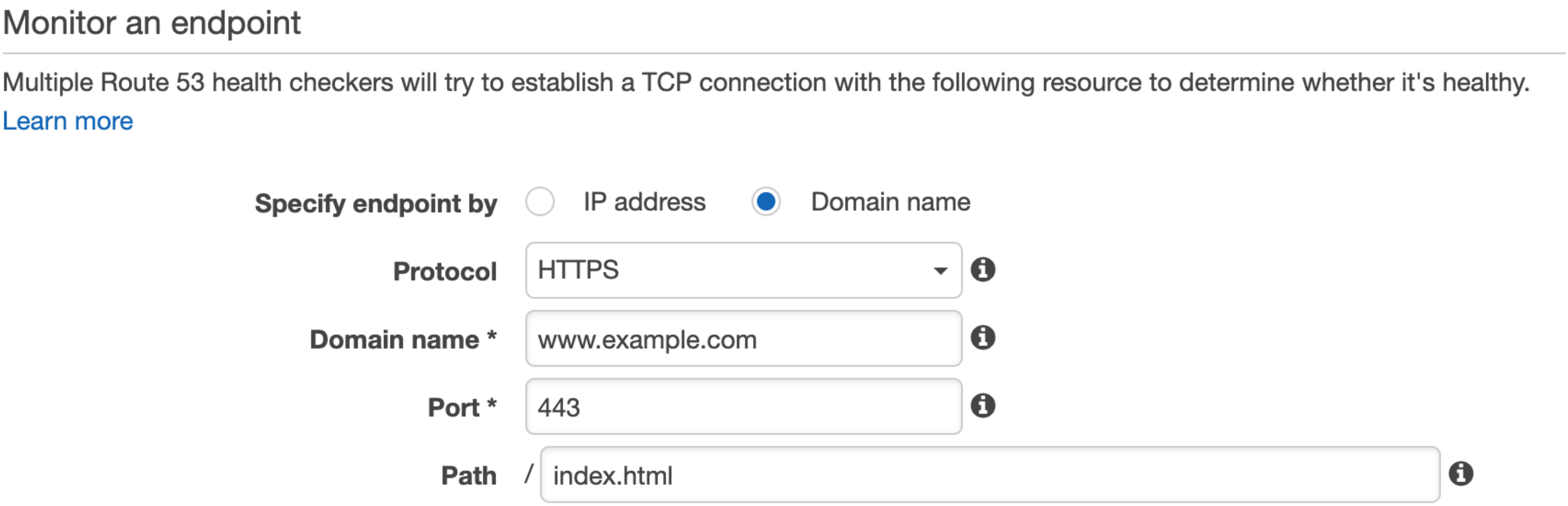
Maintain fixed IPs as targets

CloudWatch alarms on QPS

# Resolver – Processing Order



# Route 53 Health Checks - Endpoint

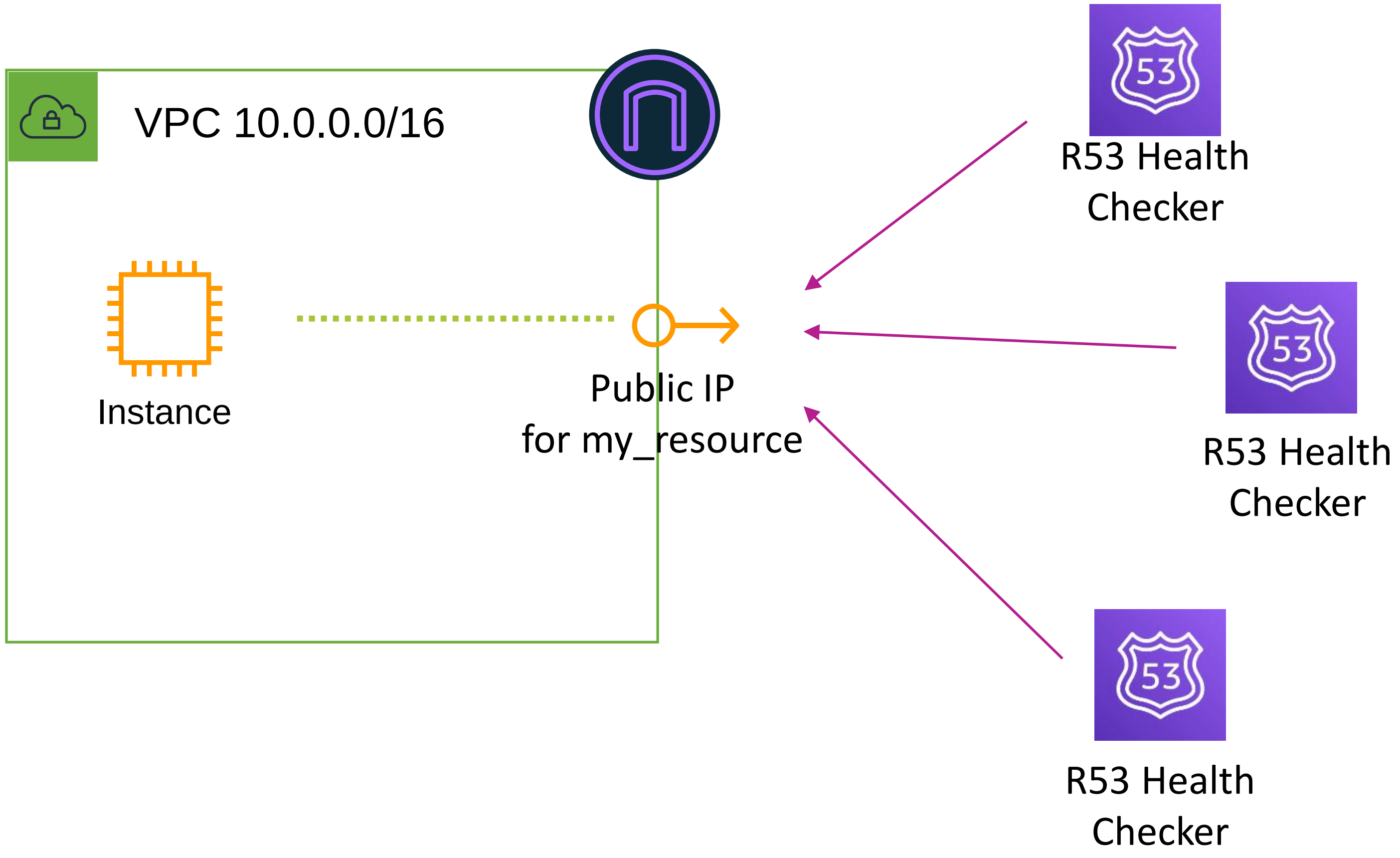


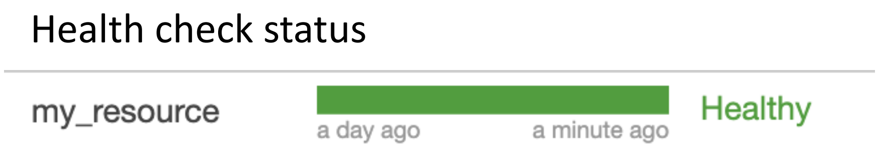
## Monitor an endpoint

Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy.
Learn more

|  |  |
|---|---|
| **Specify endpoint by** | ○ IP address ● Domain name |
| **Protocol** | HTTPS |
| **Domain name *** | www.example.com |
| **Port *** | 443 |
| **Path** | / index.html |

# Route 53 Health Checks - Endpoint



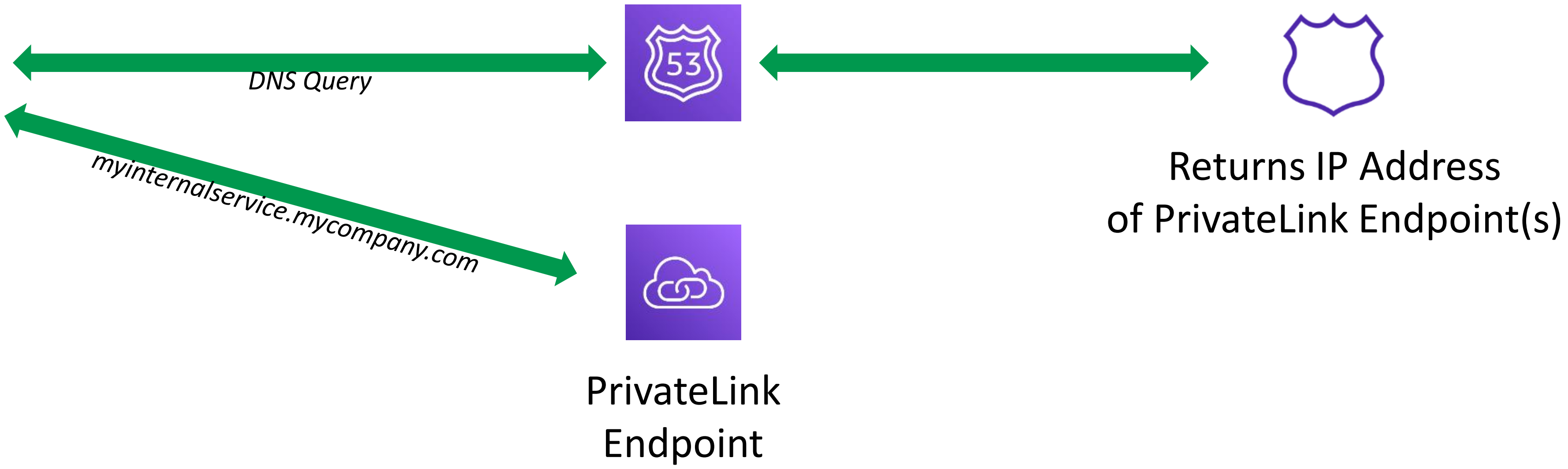


Health check status

my_resource 🟩 Healthy

a day ago a minute ago

# Route 53 PrivateLink Support



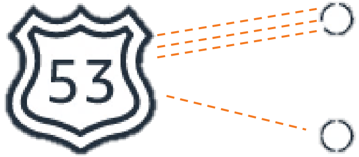
- When configuring PrivateLink, you can specify a Private DNS name and Route 53 resolver will resolve it to the PrivateLink endpoint!

# Route 53 Routing Policies

Seven basic routing policies for fine-grained control of Route 53 query responses

## Simple Routing

## Weighted



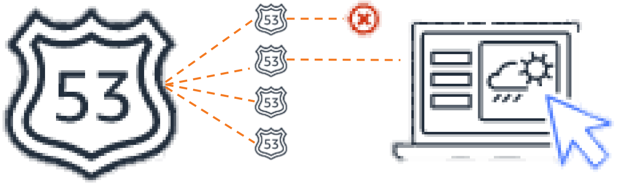
## Geolocation (Users)

## Geoproximity (Resources)

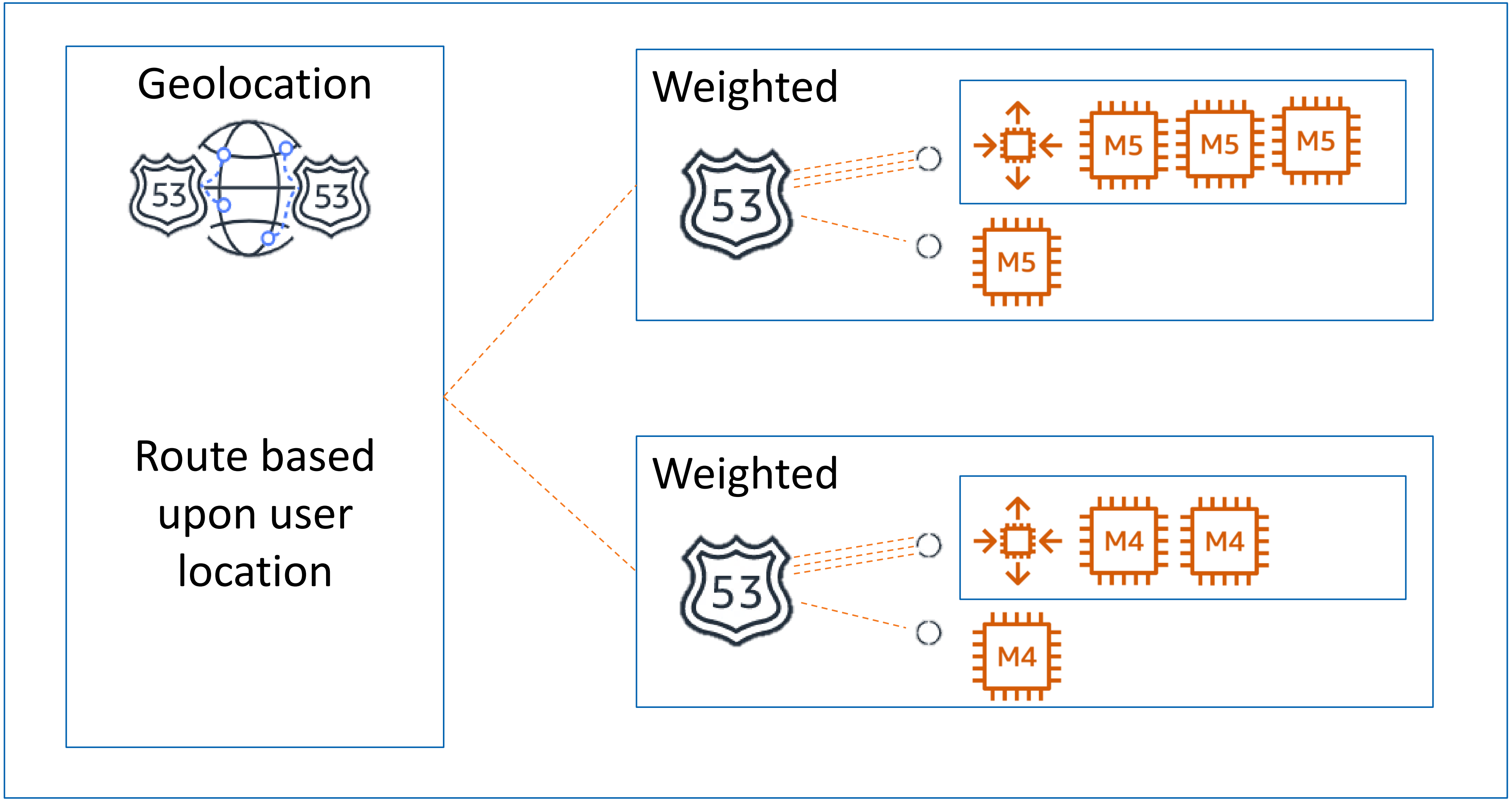
## Latency

## Failover

## Multi-value Answer

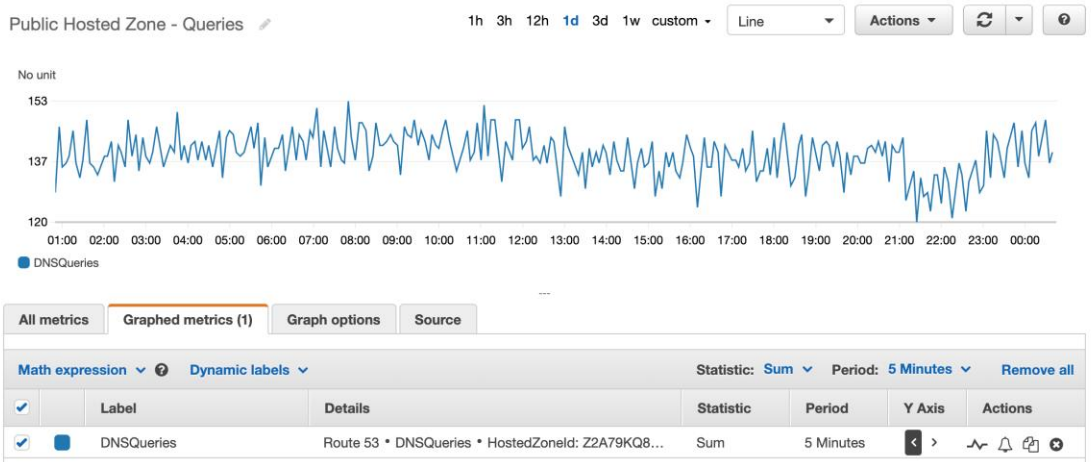


# Route 53 Advanced Traffic Policies



# Route 53 Monitoring

## CloudWatch Metrics



Statistic: Sum Period: 5 Minutes

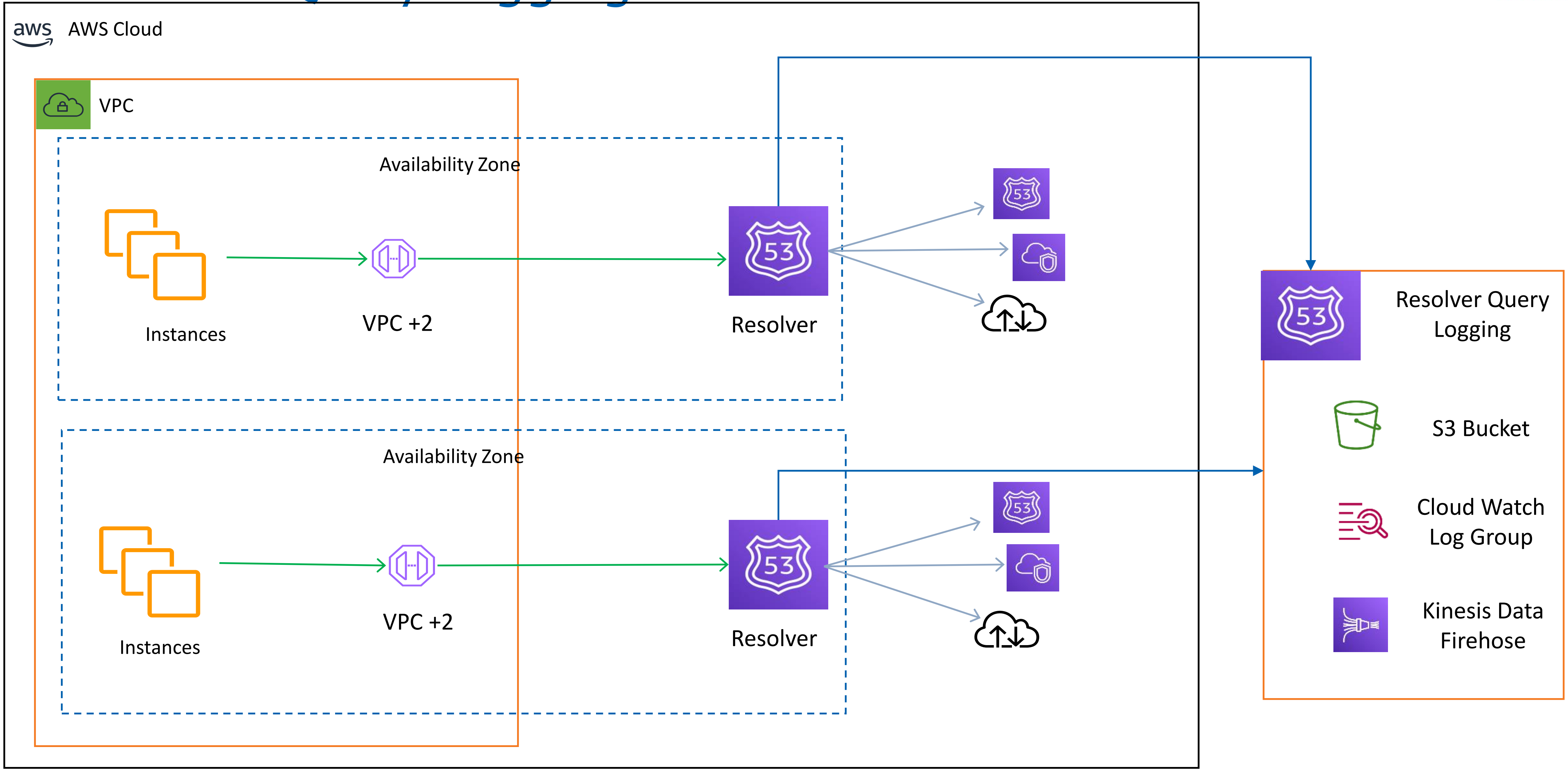
| ☑ | | Label | Details | Statistic | Period | Y Axis | Actions |
|---|---|---|---|---|---|---|---|
| ☑ | 🟦 | DNSQueries | Route 53 • DNSQueries • HostedZoneId: Z2A79KQ8... | Sum | 5 Minutes | | |

## CloudWatch Logs

**EXAMPLE LOG:**

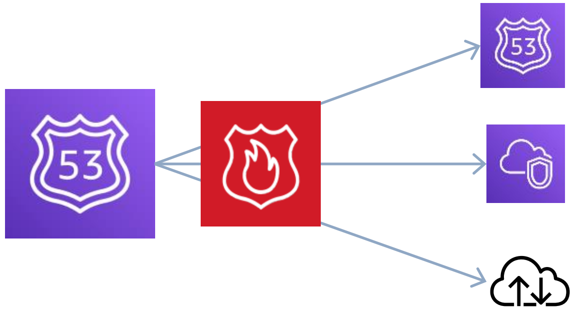
```
1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP FRA6 192.168.1.1 -
1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP IAD12 192.168.3.1 192.168.222.0/24
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP FRA6 2001:db8::1234 2001:db8:abcd::/48
1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP IAD12 192.168.3.1 192.168.111.0/24
1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP JFK5 192.168.1.2 -
```

# Route 53 Query Logging



# Route 53 Resolver DNS Firewall

- Firewall for the Route 53 Resolver and Hybrid Networks
- Easily deny/allow DNS traffic across all VPCs centrally
- Highly available, managed service
- Managed DNS Firewall Domain Lists:
  - Choice of AWS or Custom Rules



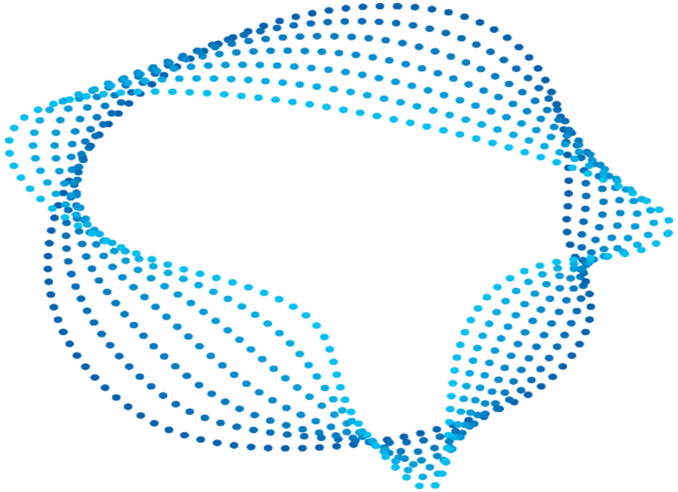
Choose from AWS Managed Lists or upload your own domain lists

Granular event detail with CloudWatch and DNS query logs

Partner Integrations:

FIREEYE™

HashiCorp Terraform



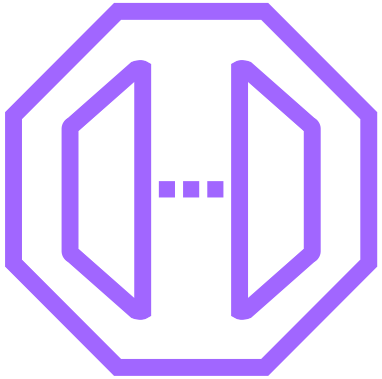
# Gateway Endpoints, Interface Endpoints (PrivateLink)

# Gateway VPC Interface VPC endpoints

- **Gateway VPC endpoints**
- Supports S3 and DynamoDB
- No per-hour or per-GB charge
- Supports connectivity from inside VPC only
- Clients reach S3 “at” its public IP

- **Interface VPC endpoints**
- Supports over 100+ AWS services
- Charged on a per hour, per GB, per AZ basis
- Supports connectivity from across Direct Connect/VPN/Transit Gateway
- Use private IP address from your VPC to access AWS services

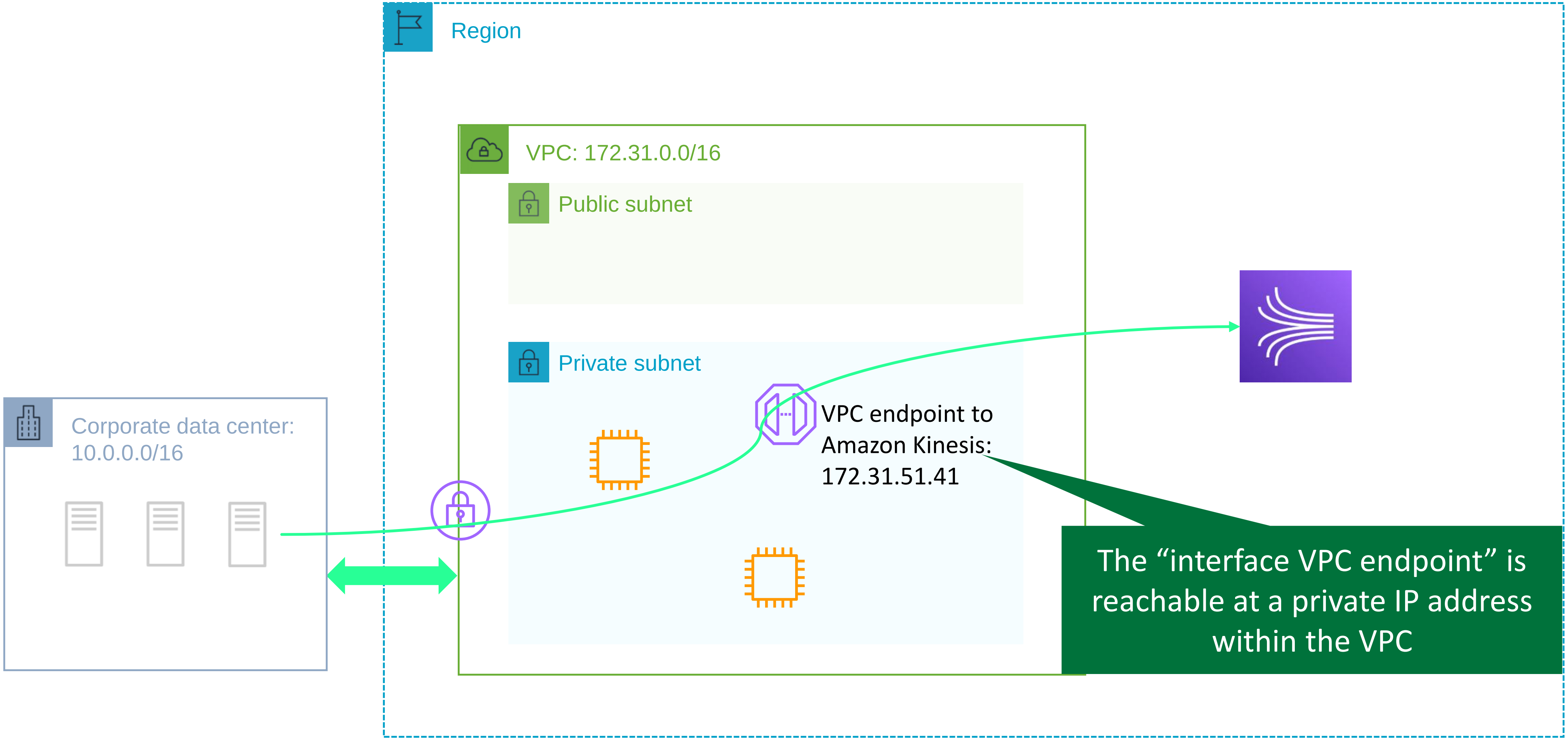
# What do VPC interface endpoints help to accomplish?



“S3 in my VPC” = VPC endpoint

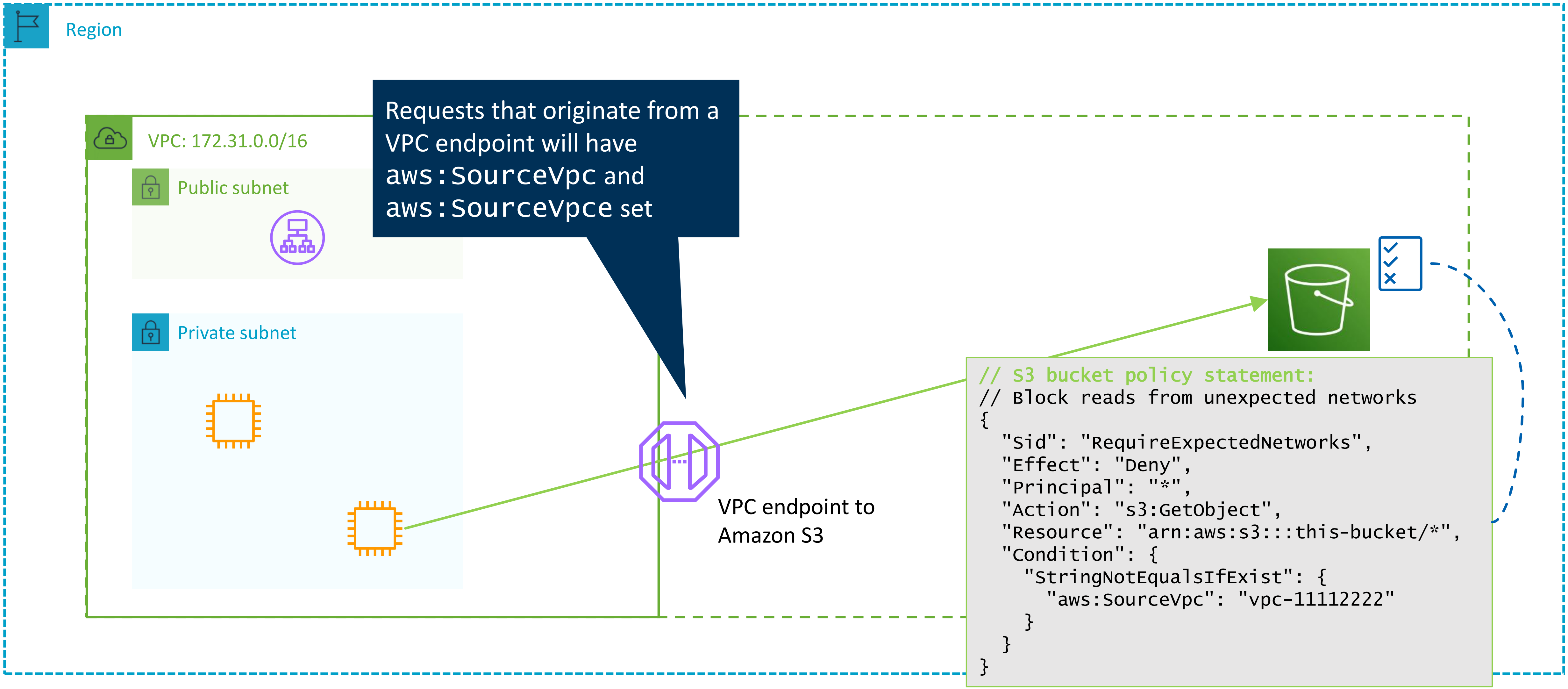
- **Connectivity:** network connectivity to the service without a requirement for an outbound route to the internet
- **Authorization:** a scalable means to identify traffic originating from this VPC for authorization purposes
- **Perimeter policy:** a network-perimeter authorization policy that covers all service traffic originating from this VPC

# VPC interface endpoint (powered by PrivateLink)



The “interface VPC endpoint” is reachable at a private IP address within the VPC

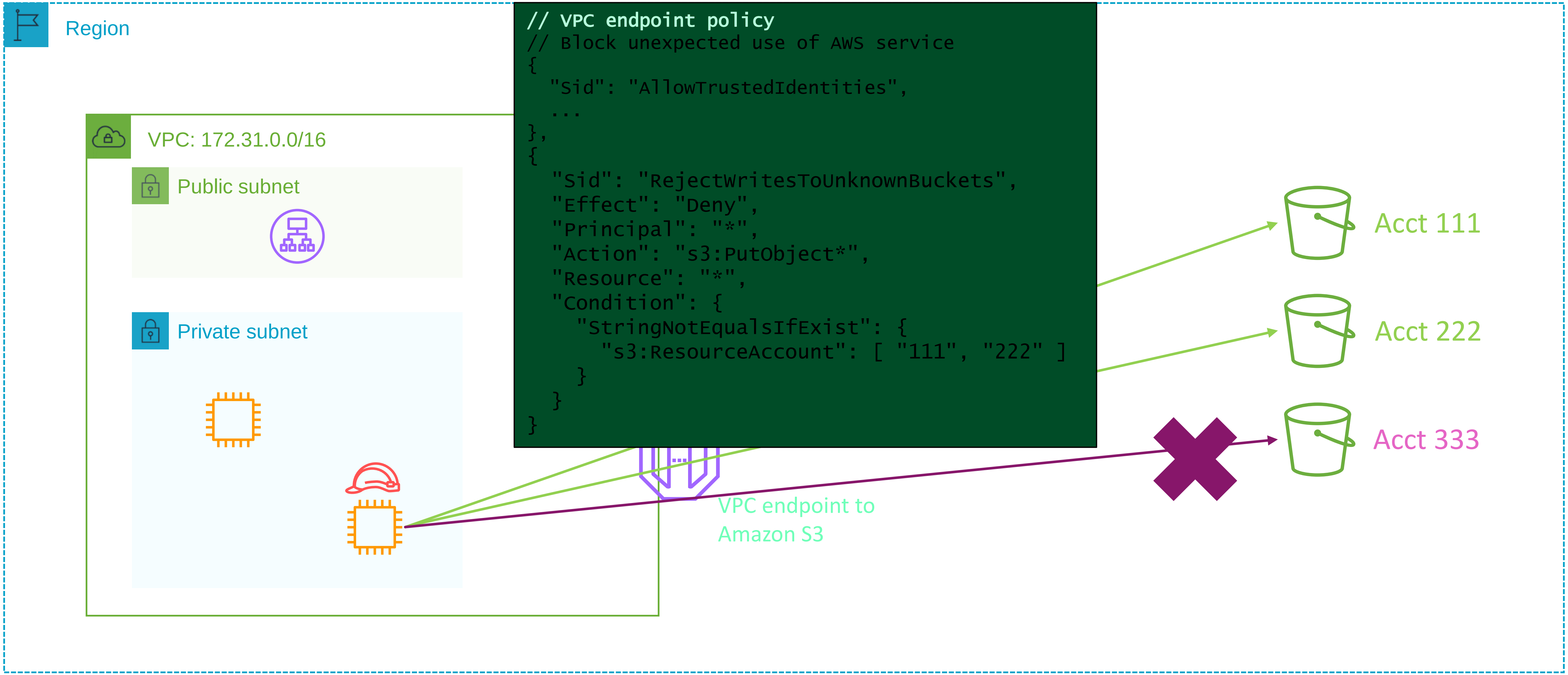
# VPC endpoints: Authorization example



Requests that originate from a VPC endpoint will have `aws:SourceVpc` and `aws:SourceVpce` set

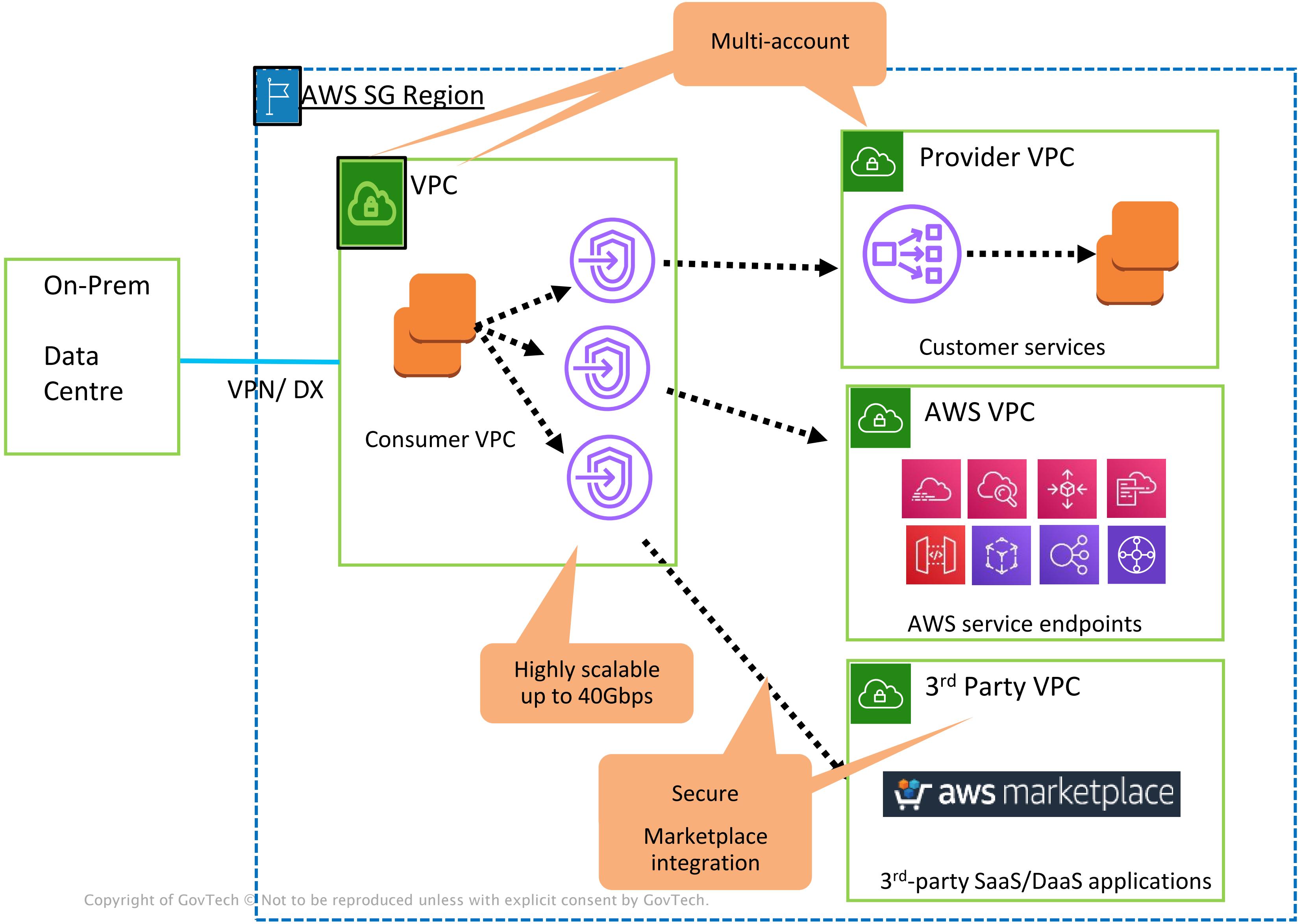
```
// S3 bucket policy statement:
// Block reads from unexpected networks
{
  "Sid": "RequireExpectedNetworks",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::this-bucket/*",
  "Condition": {
    "StringNotEqualsIfExist": {
      "aws:SourceVpc": "vpc-11112222"
    }
  }
}
```

# Using VPCE policies to enforce Perimeter rules



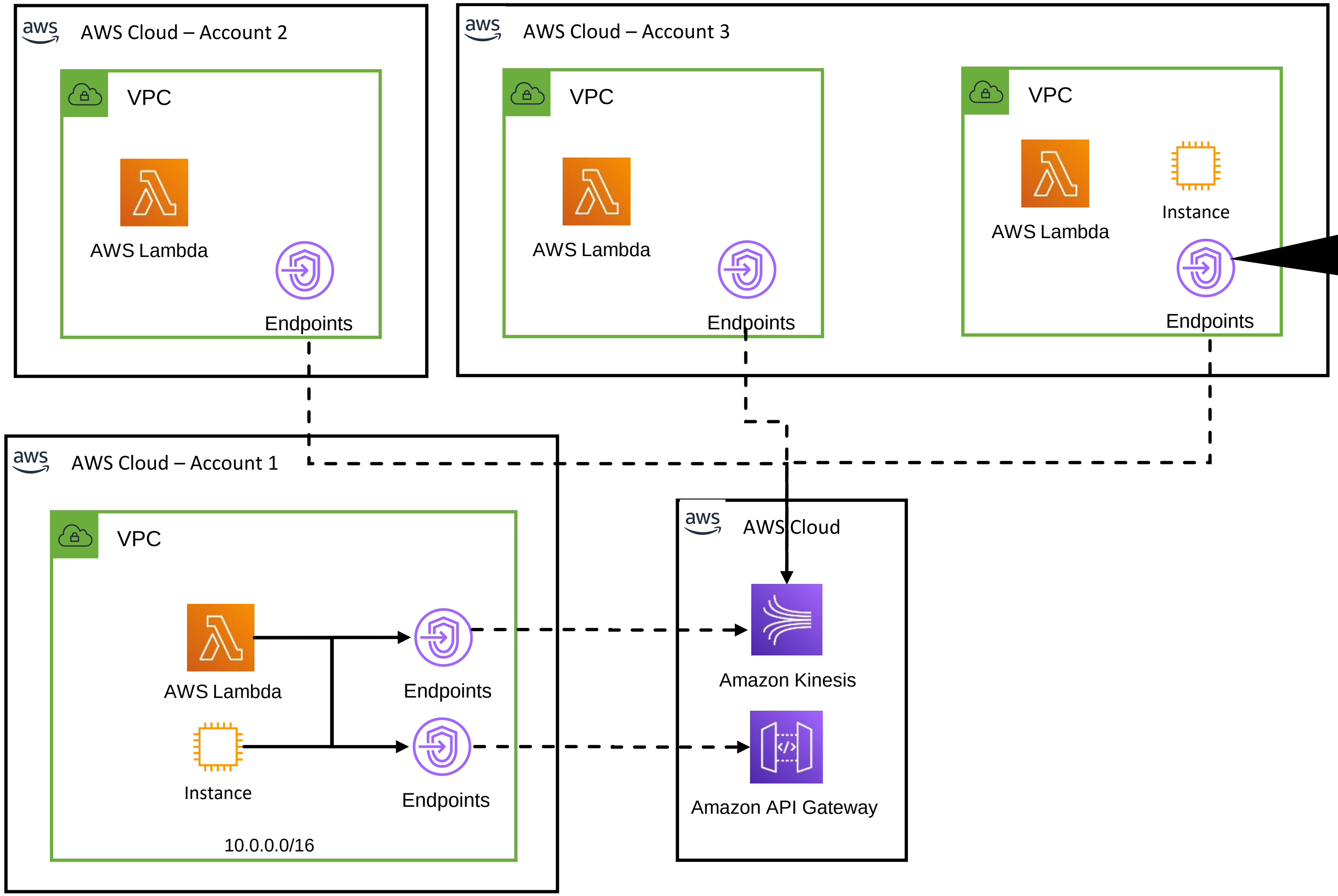
```
// VPC endpoint policy
// Block unexpected use of AWS service
{
  "Sid": "AllowTrustedIdentities",
  ...
},
{
  "Sid": "RejectWritesToUnknownBuckets",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject*",
  "Resource": "*",
  "Condition": {
    "StringNotEqualsIfExist": {
      "s3:ResourceAccount": [ "111", "222" ]
    }
  }
}
```

# VPC Interface Endpoints – Use Cases



- Ensure security, privacy, and compliance
- Reduce costs
- Add agility
- Enable hybrid cloud

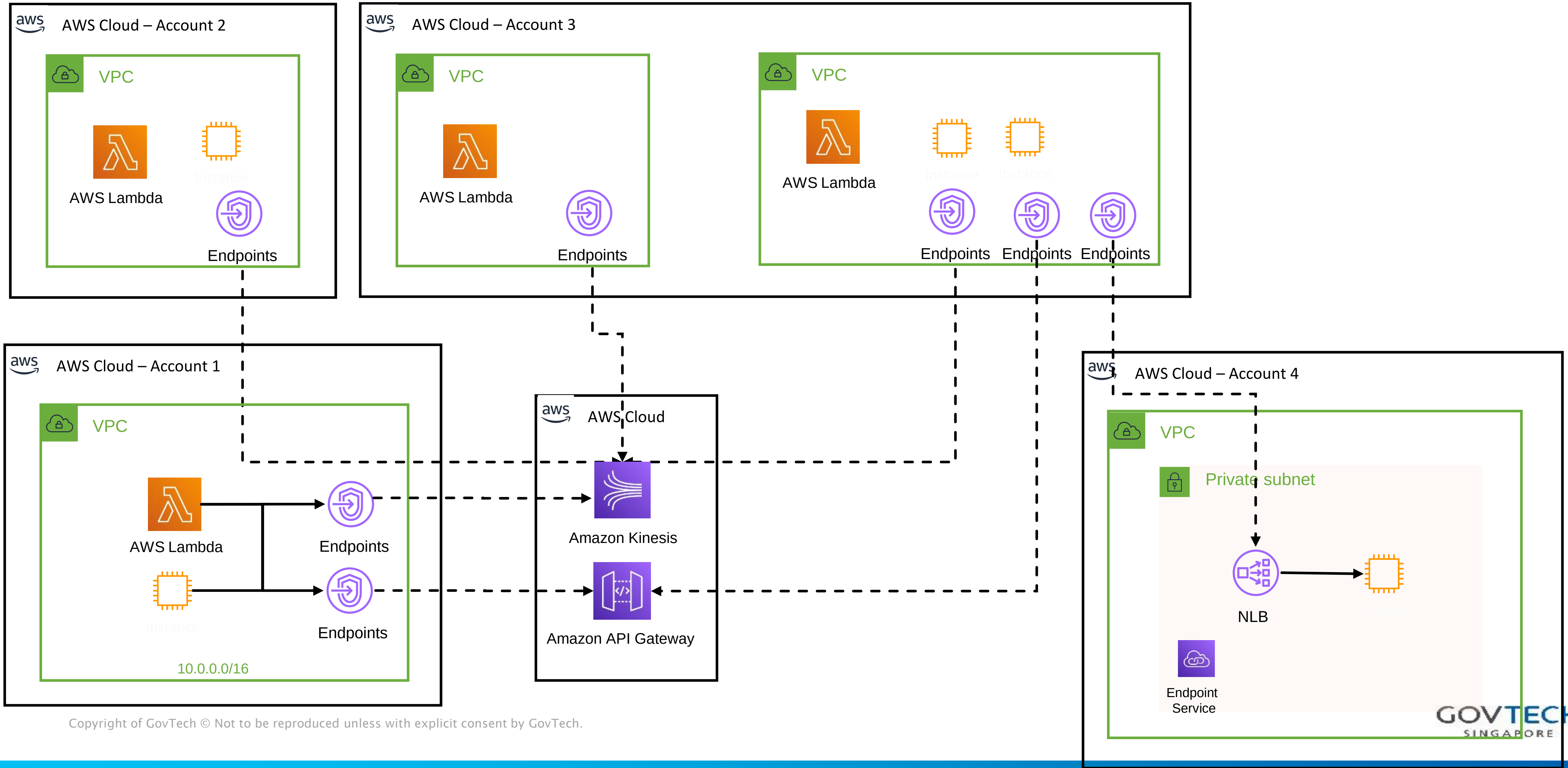
# Decentralized Endpoint Architecture



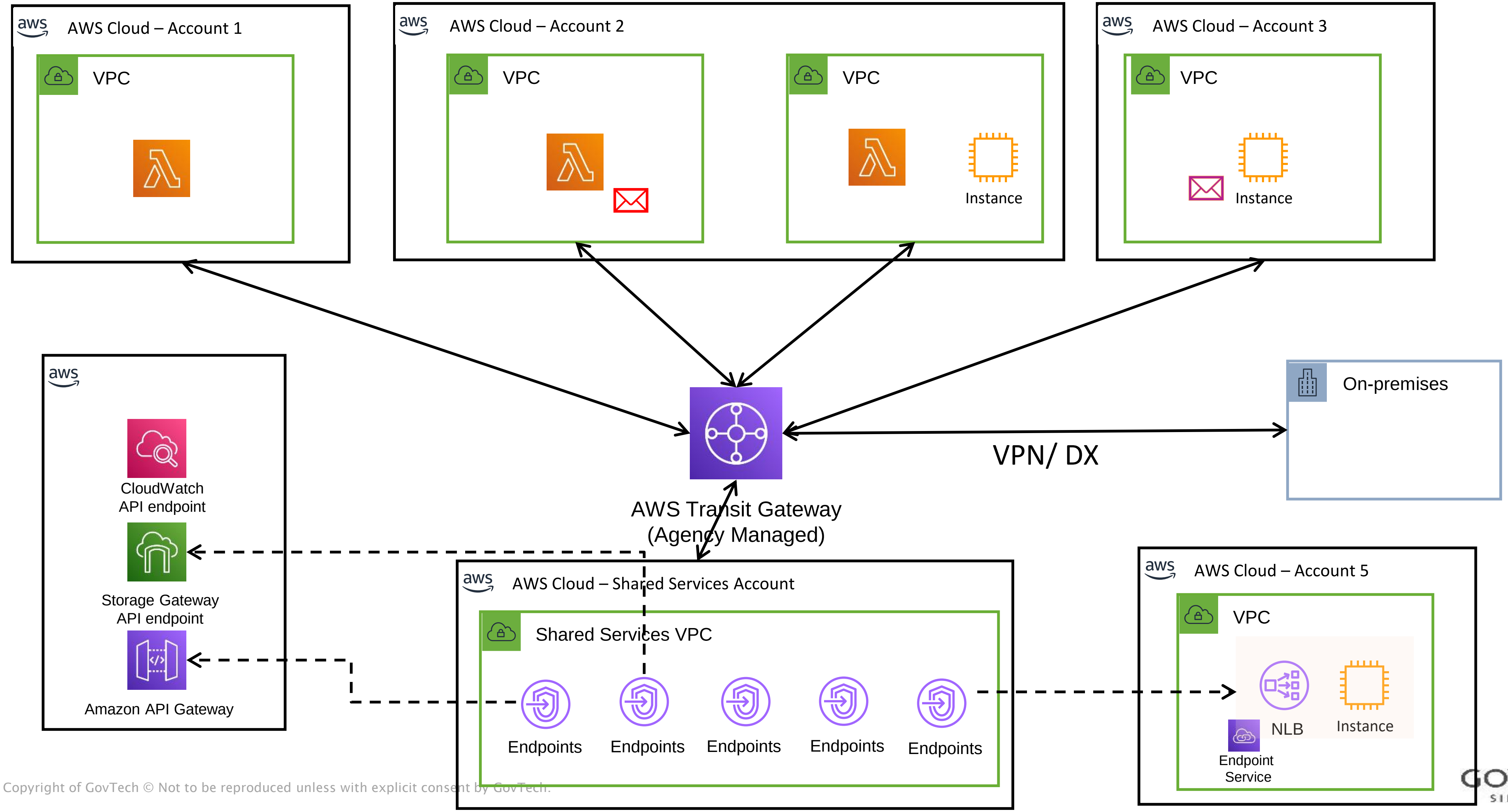
## ENDPOINT POLICY

```
{
  "Statement":[
    {
      "Effect":”Allow",
      "Principal":"*",
      "Action":"kinesis:*",
      "Resource":
        "arn:aws:kinesis:region:account-
id:stream/stream-name”
    }
  ]
}
```

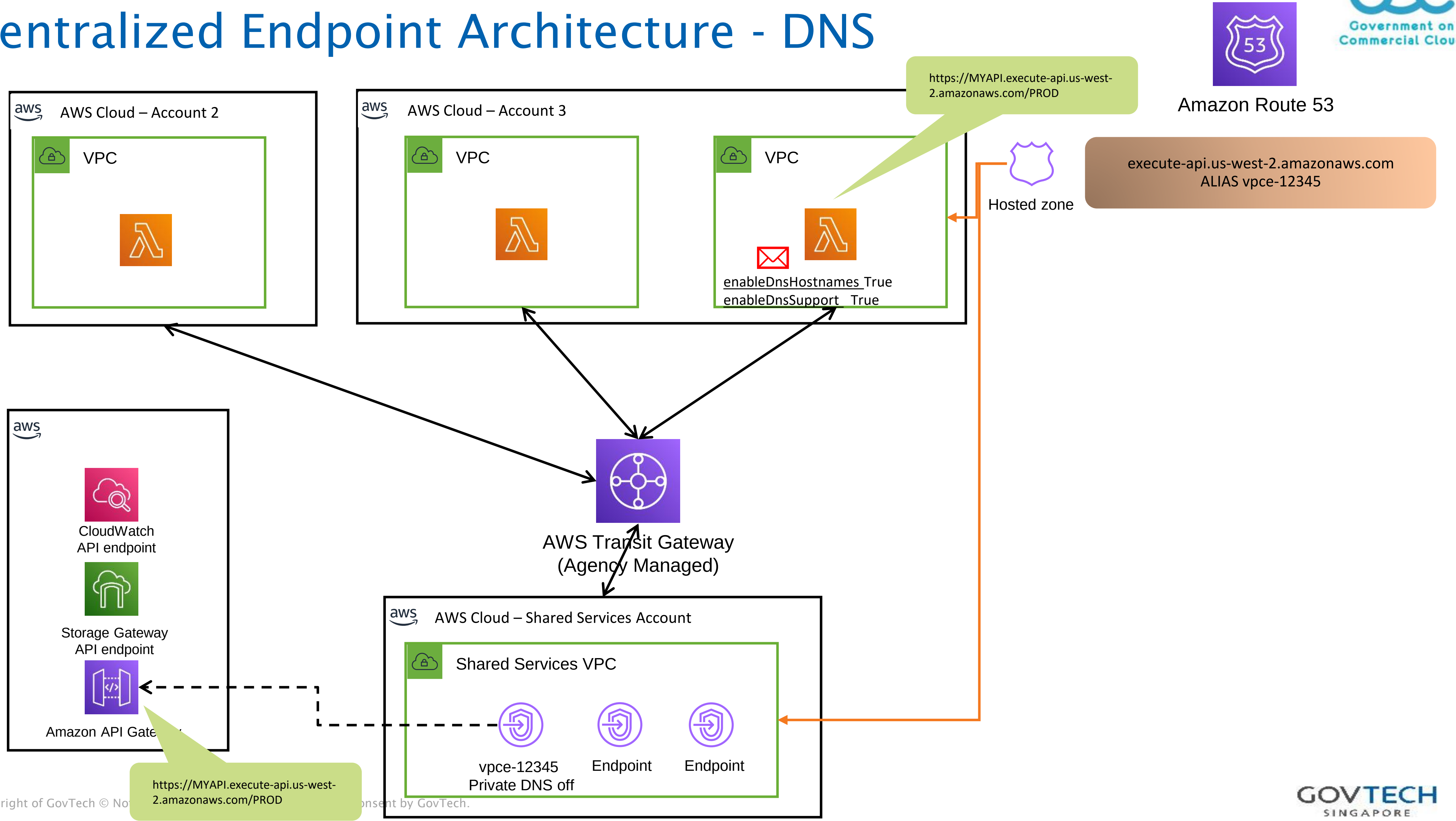
# Decentralized Endpoint Architecture



# Centralized Endpoint Architecture – TGW( Agency Managed )



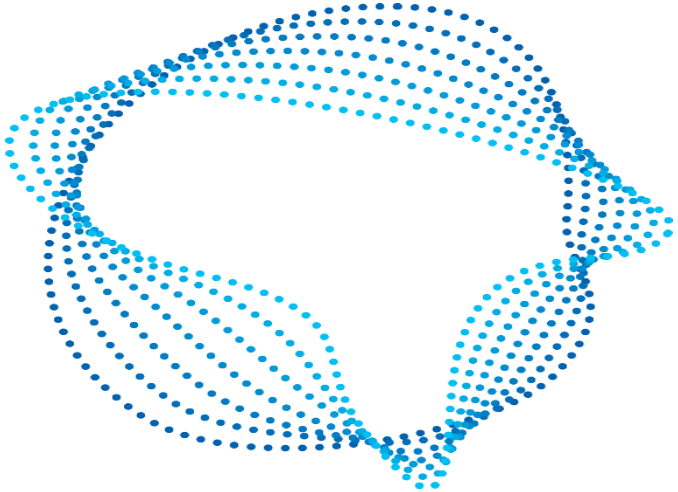
# Centralized Endpoint Architecture - DNS



https://MYAPI.execute-api.us-west-2.amazonaws.com/PROD

https://MYAPI.execute-api.us-west-2.amazonaws.com/PROD

AWS Elastic LBs and Gateway LB



# Elastic Load Balancers(ALB/NLB) & Gateway Load Balancer

GOVTECH SINGAPORE

# Elastic Load Balancing Overview

## Benefits

- Distributed incoming traffic across multiple targets
- TLS offloading and user authentication
- Capable of handling rapid changes in traffic
- Cost effective

## Key advancements

- Support for redirects and fixed responses
- Slow start support for newly registered targets
- Cross-zone load balancing for Network Load Balancer
- Application Load Balancer support for user authentication
- Tag-based filtering in API and Management Console

Application Load Balancer | Network Load Balancer | Gateway Load Balancer

# Application Load Balancer

Target EC2 instances, Lambda functions, and IP-based endpoints

Broad protocol support including grpc, WebSockets, HTTP, HTTP/2, SSL, and IPv6

Application resiliency with integrated high availability, health checks, and monitoring

Content-based routing, session-affinity, and integrated user authentication

✓ Target workloads across AWS and on-prem

✓ Integrate with AWS WAF and Global Accelerator

✓ Connect your Kubernetes environment with ALB Ingress Controller

✓ Build secure apps with HTTP Guardian and S2N

# Network Load Balancer

Target EC2 instances and IP-based endpoints

Protocol support including TCP, UDP, TLS, ALPN, and IPv6

Application resiliency with integrated high availability, health checks, and monitoring

Support for static IP, source IP preservation, and sticky sessions

- ✓ Target workloads across AWS and on-prem
- ✓ Seamlessly react to sudden changes in application load
- ✓ Build more resilient apps with zonal awareness
- ✓ Improve target performance by offloading TLS at the NLB

# Gateway Load Balancer

INTRODUCING

## Gateway Load Balancer

Reduce complexity and deploy faster

Elastically scale and reduce costs

Improve appliance availability

Supported by leading appliance vendors

# Network appliances

Transparent to network traffic

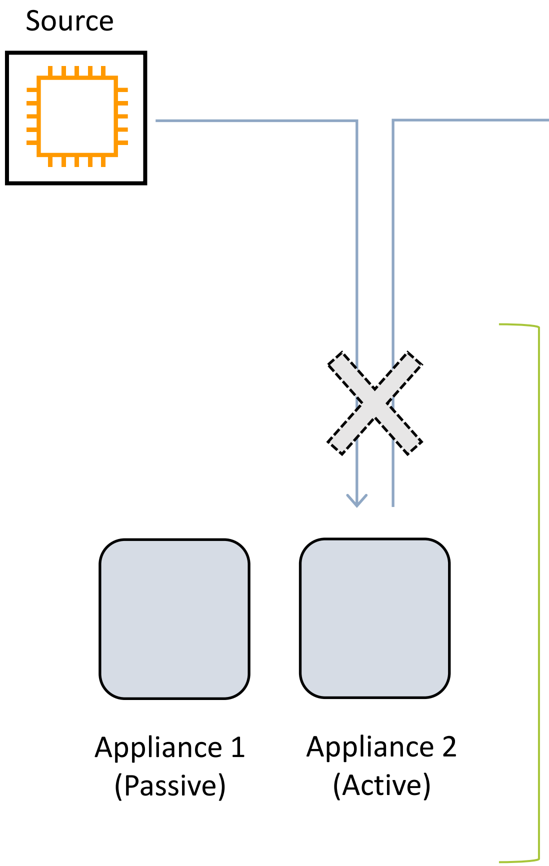
Security, monitoring, analytics, and other use cases

Often required by policy, or due to expertise and investment

Use the same Network Appliances on AWS and Hybrid Environments

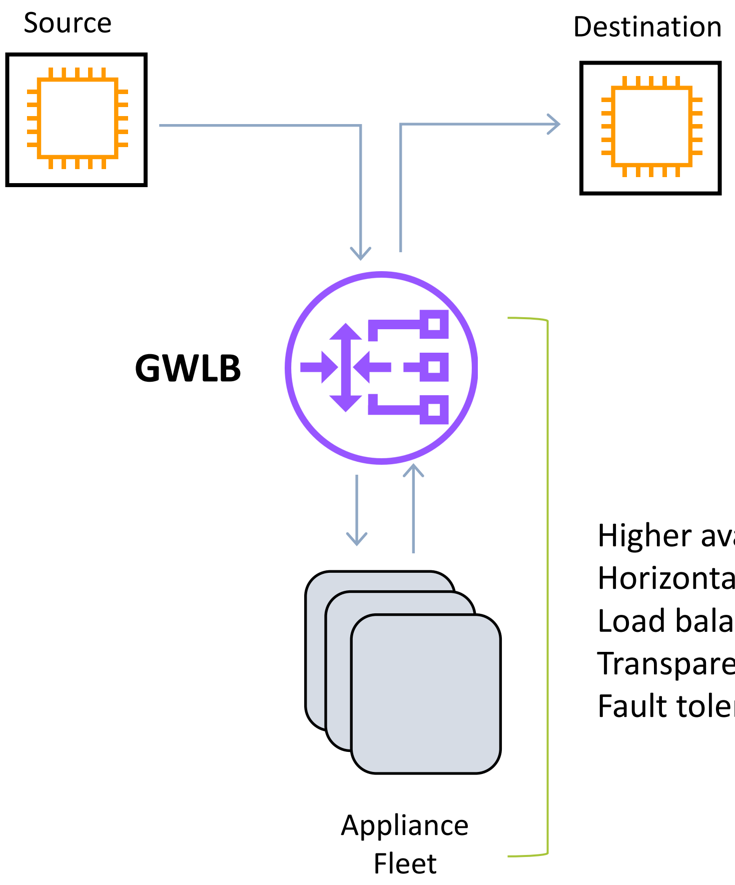
# Challenges today and benefits now available

## **Before** Gateway Load Balancer



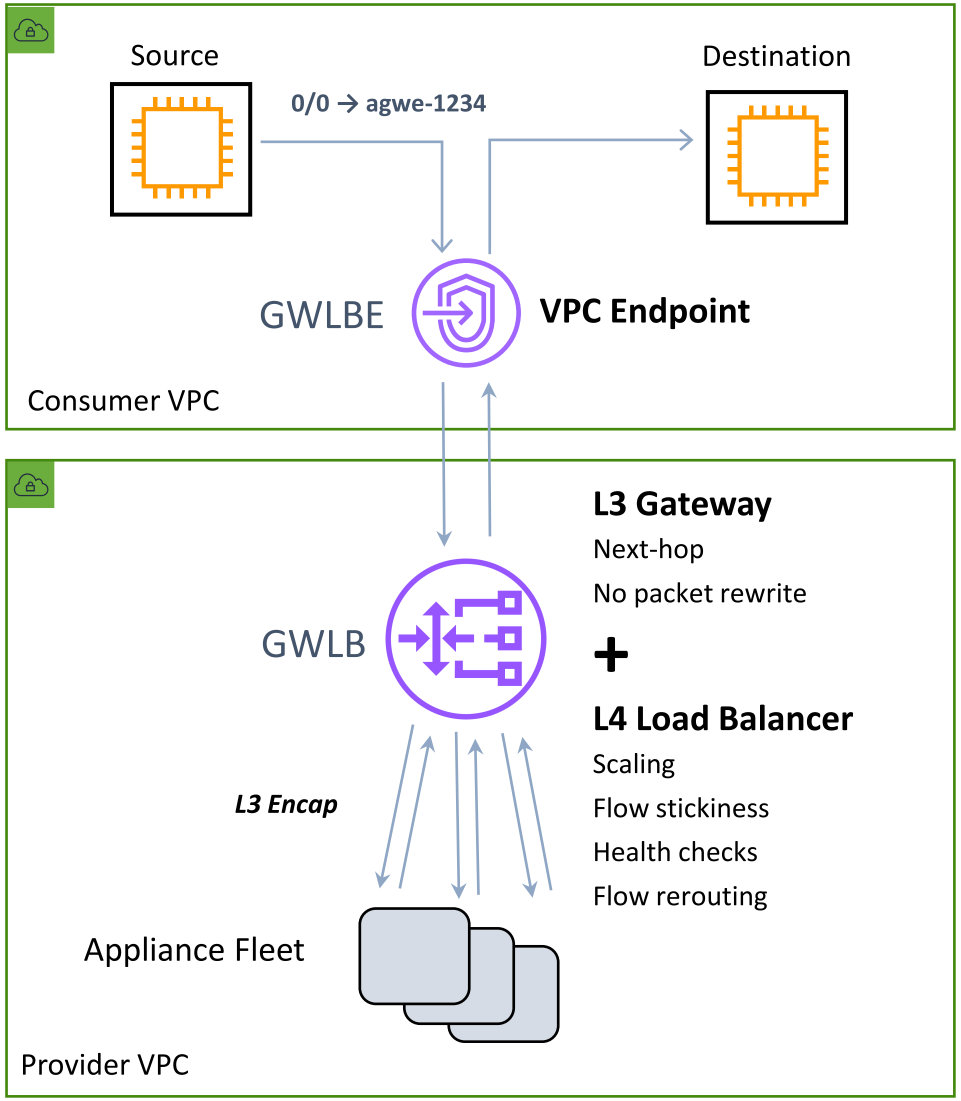
Central point of failure
Limited scale
Passive appliances sit idle
Mixed admin domains

## **After** Gateway Load Balancer



Higher availability
Horizontal scaling
Load balancing
Transparent
Fault tolerant

# Gateway Load Balancer: At-a-glance



## Components

- Gateway Load Balancer Endpoint (GWLBE) - A new type of VPC endpoint that can be a next-hop in a VPC route table
- Gateway Load Balancer (GWLB) - A new type of load balancer that includes L3 Gateway + L4 Load Balancer capabilities
- Both components powered by AWS Hyperplane

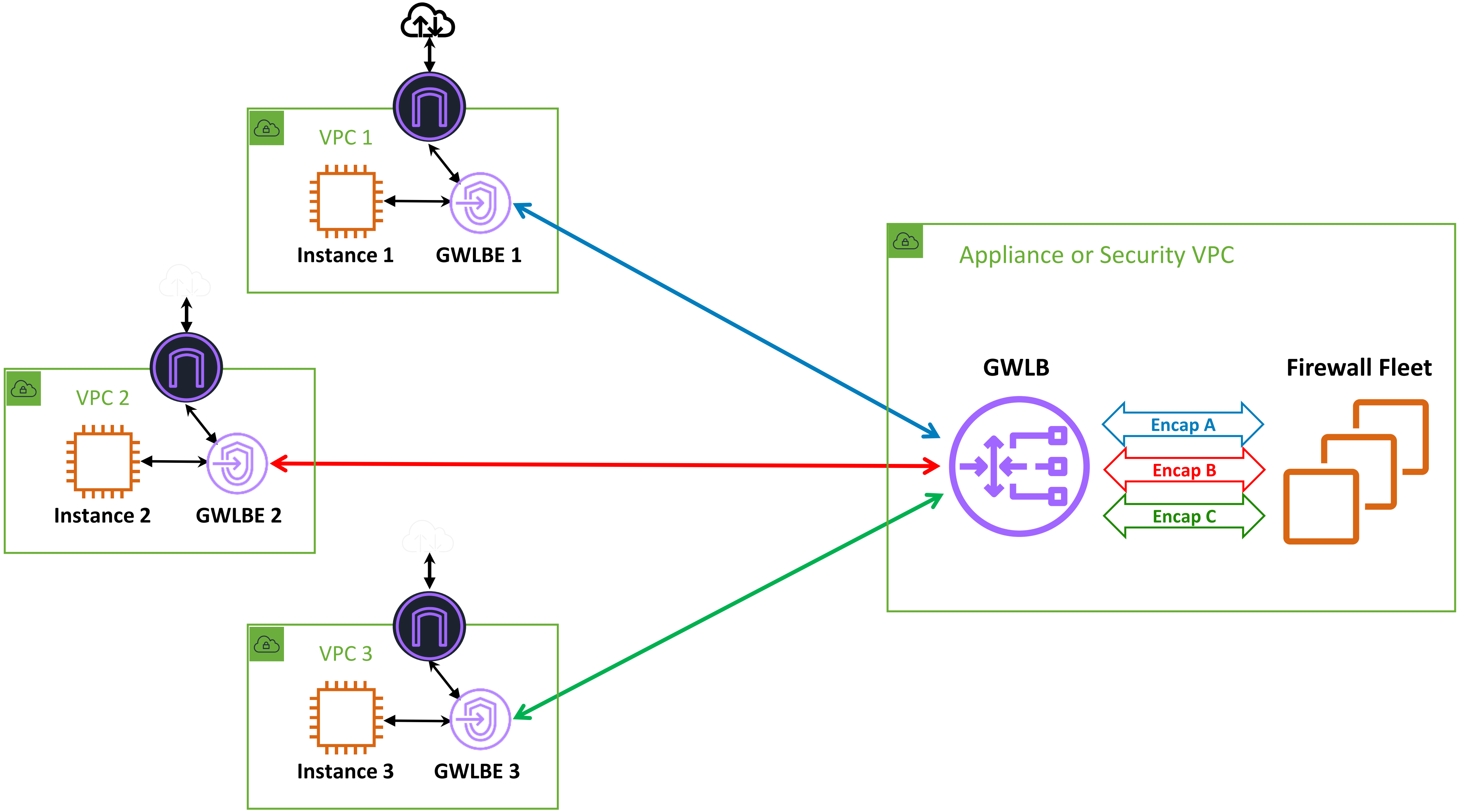
## Benefits

- Provide horizontal scaling to appliances
- Provide fault tolerance to appliances
- Transparent to network traffic, no change to source traffic
- Separate security and user admin domains, share across different VPCs and AWS accounts
- Provide appliance-as-a-service, (e.g. Firewall-as-a-service)

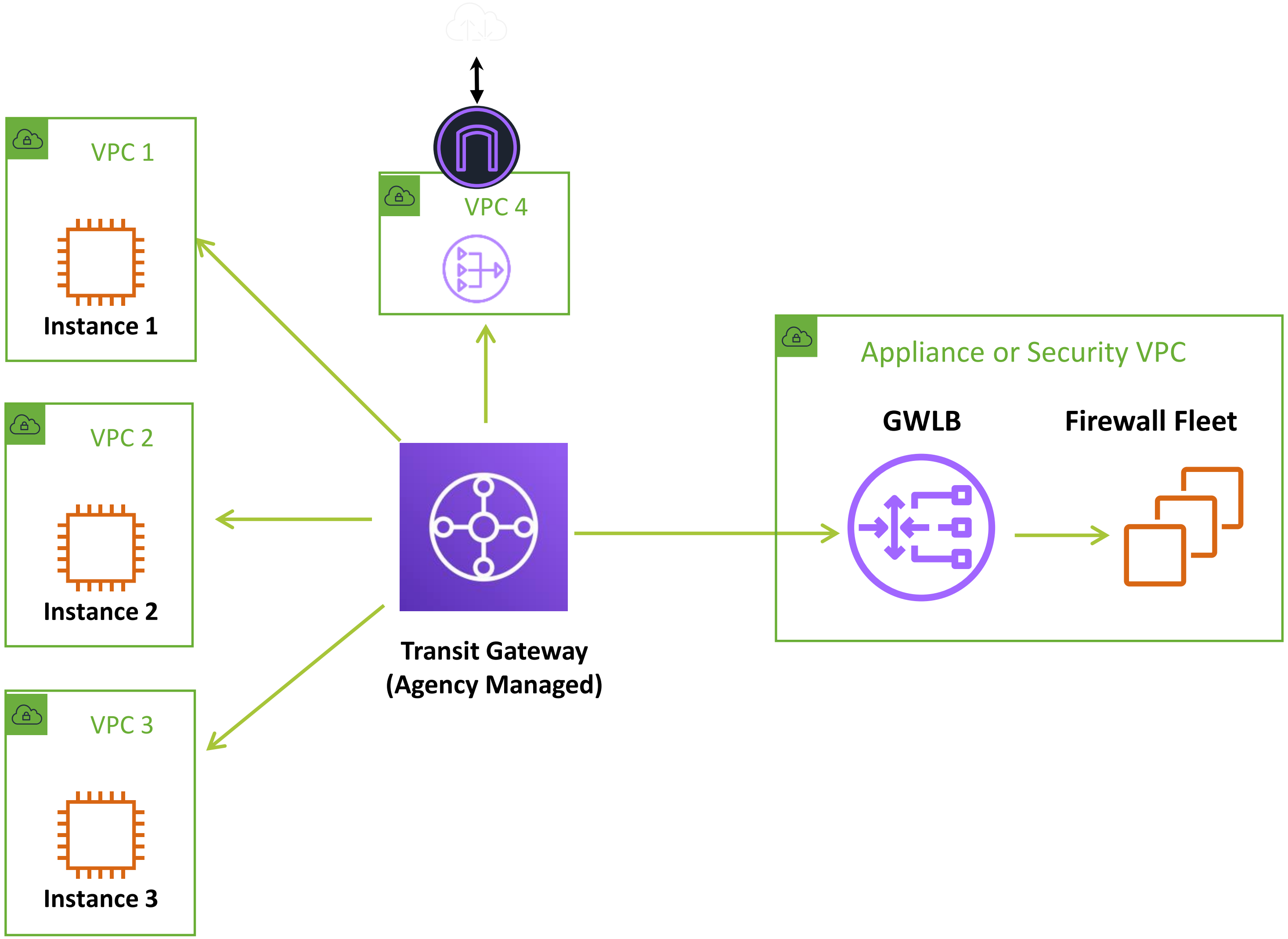
## Deployment

- Create GWLB and appliance fleet using steps similar to NLB
- Send traffic to GWLB/GWLBE by updating VPC route tables

# Distributed security inspection with GWLB



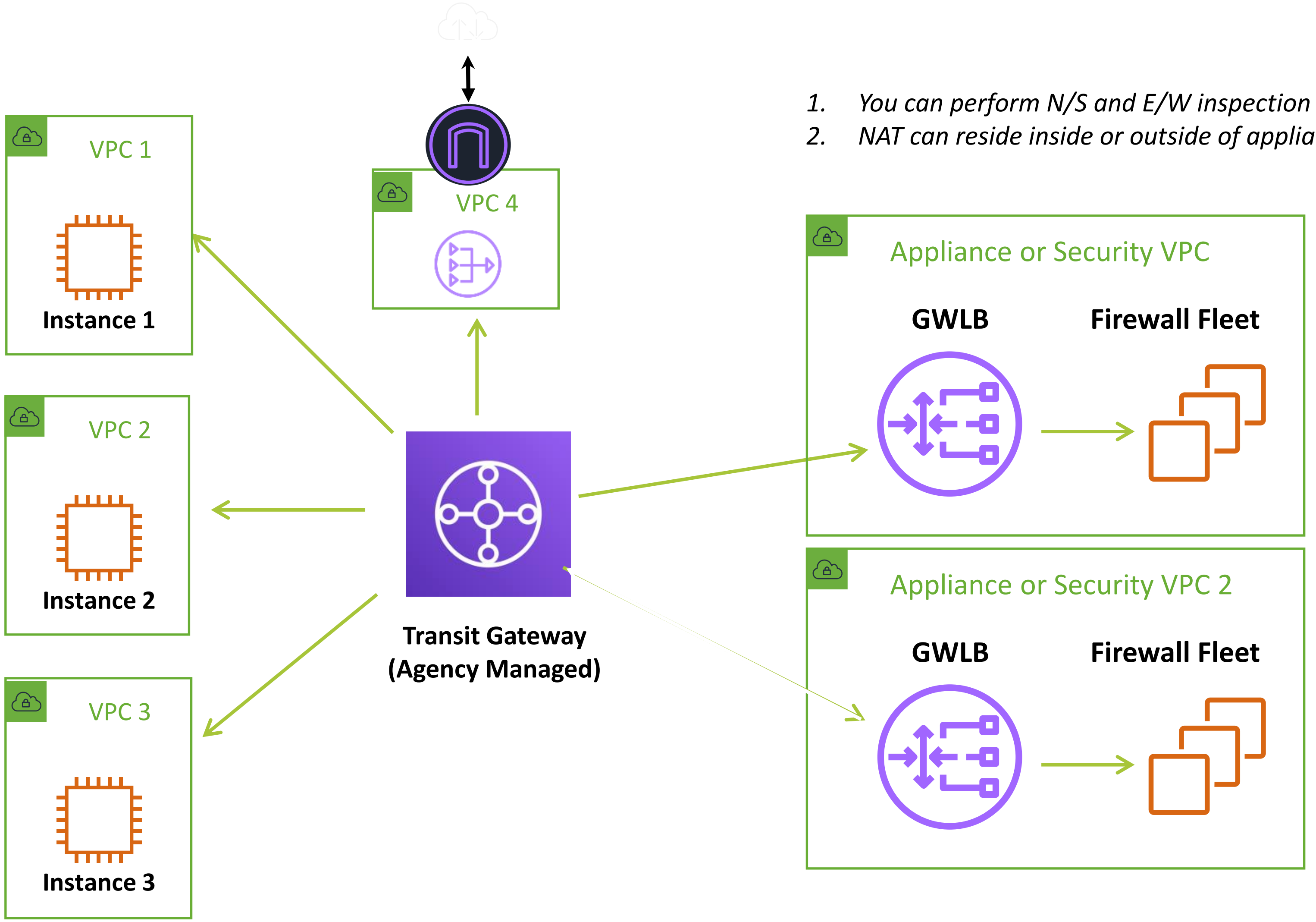
# Centralized security inspection with TGW( Agency Managed )



North-south inspection
(Traffic to/from internet)

# VPC to VPC Inspection with TGW( Agency Managed )

1. *You can perform N/S and E/W inspection using same fleet.*
2. *NAT can reside inside or outside of appliance fleet VPC*



North-south inspection
(Traffic to/from internet)

East-west inspection
(VPC to VPC traffic)

# THANK YOU

Questions and Answers

# We Want to Hear Your Feedback!

https://form.gov.sg/625cbdaa5ea46200123d92c5

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg