



Making PrivateLink The New Normal

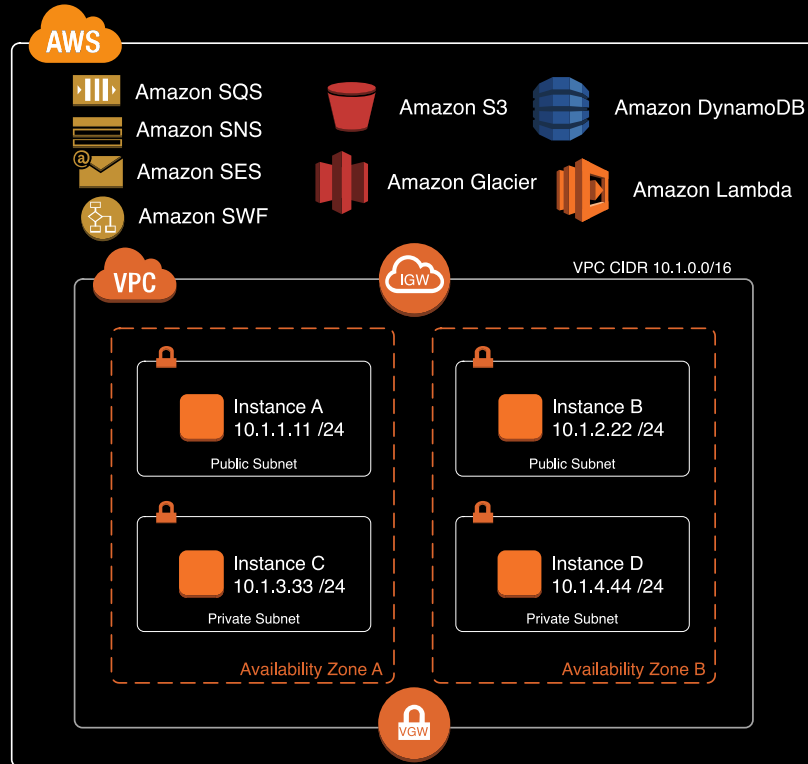
May 2018

Nick Matthews, Principal Solutions Architect

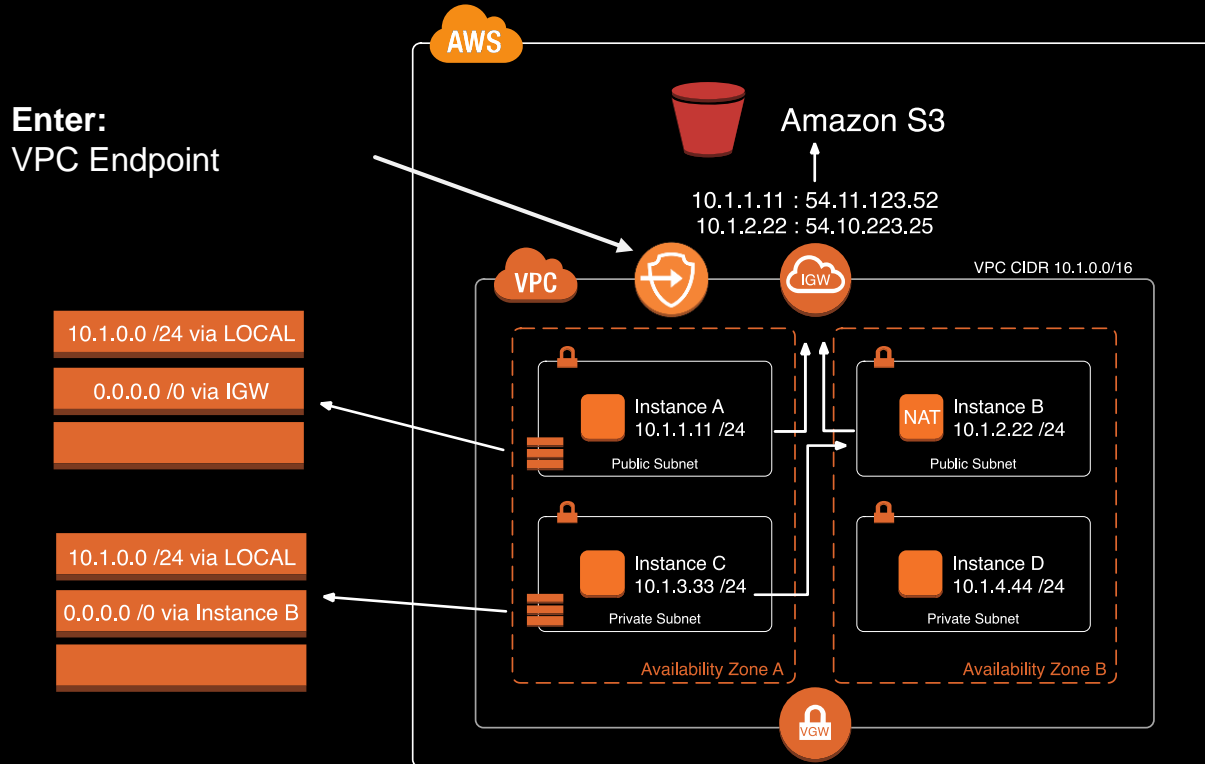
 @nickpowpow



VPC Endpoint **Introduction**



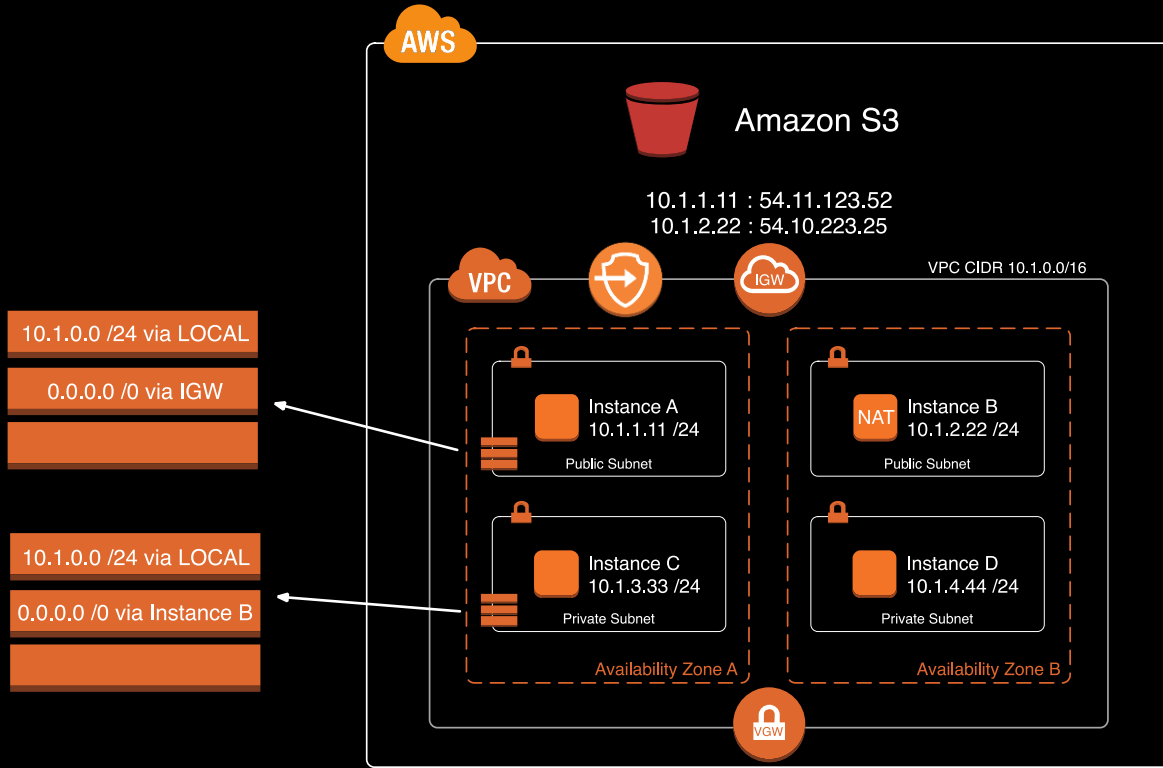
Public Access to Amazon S3



Without Endpoints:

- Instances need public connectivity
- Security groups required to block outside access
- Mindset that customers are traversing the public internet

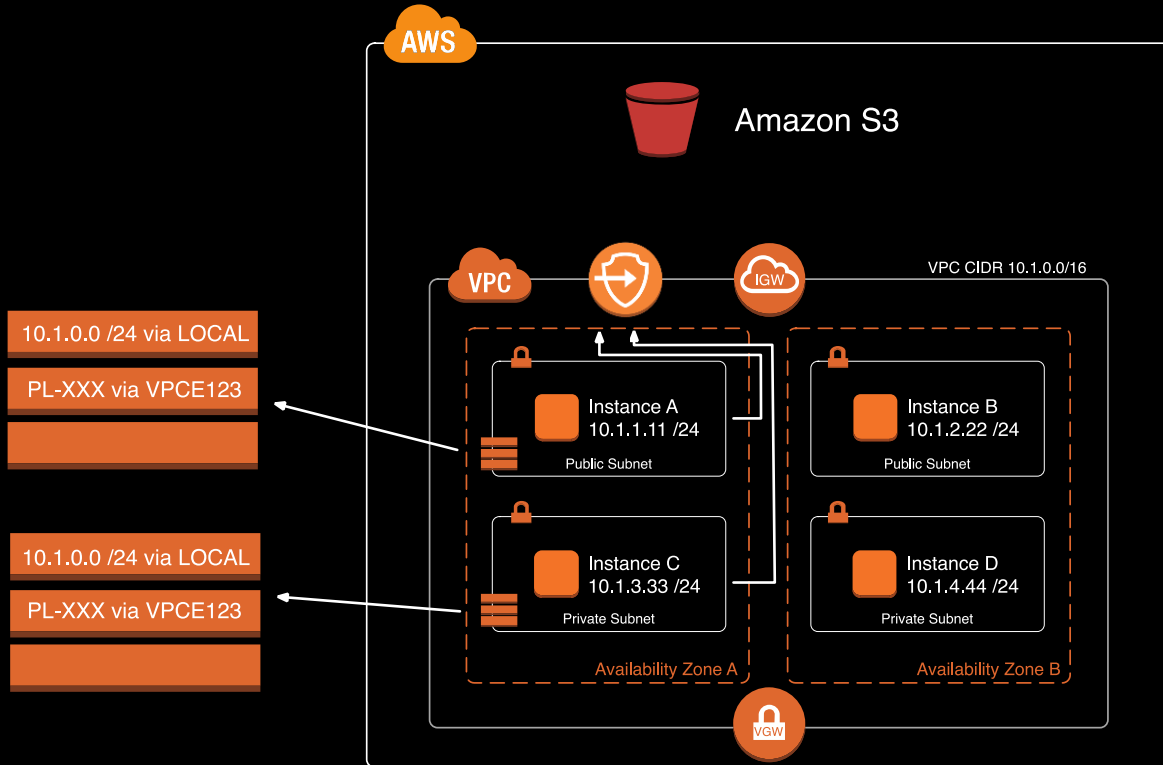
VPC Endpoints for Amazon S3



We no longer need the following for Amazon S3 access:

- Public addresses per instance
- Default routes pointing to an internet gateway
- NAT Instances
- Or even an internet gateway!

VPC Endpoints for Amazon S3



After the VPCE is created:

- "Prefix-List" entries are needed for each route table.
- Now all traffic for the PL-XXX destinations will traverse the VPCE instead of the internet gateway.

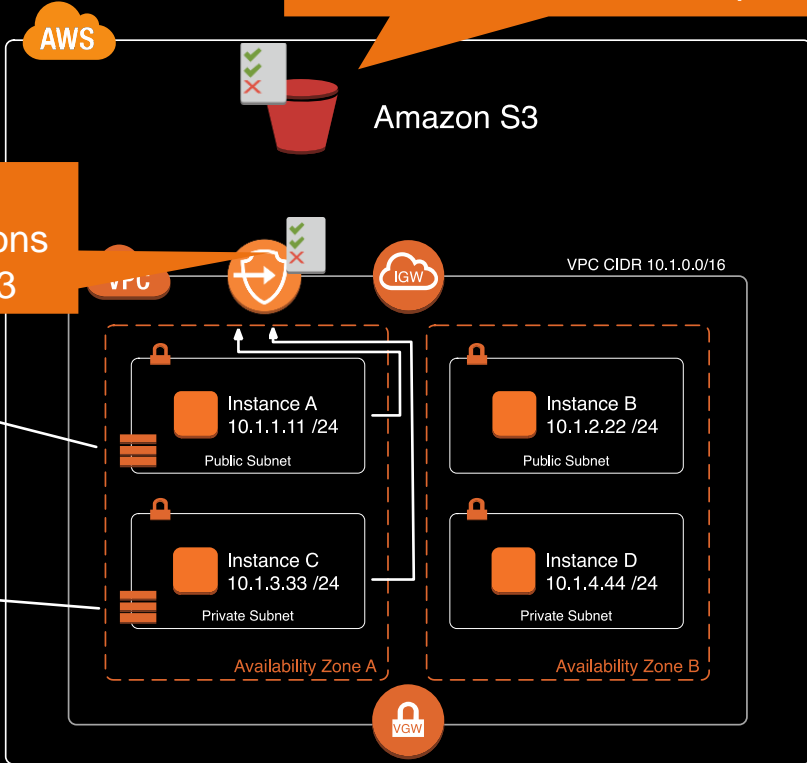
VPC Endpoints for Amazon S3

IAM Policy at S3 Bucket: Make accessible from VPC Endpoint only

IAM Policy at VPC Endpoint: Restrict actions of VPC in Amazon S3

- 10.1.0.0 /24 via LOCAL
- PL-XXX via VPCE123

- 10.1.0.0 /24 via LOCAL
- PL-XXX via VPCE123



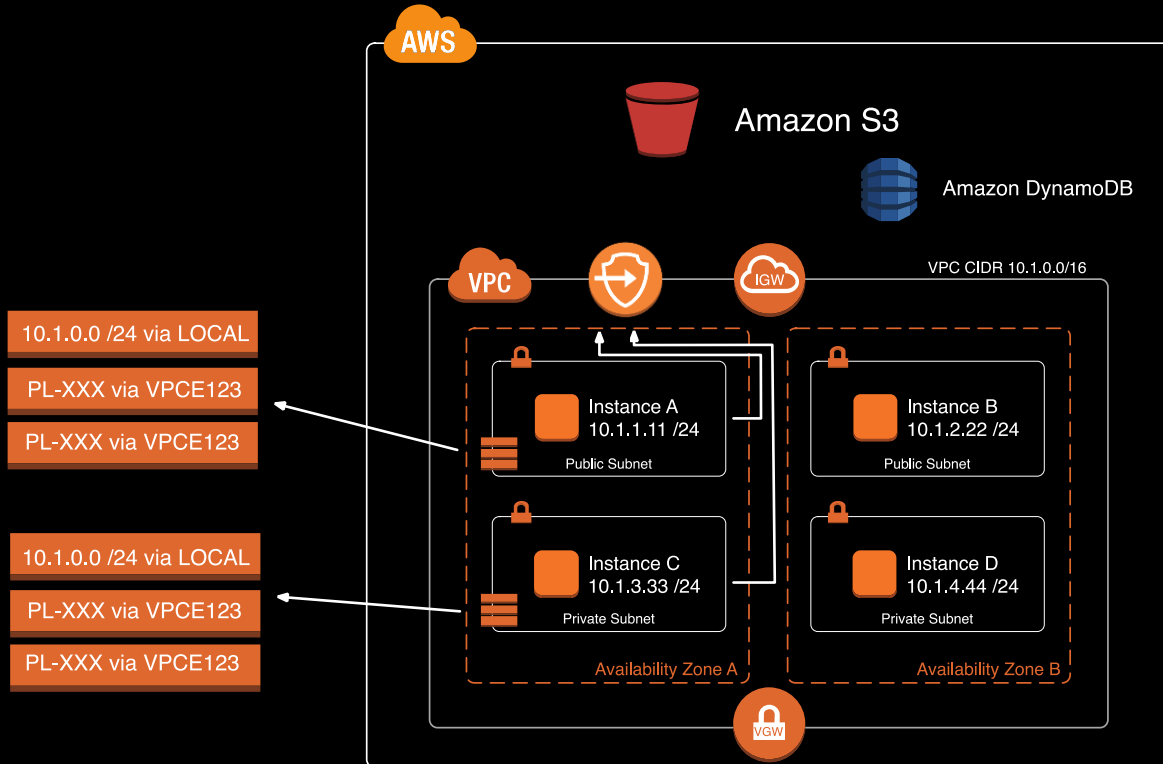
Restricting Access to Amazon S3:

- IAM Policy at VPC Endpoints restricting access
- IAM Policy at S3 bucket restricting access



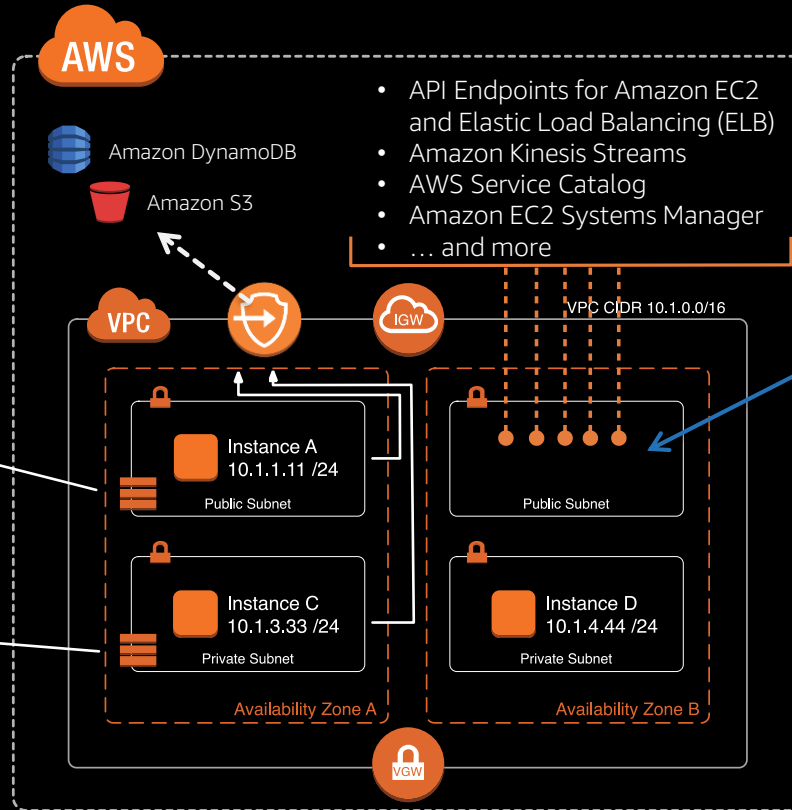
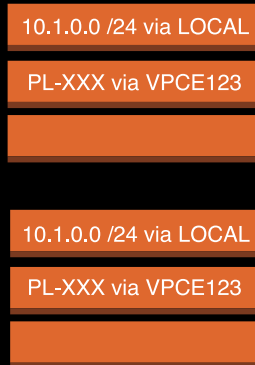
VPC Endpoints for Amazon S3

Other services like Amazon DynamoDB



Introducing PrivateLink for AWS Services

- No Route Table update required



AWS PrivateLink:

- PrivateLink is a way to reach additional public services, privately from your VPC

Each PrivateLink VPCE consists of multiple network interfaces, using IP addresses from the assigned subnets

Introducing PrivateLink for AWS Services

- No Route Table update required

10.1.0.0 /24 via LOCAL
PL-XXX via VPCE123



AWS PrivateLink:

- PrivateLink is a way to reach additional public services, privately from your VPC

Each PrivateLink VPCE consists of multiple network interfaces, using IP addresses from the assigned subnets

ec2.eu-west-1.amazonaws.com

AWS PrivateLink

How it works

Endpoints > Create Endpoint

Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service. An interface endpoint is powered by [PrivateLink](#), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.

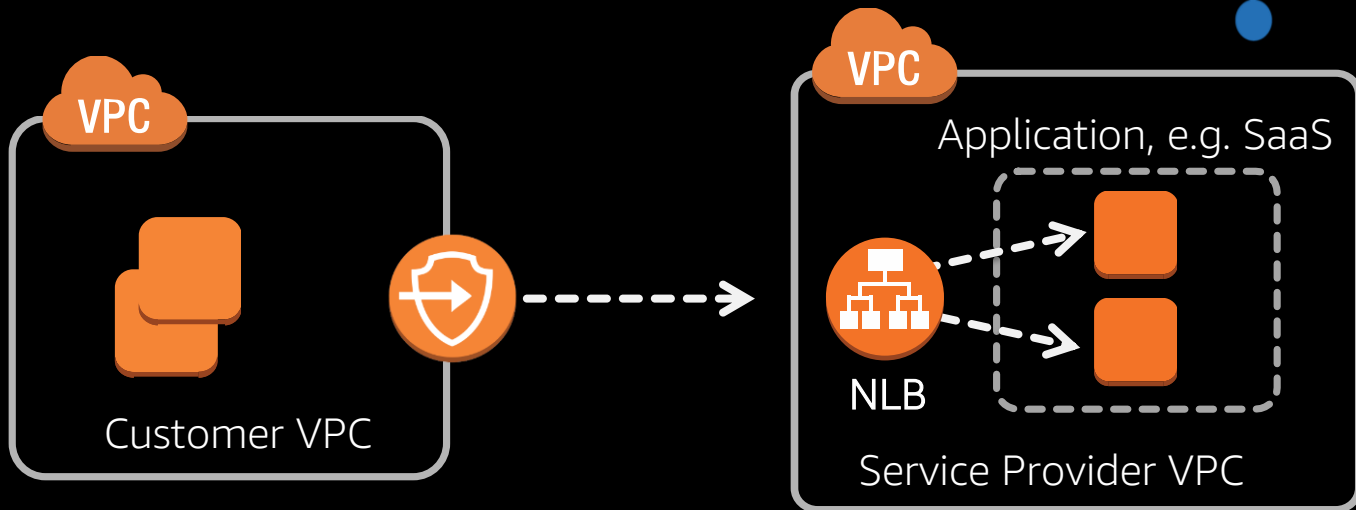
Service Name	Owner	Type
<input type="radio"/> com.amazonaws.us-east-2.dynamodb	amazon	Gateway
<input type="radio"/> com.amazonaws.us-east-2.ec2	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-2.ec2messages	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-2.elasticloadbala...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-2.kinesis-streams	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-2.kms	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-2.s3	amazon	Gateway
<input type="radio"/> com.amazonaws.us-east-2.servicecatalog	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-2.sns	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-2.ssm	amazon	Interface

Type: Gateway

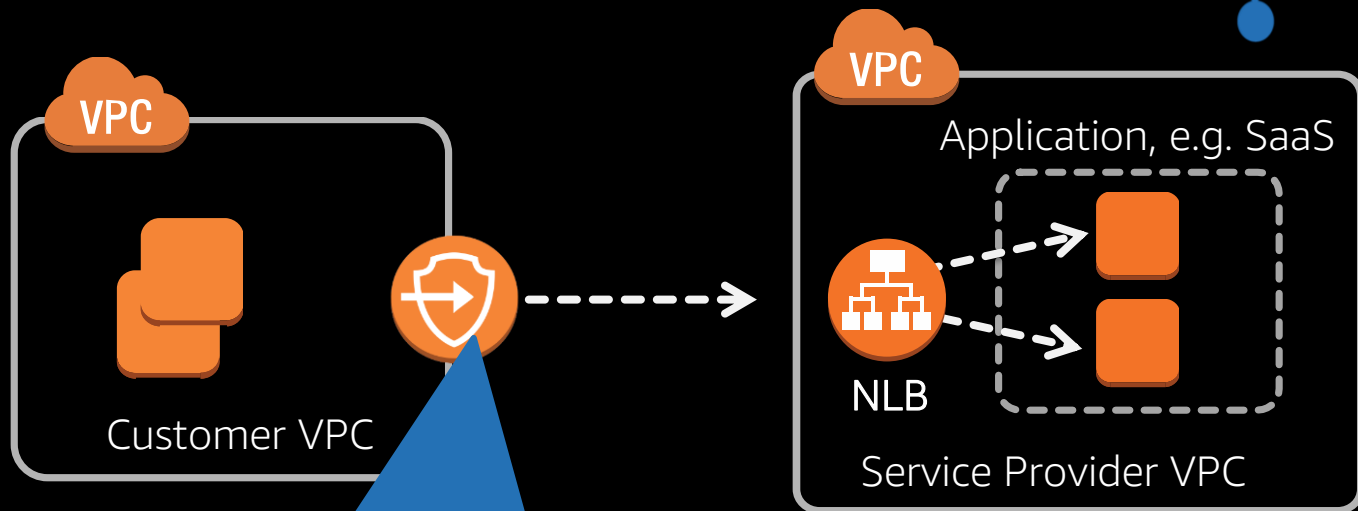
Type: Interface

amazon	Gateway	
amazon	Interface	
amazon	Interface	
a...	amazon	Interface
ms	amazon	Interface
amazon	Interface	
amazon	Gateway	
og	amazon	Interface
amazon	Interface	
amazon	Interface	

And now AWS PrivateLink for service providers

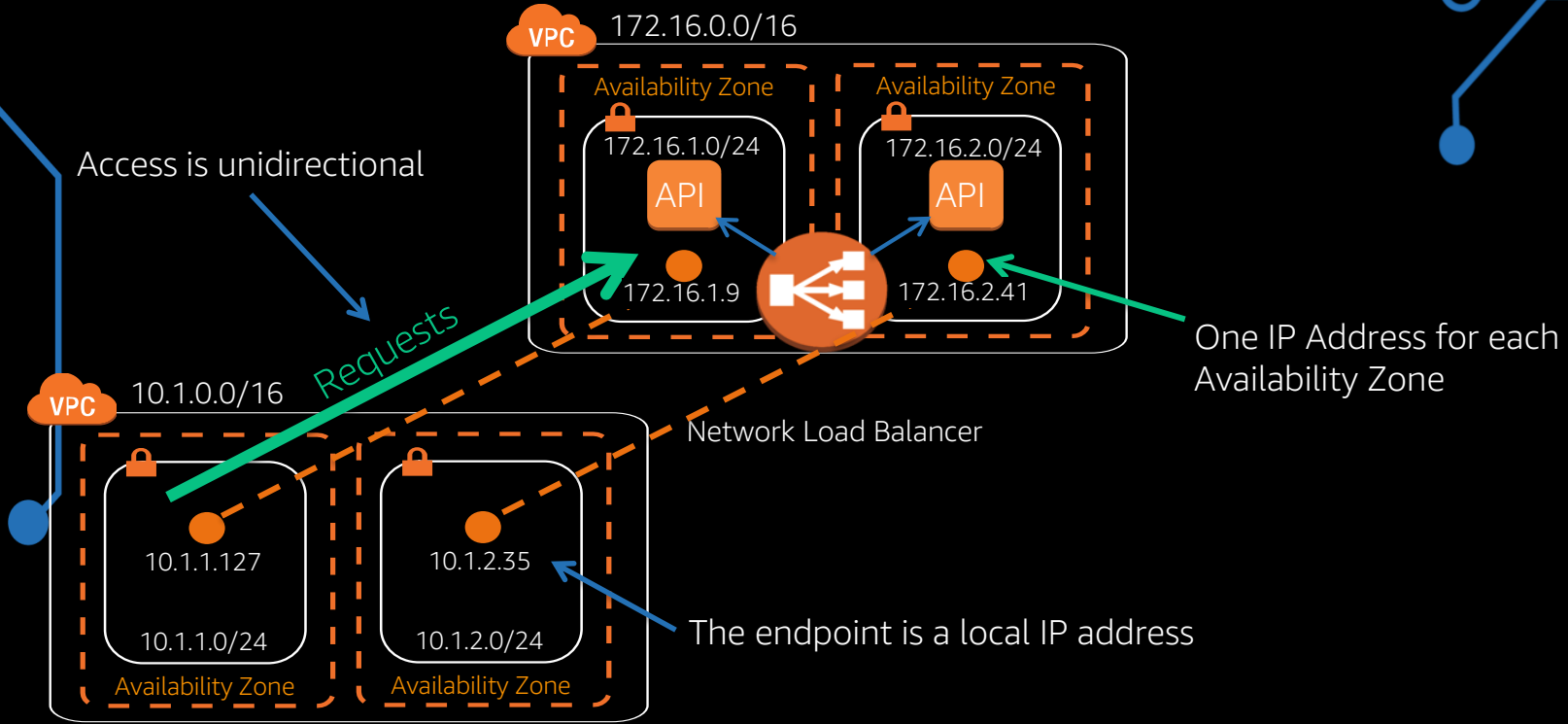


And now AWS PrivateLink for service providers



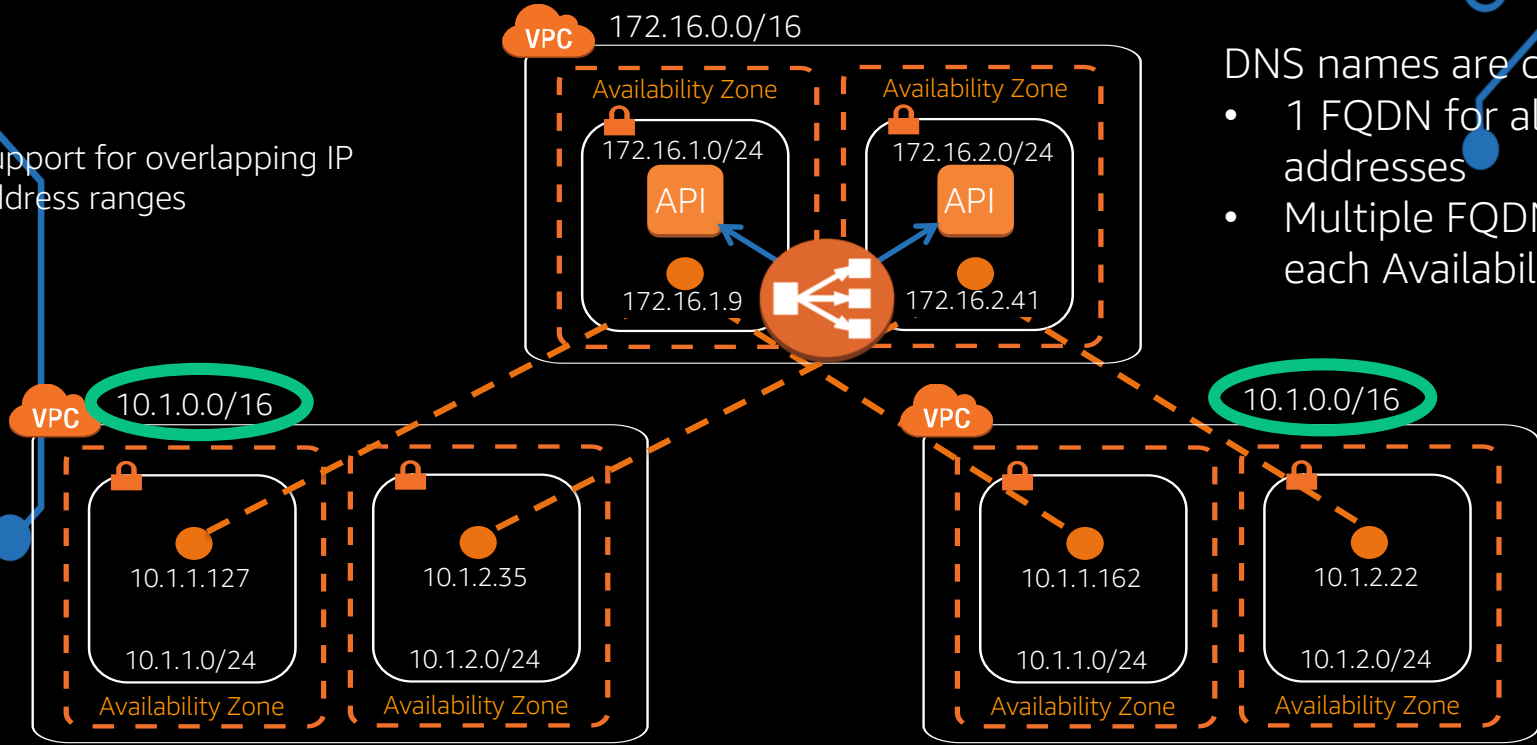
VPC Endpoint: vpce-2222.foo.amazon.com

PrivateLink – How it Works



PrivateLink – How it Works

Support for overlapping IP address ranges



DNS names are created:

- 1 FQDN for all IP addresses
- Multiple FQDNs, one for each Availability Zone

...thousands

VPC Endpoint: `vpce-xxxx.vpce-svc-xxxx.us-east-2.vpce.amazonaws.com`



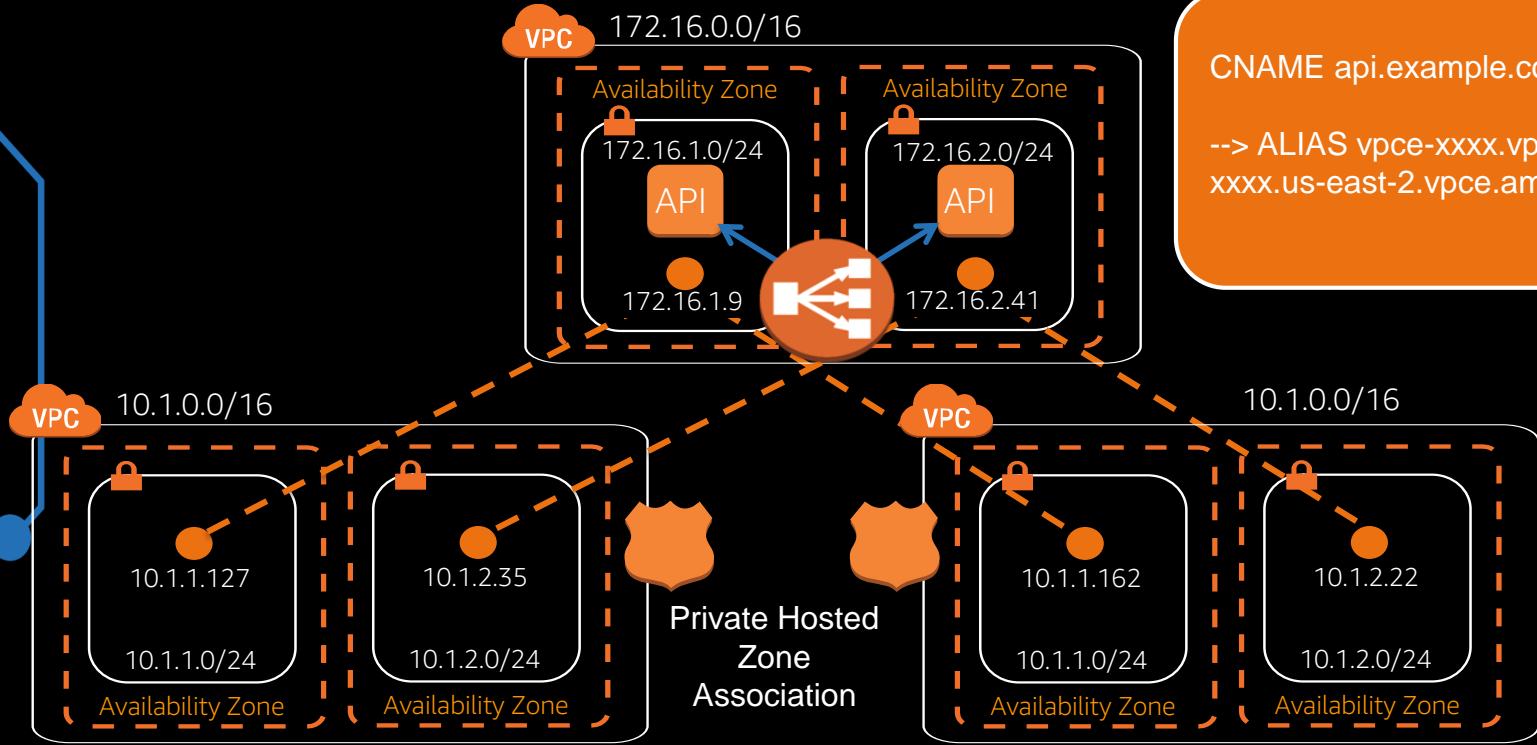
PrivateLink – How it Works



Amazon Route 53 Private Hosted Zone

CNAME api.example.com

--> ALIAS vpce-xxxx.vpce-svc-xxxx.us-east-2.vpce.amazonaws.com



...thousands

VPC Endpoint: api.example.com



Enhancement for Marketplace Services: Vanity DNS Names

Service Base DNS Name

vpce-svc-1a2b3c4d.us-east-1.vpce.amazonaws.com

Service ID

Region

Sub Domain

Endpoints DNS Name on Client Side

vpce-12345.vpce-svc-1a2b3c4d.us-east-1.vpce.amazonaws.com

vpce-67890.vpce-svc-1a2b3c4d.us-east-1.vpce.amazonaws.com

VPC Endpoint ID

Enhancement for Marketplace Services: Vanity DNS Names

Service **Vanity** DNS Name

us-east-1.vpce.myexample.com

Region

Sub Domain

Endpoints DNS Name on Client Side

vpce-12345.us-east-1.vpce.myexample.com

vpce-67890.us-east-1.vpce.myexample.com

VPC Endpoint ID

Easier Recognition of Service Endpoints

Straight-forward TLS Termination

AWS Marketplace Integration

Discoverability of the services when customers purchase SaaS on AWS Marketplace

PrivateLink

You can now discover, purchase, and provision AWS PrivateLink Enabled SaaS products through AWS Marketplace. AWS PrivateLink enables you to securely pass data directly to a SaaS application without ever leaving the AWS Network.



Easily create secure endpoints
AWS Marketplace confirms each seller's endpoint DNS name, making it easier to find and set up the endpoints you need.

No public IP address
Connect directly from your Amazon VPC without requiring traffic to traverse across the Internet.

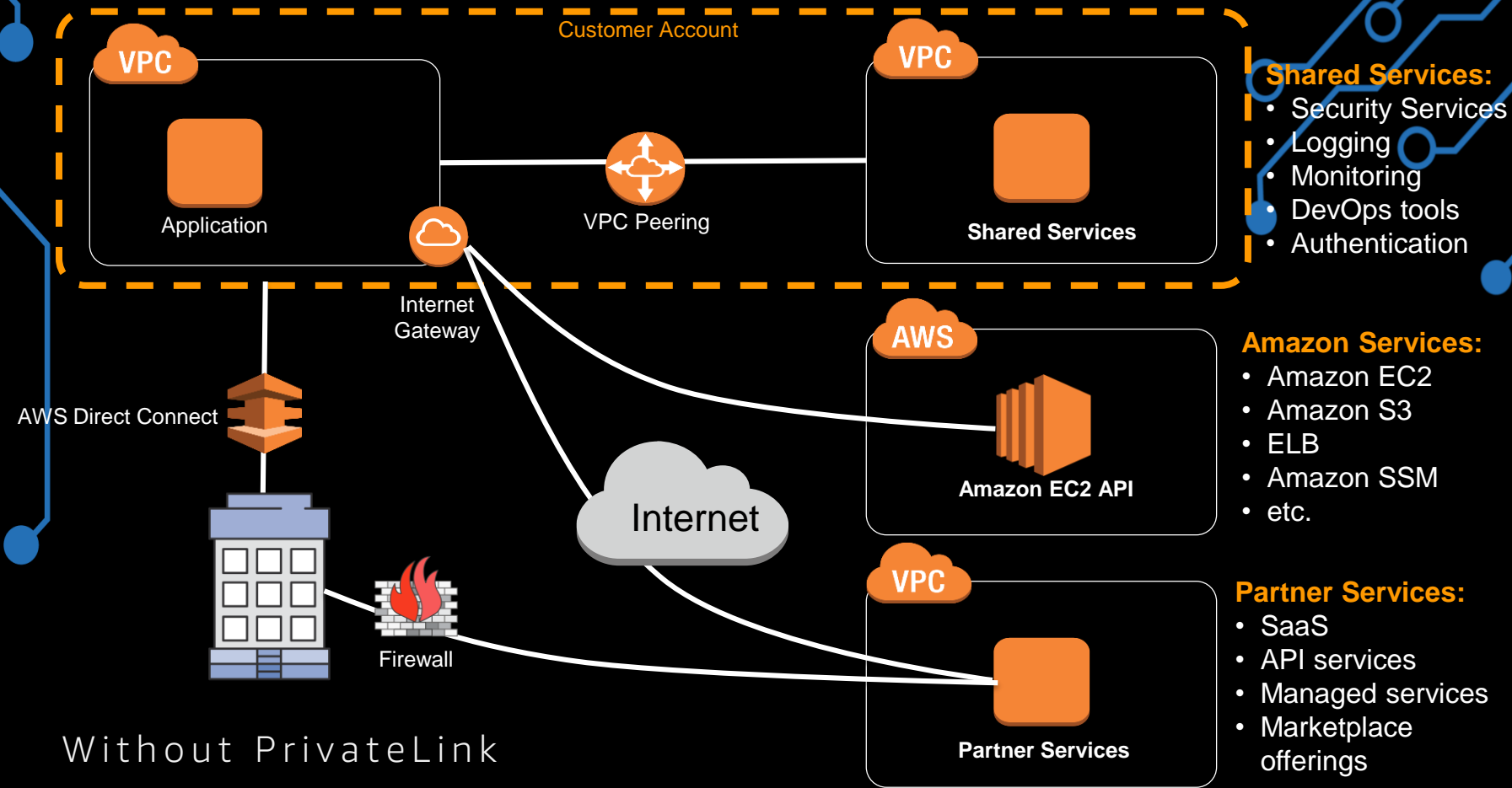
Curated SaaS products
Find products architected to run on AWS from popular software vendors.

Featured Products with PrivateLink

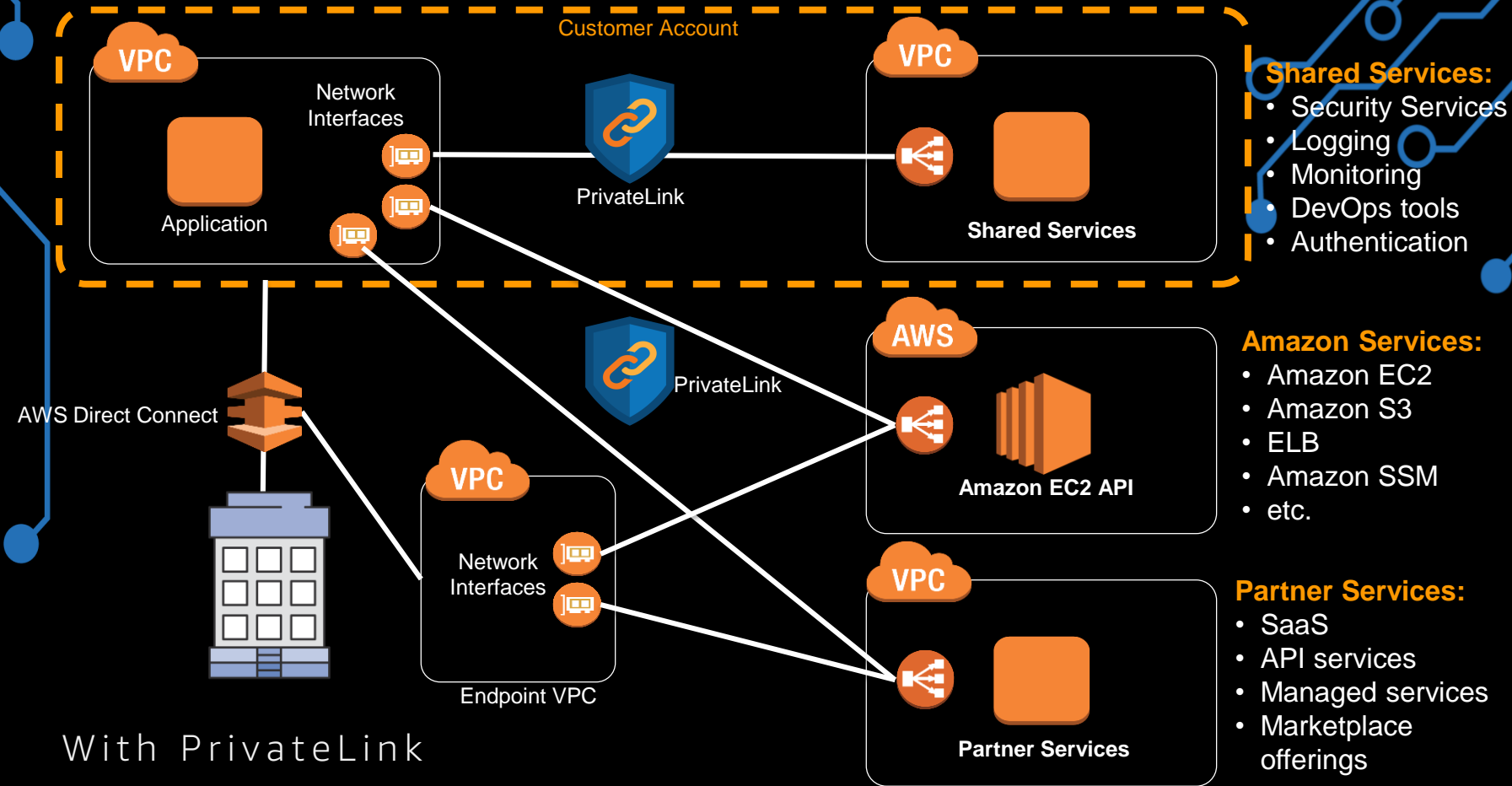
 Aqua Container Image Security Scanner	 Dynatrace - Cloud-Native Monitoring powered by AI	 SigOpt	 Cisco Stealthwatch Cloud Public Cloud Monitoring - Metered
 Cisco Stealthwatch Cloud Public Cloud Monitoring - Contracts	 CA Infrastructure Management Essentials	 CA App Experience Analytics Essentials	 CA Application Performance Management Essentials



PrivateLink Use Cases



Without PrivateLink





- Shared Services:**
- Security Services
 - Logging
 - Monitoring
 - DevOps tools
 - Authentication

- Amazon Services:**
- Amazon EC2
 - Amazon S3
 - ELB
 - Amazon SSM
 - etc.

- Partner Services:**
- SaaS
 - API services
 - Managed services
 - Marketplace offerings

1

Shared Services PrivateLink

Benefits:

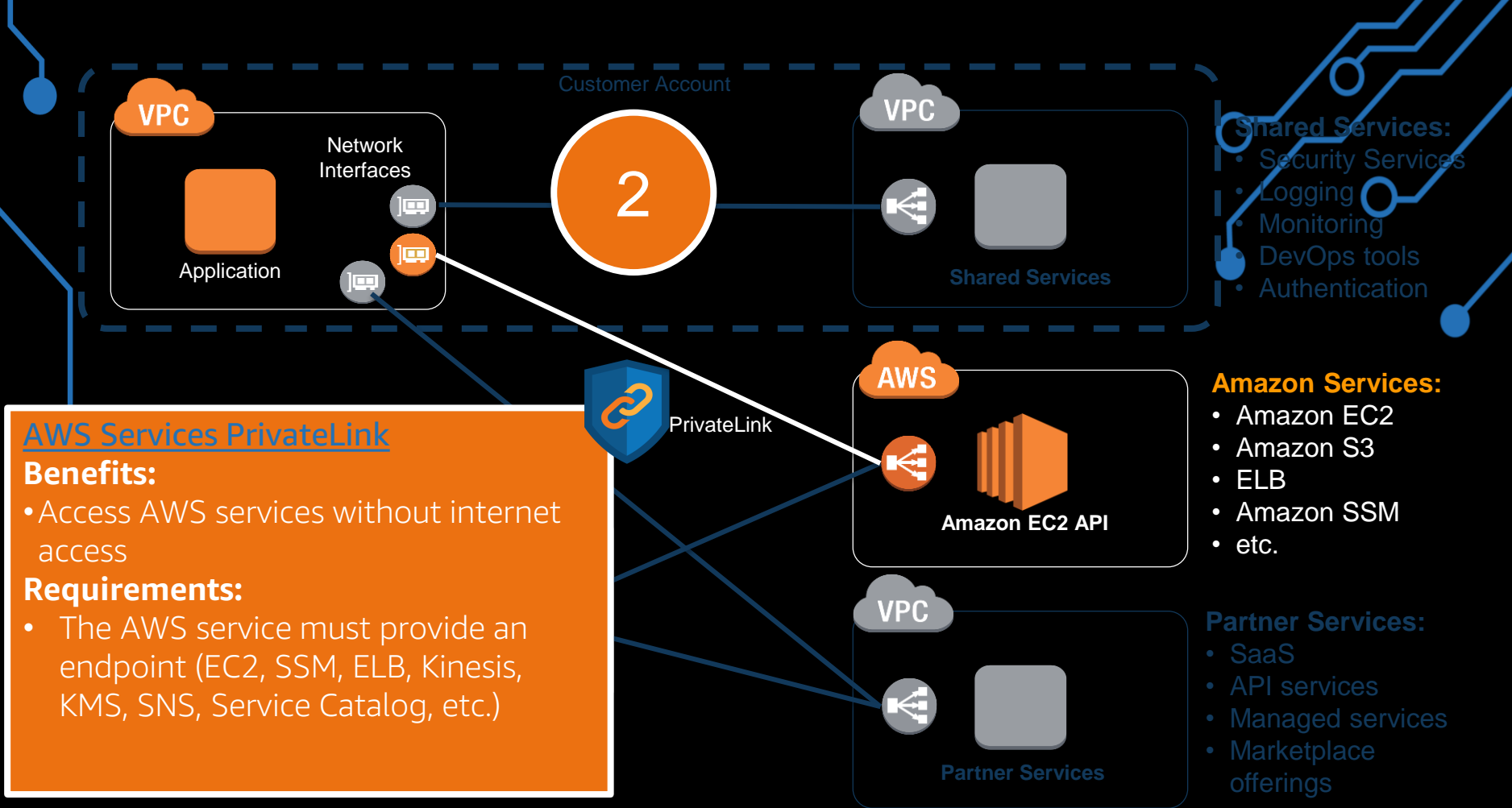
- More scalable than VPC peering, thousands versus 100
- More granular application access, compared to full VPC access
- Support for overlapping VPC CIDR ranges

Requirements:

- Service must be compatible with NLB

With PrivateLink

Partner Services



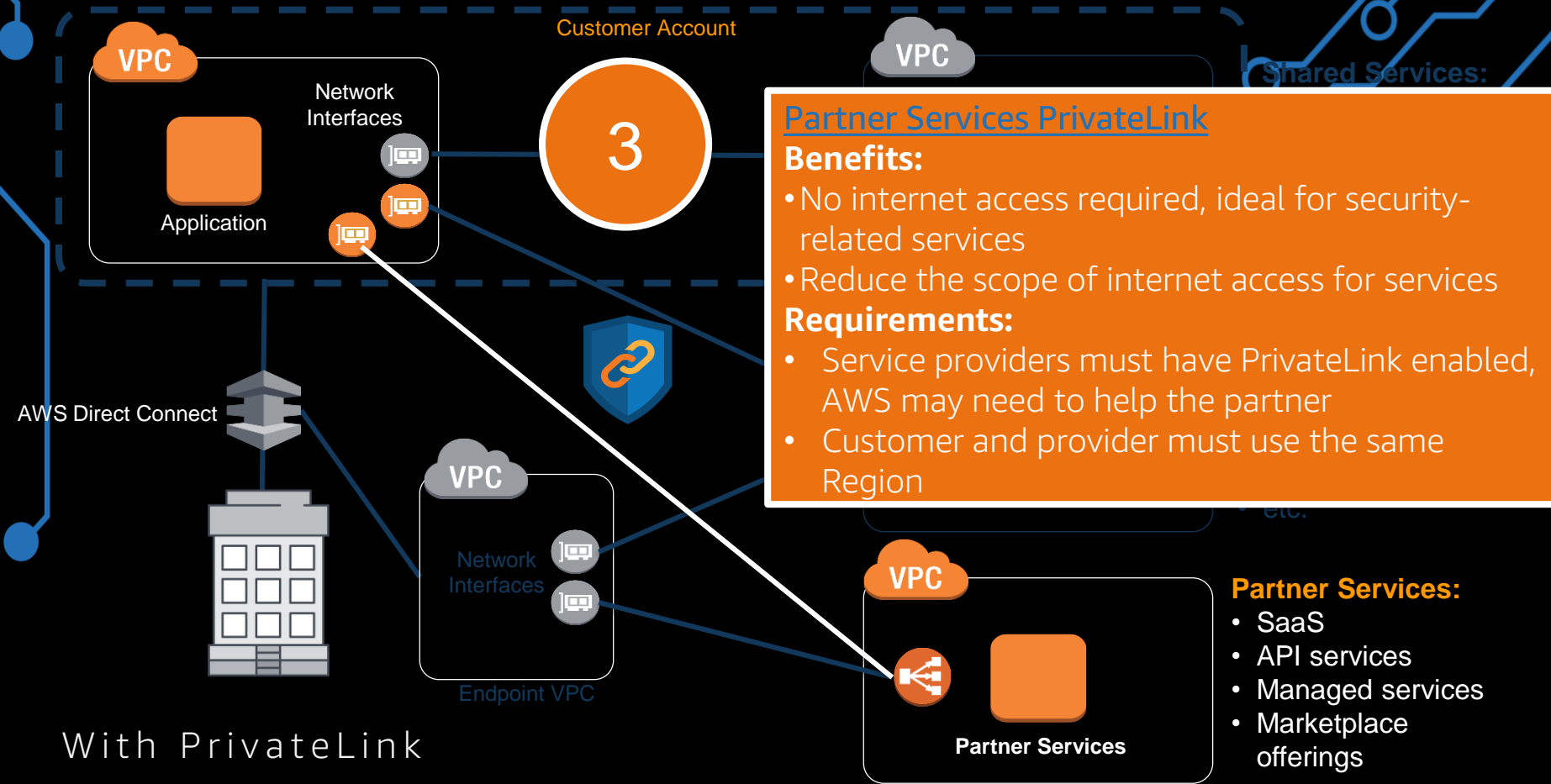
AWS Services PrivateLink

Benefits:

- Access AWS services without internet access

Requirements:

- The AWS service must provide an endpoint (EC2, SSM, ELB, Kinesis, KMS, SNS, Service Catalog, etc.)



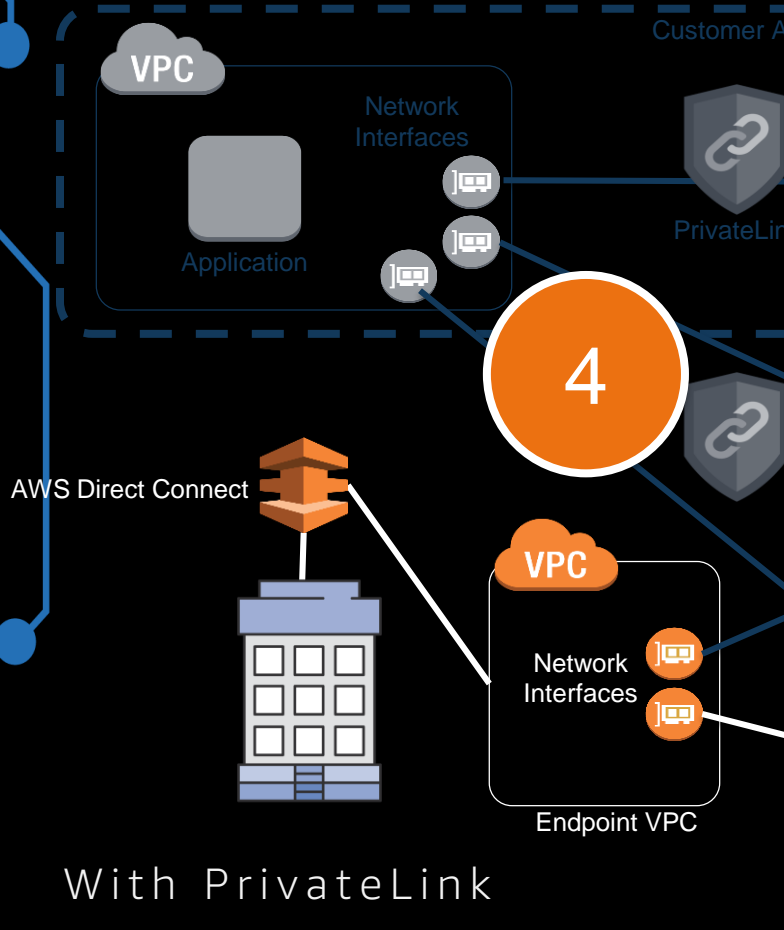
On-premises to AWS PrivateLink

Benefits:

- Allows on-premises customers to access services in a secure and scalable design
- Send sensitive information over private connectivity
- Service providers have an easily repeatable pattern
- The service target can also be on-premises

Requirements:

- Service must be compatible with NLB
- Customer or service provider must have an AWS Direct Connect port



With PrivateLink

Partner Services:

- SaaS
- API services
- Managed services
- Marketplace offerings




PrivateLink **Design Alternatives**


Designing Endpoints with Network Load Balancer


- Private Link is natively available within the same AWS Region, how do you handle global connectivity?
 - **AWS Direct Connect gateway may help, inter-region peering is currently incompatible.**
- Resources like databases or logging servers may not be compatible with load balancing
 - **May require an NLB per resource**
- Application Load Balancer is not currently supported
 - **Front the service with NLB in front of ALB**

<https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/>

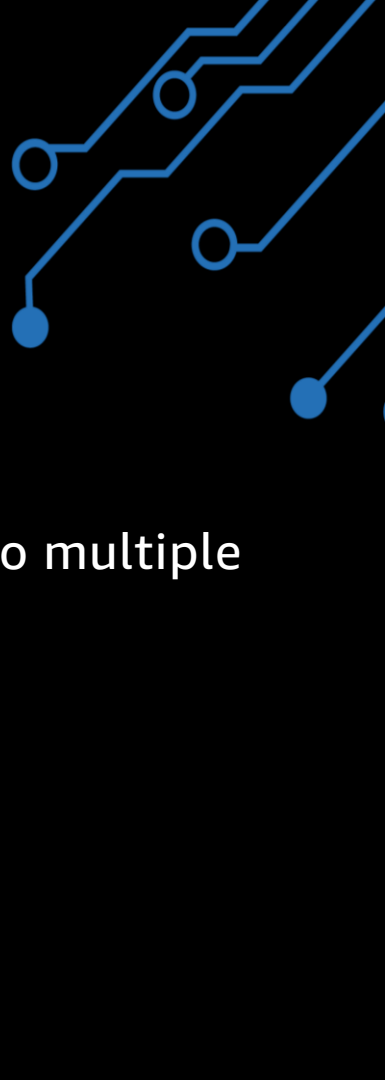


Designing Endpoints– Protocols

- Provided services cannot initiate new connections
 - Use VPC peering
 - Provided services must be TCP, no SSL offload
 - SSL offload can use the ALB-behind-NLB model
 - The NLB network interface is not routable, doesn't work for routers, firewalls, proxies, etc.
 - Transit VPC or other approaches more suitable
- 



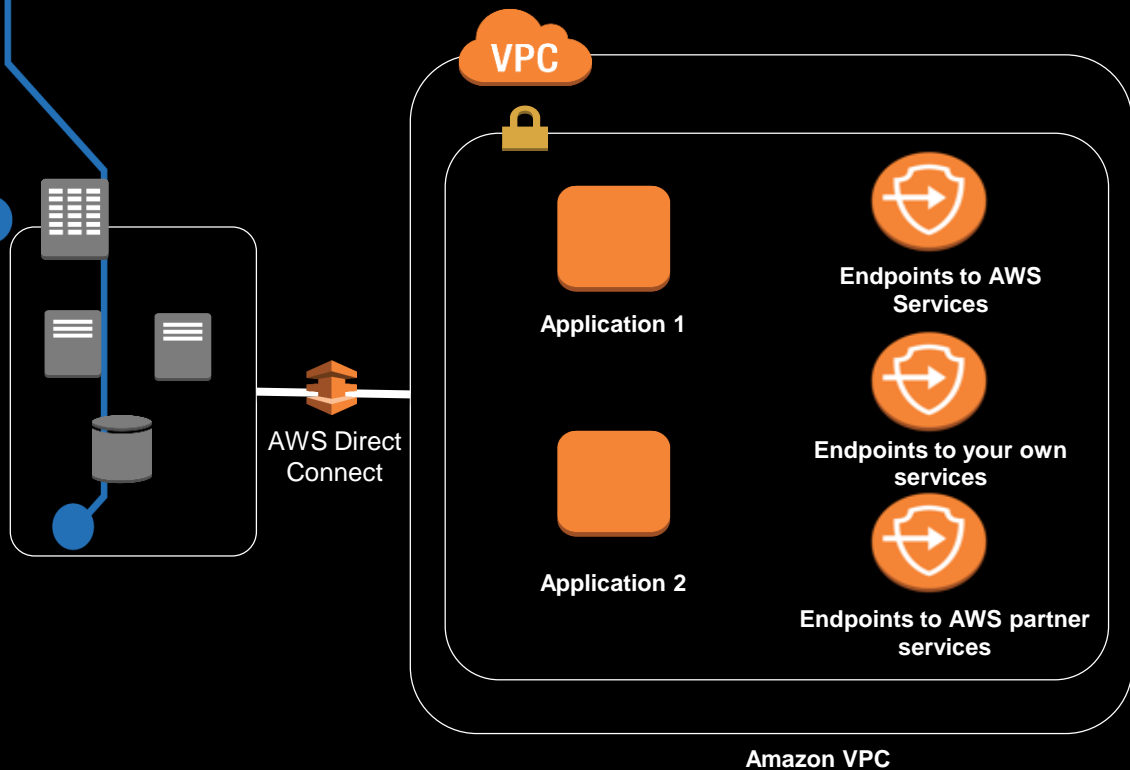
What Are Good Candidate PrivateLink Services?

- APIs, microservices
 - Multi-tenant TCP services
 - Anything currently behind Elastic Load Balancing useful to multiple VPCs
 - Services that process sensitive data
 - Sharing services in sensitive environments
- 



Final Thoughts

AWS PrivateLink—Service User



Interface Endpoints

Local IP, No Route Table Entry

Can Span Multiple Availability Zones

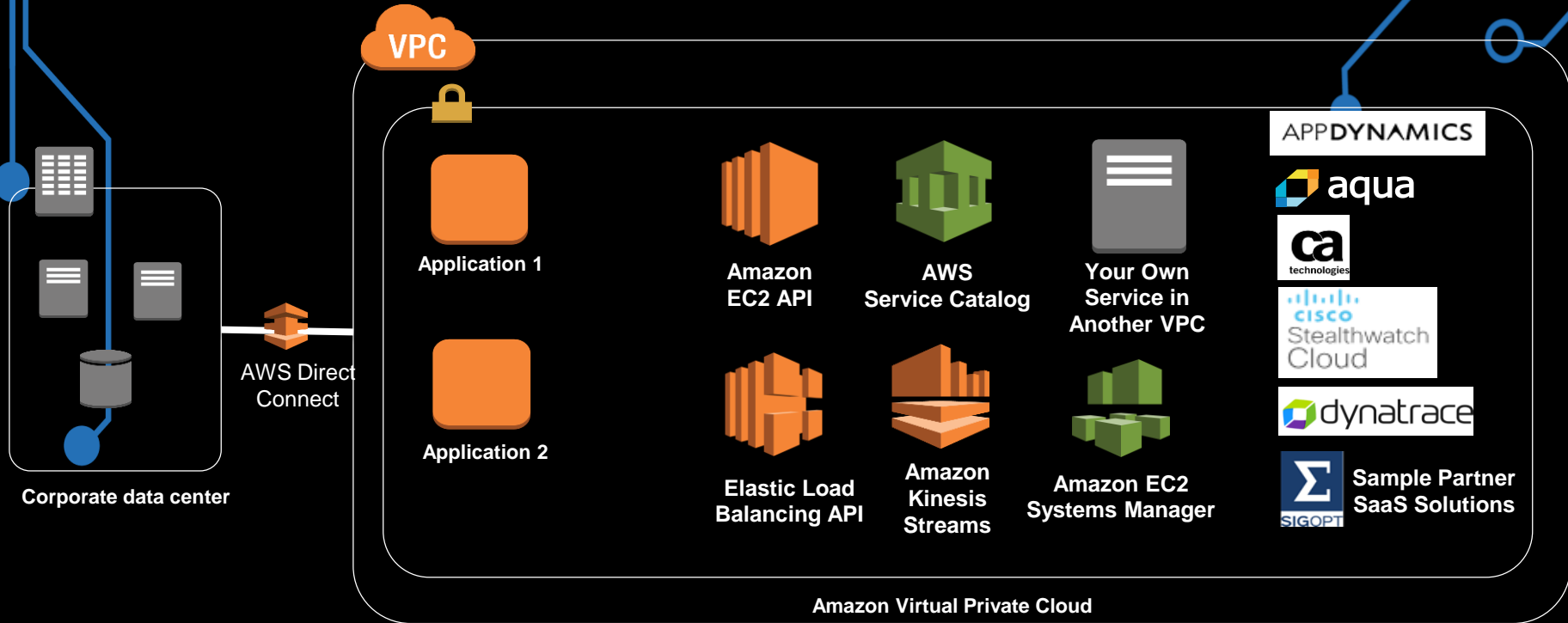
DNS Name on the Endpoints

- Publicly Resolvable Regional and Zonal DNS name that maps to the local IP of the endpoints
- NLB Health Check Aware

Security Group Integration

Accessible over AWS Direct Connect

The World with AWS PrivateLink



Use Cases



Centralized internal services such as logging, monitoring, and workloads serving various VPCs


Microservices and APIs, container systems

SaaS services with customer applications in other **VPCs** and **on-premises networks**



AWS PrivateLink Benefits

AWS PrivateLink enables customers to use **one set of services** across on-premises networks and Amazon VPCs





Benefits of AWS PrivateLink

AWS PrivateLink is **highly reliable** and **horizontally scalable** on the service and client side






Benefits of AWS PrivateLink

AWS PrivateLink reduces operational overhead.

Support for overlapping addresses and reduced management points.



Benefits of AWS PrivateLink



AWS PrivateLink is a **secure model**. The service owner is only exposing a **service concept** and the connection is **always initiated by the service user**. Users do not need to configure internet connectivity.



Thank you!