
AWS
re:Invent

CMP310

AWS Outposts: An in-depth look at hybrid cloud use cases

Matt Lehwess

Principal Developer Advocate

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Outposts:

Bringing AWS on-premises



Same AWS-designed infrastructure as in AWS data centers (built on AWS Nitro System)



Fully managed, monitored, and operated by AWS as if in AWS Regions



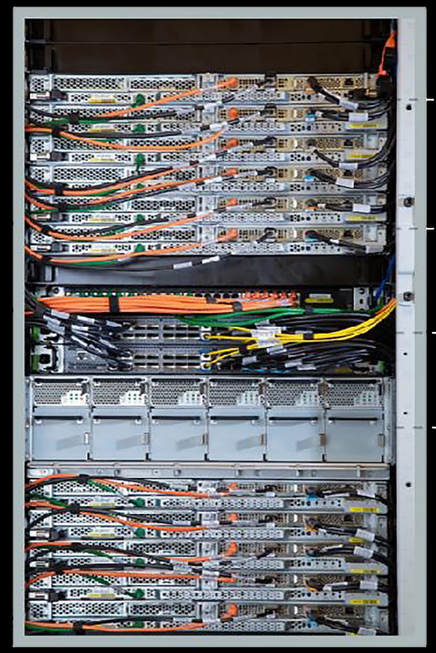
Single pane of management in the cloud providing the same APIs and tools as in AWS Regions

AWS Outposts: The hardware





Patch Panels
1/10/40/100G Network
Fiber Uplink Options



Hosts

Network Switches

Power Shelf
Redundant Centralized
Power Conversion Unit

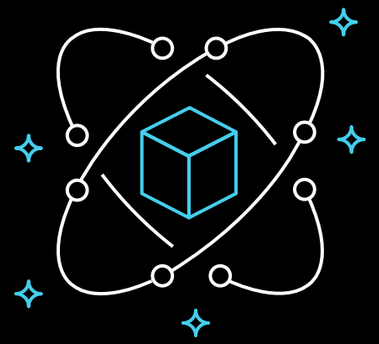


5kVA-15kVA Power Supply
Redundant feeds supported

Bus Bar

AWS Outposts: Use cases

Low Latency



Rendering, inference, data processing

Application Modernization



Modernize enterprise applications running at the edge

Data Residency



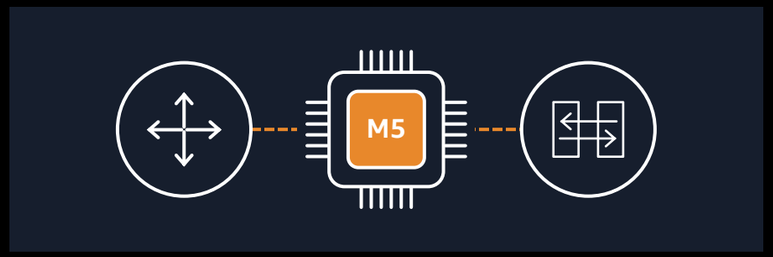
Regulatory, security, process requirements

Local Data Processing

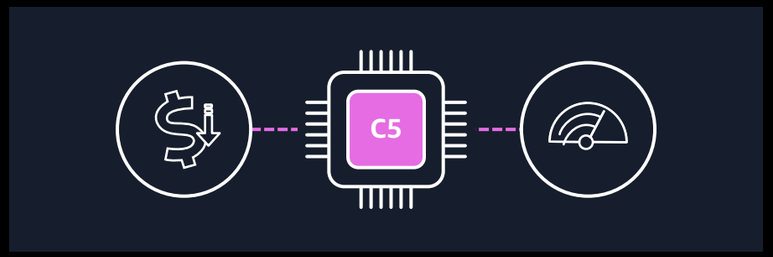


Local control systems, 5G/IOT

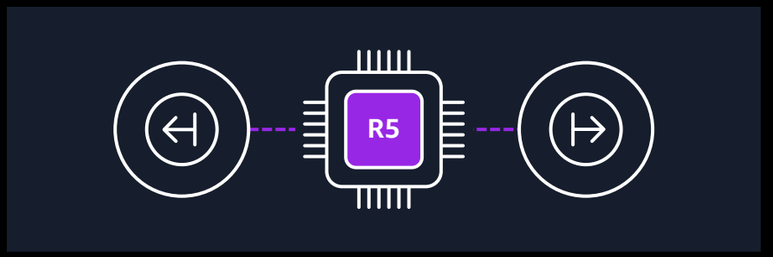
Build on the same Amazon EC2 instances and Amazon EBS volumes



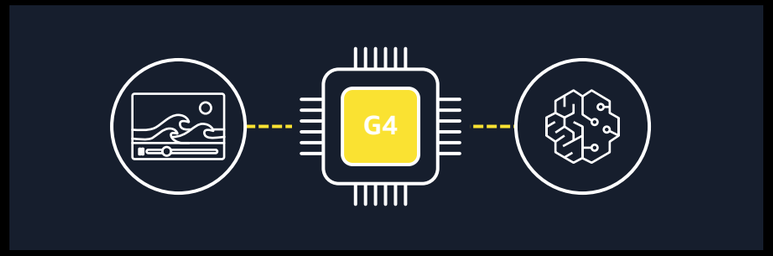
For general-purpose applications



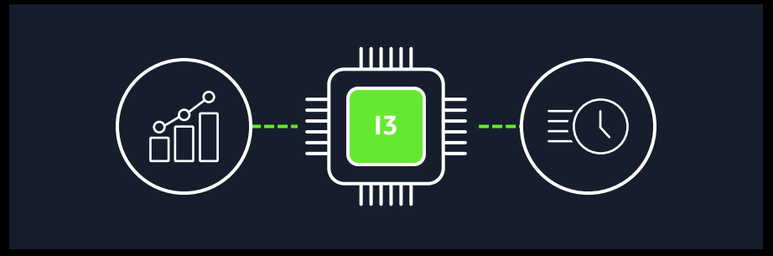
For compute-intensive applications (media transcoding, gaming servers, machine learning inference)



For memory-intensive applications (databases, in-memory caches, real-time data analytics)



For machine learning inference and graphics workstations



For I/O-intensive applications (NoSQL databases, in-memory or transactional databases, distributed file systems)



Local instance storage and EBS gp2 volumes for temporary and persistent storage

Amazon EC2 instances on premises powered by Intel Technologies

Consistent infrastructure

Build on the same EC2 instances featuring Intel Xeon processors, on premises as in the cloud



2.5 GHz Intel Xeon Scalable Processors **(Skylake)**

Consistent application performance

Leverage the same workload performance enhancements on Outposts as instances running in the cloud



Intel Xeon E5 v4 processors (Broadwell)

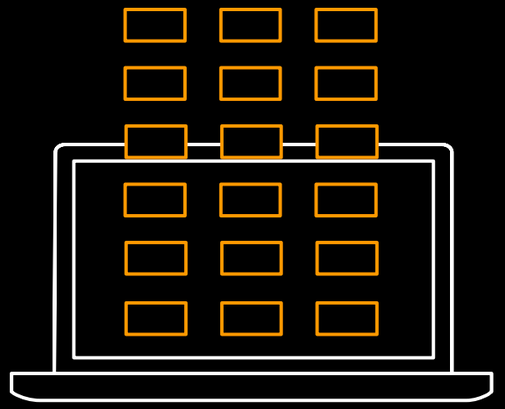
Custom 3.0 GHz Intel Xeon Scalable Processors (Skylake)

Ease of application migration

Seamlessly migrate your applications on Outposts to AWS

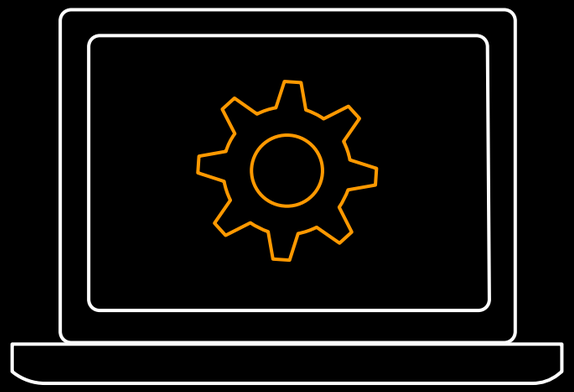


2nd Generation Intel Xeon Scalable Processors (Cascade Lake)



Run AWS services locally

- **Compute and storage**
  Amazon EC2 instances and Amazon EBS volumes
- **Networking**
  Amazon Virtual Private Cloud (Amazon VPC)
  Amazon Application Load Balancer (Amazon ALB)
- **Database**
  Amazon Relational Database Service (Amazon RDS)
- **Containers**
  Amazon Elastic Container Service (Amazon ECS) and
  Amazon Elastic Kubernetes Service (Amazon EKS)
- **Data processing**
  Amazon Elastic Map Reduce (Amazon EMR)
- **Local storage**
  Amazon S3



With the same AWS APIs and tools as in the AWS Region

- Amazon EC2 Auto Scaling groups
- AWS CloudFormation
- Amazon CloudWatch
- AWS CloudTrail
- AWS Elastic Beanstalk
- AWS Cloud9

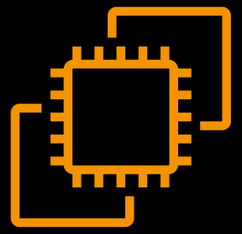
and more . . .



Amazon VPC Networking

To understand AWS Outposts, we need to first understand Amazon VPC networking

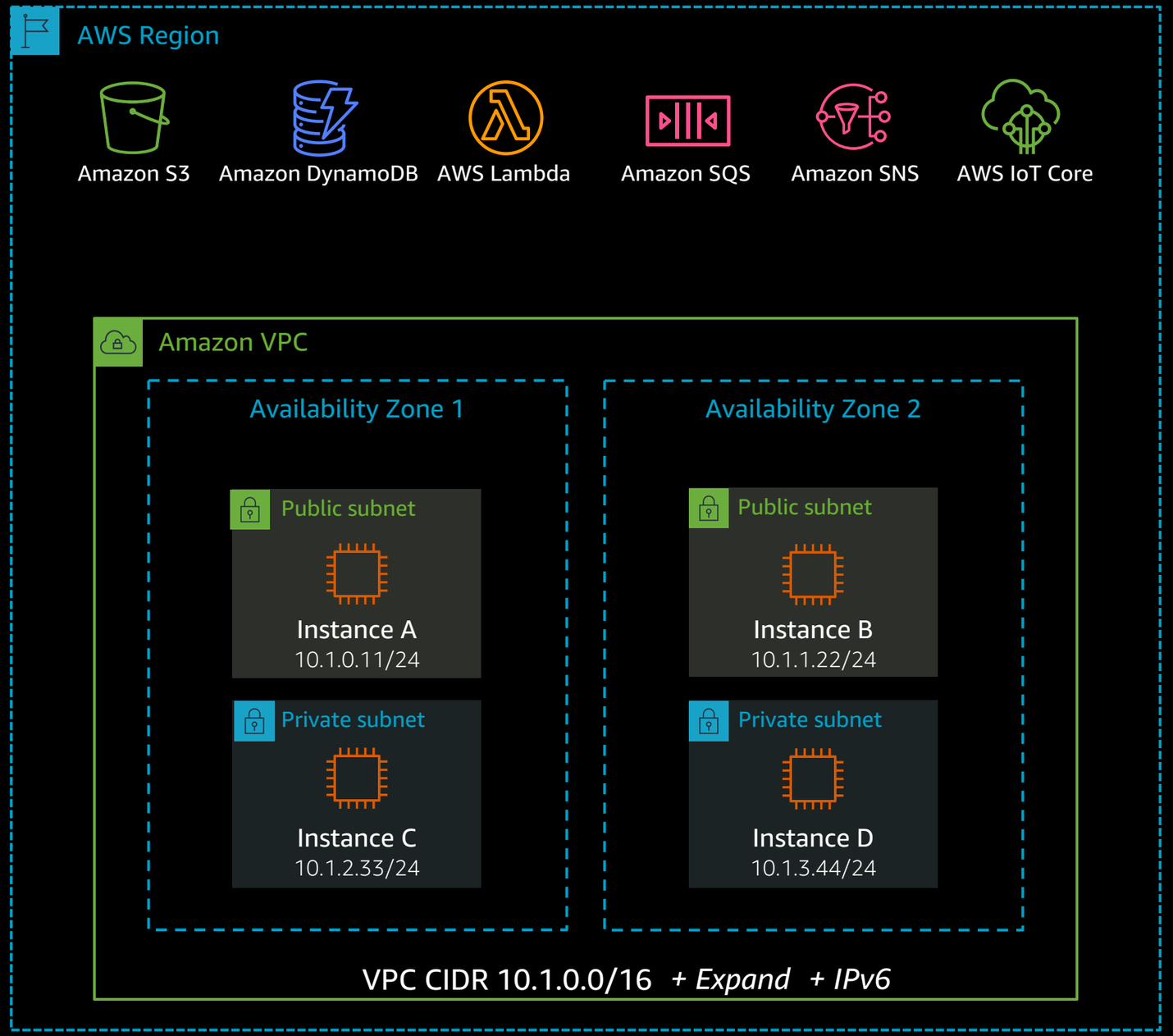
Amazon VPC networking

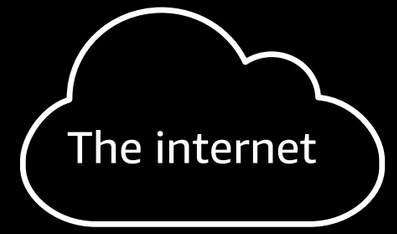


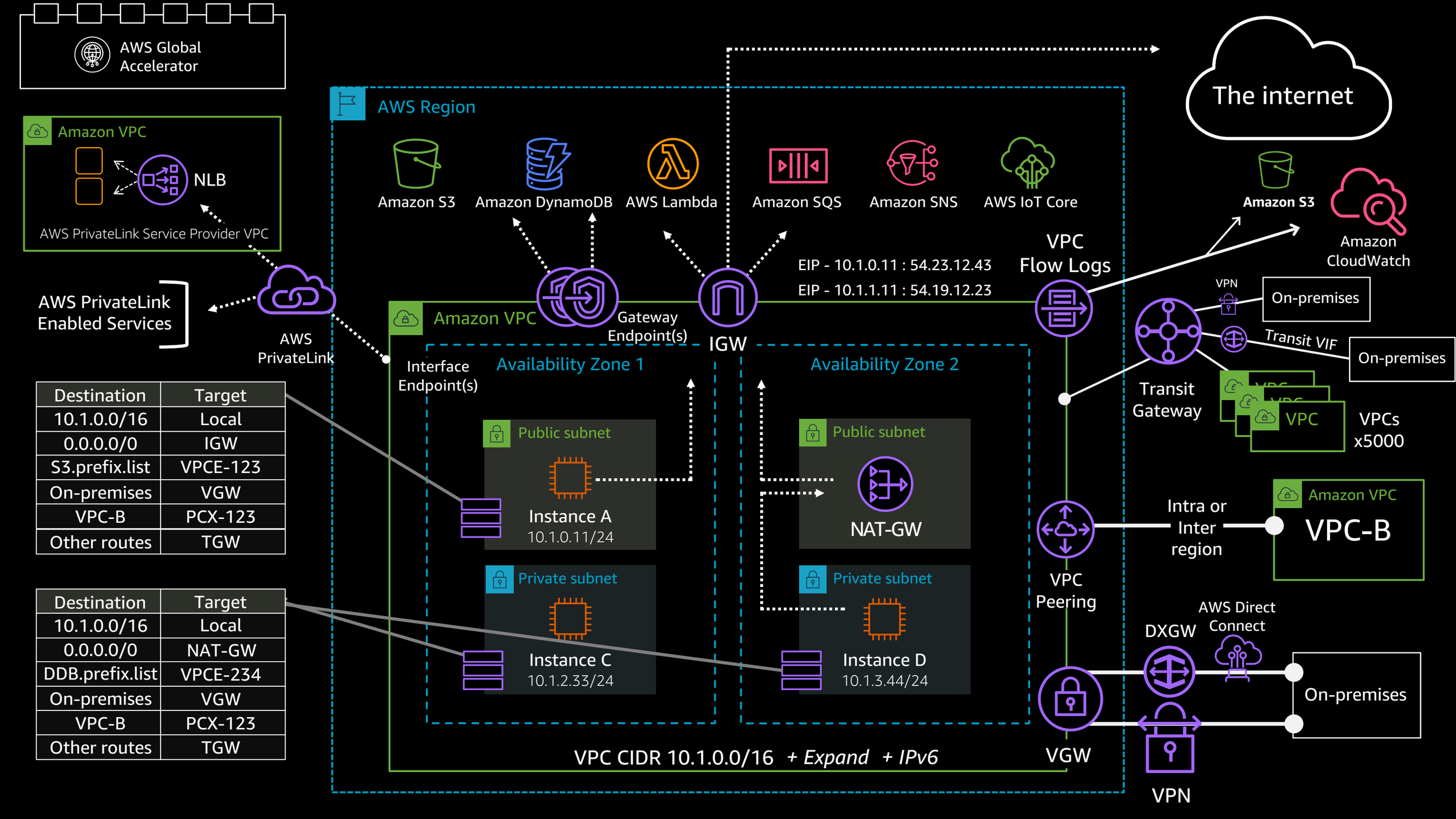
Amazon EC2



Amazon VPC

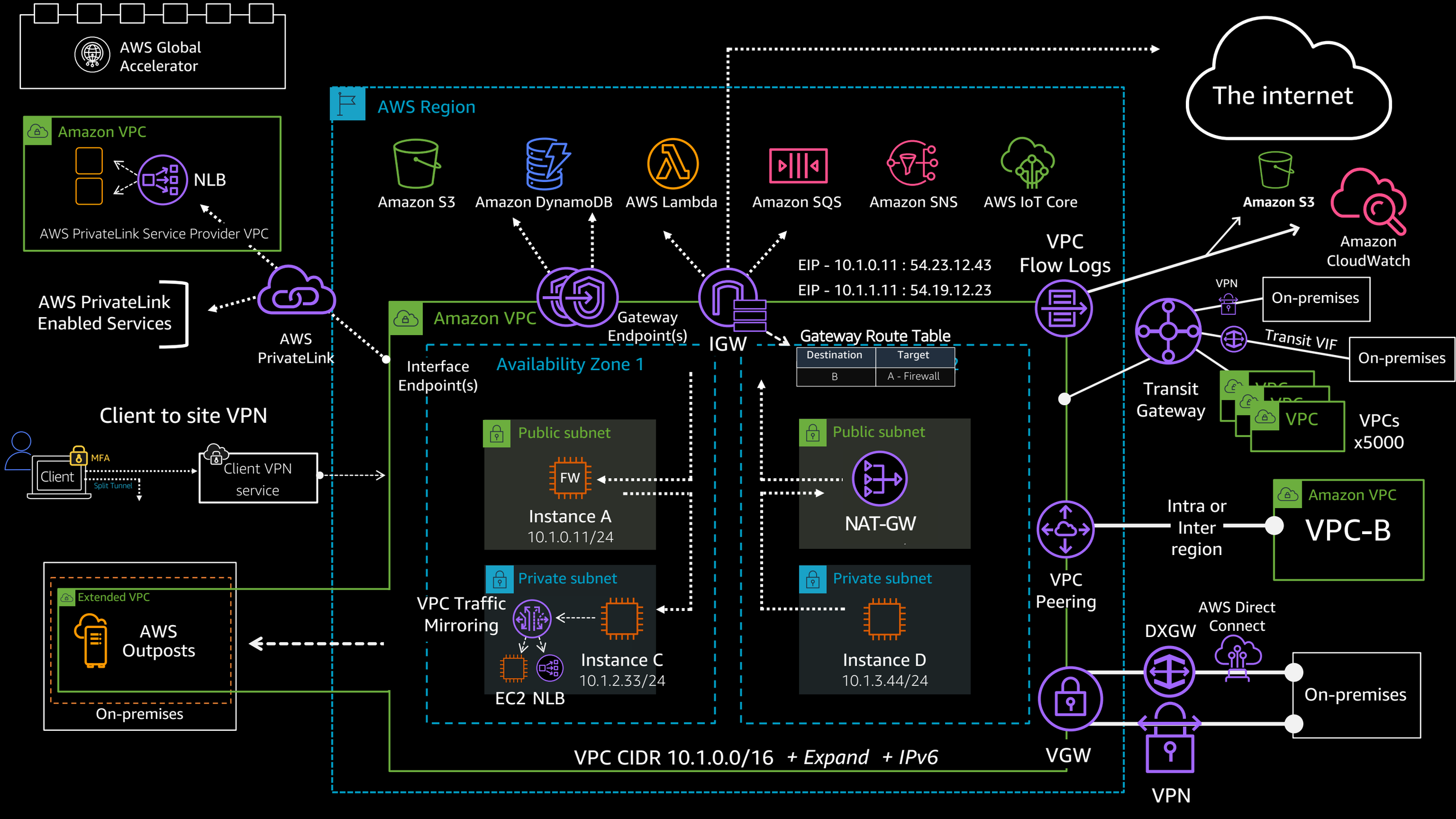






Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other routes	TGW

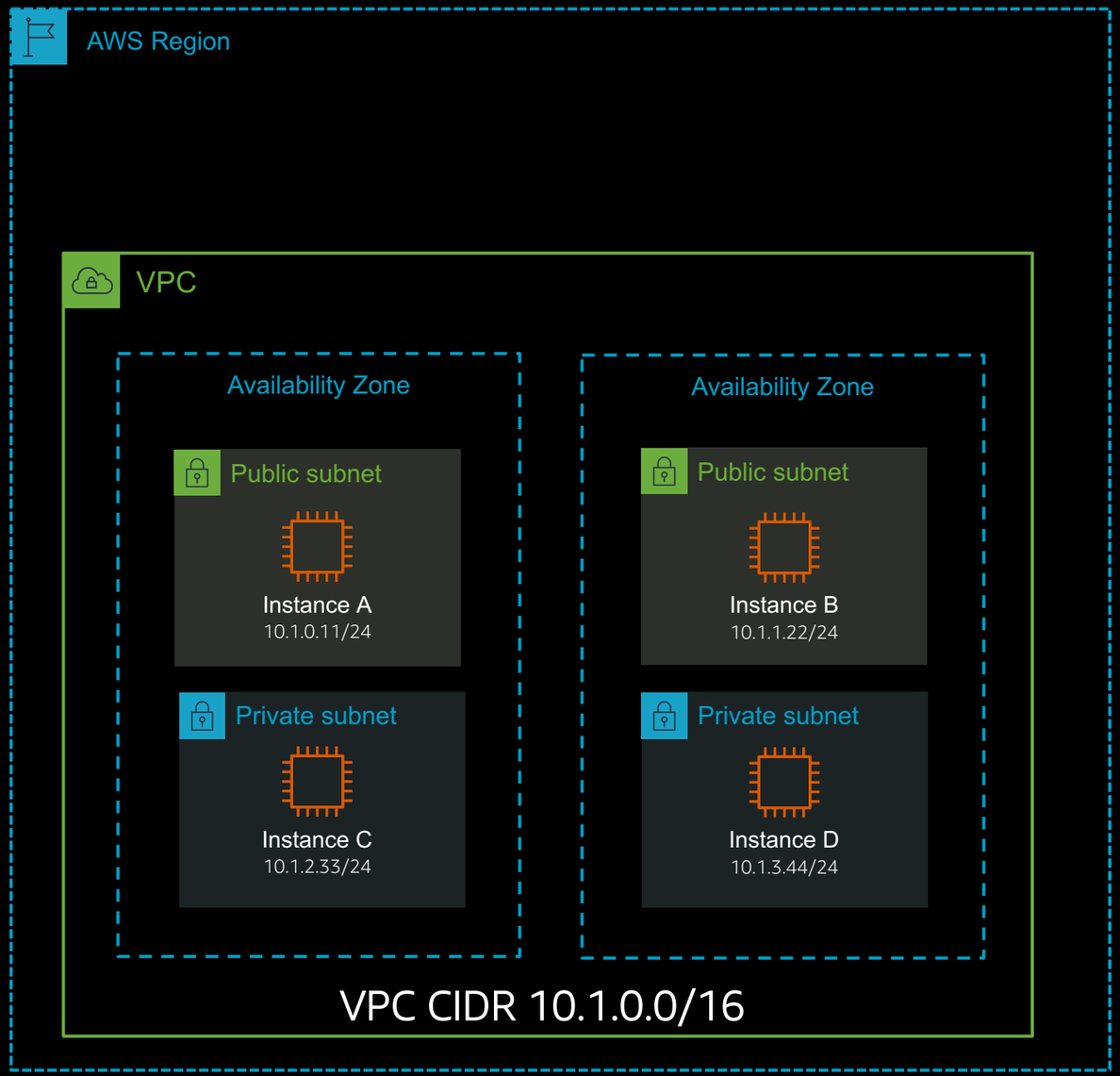
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW
DDB.prefix.list	VPCE-234
On-premises	VGW
VPC-B	PCX-123
Other routes	TGW


AWS Global Accelerator
The internet
AWS Region
Amazon VPC
NLB
AWS PrivateLink Service Provider VPC
Amazon S3
Amazon DynamoDB
AWS Lambda
Amazon SQS
Amazon SNS
AWS IoT Core
Amazon S3
Amazon CloudWatch
VPC Flow Logs
EIP - 10.1.0.11 : 54.23.12.43
EIP - 10.1.1.11 : 54.19.12.23
AWS PrivateLink Enabled Services
AWS PrivateLink
Gateway Endpoint(s)
IGW
Amazon VPC
Gateway Route Table
Destination
Target
B
A - Firewall
Interface Endpoint(s)
Availability Zone 1
VPN
On-premises
Transit VIF
On-premises
Transit Gateway
VPC
VPCs x5000
Client to site VPN
Client
MFA
Split Tunnel
Client VPN service
Public subnet
FW
Instance A
10.1.0.11/24
Public subnet
NAT-GW
Intra or Inter region
Amazon VPC
VPC-B
Extended VPC
AWS Outposts
On-premises
Private subnet
VPC Traffic Mirroring
Instance C
10.1.2.33/24
EC2 NLB
Private subnet
Instance D
10.1.3.44/24
VPC Peering
AWS Direct Connect
DXGW
On-premises
VPC CIDR 10.1.0.0/16 + Expand + IPv6
VGW
VPN

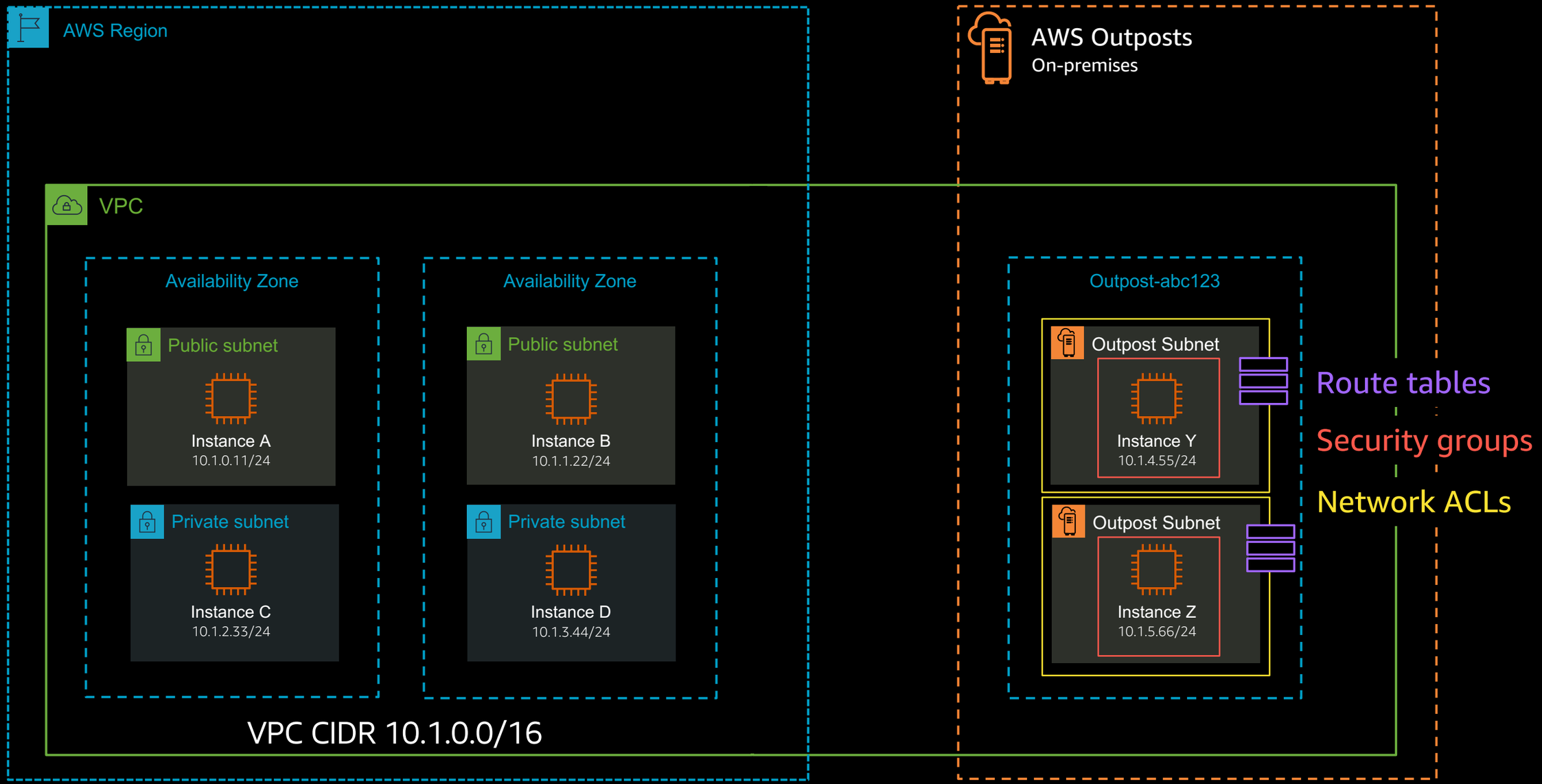


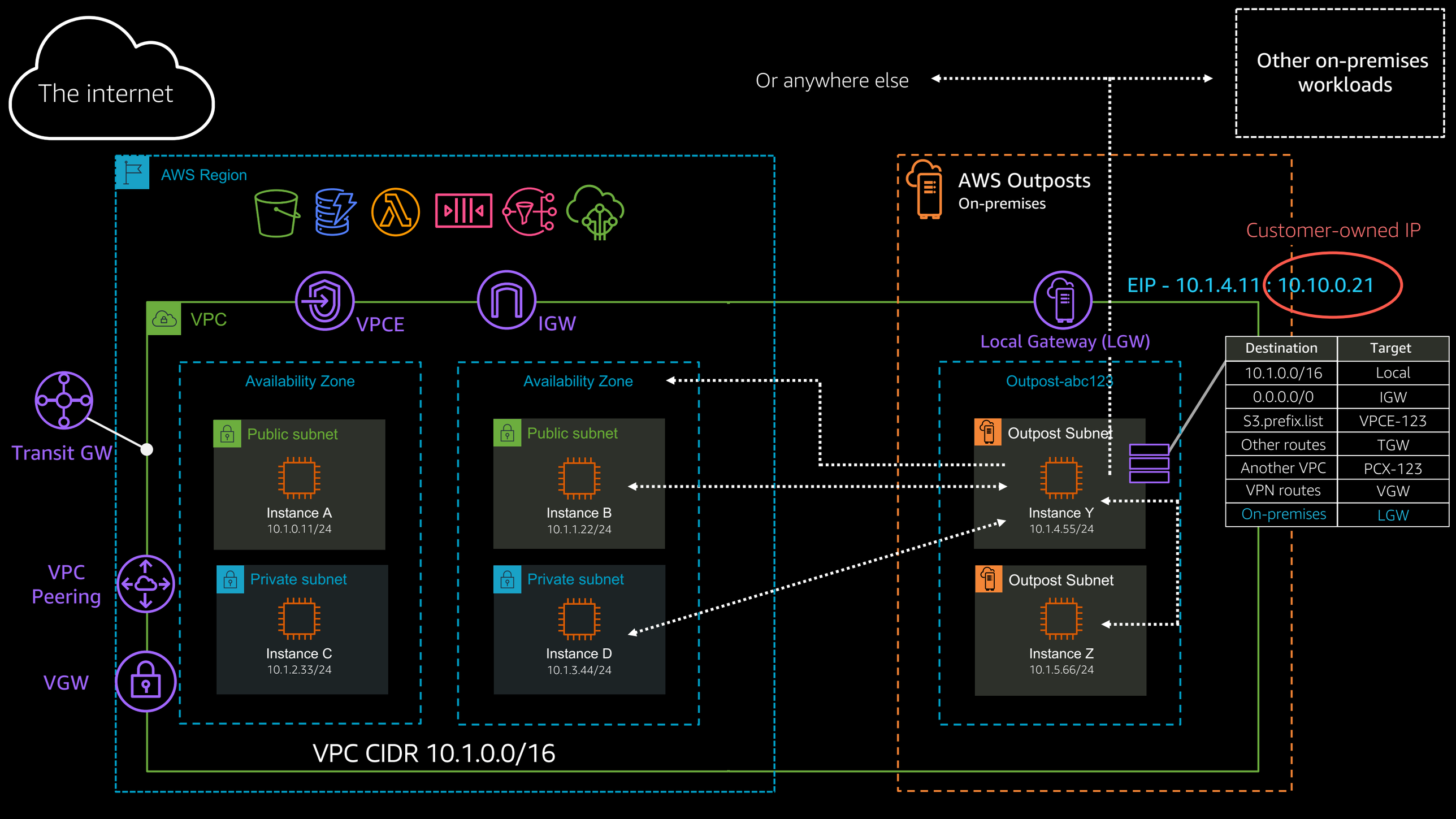
Amazon VPC Networking

Now, let’s dive into Amazon
VPC networking for AWS Outposts


AWS Region
VPC
Availability Zone
Public subnet
Instance A
10.1.0.11/24
Private subnet
Instance C
10.1.2.33/24
Availability Zone
Public subnet
Instance B
10.1.1.22/24
Private subnet
Instance D
10.1.3.44/24
VPC CIDR 10.1.0.0/16

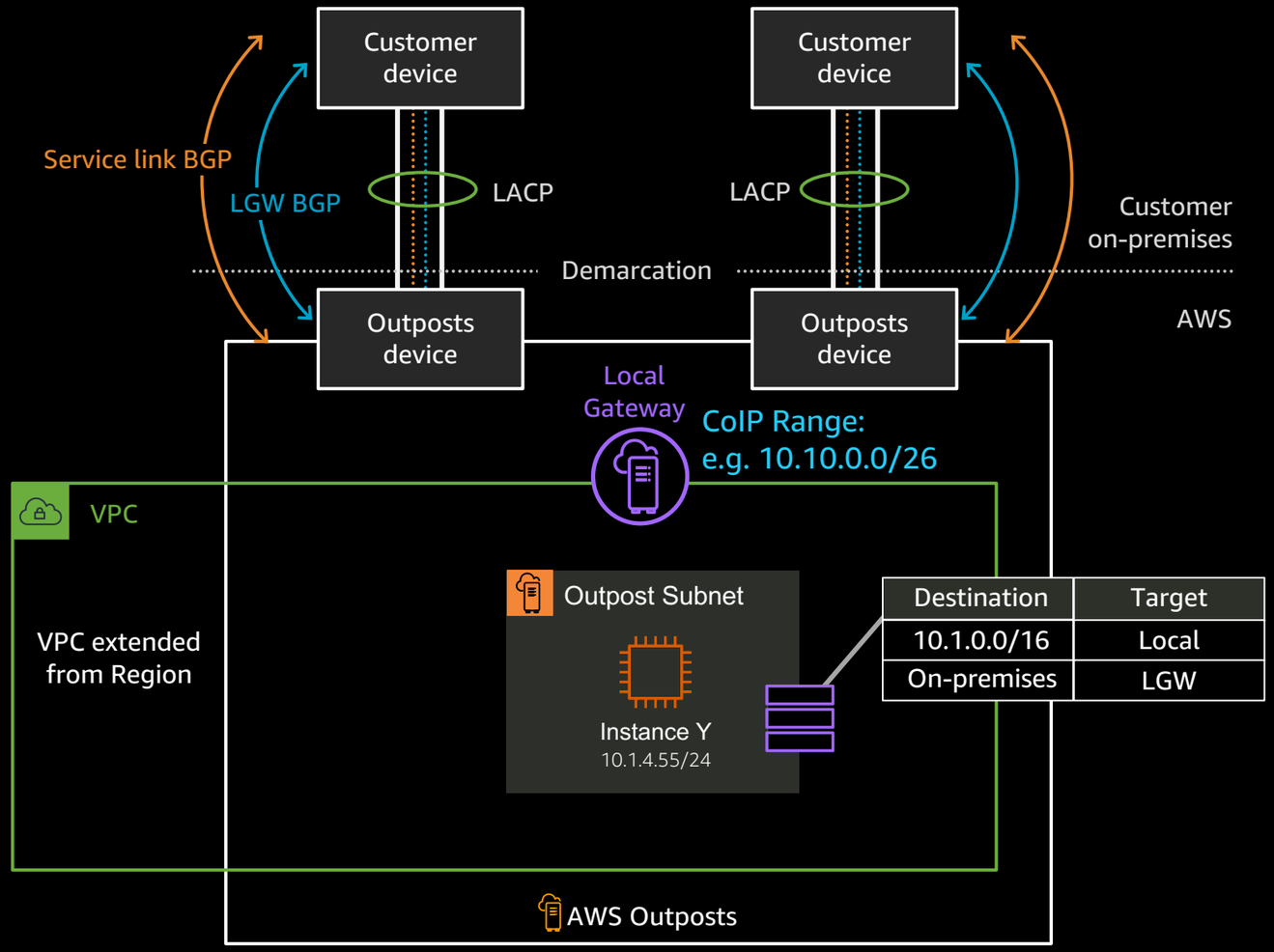
Access to the same networking constructs as the AWS Region




The internet
Or anywhere else
Other on-premises workloads
AWS Region
AWS Outposts
On-premises
Customer-owned IP
EIP - 10.1.4.11 : 10.10.0.21
VPC
VPCE
IGW
Local Gateway (LGW)
Transit GW
Availability Zone
Availability Zone
Outpost-abc123
Public subnet
Instance A
10.1.0.11/24
Public subnet
Instance B
10.1.1.22/24
Outpost Subnet
Instance Y
10.1.4.55/24
Private subnet
Instance C
10.1.2.33/24
Private subnet
Instance D
10.1.3.44/24
Outpost Subnet
Instance Z
10.1.5.66/24
VPC Peering
VGW
VPC CIDR 10.1.0.0/16
Destination
Target
10.1.0.0/16
Local
0.0.0.0/0
IGW
S3.prefix.list
VPCE-123
Other routes
TGW
Another VPC
PCX-123
VPN routes
VGW
On-premises
LGW

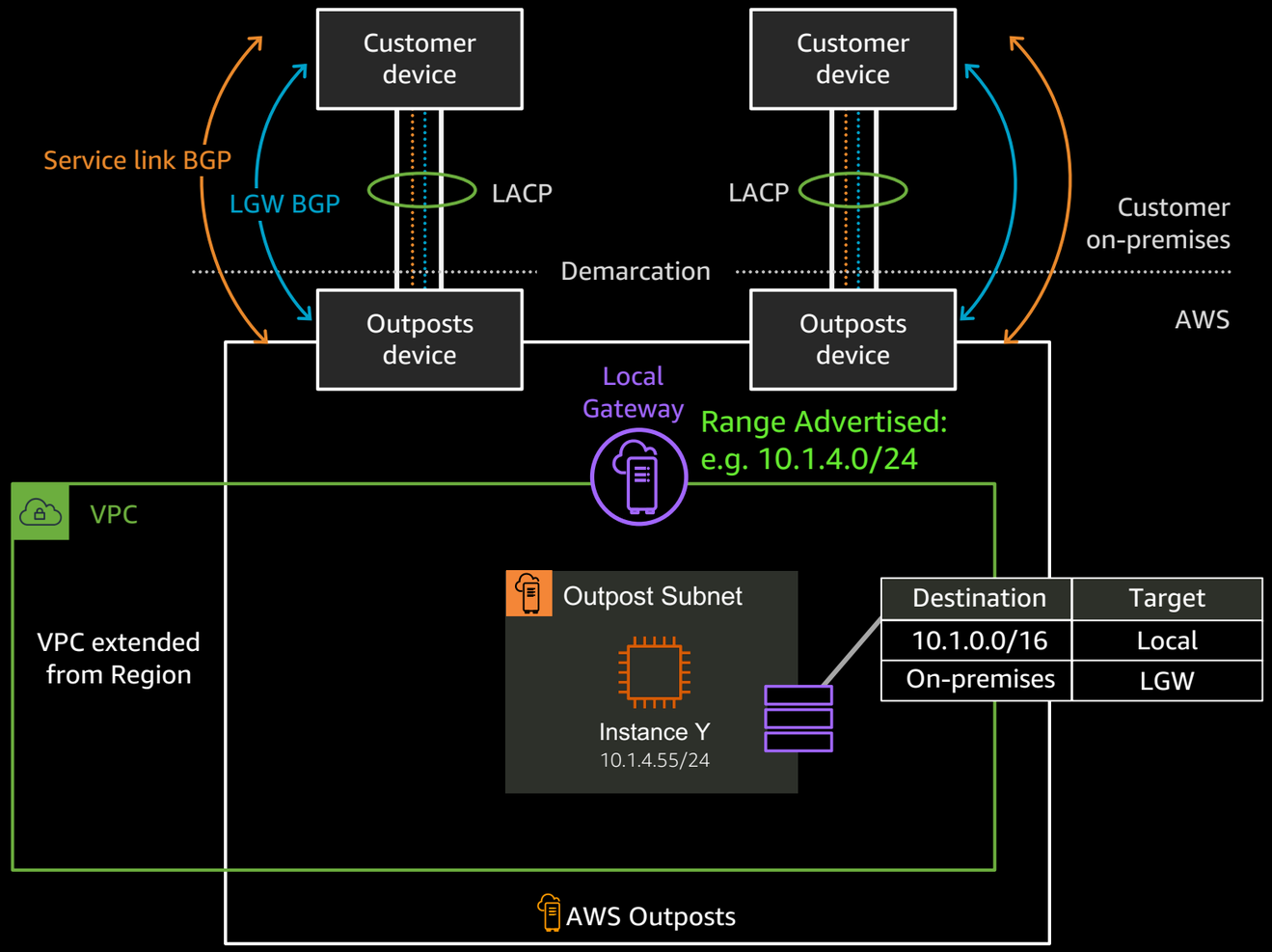
On-premises connectivity: Local Gateway (LGW)

- Multiple Outpost network devices per rack, providing physical redundancy
- Separation of service link and LGW traffic paths using Virtual LANs (VLANs)
- Multiple BGP sessions for service link and LGW
- Local Gateway (LGW) is a logical entity attached to your VPC
- Customer-owned IP addresses (CoIP) are advertised on LGW BGP sessions
- VPC configuration is distinctly separate from the physical configuration



On-premises connectivity: Local Gateway

› Coming soon! – Direct advertisement of the Outpost subnet range over the LGW BGP sessions, no CoIP required



Don’t forget to check out the Outposts reference architectures from our partners

Cisco:

https://bit.ly/37mtFvq

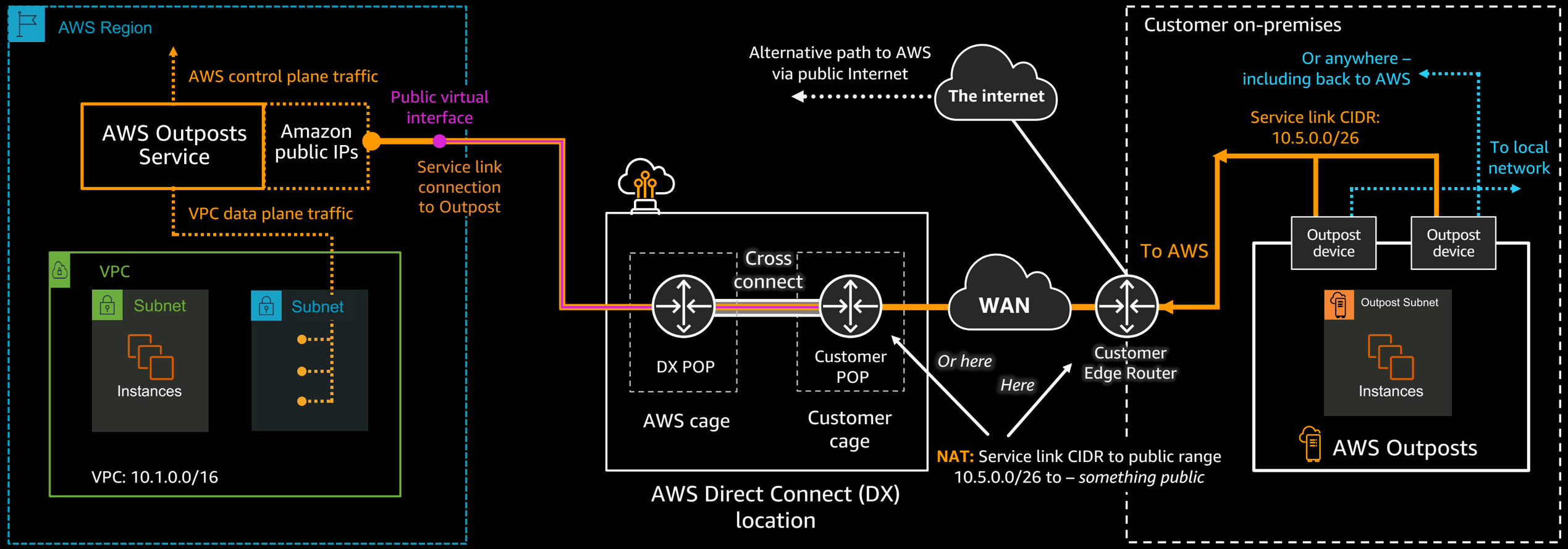
SCAN ME

Juniper:

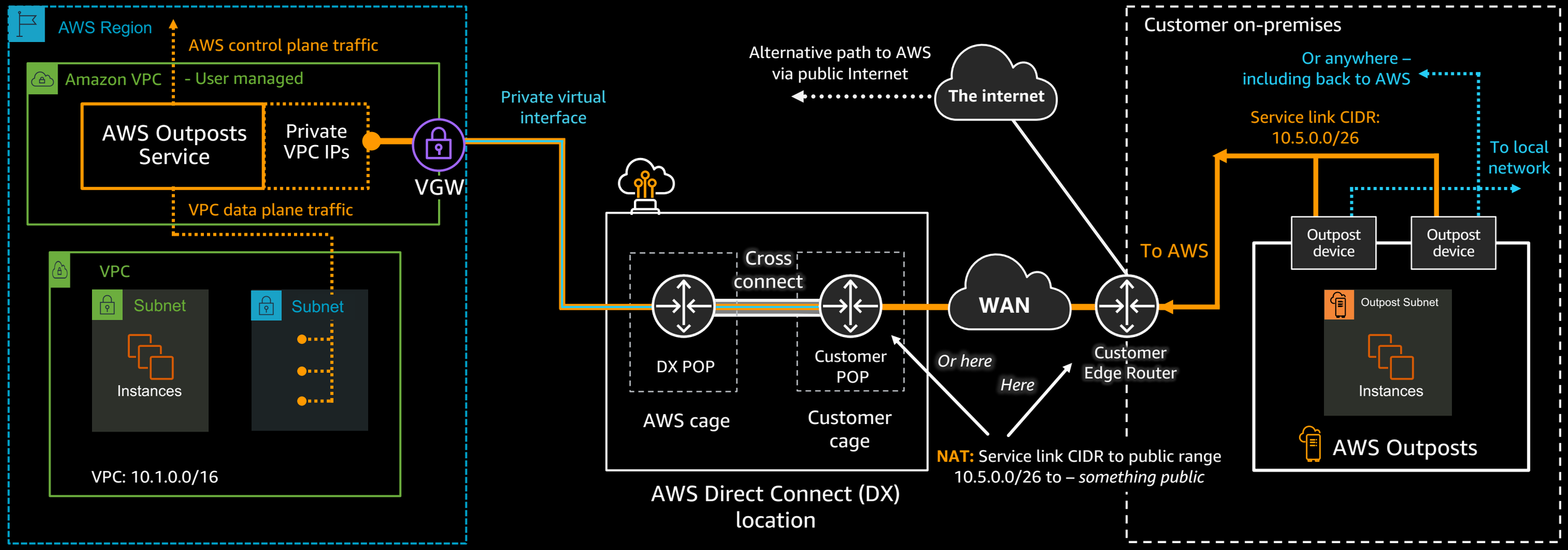
https://juni.pr/2MTkol7

SCAN ME

AWS Region connectivity: Service link

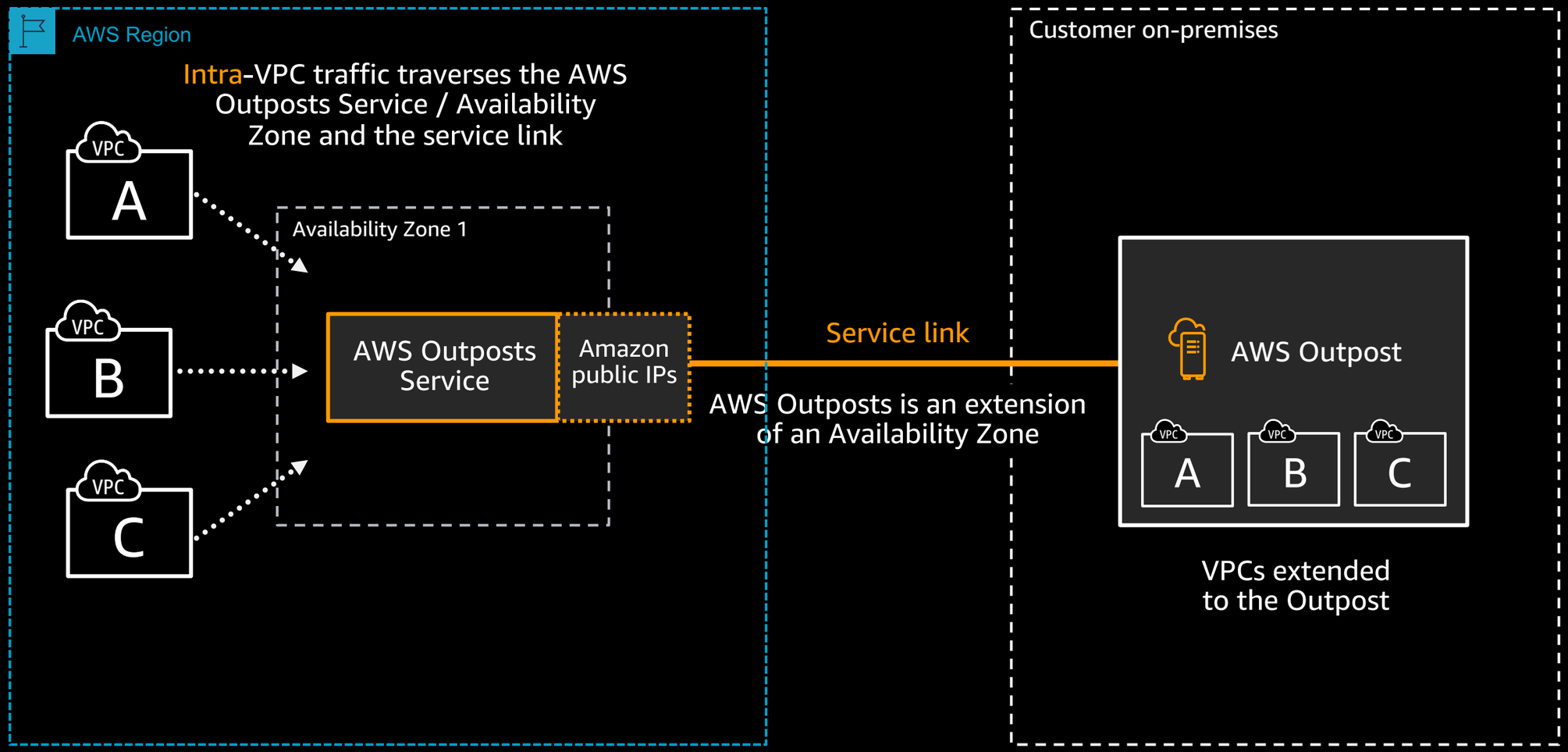


AWS Region connectivity: Service link

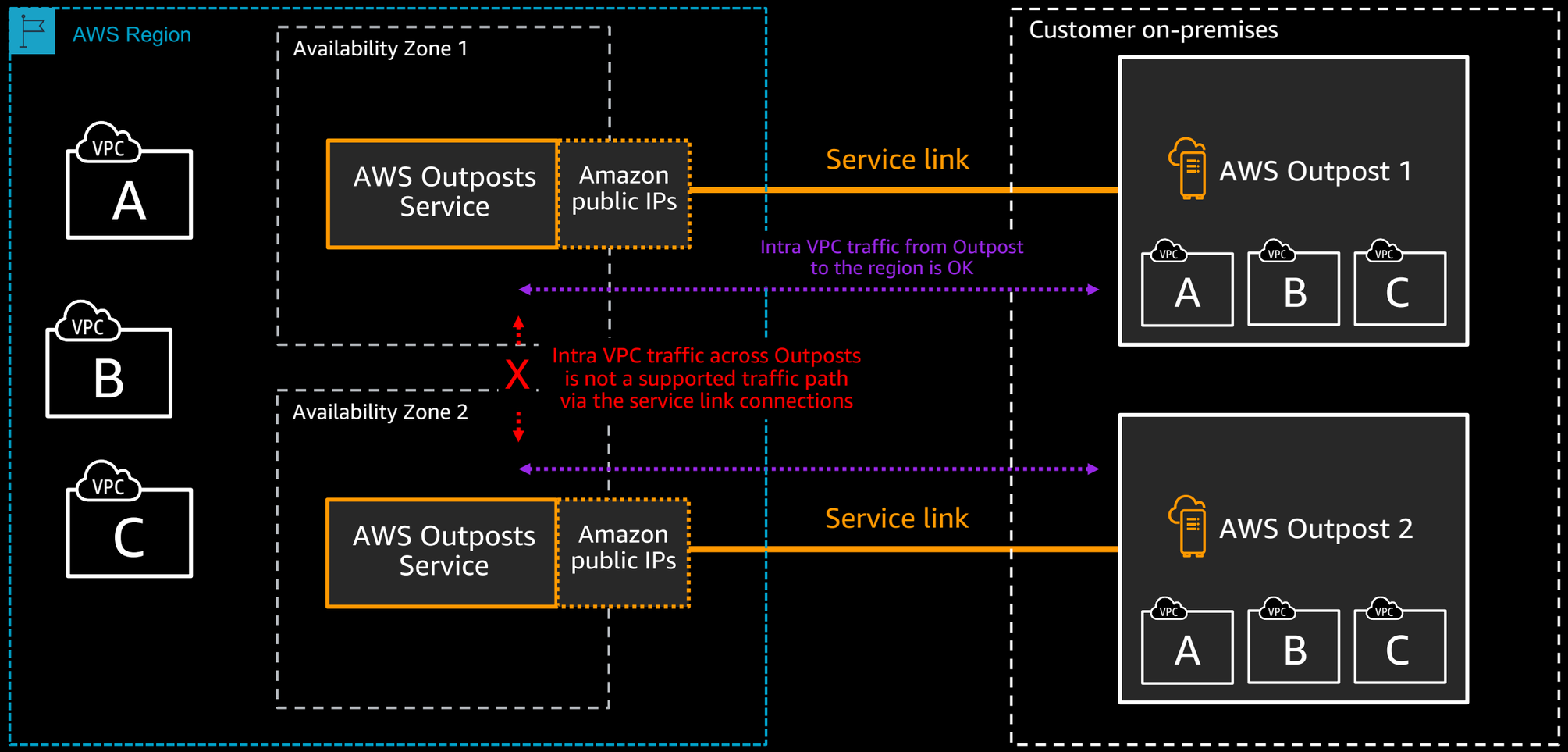


Coming soon! – Private service link connectivity

VPCs and a single Outpost deployment



VPCs and a multi-Outpost deployment

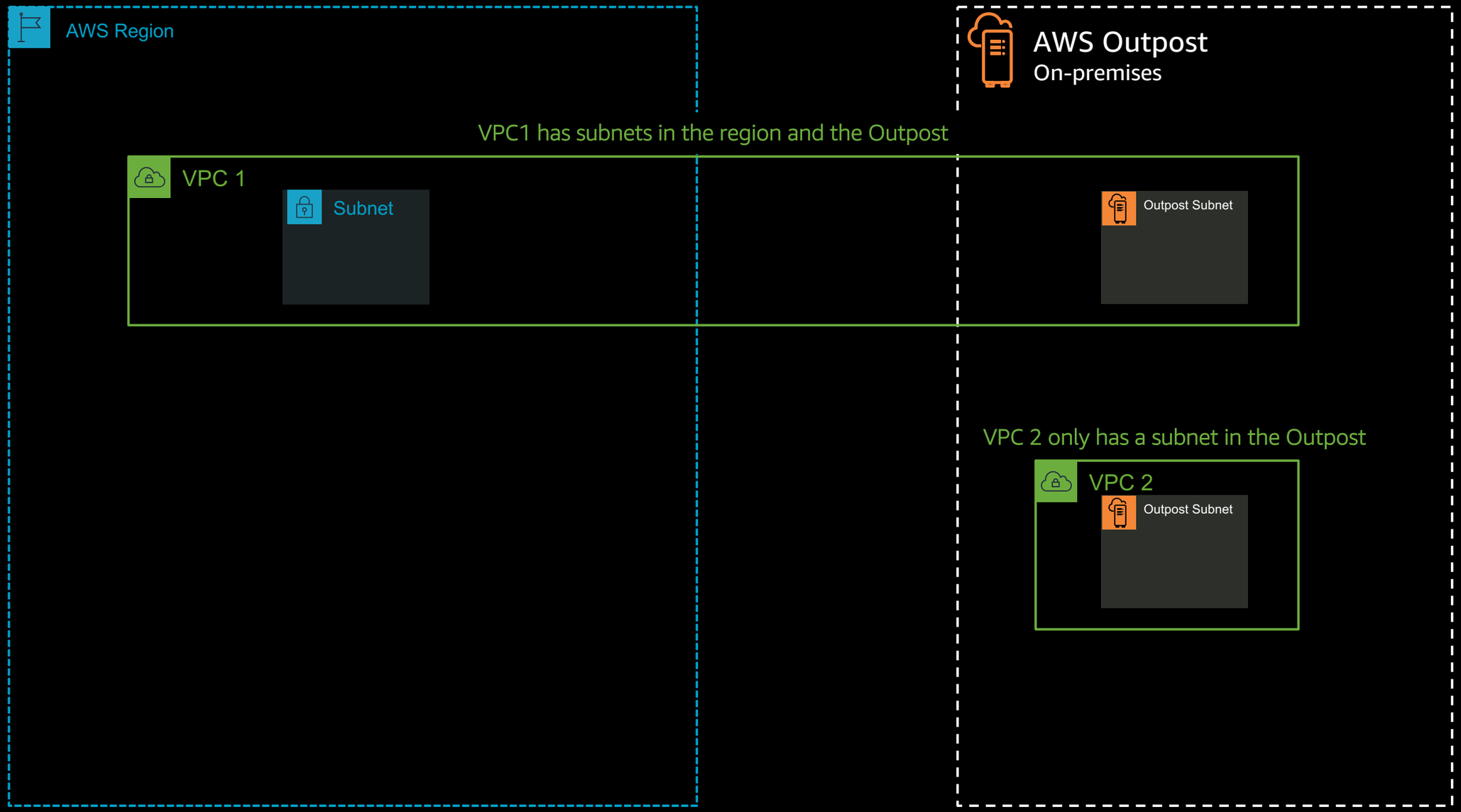




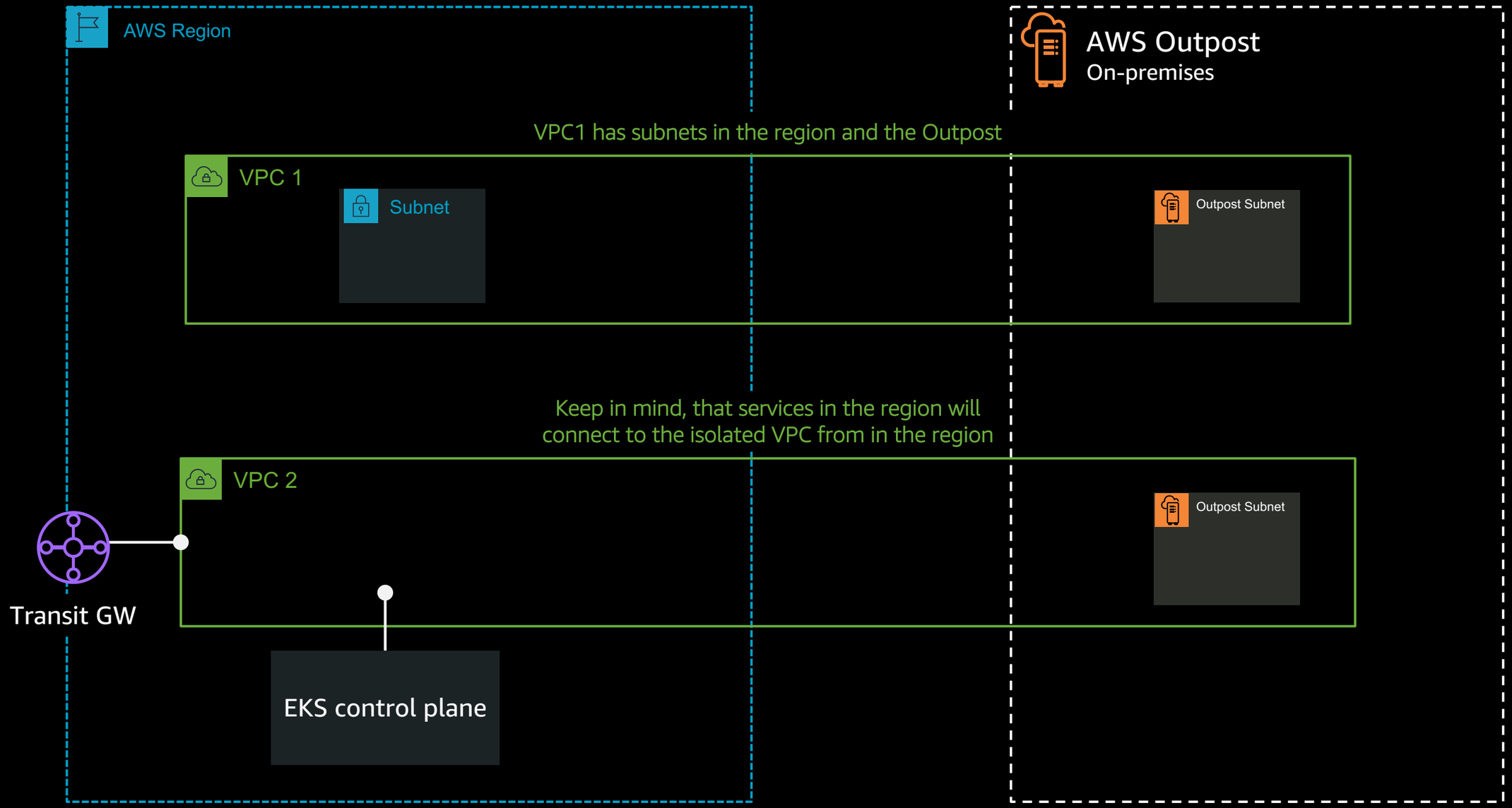
Amazon VPC Routing

To understand the Intra-VPC traffic path, we need to dive-in on VPC routing and AWS Outposts

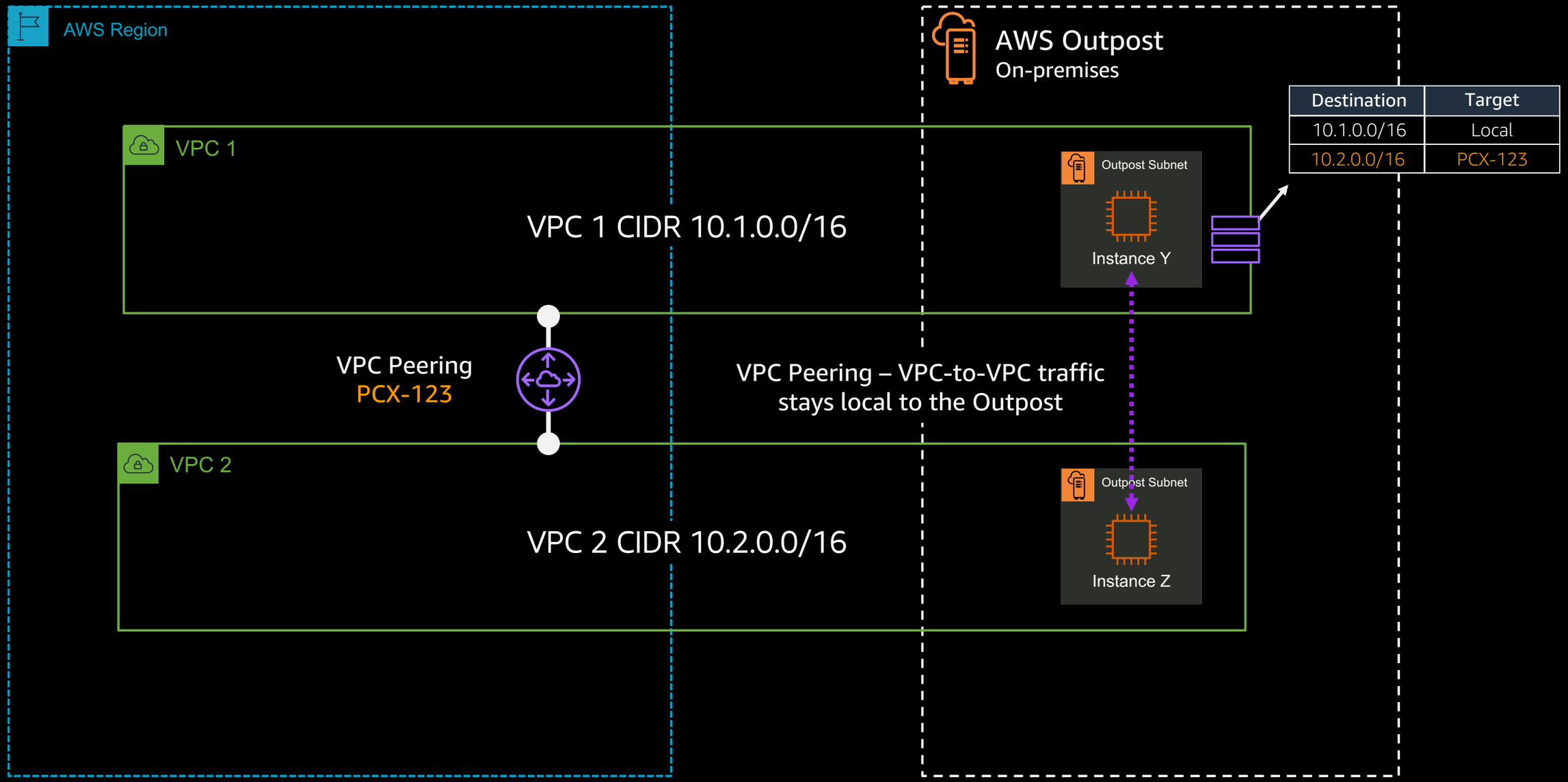
Building an isolated VPC



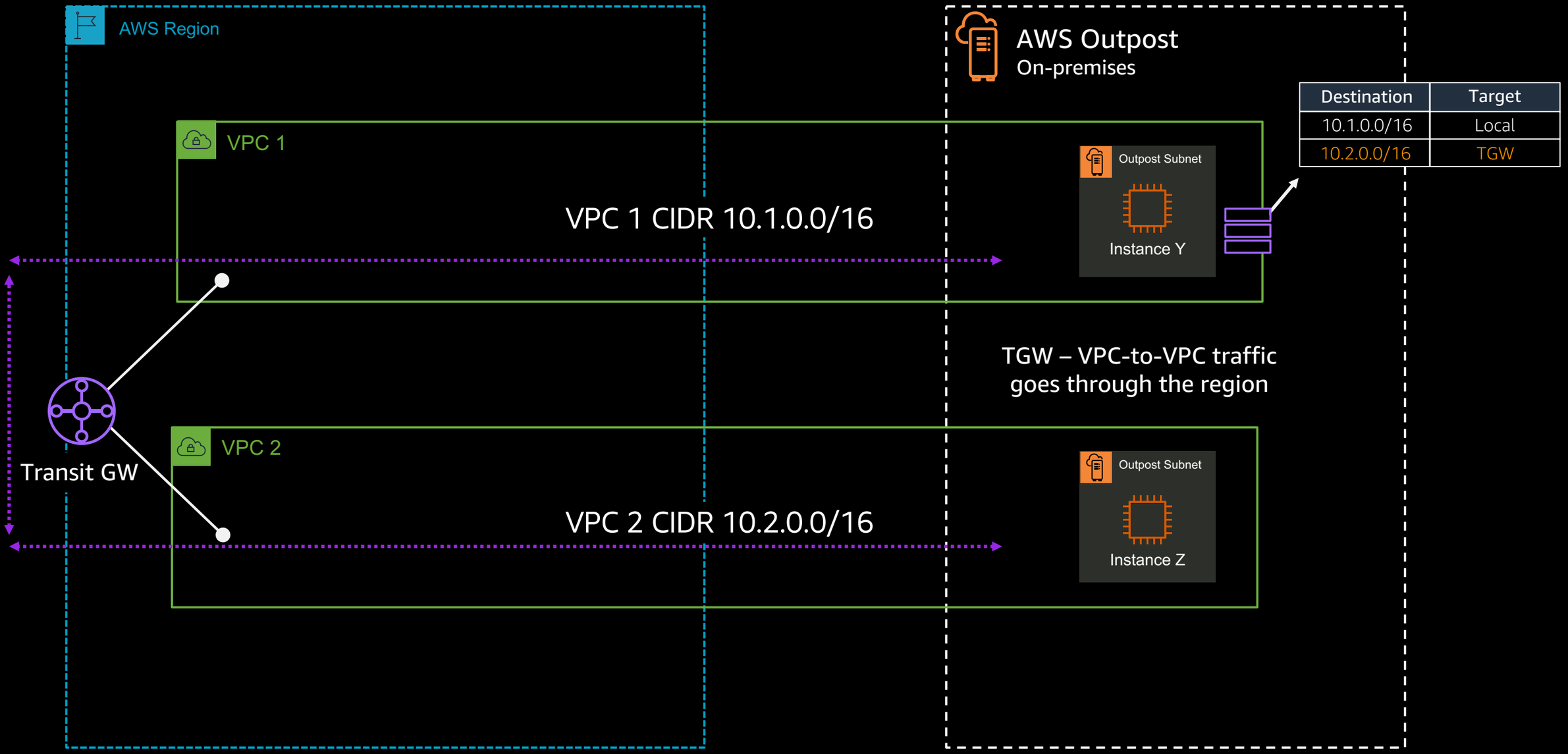
Building an isolated VPC



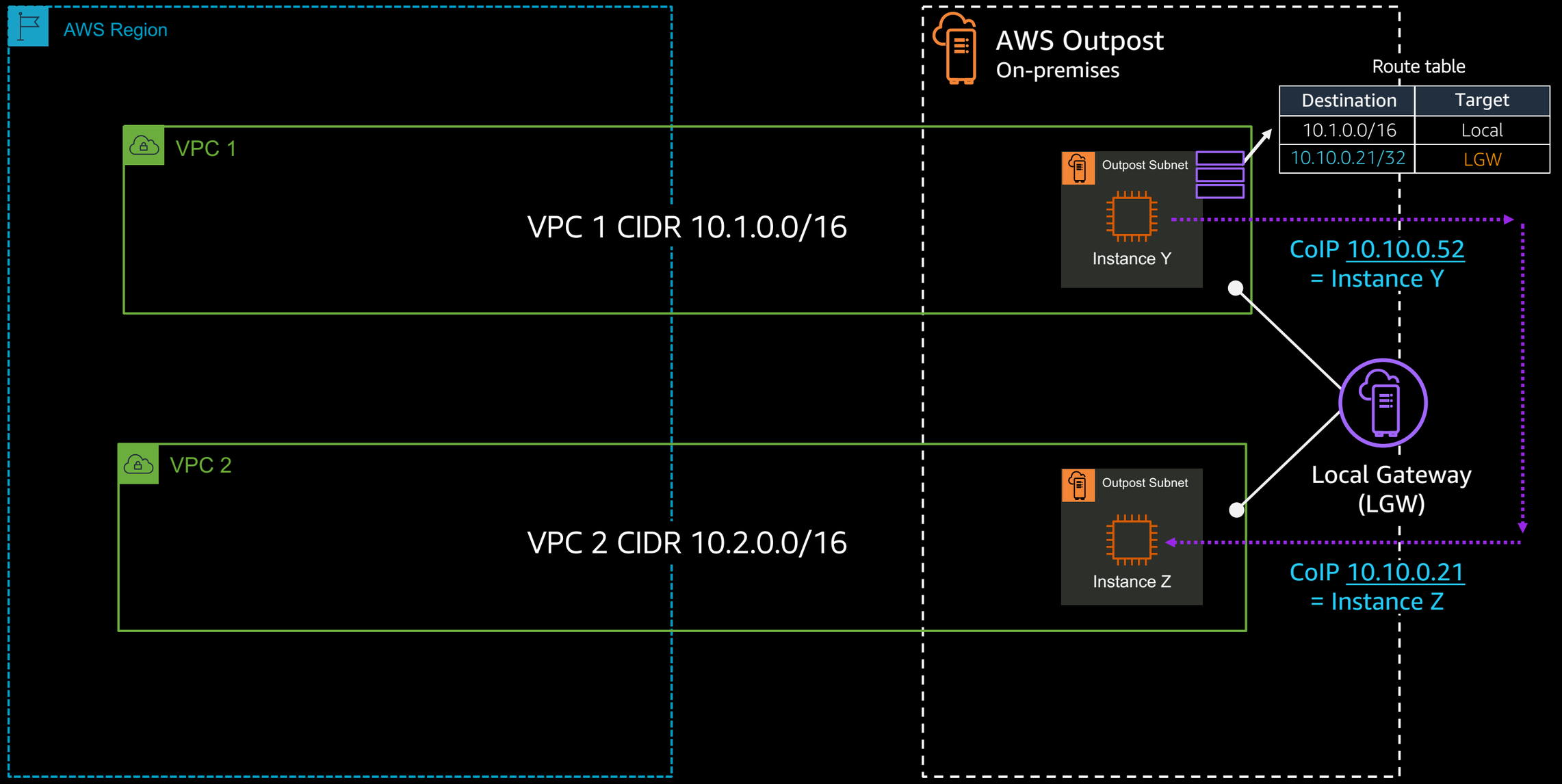
Traffic routing scenarios: VPC Peering



Traffic routing scenarios: AWS Transit Gateway

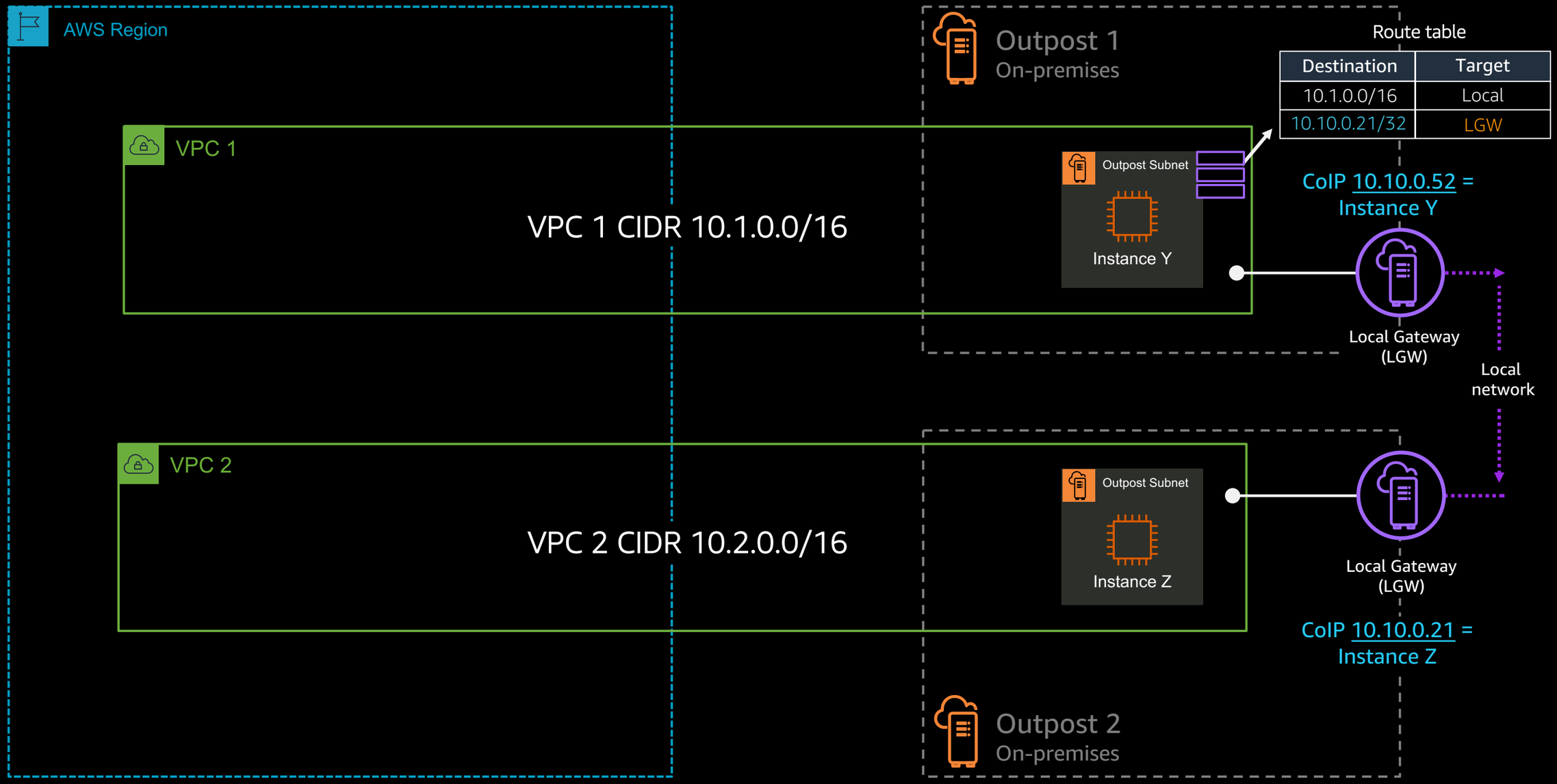


Traffic routing scenarios: Outposts Local Gateway (LGW)



Note: CoIPs are used as source and destination between VPCs via the LGW

Traffic routing scenarios: Outposts Local Gateway (LGW)



Note: Each Outpost has a separate LGW that's shared among its VPCs



AWS Outposts Architectures

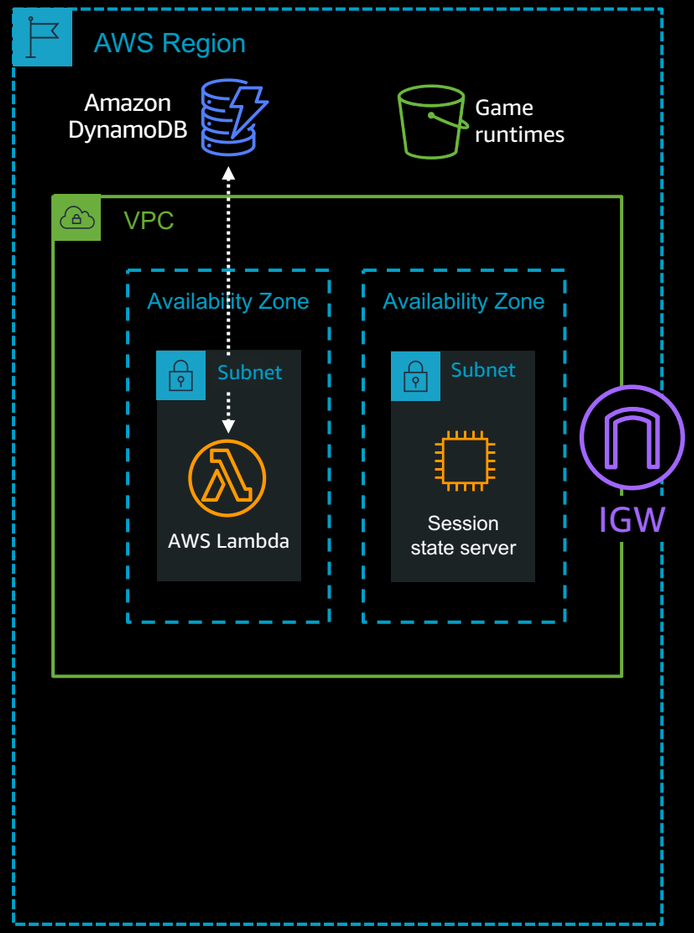
Rendering, inference, data processing? How about online games

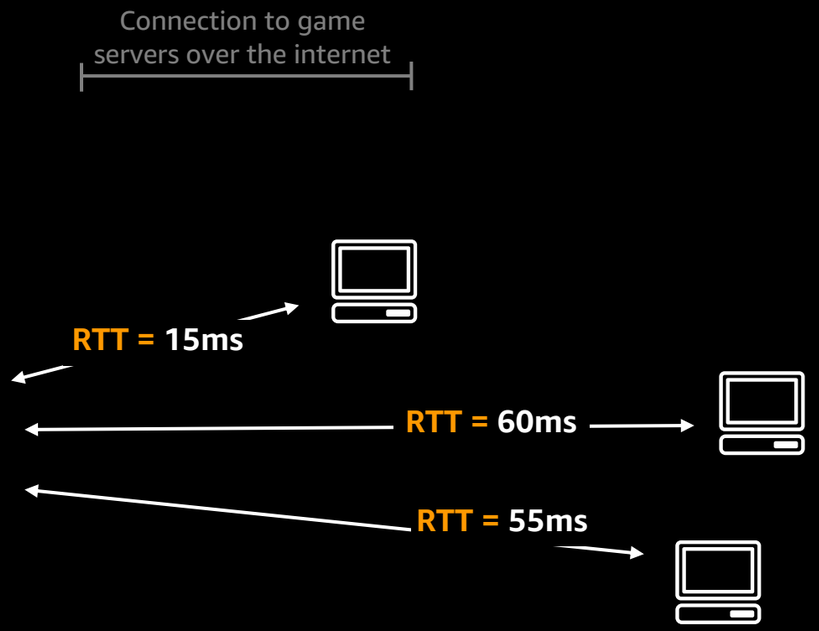


Low Latency

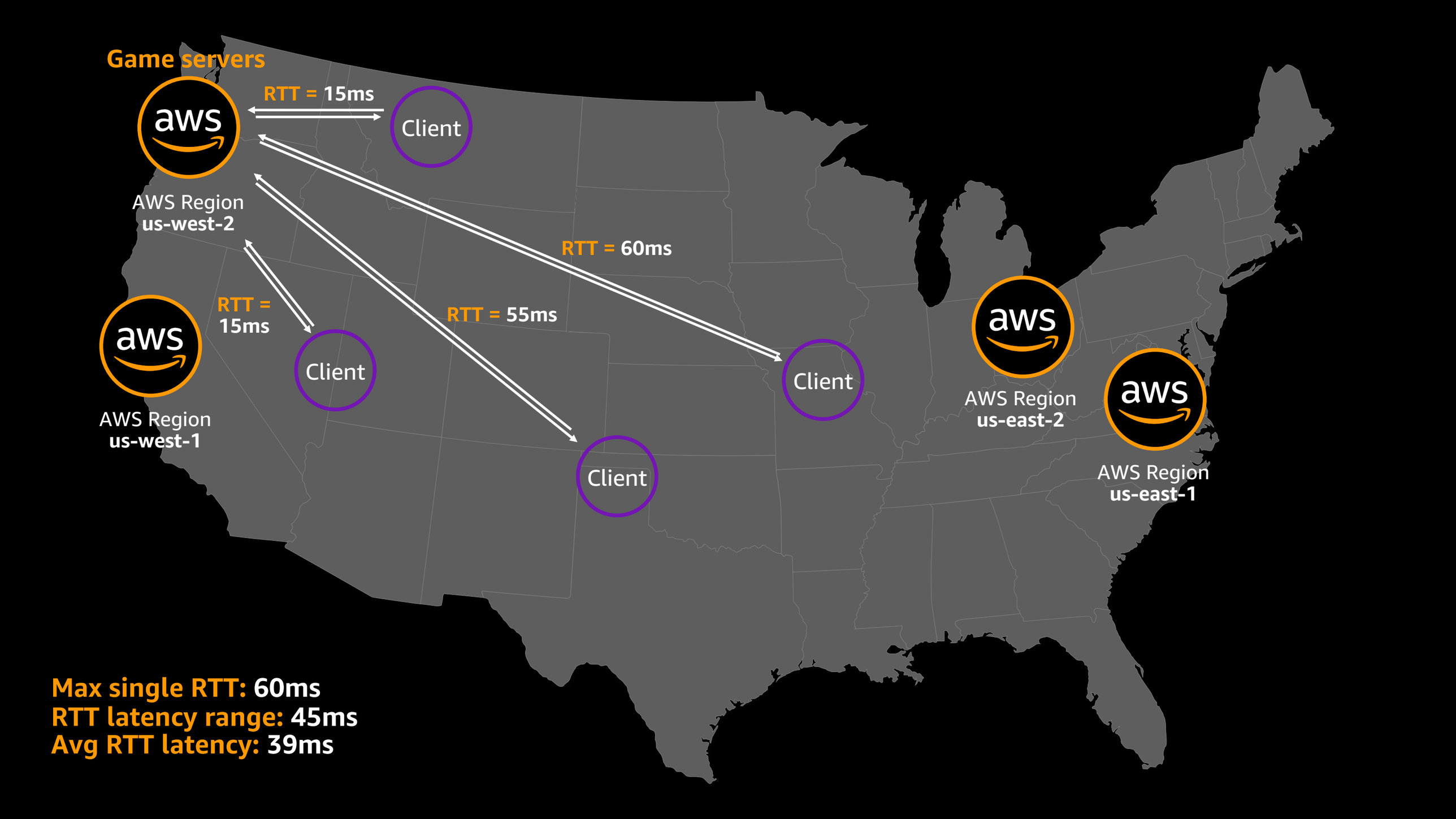
Rendering, inference, data processing

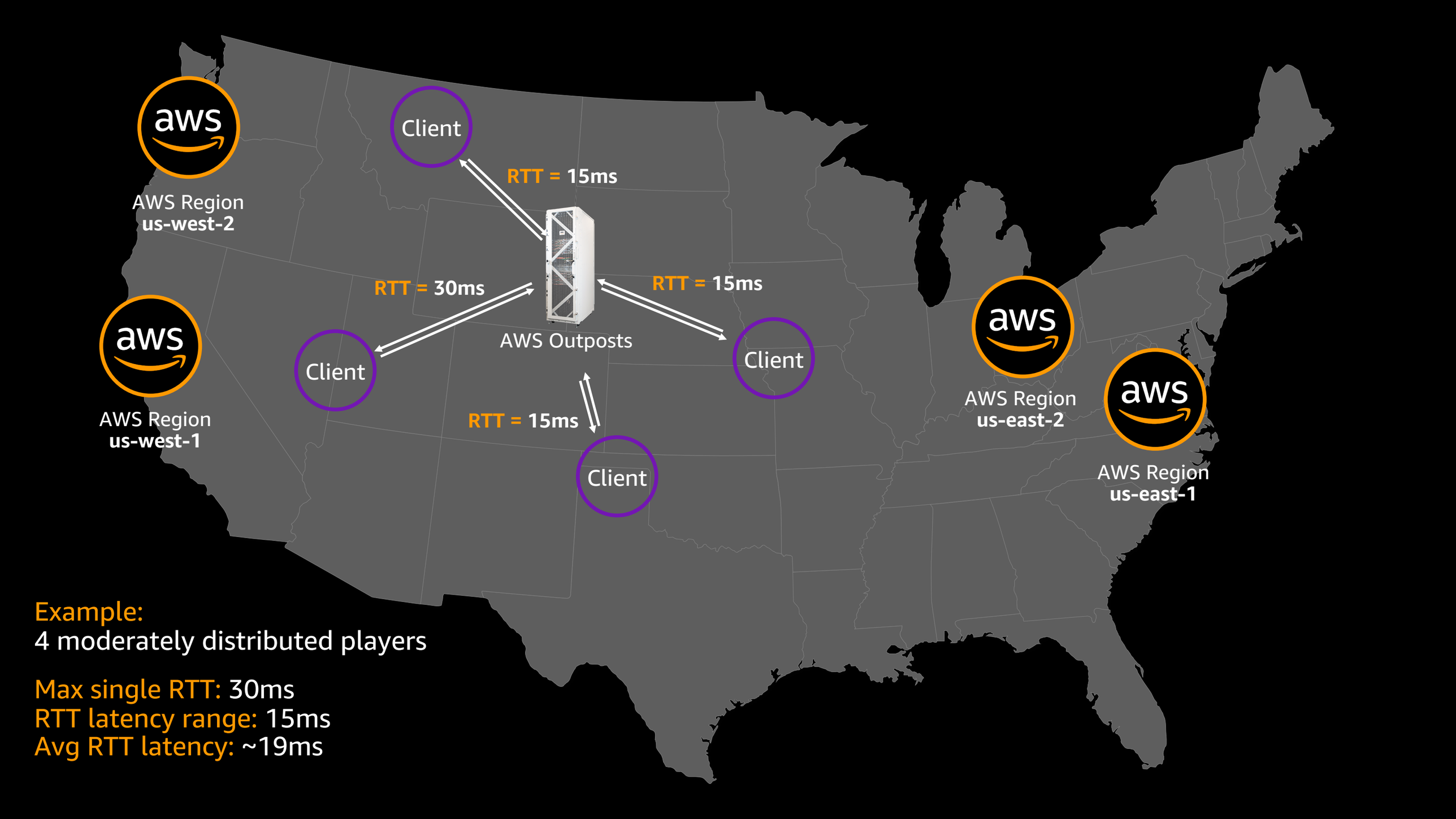
Using the AWS Region for low-latency online games





Due to the proximity of users to their closest region, a small amount of variance in latency occurs

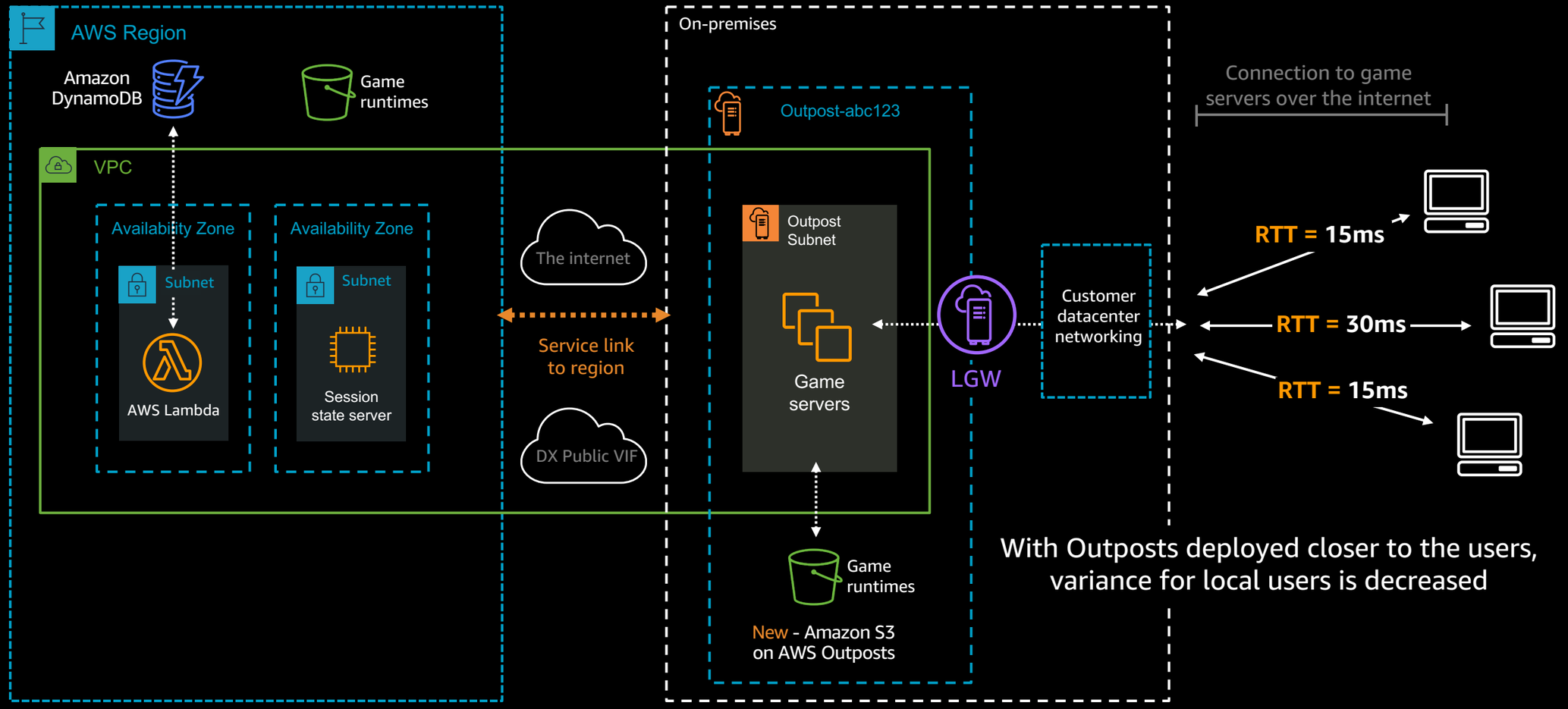

Game servers
RTT = 15ms
Client
AWS Region
us-west-2
RTT = 60ms
RTT = 15ms
RTT = 55ms
Client
Client
Client
AWS Region
us-west-1
AWS Region
us-east-2
AWS Region
us-east-1
Max single RTT: 60ms
RTT latency range: 45ms
Avg RTT latency: 39ms



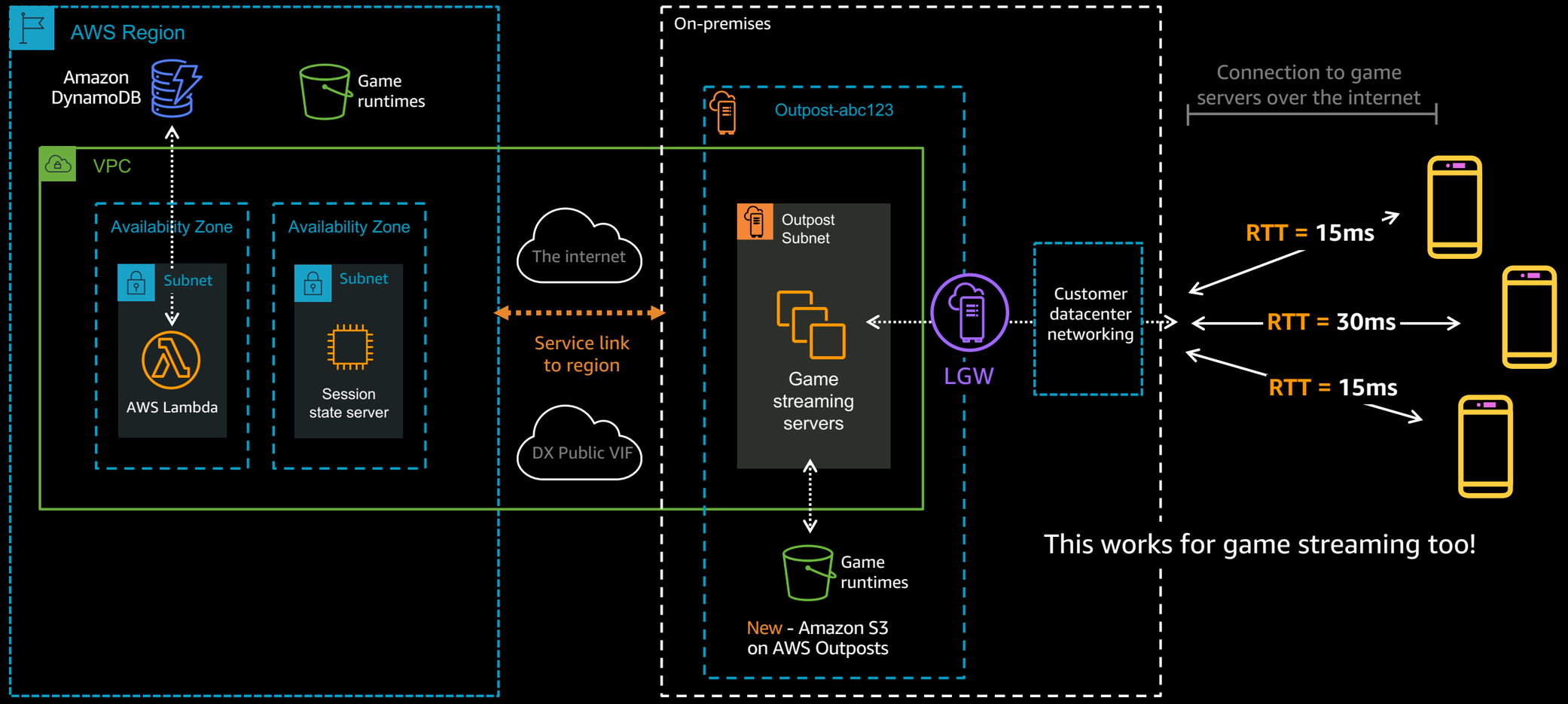
Example:
4 moderately distributed players

Max single RTT: 30ms
RTT latency range: 15ms
Avg RTT latency: ~19ms

Using AWS Outposts for low-latency online games



Using AWS Outposts for low-latency online games





AWS Outposts Architectures

Application Modernization with AWS Outposts offering the same AWS Infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility.



Low Latency

Rendering, inference, data processing



Application Modernization

Modernize enterprise applications running at the edge

Application modernization tools



AWS CloudFormation



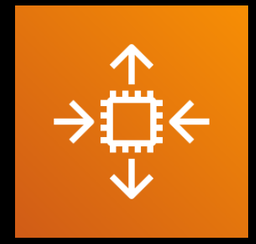
Application Load Balancer



Amazon Simple Storage Service (S3)



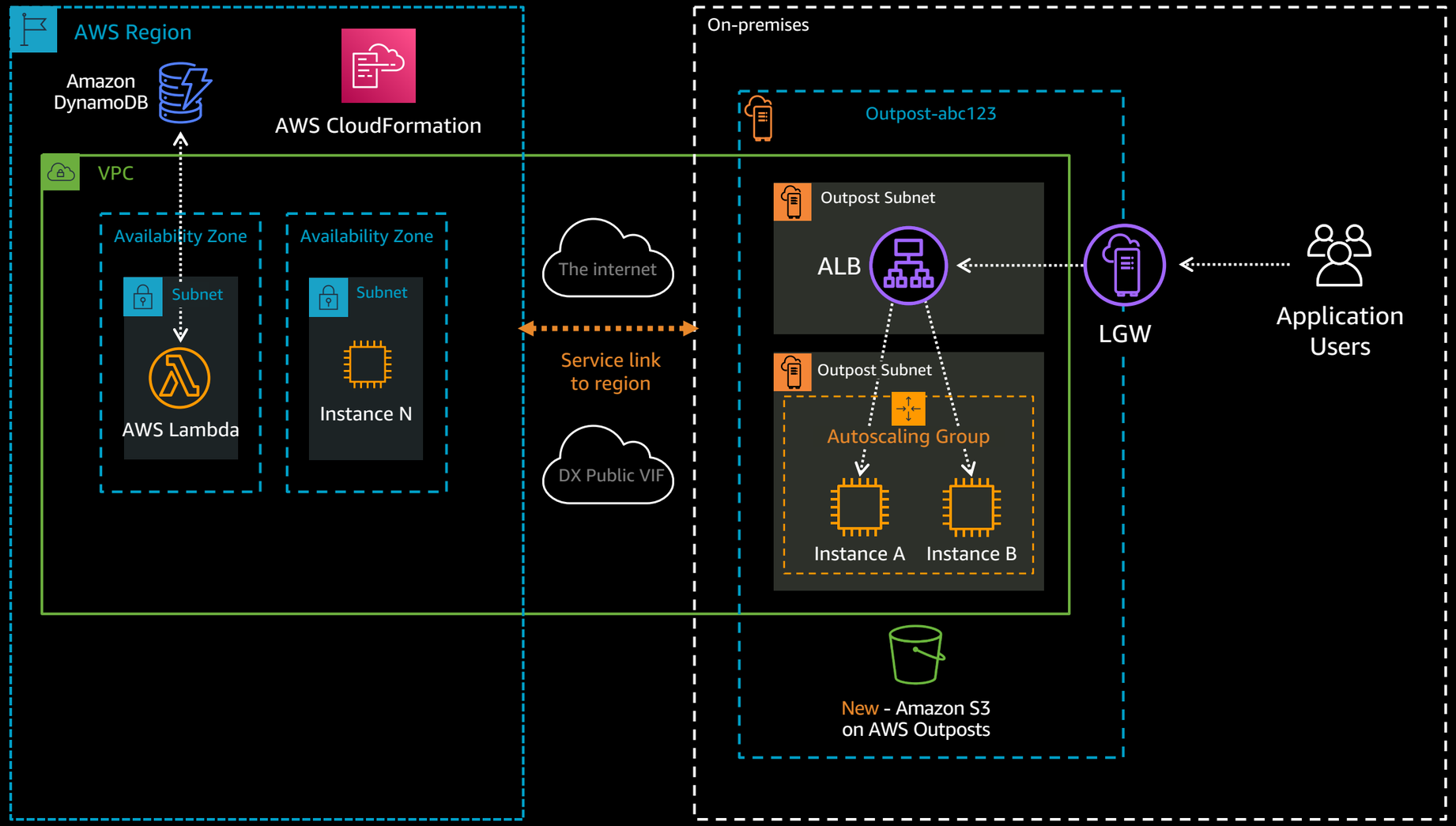
Amazon VPC



Amazon EC2 Auto Scaling

And many more!

Using AWS Outposts for application modernization





AWS Outposts Architectures

Data Residency for regulatory, security, or process requirements.



Low Latency

Rendering, inference, data processing



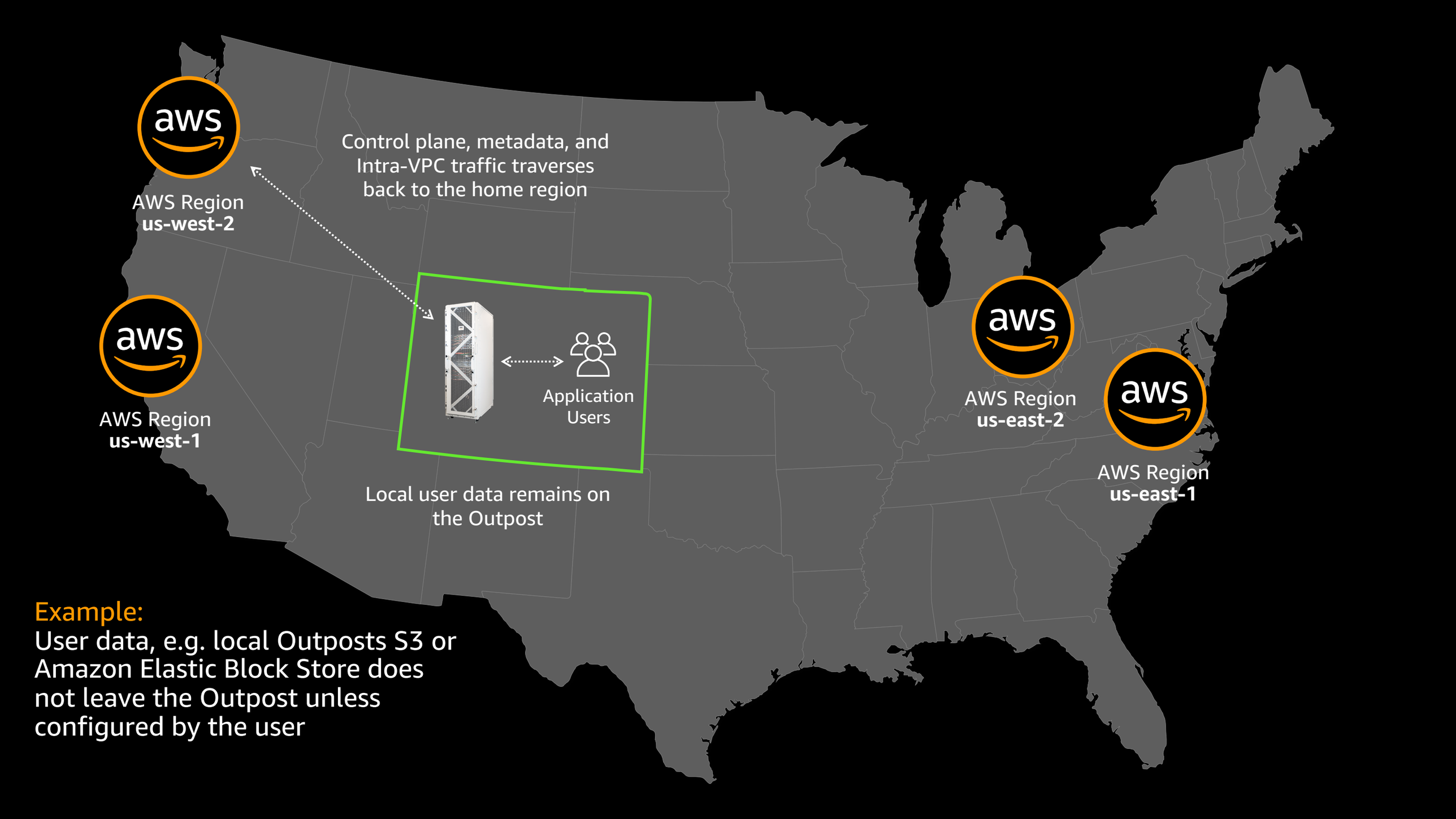
Application Modernization

Modernize enterprise applications running at the edge



Data Residency

Regulatory, security, process requirements



Example:

User data, e.g. local Outposts S3 or Amazon Elastic Block Store does not leave the Outpost unless configured by the user



AWS Outposts Architectures

AWS Outposts for Local Data Processing



Low Latency

Rendering, inference, data processing



Application Modernization

Modernize enterprise applications running at the edge



Data Residency

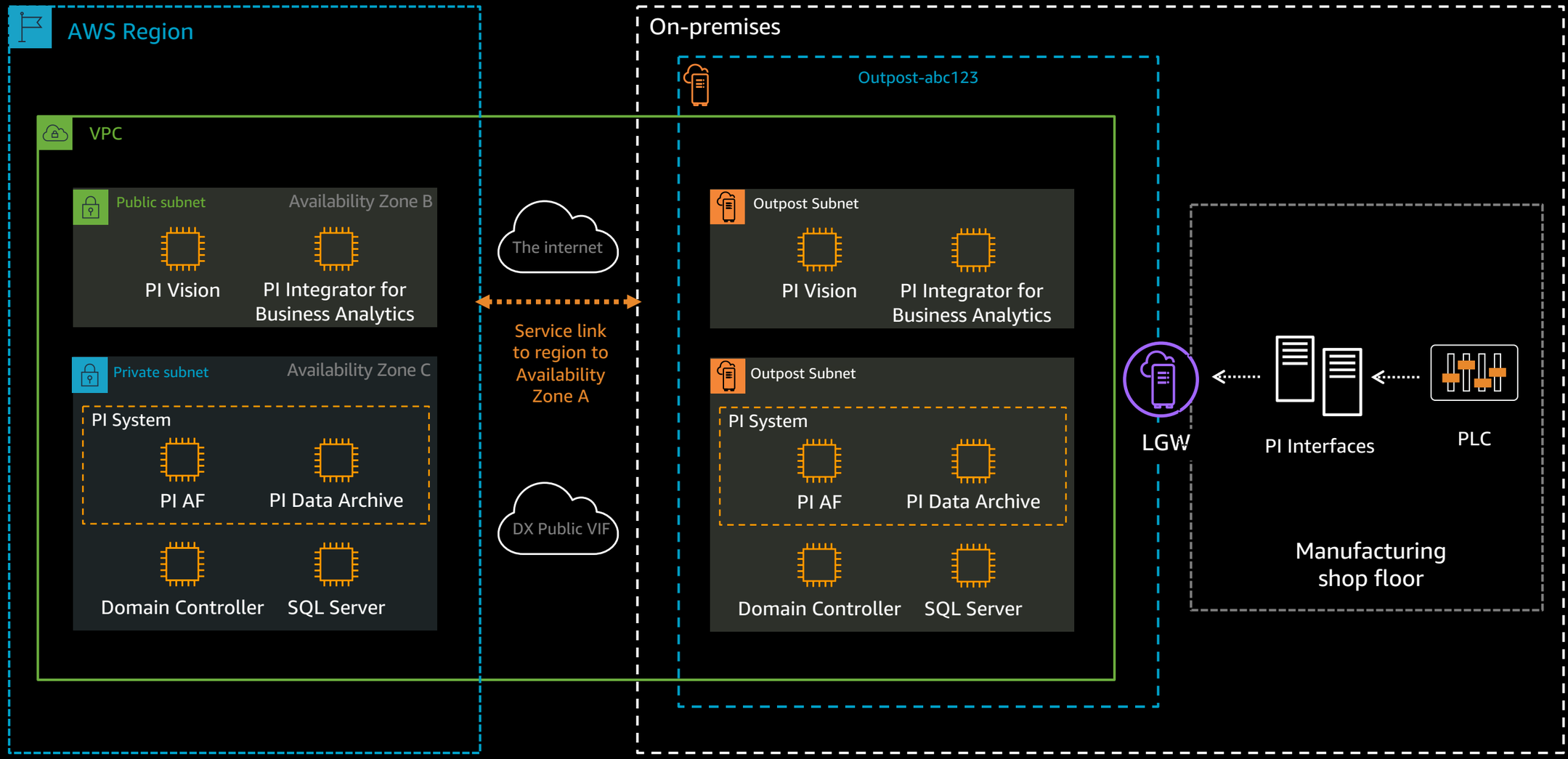
Regulatory, security, process requirements



Local Data Processing

Local control systems, 5G/IOT

Using AWS Outposts for local data processing





AWS Outposts Architectures



Low Latency

Rendering, inference, data processing



Application Modernization

Modernize enterprise applications running at the edge



Data Residency

Regulatory, security, process requirements

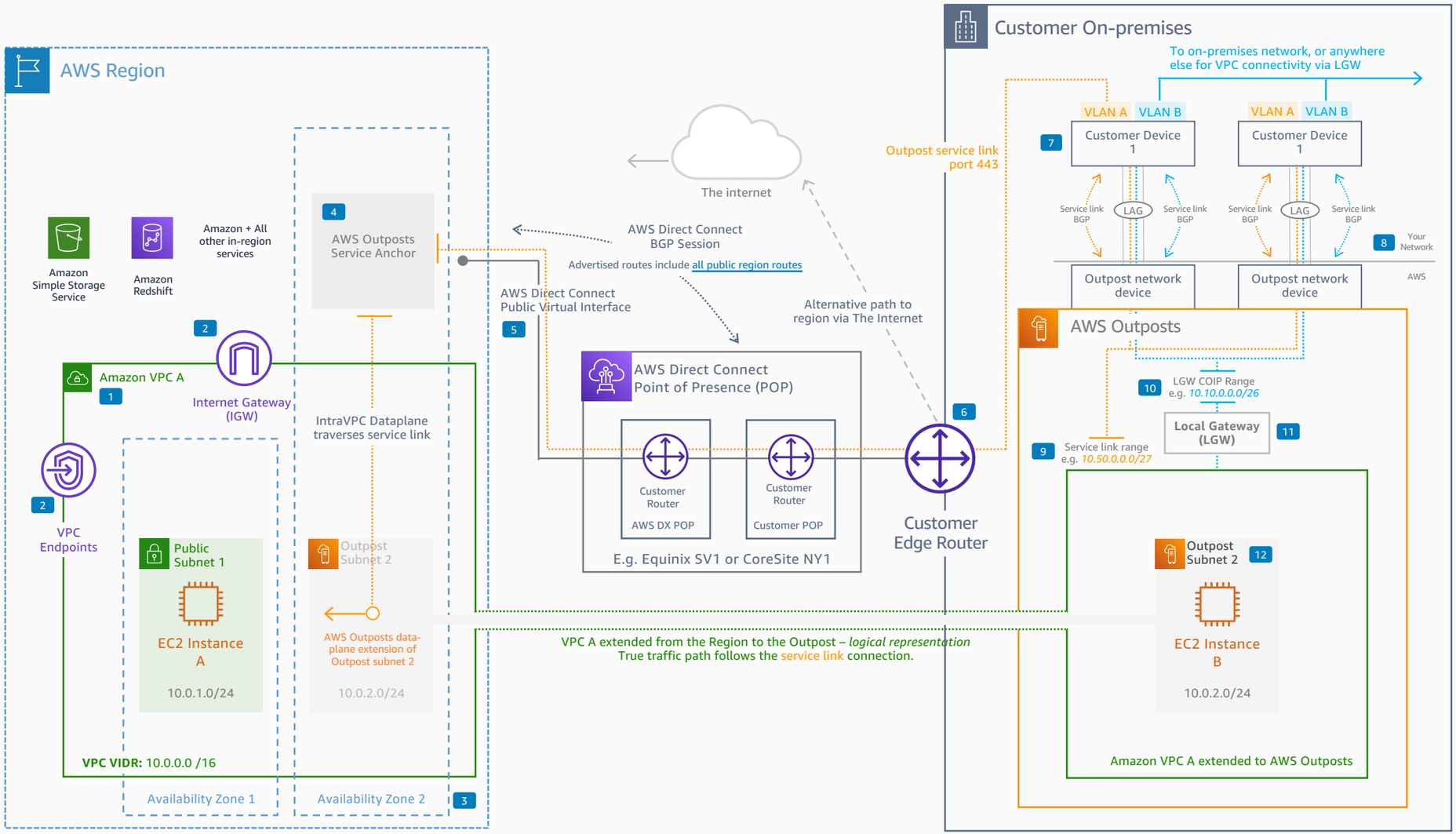


Local Data Processing

Local control systems, 5G/IOT

AWS Outposts – Networking Reference Architecture

An architectural overview of AWS Outposts connectivity for LAN, WAN, and Amazon VPC



1. Multiple AWS Virtual Private Cloud (VPC) can be associated with the same outpost.
2. Region level services can be connected to from the outpost via intra-VPC connectivity.
3. An outpost is homed to an availability zone.
4. **AWS Outposts** service link anchor is created within the availability zone of your choosing and fronted by public Amazon IPs. The Outpost will need connectivity back to these IPs to establish it's service-link connection for both control plane and data plane traffic.
5. An **AWS Direct Connect** public virtual interface (VIF) can be used to connect back to the AWS Outposts service anchor IPs. The direct connect public VIF will advertise all of the Amazon public ranges from Amazon to your router.
6. An edge router with either a **Direct Connect** connection back to the region or public internet can be used to reach the **Outposts** service anchor in the region. Network Address Translation (NAT) or Port Address Translation (PAT) can be used with this device for the service link. Service link establishment is initiated from the Outpost, never from the region.
7. Customer Devices need to support:
   Link aggregation - connections to the Outpost network devices will be added to a link aggregation group using LACP

   VLANs - Point to point virtual LANs (VLANs) are configured between each Outpost network device and your customer device. VLAN A is used for service link connectivity back to the AWS region, and VLAN B is used for Local Gateway (LGW) connectivity towards your on-premises network.

   Dynamic routing - Border Gateway Protocol (BGP) will be configured between each customer device and Outpost network device for each VLAN. 4 total BGP sessions are shown here between devices.
8. Demarcation between your network and the Outpost. The demarcation is the physical patch panel at the top of the rack. Fibers to the patch panel will be provided by you.
9. A Classless Inter-Domain Routing (CIDR) range is provided by you for the service link. This range is a /26 private or public IP range. The service link infrastructure range is used to address infrastructure in the outpost that needs connectivity back to the Outpost anchor in the AWS region.
10. A Classless Inter-Domain Routing (CIDR) range is provided by you for the LGW. This range, called the "Customer Owned IP" range (CoIP) range, is used by you to address instances inside the Outpost with Elastic IPs from this range that need connectivity to your on-premises workloads.
11. The Local Gateway, one per outpost, attached to one or multiple VPCs within the outpost. The LGW provides the NAT function between the Outpost VPC range and the appropriate Elastic IPs from the COIP range.
12. An Outpost subnet, created in an **Amazon VPC**, in an account that has an Outpost associated with it. Outpost subnets can also be shared with other accounts within the same organization.

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture



AWS Outposts – Networking Reference Architecture

An architectural overview of AWS Outposts connectivity for LAN, WAN, and Amazon VPC

© 2020, Amazon Web Services, Inc. or its Affiliates.



More resources

How AWS Outposts Works

https://amzn.to/2U4TJ9E

SCAN ME

AWS Outposts Overview

https://aws.amazon.com/outposts/

SCAN ME

More Resources –

https://bit.ly/3embZ6K

SCAN ME



Related sessions

NET202: Go global with AWS multi-Region network services

NET203: Demystifying data transfer on AWS

NET205: Building networks with solutions from APN & AWS Marketplace Partners

NET303: Shared VPCs, lessons learned, and best practices

CMP208: AWS Outposts: Cloud where you want it

CMP309: AWS Outposts: Bringing the AWS experience on premises

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.