
AWS
re:Invent

NET205

Building with AWS PrivateLink, Gateway Load Balancer, and AWS Partners

James Wenzel

Sr. Partner Solutions Architect, Networking

AWS

AWS re:Invent

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

Agenda

Building blocks

- VPC and public services
- TGW
- Ingress Routing

ENIs explained

GWLB (Gateway Load Balancer)

AWS PrivateLink

Putting it all together

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

Desired outcomes

Secure your network to protect yourself and your customers

Connect to your workloads

Connect your workloads to your providers

Connect your workloads to your customers

Secure your network protecting you and your customers

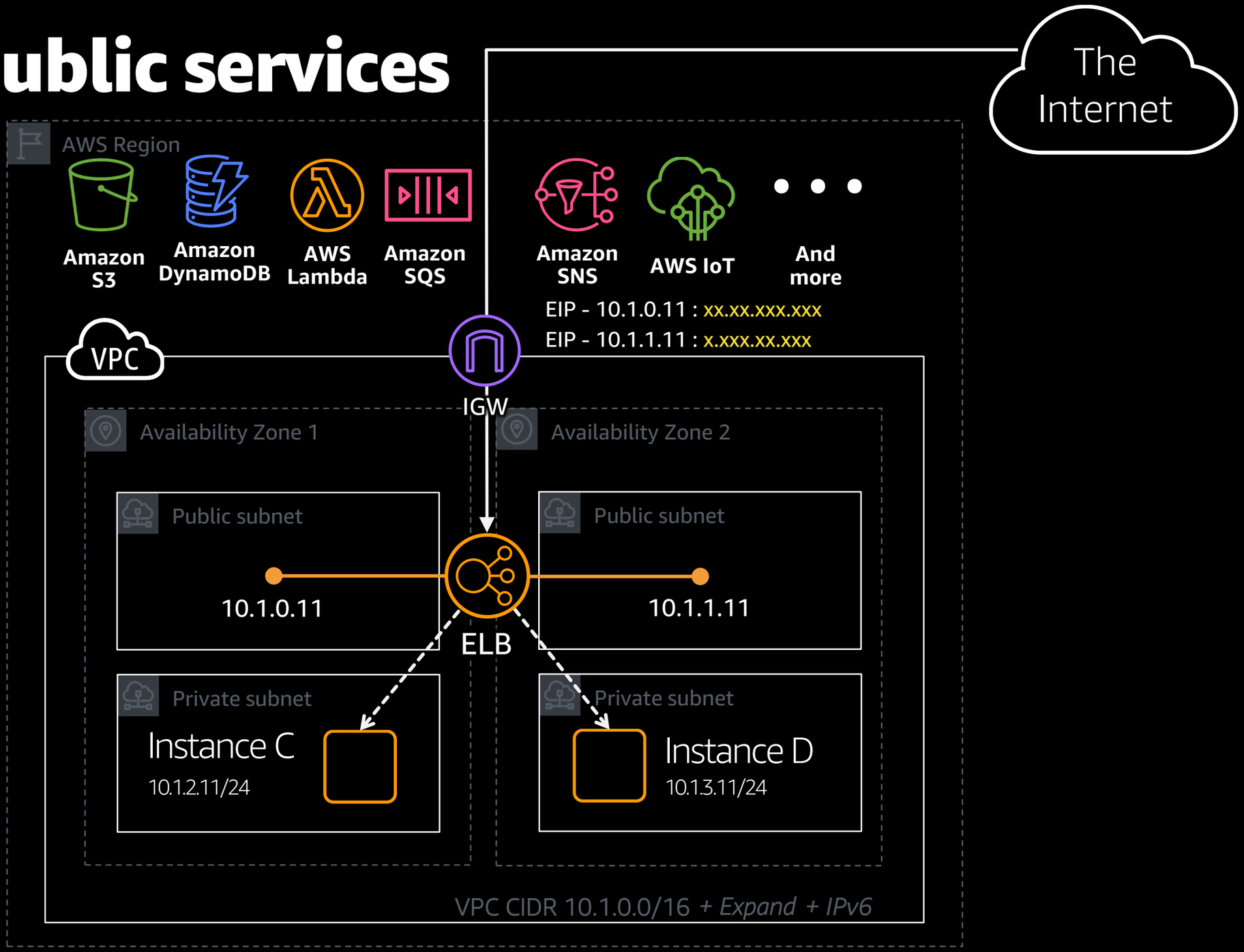
Building blocks



AWS re:Invent

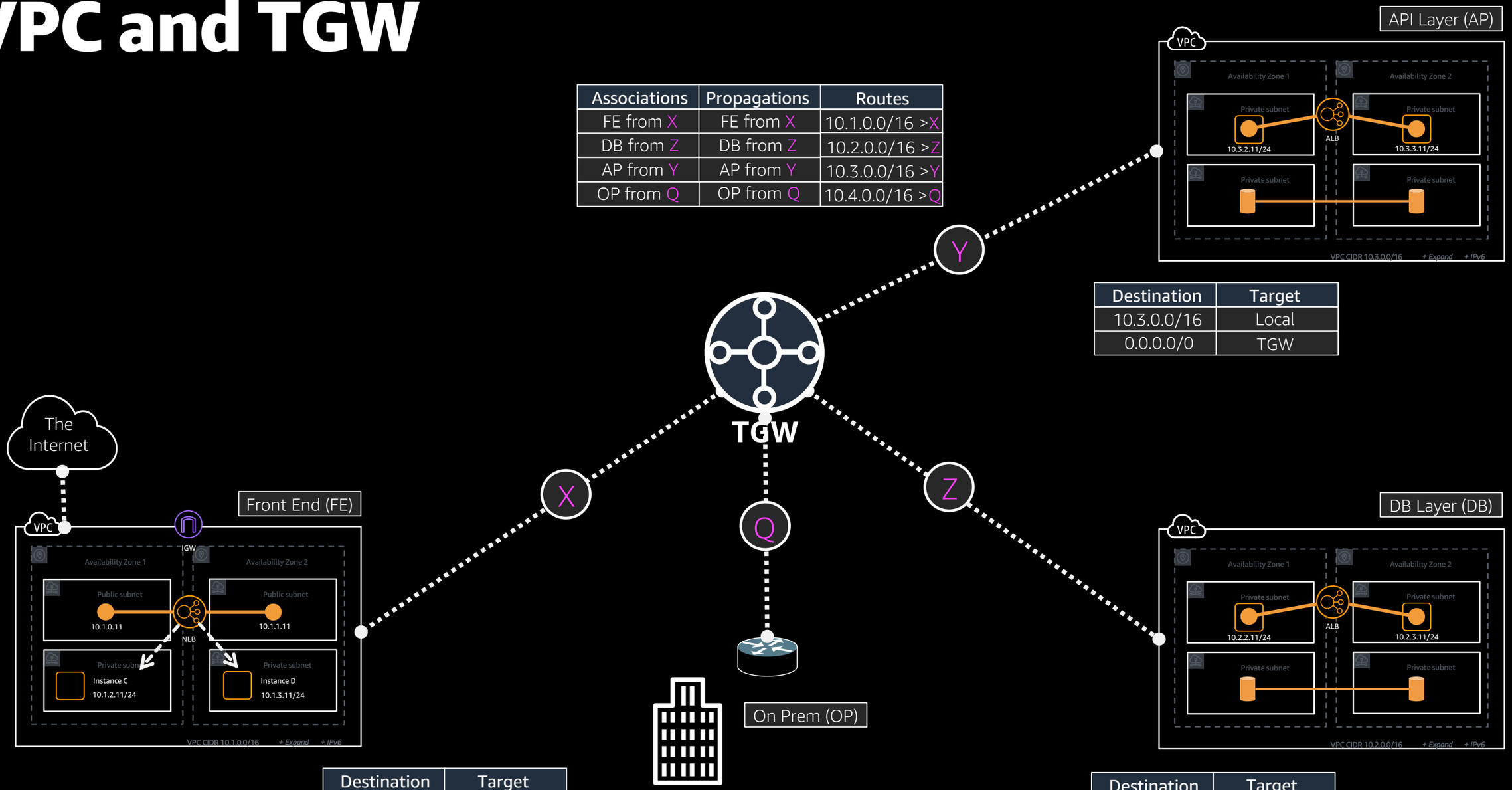
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC and public services



VPC and TGW

Associations	Propagations	Routes
FE from X	FE from X	10.1.0.0/16 >X
DB from Z	DB from Z	10.2.0.0/16 >Z
AP from Y	AP from Y	10.3.0.0/16 >Y
OP from Q	OP from Q	10.4.0.0/16 >Q



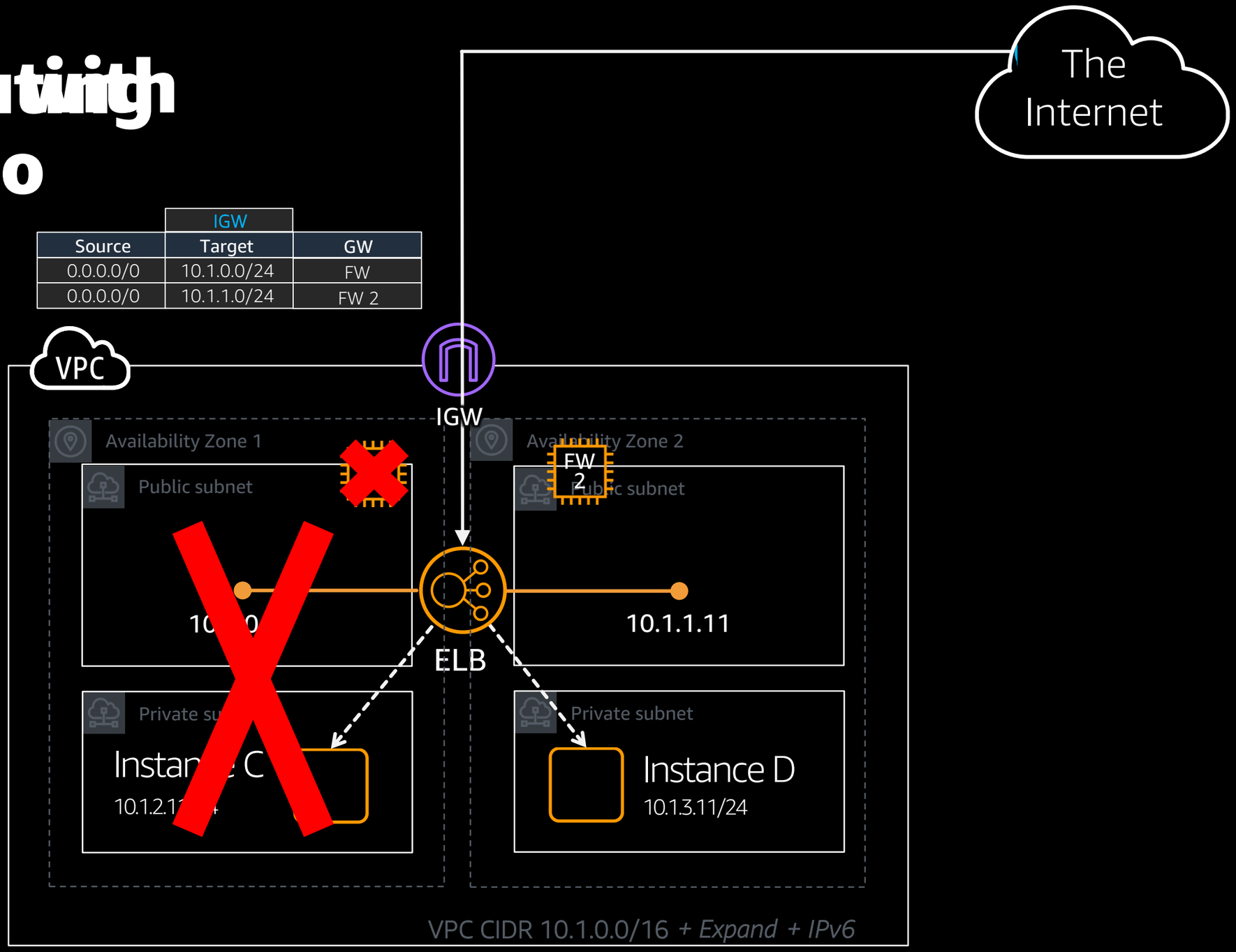
Destination	Target
10.3.0.0/16	Local
0.0.0.0/0	TGW

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
10.0.0.0/8	TGW

Destination	Target
10.2.0.0/16	Local
0.0.0.0/0	TGW

Limitations with this scenario

IGW		
Source	Target	GW
0.0.0.0/0	10.1.0.0/24	FW
0.0.0.0/0	10.1.1.0/24	FW 2



We have a solution for this!

ENI-based services

GWLB and AWS PrivateLink

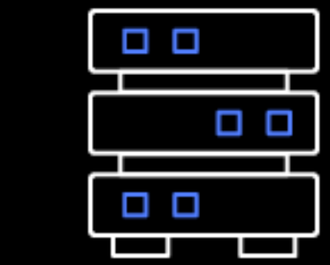


AWS re:Invent

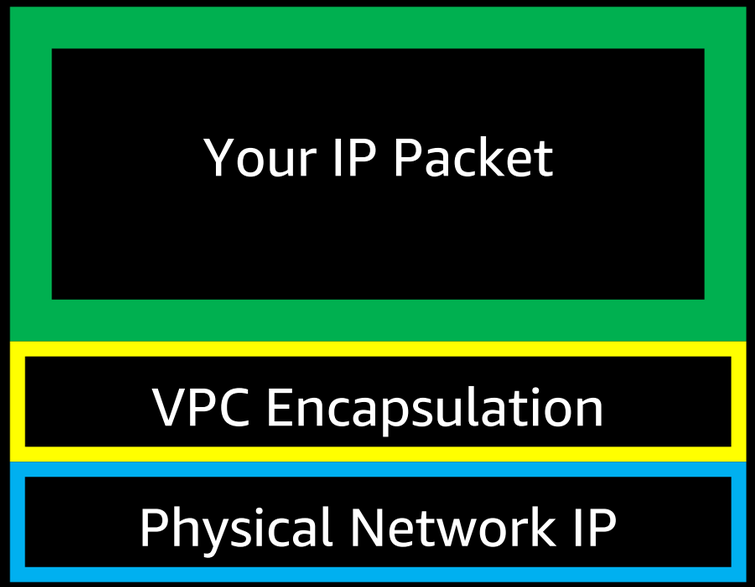
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

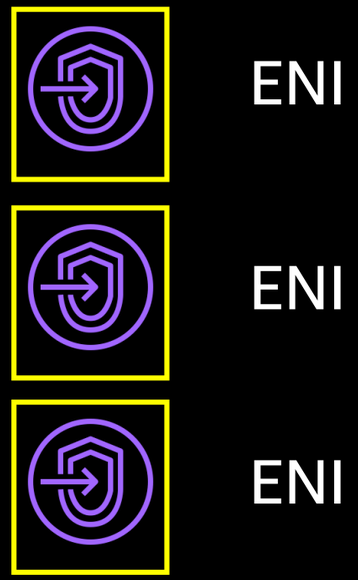
AWS PrivateLink and GWLB under the hood

Hyperplane based ENI: Explained



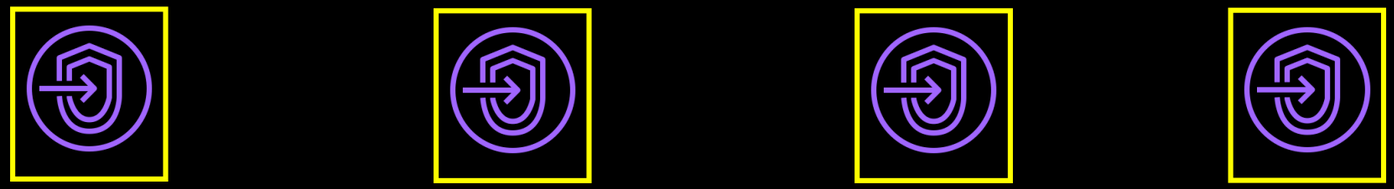
Physical Host





AWS PrivateLink and GWLB under the hood

Hyperplane based ENI: Benefits



10 – 40 Gbps throughput speeds

Redundant and scalable software defined networking

Hyperplane based ENIs only need to know about flows

Transactional state decision performed in tens of microseconds

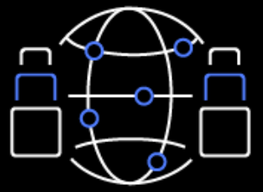
GWLB
(Gateway Load Balancer)



AWS re:Invent

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

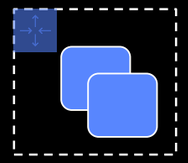
GWLB



Access appliances in another VPC



Remains in AWS's private network



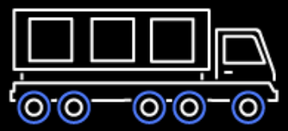
Device auto scaling



Mutually initiated



Satisfy security



Add agility

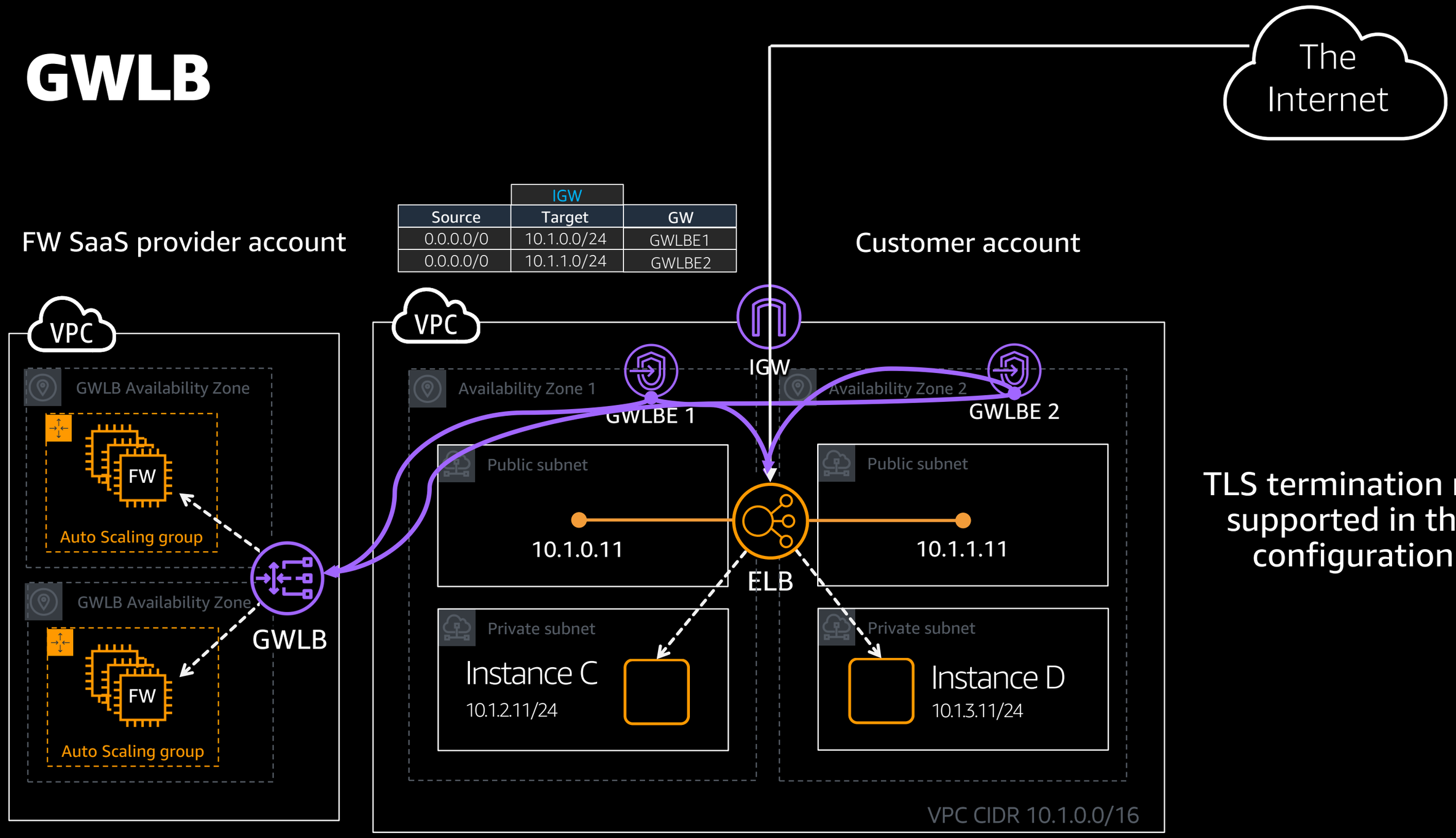


Reduce costs



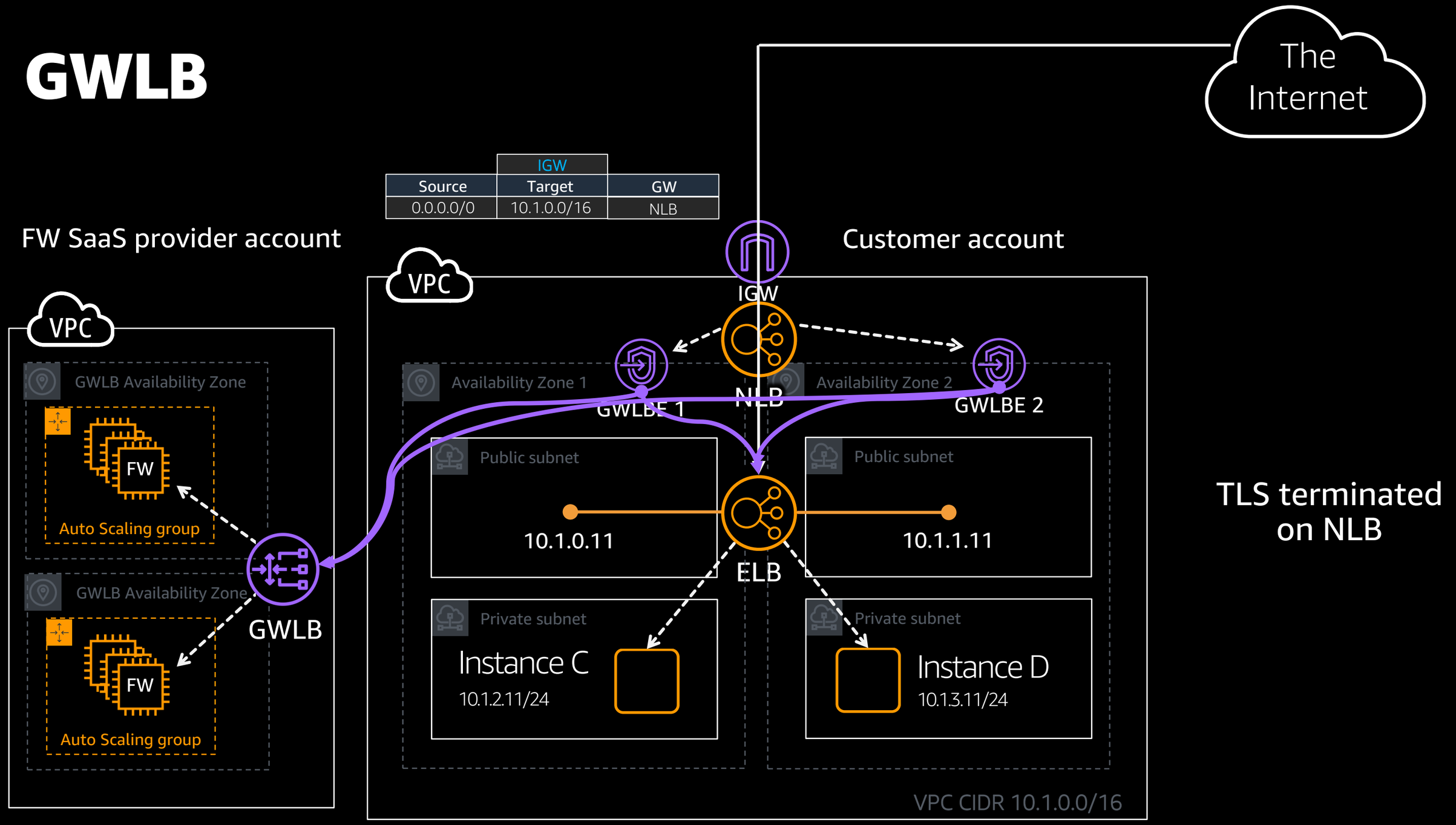
Maintains flows

GWLB

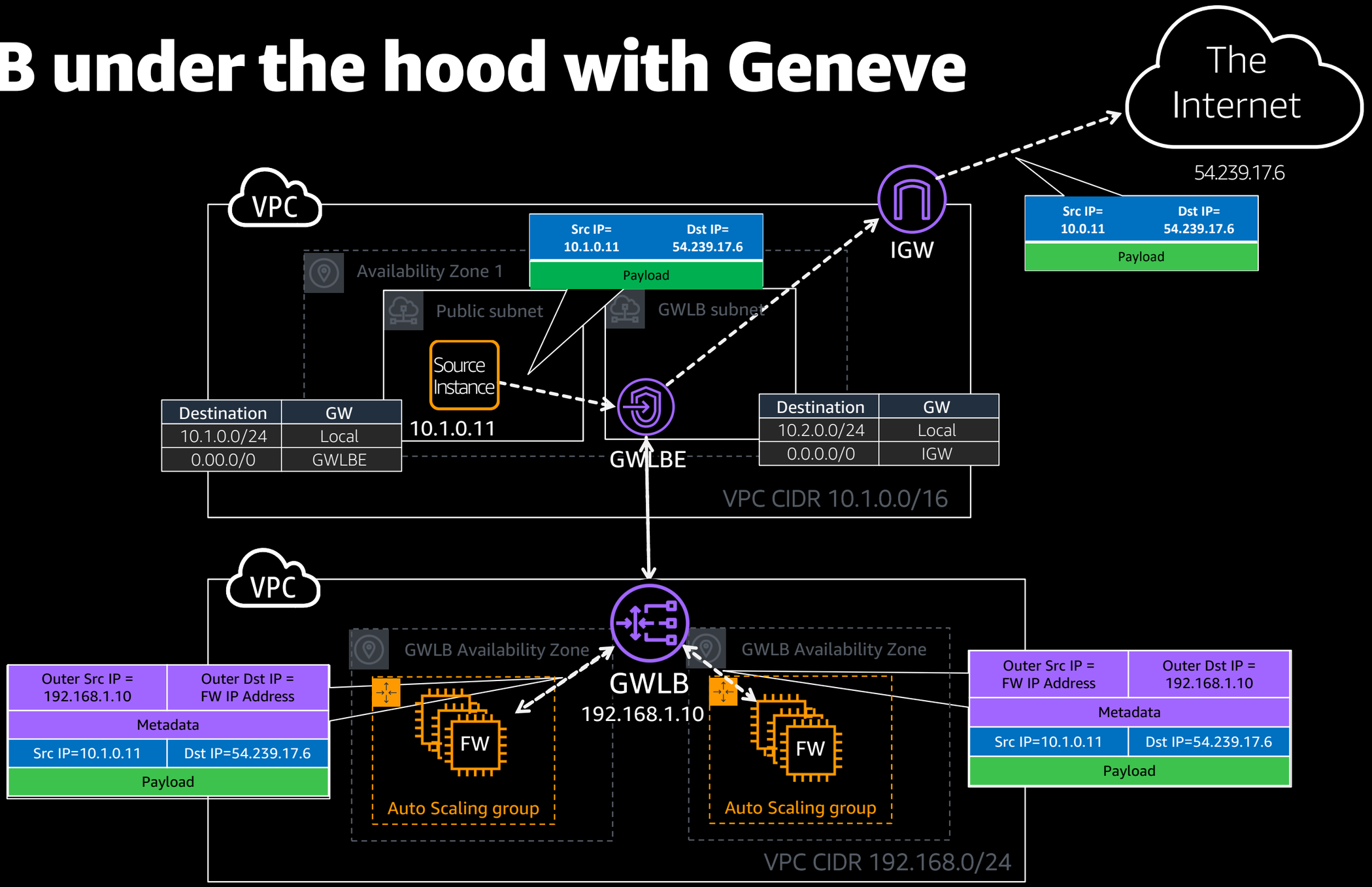


TLS termination not supported in this configuration

GWLB

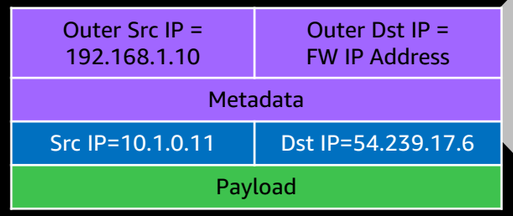

The Internet
IGW
Source
Target
GW
0.0.0.0/0
10.1.0.0/16
NLB
FW SaaS provider account
Customer account
VPC
VPC
IGW
GWLB Availability Zone
FW
Auto Scaling group
GWLB Availability Zone
FW
Auto Scaling group
GWLB
Availability Zone 1
Availability Zone 2
GWLBE 1
NLB
GWLBE 2
Public subnet
Public subnet
10.1.0.11
10.1.1.11
ELB
Private subnet
Instance C
10.1.2.11/24
Private subnet
Instance D
10.1.3.11/24
VPC CIDR 10.1.0.0/16
TLS terminated on NLB

GWLB under the hood with Geneve



GWLB

Traffic between GWLB and appliances is encapsulated in GENEVE packet



Tunnel IPv4 Header:

```
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |Version|  IHL  |Type of Service|          Total Length         |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |         Identification        |Flags|      Fragment Offset    |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |  Time to Live |Protocol=17 UDP|         Header Checksum       |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                       Tunnel Source IPv4 Address                |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                    Tunnel Destination IPv4 Address              |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | UDP Source Port (undefined)   | UDP Destination Port = 6081   |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |          UDP length           |         UDP Checksum          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

28 Octets

Geneve Tunnel Header (for IPv4 payload):

```
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |V=0|Opt Len = 7|O|C|    Rsvd.  |      Protocol Type = 0x0800   |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    Virtual Network Identifier (VNI) = 0       |    Reserved   |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Geneve Tunnel Options:

```
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    Option Class = 0x0108      |    Type = 1   |R|R|R| Len = 2 |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                        64-bit GWLBE ENI id                    |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    Option Class = 0x0108      |    Type = 2   |R|R|R| Len = 2 |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                        64-bit Attachment ID                   |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    Option Class = 0x0108      |    Type = 3   |R|R|R| Len = 1 |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                      32-bit Flow Cookie                       |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

40 Octets

Original IPv4 Packet follows …

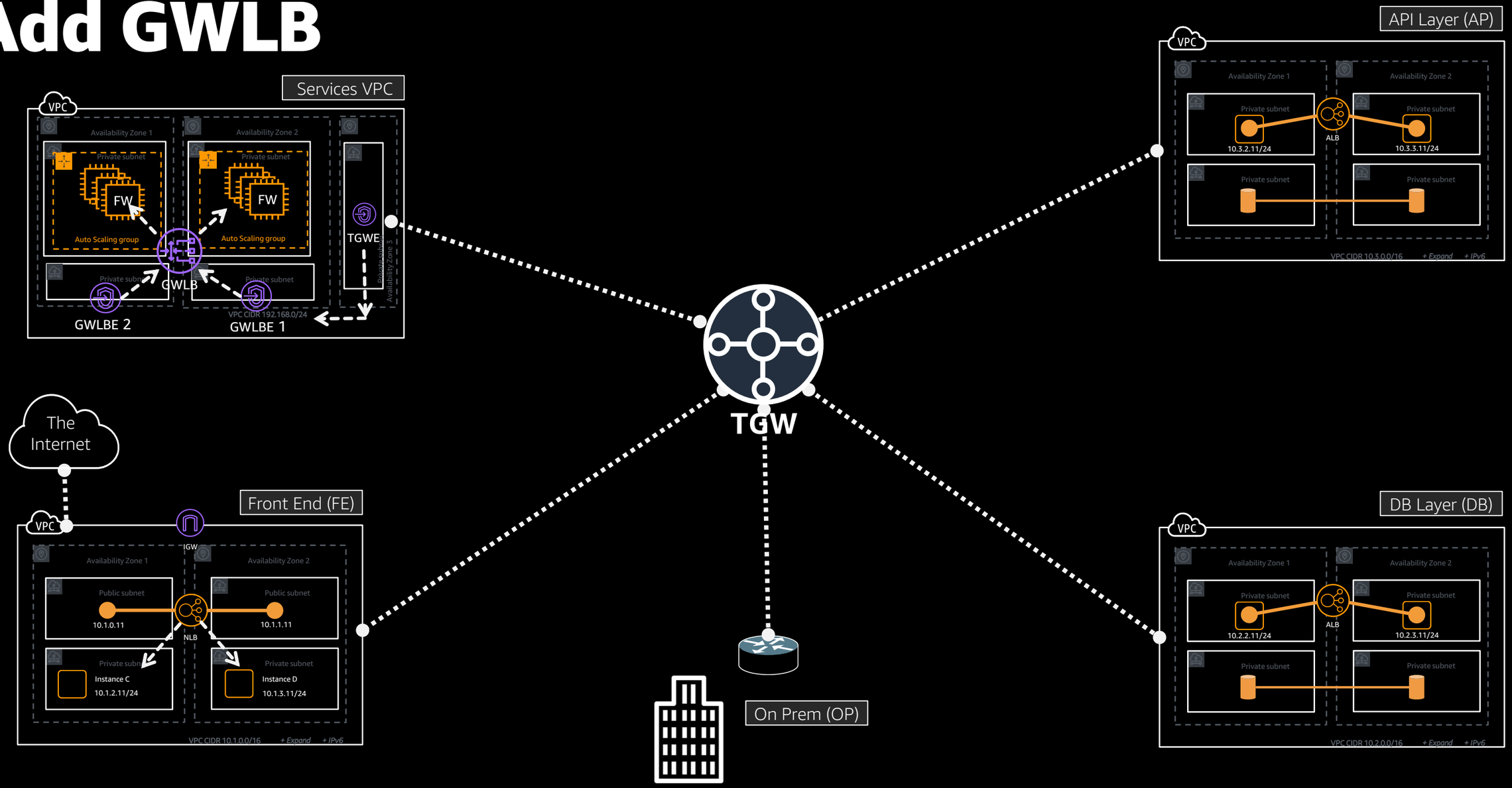
Adding GWLB to our architecture



AWS re:Invent

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

Add GWLB


Services VPC
VPC
Availability Zone 1
Availability Zone 2
Private subnet
FW
Auto Scaling group
GWLB
TGWE
Availability Zone 3
GWLBE 2
GWLBE 1
VPC CIDR 192.168.0/24
API Layer (AP)
10.3.2.11/24
ALB
10.3.3.11/24
VPC CIDR 10.3.0.0/16
+ Expand
+ IPv6
TGW
The Internet
Front End (FE)
IGW
Public subnet
10.1.0.11
NLB
10.1.1.11
Instance C
10.1.2.11/24
Instance D
10.1.3.11/24
VPC CIDR 10.1.0.0/16
DB Layer (DB)
10.2.2.11/24
10.2.3.11/24
VPC CIDR 10.2.0.0/16
On Prem (OP)

GWLB Launch Partners & Providers

Advanced Security Partners:
Provide advanced security capabilities using GWLB













Analytics Partners and Providers:
Provide analytics capabilities using GWLB







Orchestration Partners:
Orchestrate networks that use GWLB







System Integration Partners:
Can implement architectures using GWLB



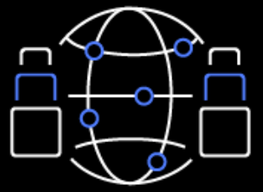
AWS PrivateLink



AWS re:Invent

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

AWS PrivateLink



Access a service in another VPC



Remains in AWS's private network



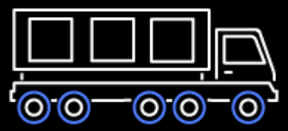
Uni-directional communication



Mutually initiated



Satisfy security (does not require an IGW)



Add agility



Reduce costs

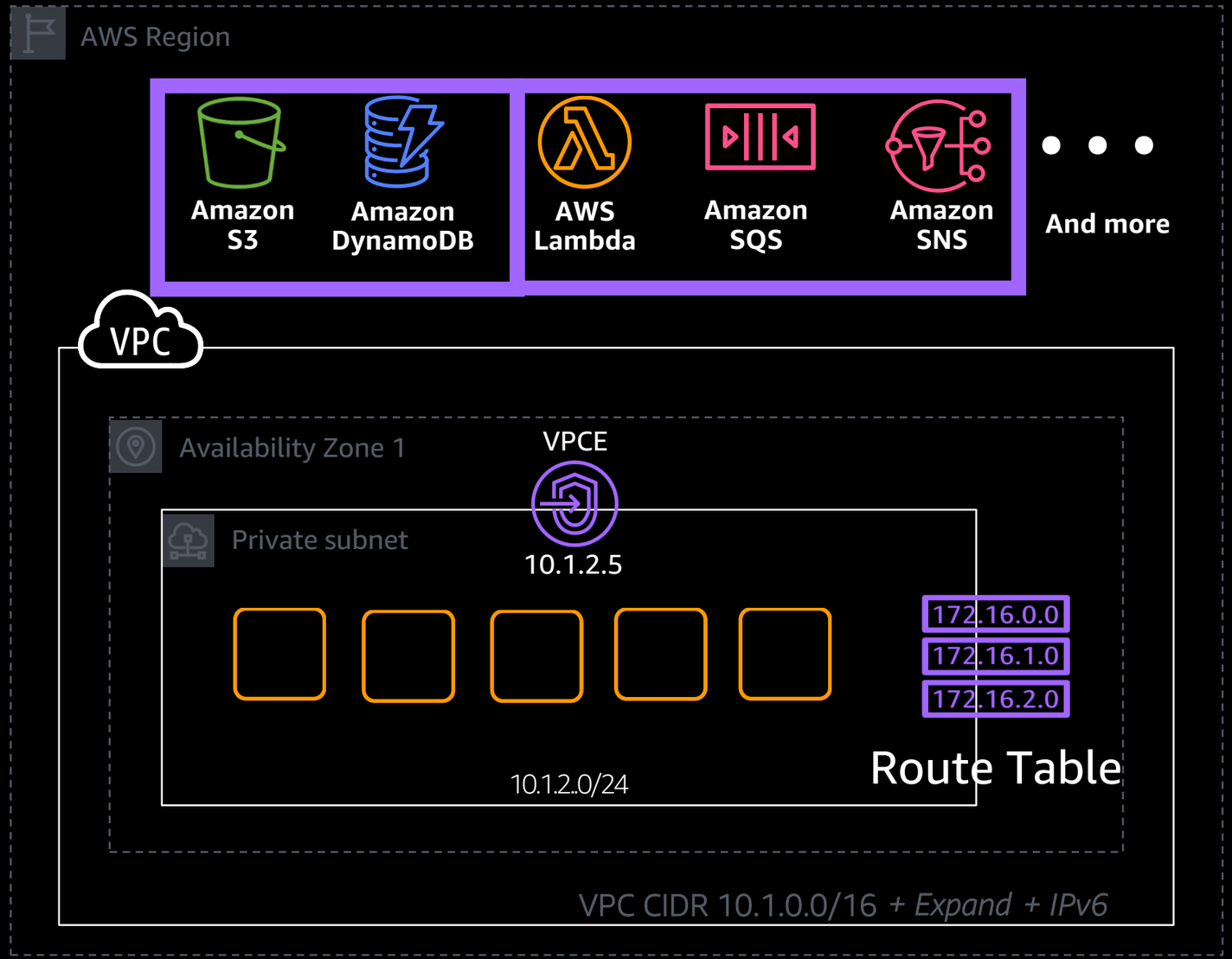


Enable hybrid cloud

AWS PrivateLink services endpoint types

Gateway

Interface



AWS services available via AWS PrivateLink

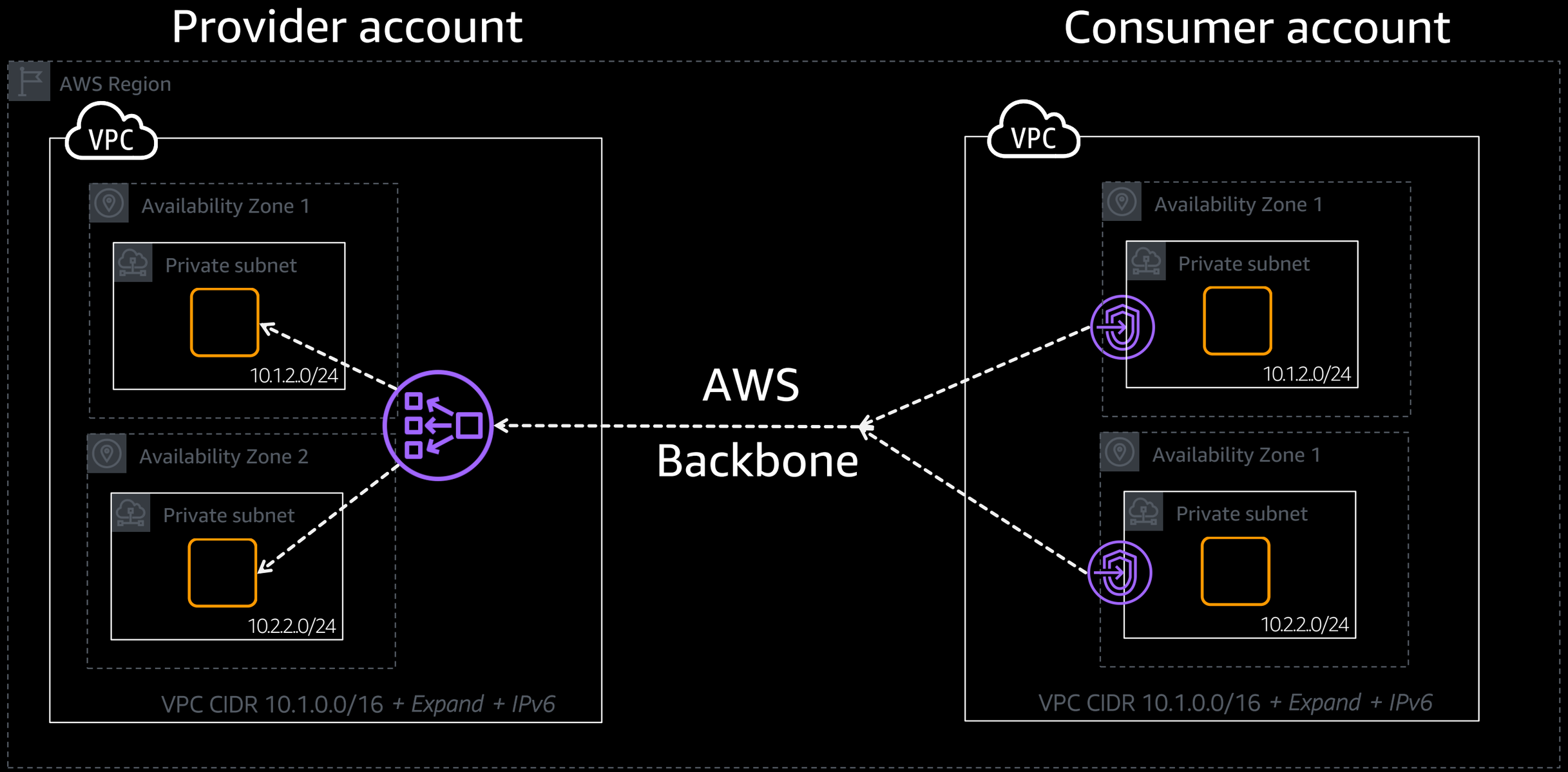
- Amazon API Gateway
- Amazon AppStream 2.0
- AWS App Mesh
- Application Auto Scaling
- Amazon Athena
- AWS Auto Scaling
- Amazon Cloud Directory
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- AWS Config
- AWS DataSync
- Amazon EC2 API
- Amazon EC2 Auto Scaling
- Amazon Elastic File System
- Elastic Load Balancing
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Glue
- AWS Key Management Service
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- Amazon Rekognition
- Amazon SageMaker and Amazon SageMaker Runtime
- Amazon SageMaker Notebook
- AWS Secrets Manager
- AWS Security Token Service
- AWS Server Migration Service
- AWS Service Catalog
- Amazon SNS
- Amazon SQS
- AWS Step Functions
- AWS Systems Manager
- AWS Storage Gateway
- AWS Transfer for SFTP
- Amazon WorkSpaces

- With many more…. and more to come!

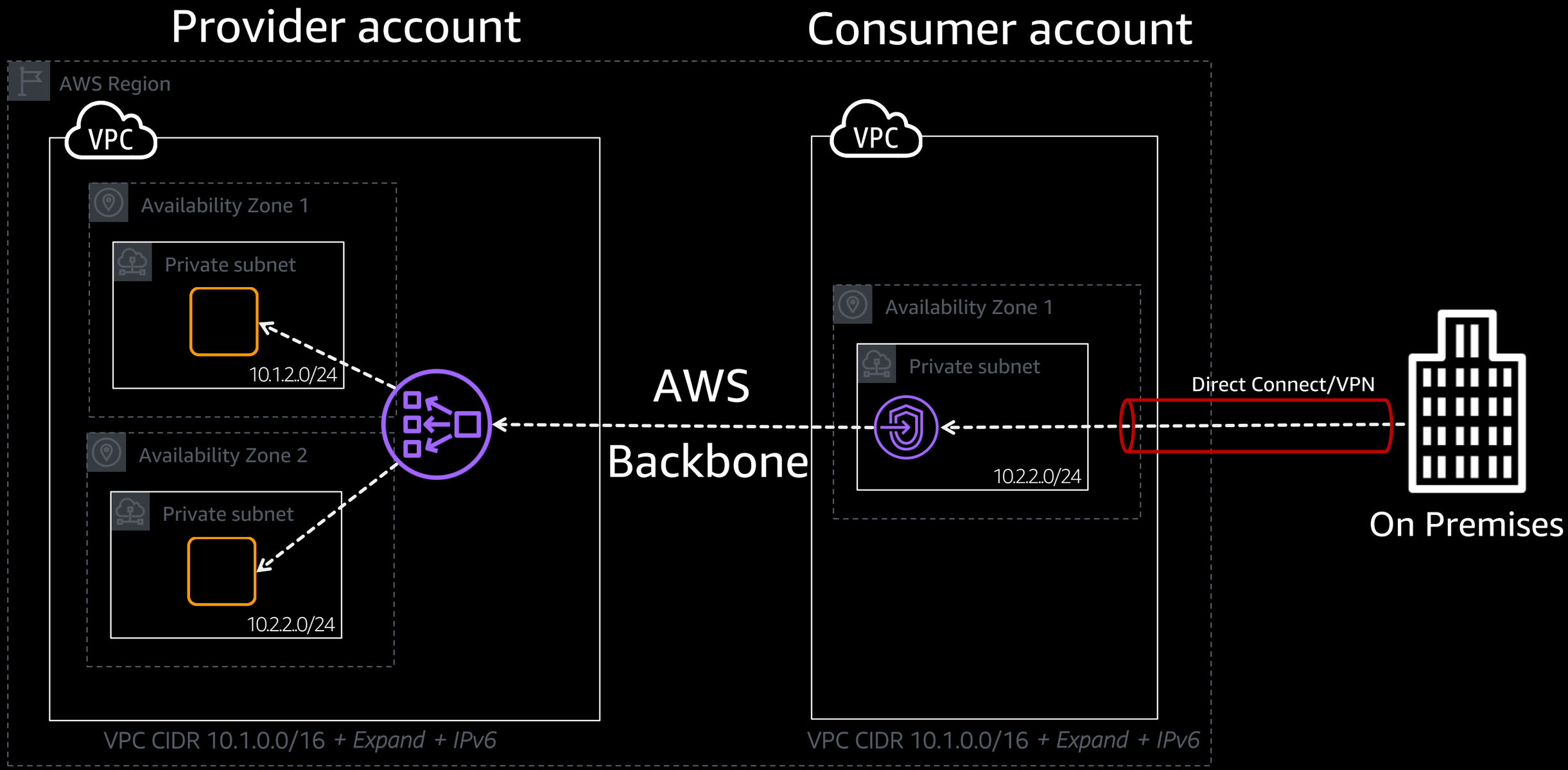


AWS PrivateLink, since being launched in 2018, has 92 AWS services on-board as of October 2020

AWS PrivateLink – Hosting your own service



AWS PrivateLink – Hybrid architecture



AWS PrivateLink

How do I get the source IP Address?

Enable Proxy Protocol version 2

To enable proxy protocol v2 using the new console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/
2. On the navigation pane, under **LOAD BALANCING**, choose **Target Groups**
3. Choose the name the target group to open its details page
4. On the **Group details** page, in the **Attributes** section, choose **Edit**
5. On the **Edit attributes** page, select **Proxy protocol v2**
6. Choose **Save changes**

AWS PrivateLink

A note about PPv2: What does it look like?

Provides a binary encoding of the proxy protocol header.

The NLB prepends a proxy protocol header to the TCP data.

It does not discard or overwrite any existing data, including any proxy protocol headers already present.

It is possible to receive more than one proxy protocol header.

The first proxy protocol header might not be the one from your Network Load Balancer, the order is set by the path of the packets, and includes pathing before the NLB.

AWS PrivateLink

A note about PPv2: What does it look like?

PPv2 Header

Field	Length (in octets)	Description
Type	1	PP2_TYPE_AWS (0xEA)
Length	2	The length of value
Value	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	variable (value length minus 1)	The ID of the endpoint

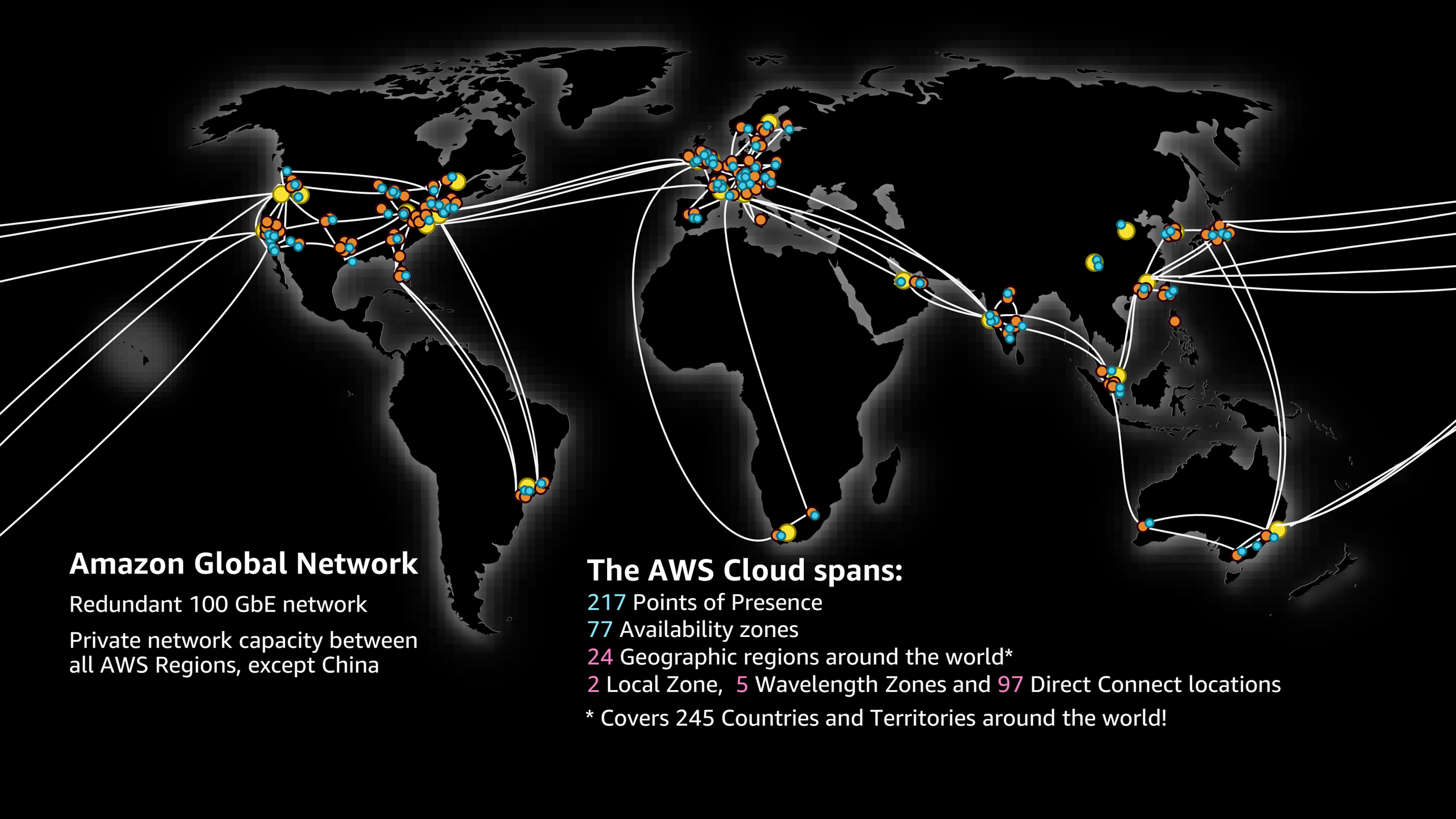
For ProProt library to parse PPV2 connection headers see:
https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot

A word on the AWS Backbone



AWS re:Invent

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



Amazon Global Network

Redundant 100 GbE network

Private network capacity between all AWS Regions, except China

The AWS Cloud spans:

217 Points of Presence
77 Availability zones
24 Geographic regions around the world*
2 Local Zone, 5 Wavelength Zones and 97 Direct Connect locations

* Covers 245 Countries and Territories around the world!

Marketplace

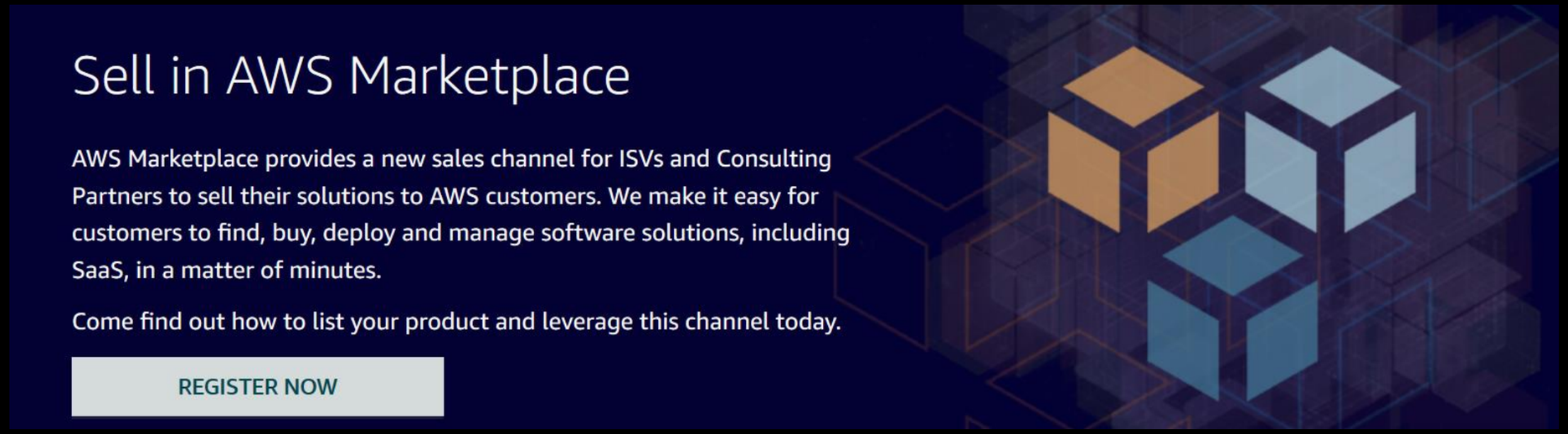


AWS re:Invent

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

Marketplace

Services discoverable when customers purchase SaaS on AWS Marketplace



Easily create secure endpoints

AWS Market Place confirms each sellers endpoint DNS name, making it easier to find and set up the endpoints your customers need

No public IP addresses

Connect services directly from VPC without requiring any internet gateways, and not traversing the internet

Curated SaaS products

Products architected to run on AWS by popular software vendors are found easily on the marketplace

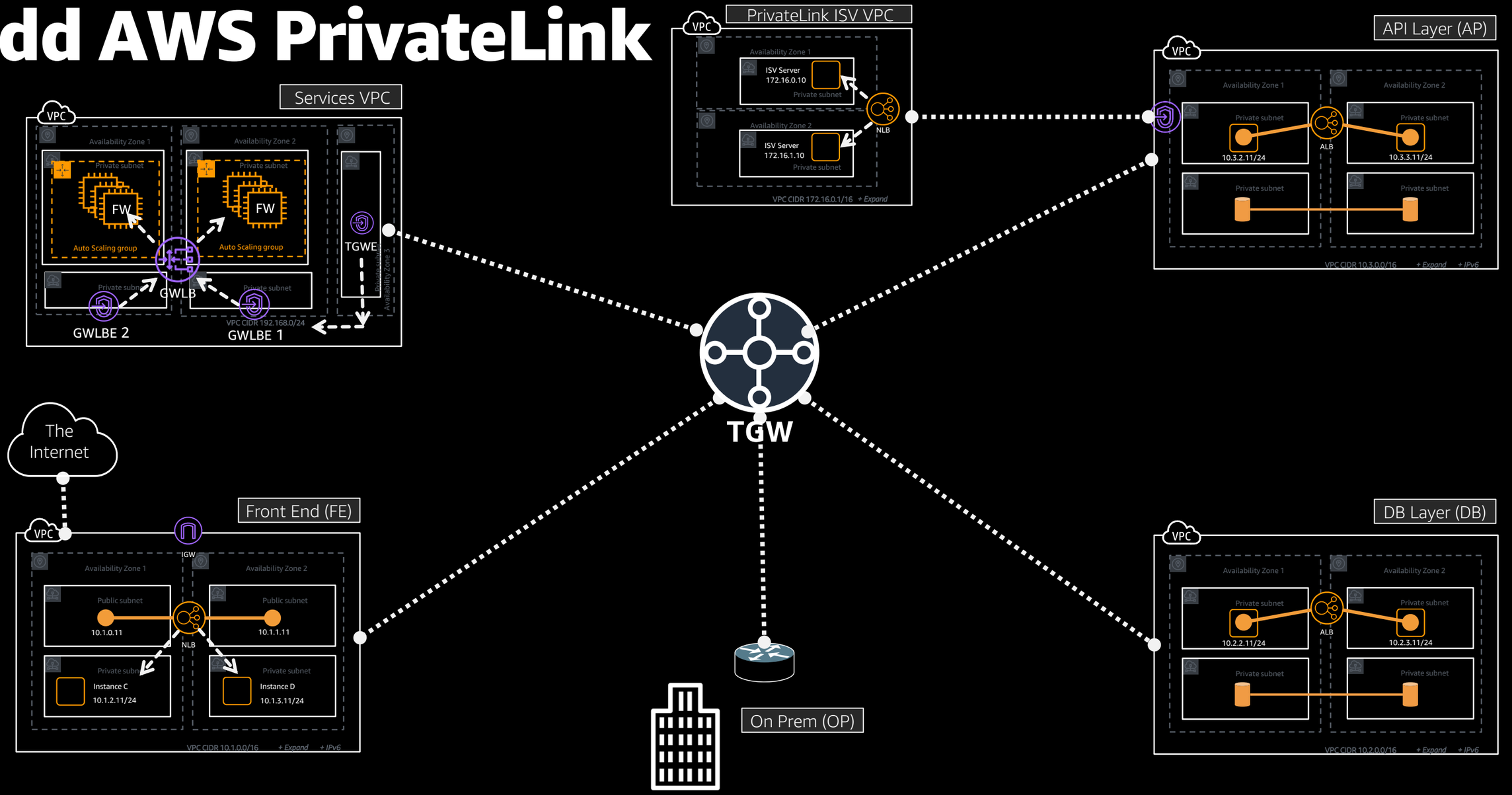
Putting it all together by adding AWS PrivateLink



AWS re:Invent

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

Add AWS PrivateLink



https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/

https://tinyurl.com/y2jafnx3

A note about infrastructure as code:

Automation



Time to recover

Rapid rollout

Troubleshooting

Thank you!

James Wenzel

Sr Partner Solutions Architect – Networking

www.linkedin.com/in/james-m-wenzel

https://networkingandcontentdelivery.splashthat.com

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.