
AWS
re:Invent

NET309

Advanced VPC design and new capabilities for Amazon VPC

Matt Lehwess

Principal Developer Advocate

AWS

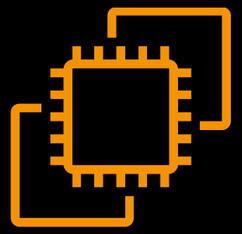
AWS re:Invent

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



Let’s take a step back in time,
to November 2019

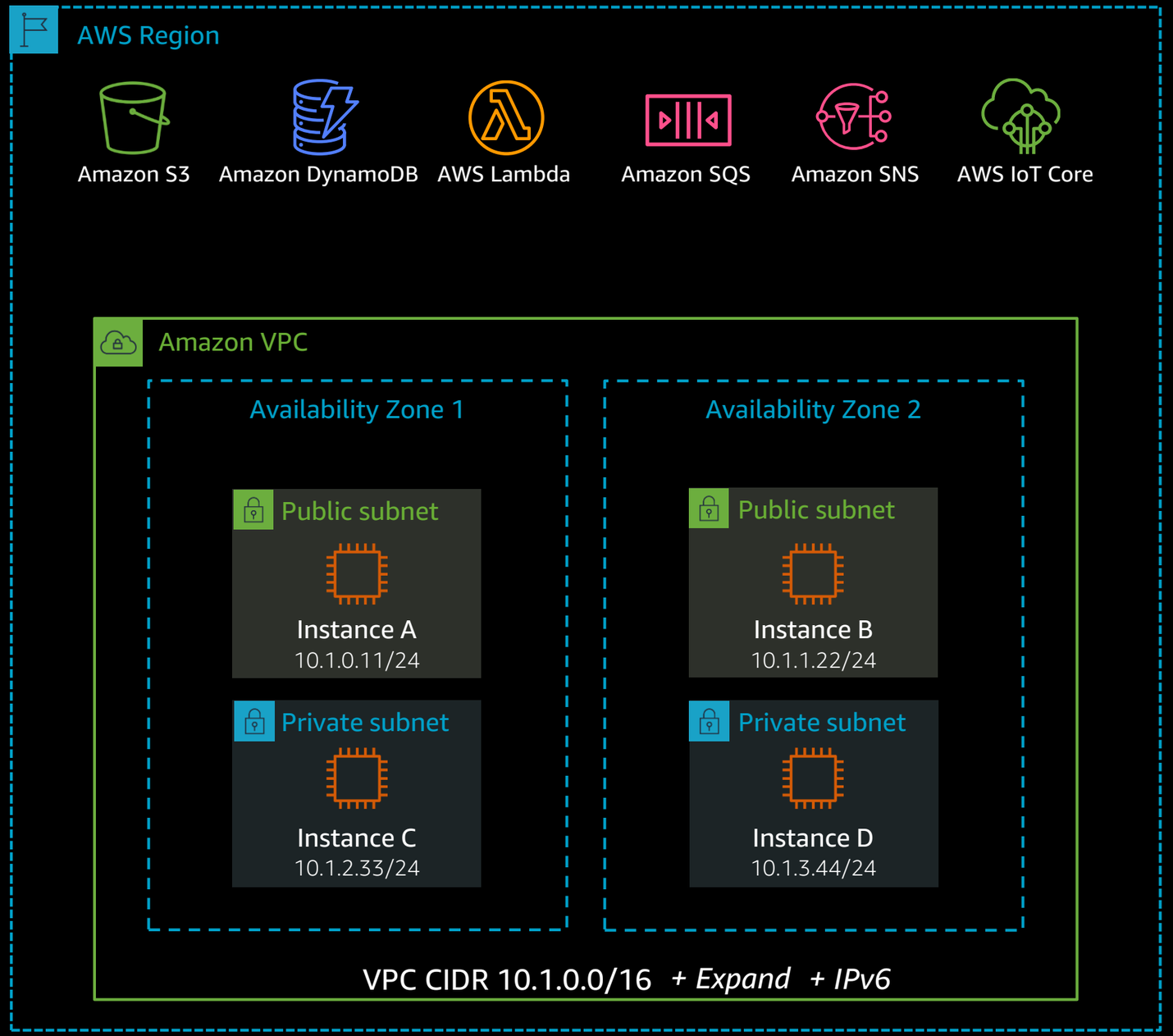
Amazon VPC networking

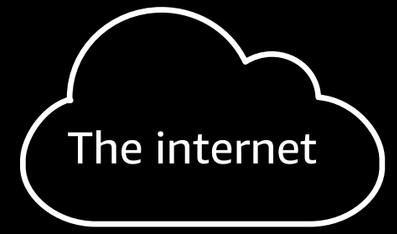


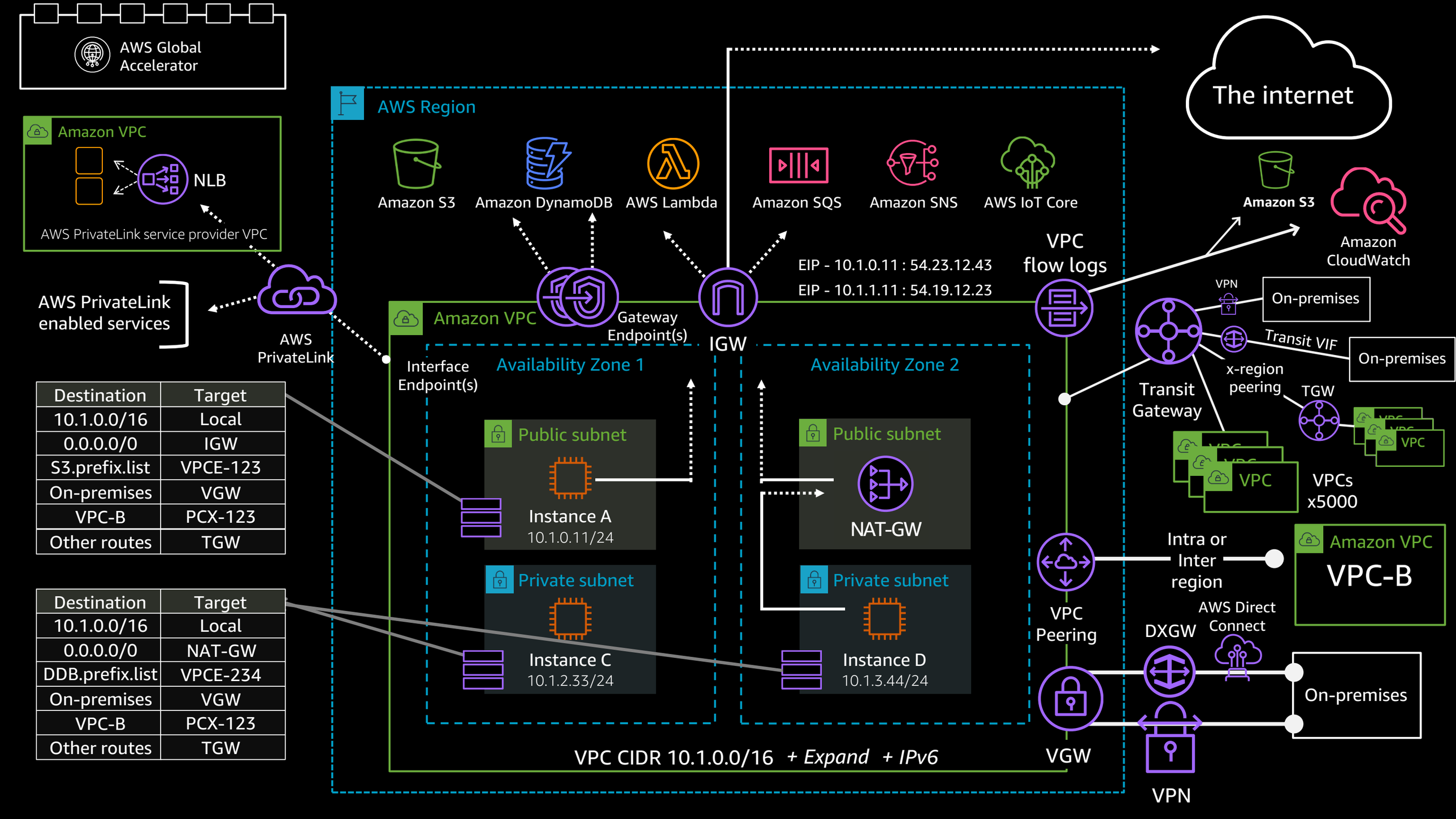
Amazon Elastic Cloud Compute (Amazon EC2)



Amazon Virtual Private Cloud (Amazon VPC)

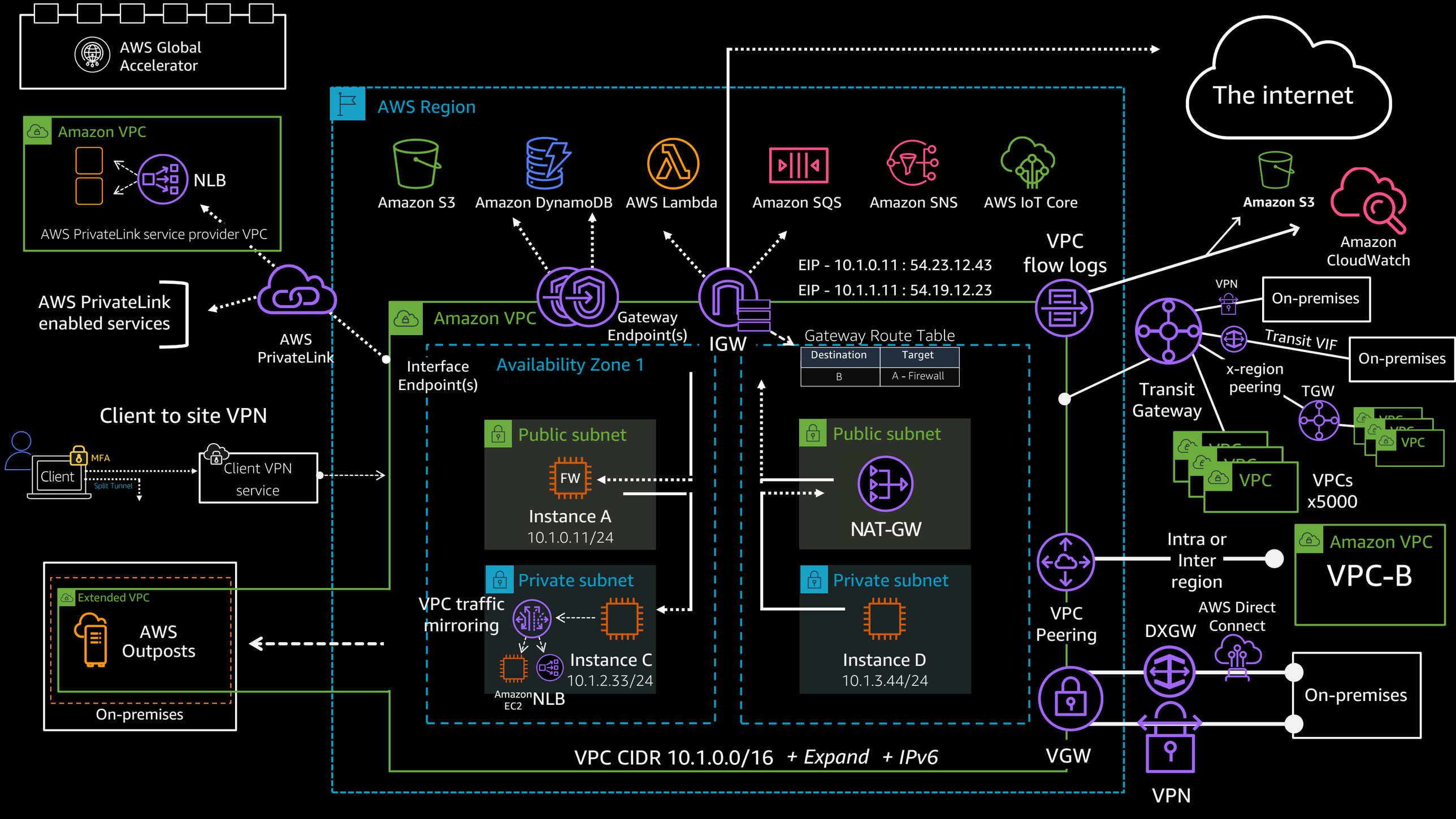




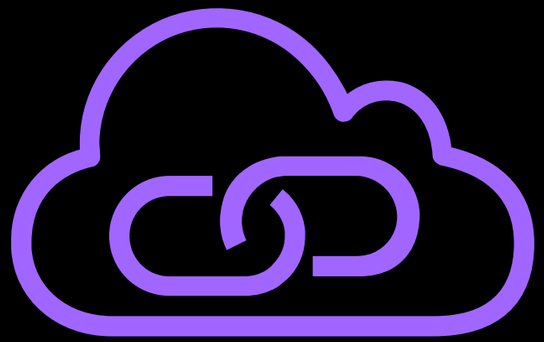


Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other routes	TGW

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
Amazon VPC
NLB
AWS PrivateLink service provider VPC
AWS PrivateLink enabled services
AWS PrivateLink
AWS Region
Amazon S3
Amazon DynamoDB
AWS Lambda
Amazon SQS
Amazon SNS
AWS IoT Core
The internet
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
Amazon VPC
Gateway Endpoint(s)
IGW
Gateway Route Table
Destination
Target
B
A - Firewall
Interface Endpoint(s)
Availability Zone 1
Public subnet
FW
Instance A
10.1.0.11/24
Public subnet
NAT-GW
Private subnet
VPC traffic mirroring
Instance C
10.1.2.33/24
Amazon EC2
NLB
Private subnet
Instance D
10.1.3.44/24
Client to site VPN
Client
MFA
Split Tunnel
Client VPN service
Extended VPC
AWS Outposts
On-premises
VPN
On-premises
Transit VIF
On-premises
x-region peering
TGW
Transit Gateway
VPC
VPCs x5000
Intra or Inter region
Amazon VPC
VPC-B
VPC Peering
AWS Direct Connect
DXGW
On-premises
VGW
VPN
VPC CIDR 10.1.0.0/16 + Expand + IPv6

AWS PrivateLink



Interface VPC endpoints

VPC endpoint services

SCAN ME

https://amzn.to/3lzxHqP

AWS PrivateLink interface endpoints documentation

AWS Privatelink: Interface endpoints

Before –

41 services supported over AWS PrivateLink

After –

92+ services supported over AWS PrivateLink

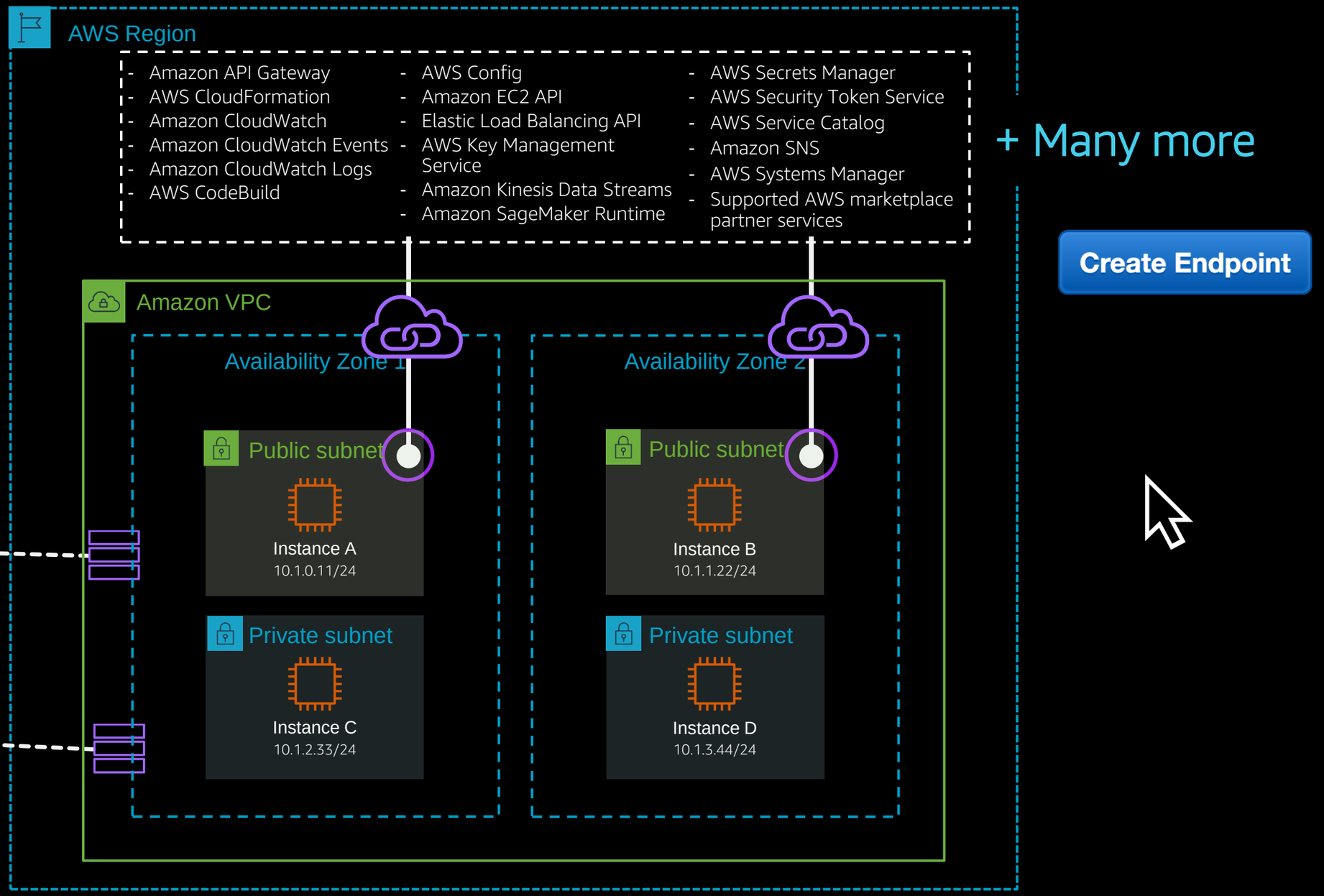
You can now add fine-grain IAM policies to interface endpoint creation for AWS services

Destination	Target
10.1.0.0/16	Local

No additional routing needed

Destination	Target
10.1.0.0/16	Local

No additional routing needed here either . . .



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.
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service category

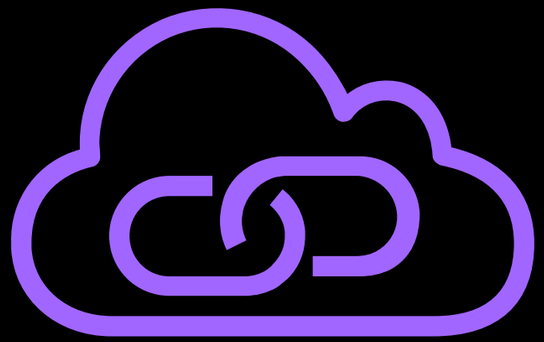
- (•) AWS services
- ( ) Find service by name
- ( ) Your AWS Marketplace services

Service Name Select a service

Filter by attributes or search by keyword 1 to 50 of 93

Service Name	Owner	Type
aws.sagemaker.us-west-2.notebook	amazon	Interface
com.amazonaws.us-west-2.access-a…er	amazon	Interface
com.amazonaws.us-west-2.acm-pca	amazon	Interface
com.amazonaws.us-west-2.application-aut…	amazon	Interface
com.amazonaws.us-west-2.appmesh-env…	amazon	Interface
com.amazonaws.us-west-2.appstream.api	amazon	Interface
com.amazonaws.us-west-2.appstream.str…	amazon	Interface
com.amazonaws.us-west-2.athena	amazon	Interface
com.amazonaws.us-west-2.autoscaling	amazon	Interface
com.amazonaws.us-west-2.autoscaling-pl…	amazon	Interface
com.amazonaws.us-west-2.awsconnector	amazon	Interface
com.amazonaws.us-west-2.cassandra	amazon	Interface
com.amazonaws.us-west-2.clouddirectory	amazon	Interface

AWS PrivateLink



Interface VPC endpoints

VPC endpoint services

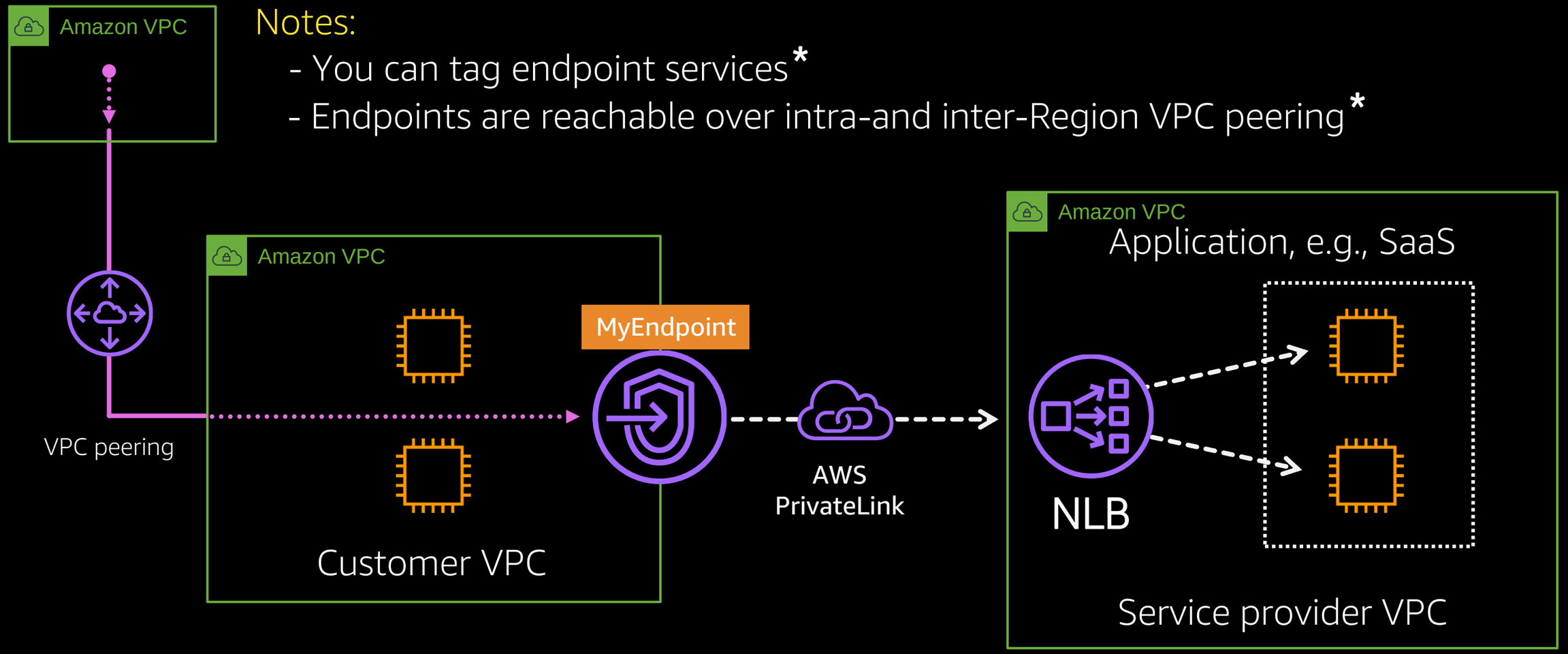
SCAN ME

https://amzn.to/2IDpkfC

AWS PrivateLink endpoint services documentation

VPC Endpoint services: Before

Powered by AWS PrivateLink



* Applicable for interface endpoints too

VPC Endpoint services: After

Powered by AWS PrivateLink

SCAN ME

https://amzn.to/2UrQvfE

Fine-grained IAM permissions for AWS PrivateLink

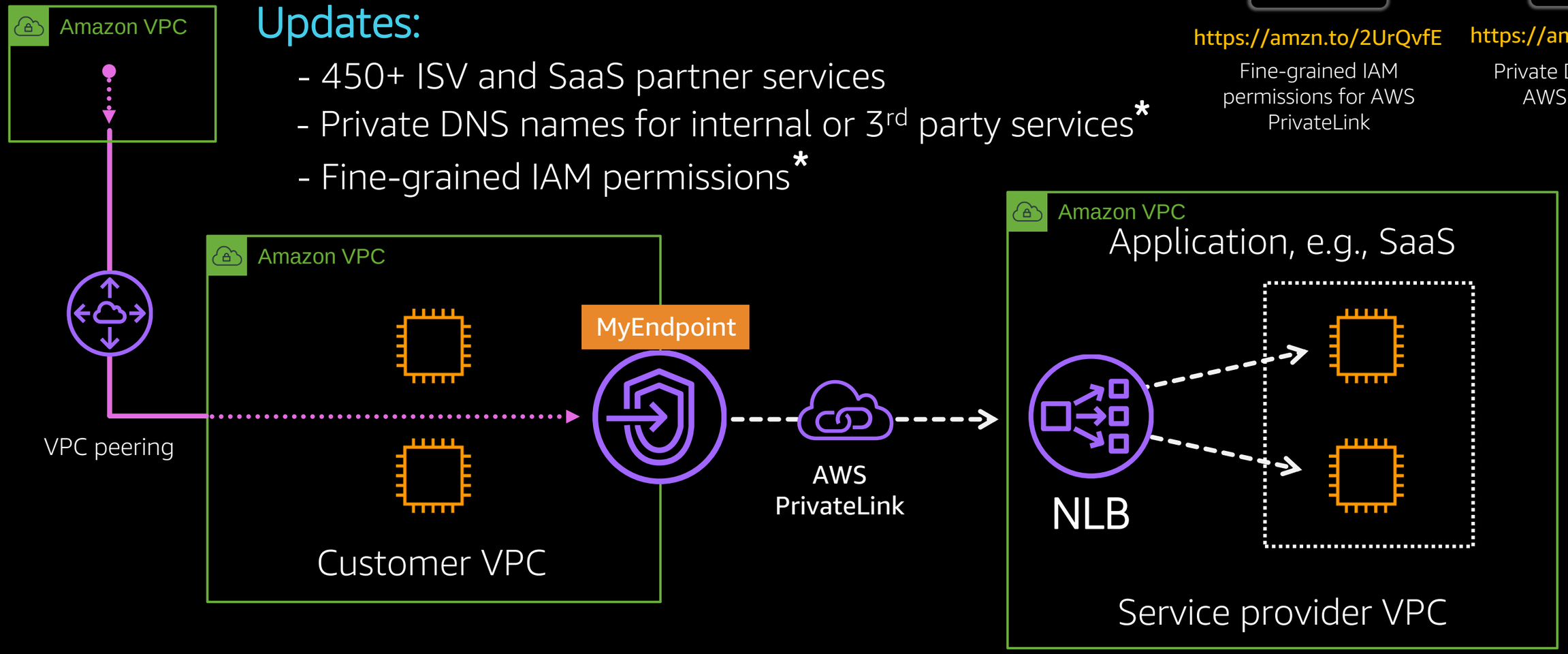
SCAN ME

https://amzn.to/2H7udgg

Private DNS names for AWS PrivateLink

Updates:

- 450+ ISV and SaaS partner services
- Private DNS names for internal or 3rd party services*
- Fine-grained IAM permissions*

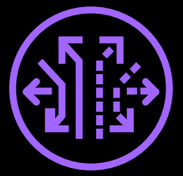


* Applicable for interface endpoints too

Monitoring and visibility



VPC flow logs



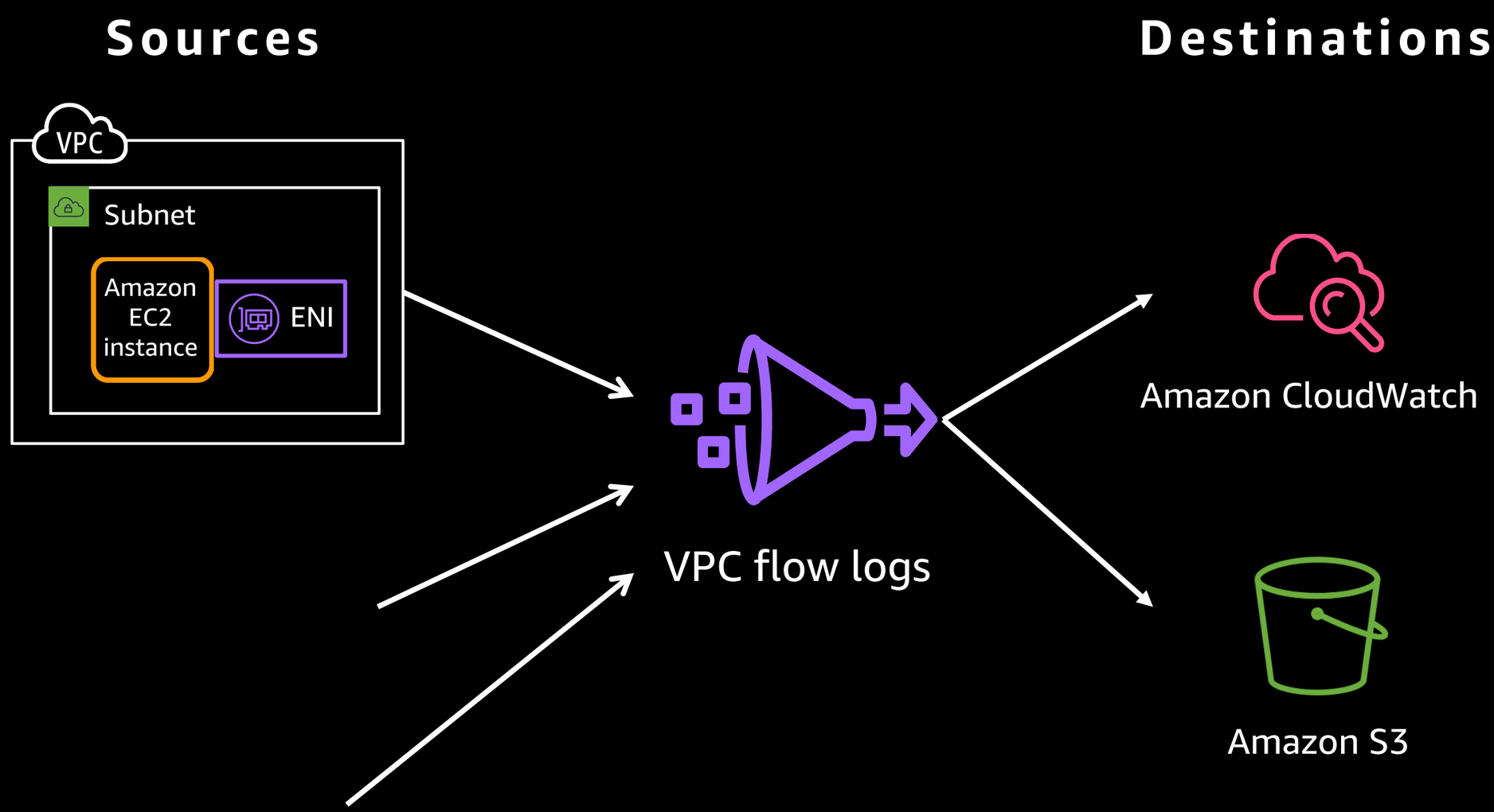
VPC traffic mirroring

SCAN ME

https://amzn.to/32PmPOh

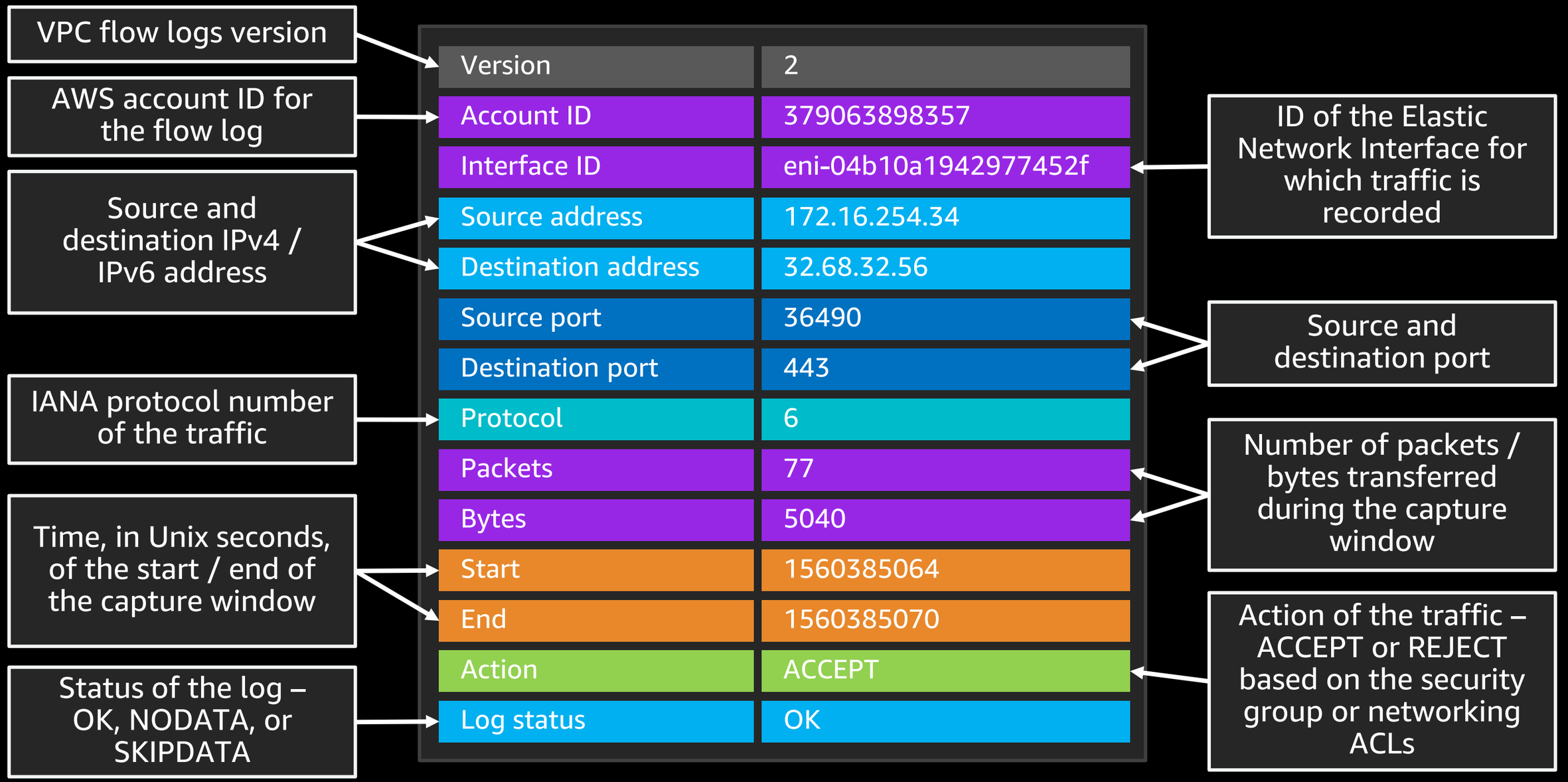
VPC flow logs documentation

VPC flow logs: Before

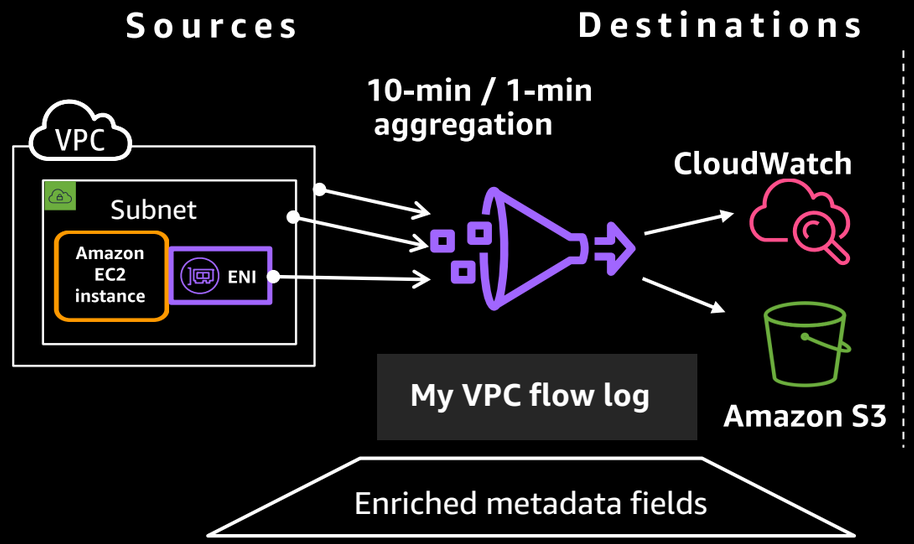


VPC flow logs: Before

Flow log contents



VPC flow logs: After



Enriched metadata fields

Region	us-east-1
Availability zone ID	use1-az2
VPC-ID	vpc-1a2b3c4d
Subnet-ID	Subnet-1122aabb
Instance-ID	i-1234567890abcdef0
TCP-flags	18
Type	IPv4
Pkt-SrcAddr	10.0.5.22
Pkt-DstAddr	172.16.5.10

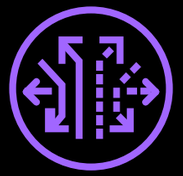
Updates –

1. Faster flow logs – up to 1-min aggregation intervals
2. Tagging support – for granular IAM and cost allocation
3. Enriched flow logs – metadata and custom format – new fields and specify which fields to return!

Monitoring and visibility



VPC flow logs



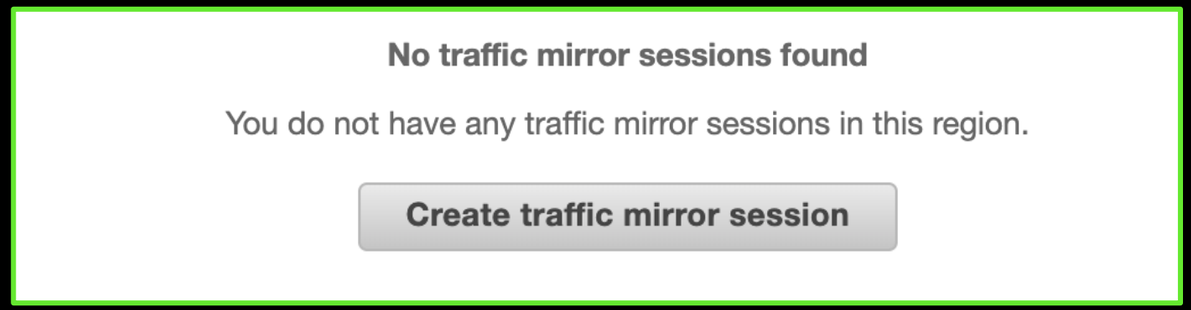
Traffic Mirroring

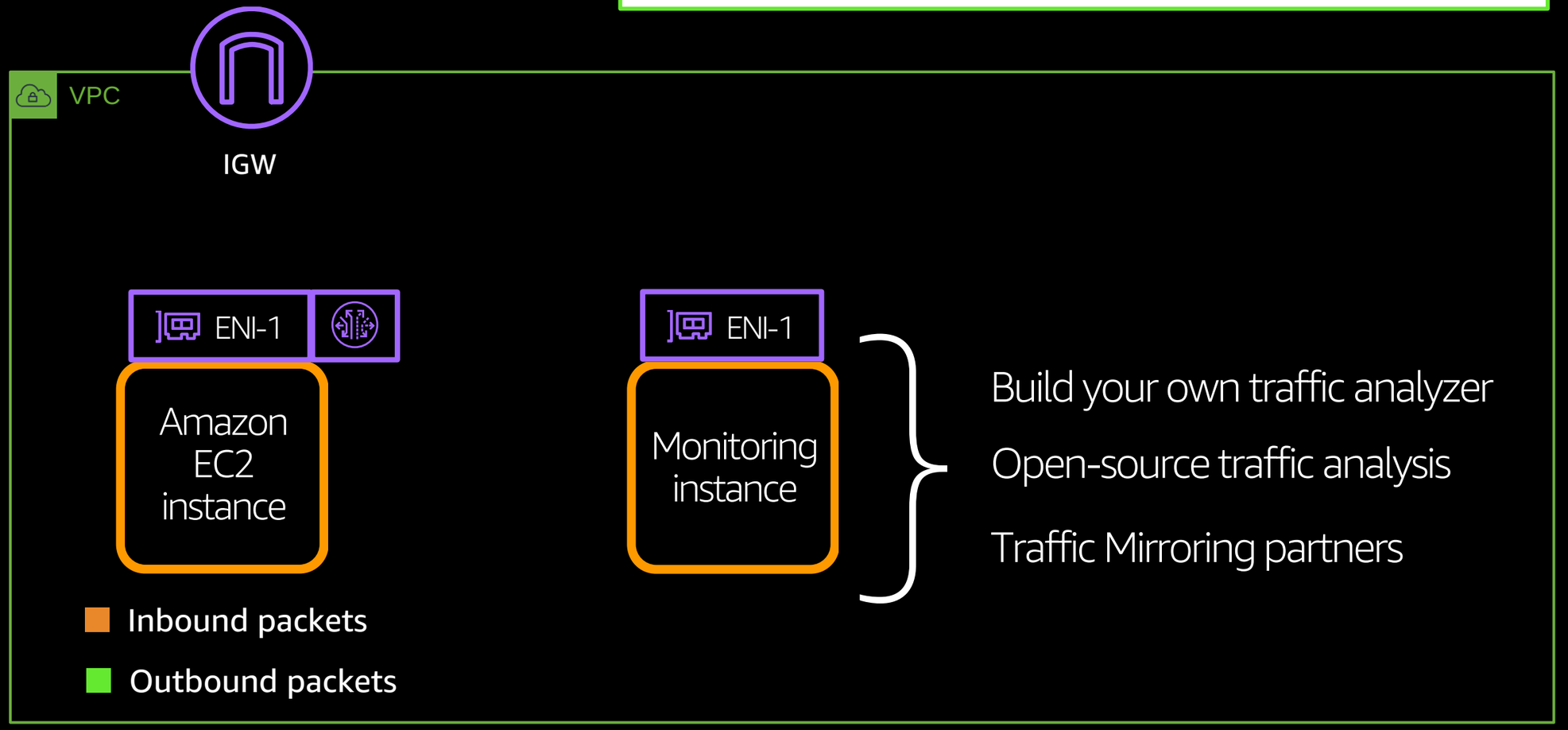
SCAN ME

https://amzn.to/32PTfbc

What is AWS traffic mirroring?

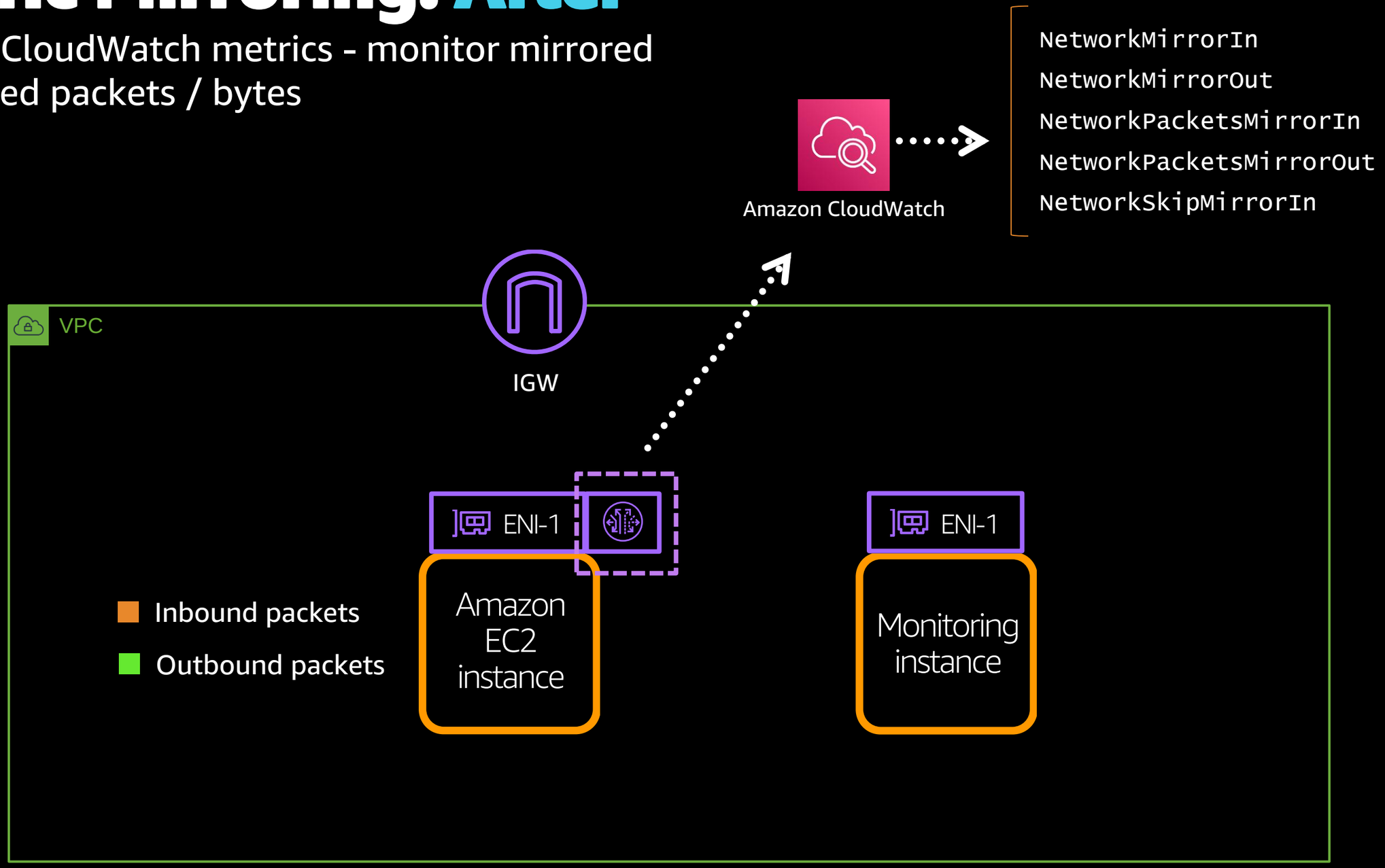
Traffic Mirroring: Before





Traffic Mirroring: After

Amazon CloudWatch metrics - monitor mirrored or dropped packets / bytes



Traffic Mirroring: After

Amazon CloudWatch metrics - monitor mirrored or dropped packets / bytes

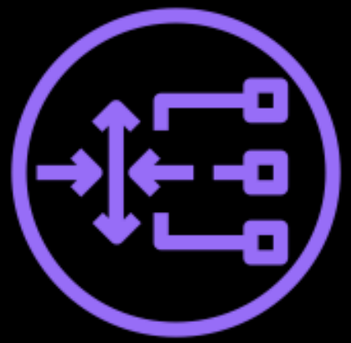
SCAN ME

https://amzn.to/3kD3TrU

Traffic mirroring metrics and dimensions

NetworkMirrorIn	The number of bytes received on all network interfaces by the instance that are mirrored
NetworkMirrorOut	The number of bytes sent out on all network interfaces by the instance that are mirrored
NetworkPacketsMirrorIn	The number of packets received on all network interfaces by the instance that are mirrored
NetworkPacketsMirrorOut	The number of packets sent out on all network interfaces by the instance that are
NetworkSkipMirrorIn	The number of bytes received, that meet the traffic mirror filter rules, that did not get mirrored because of production traffic taking priority

Gateway Load Balancer (GWLB)



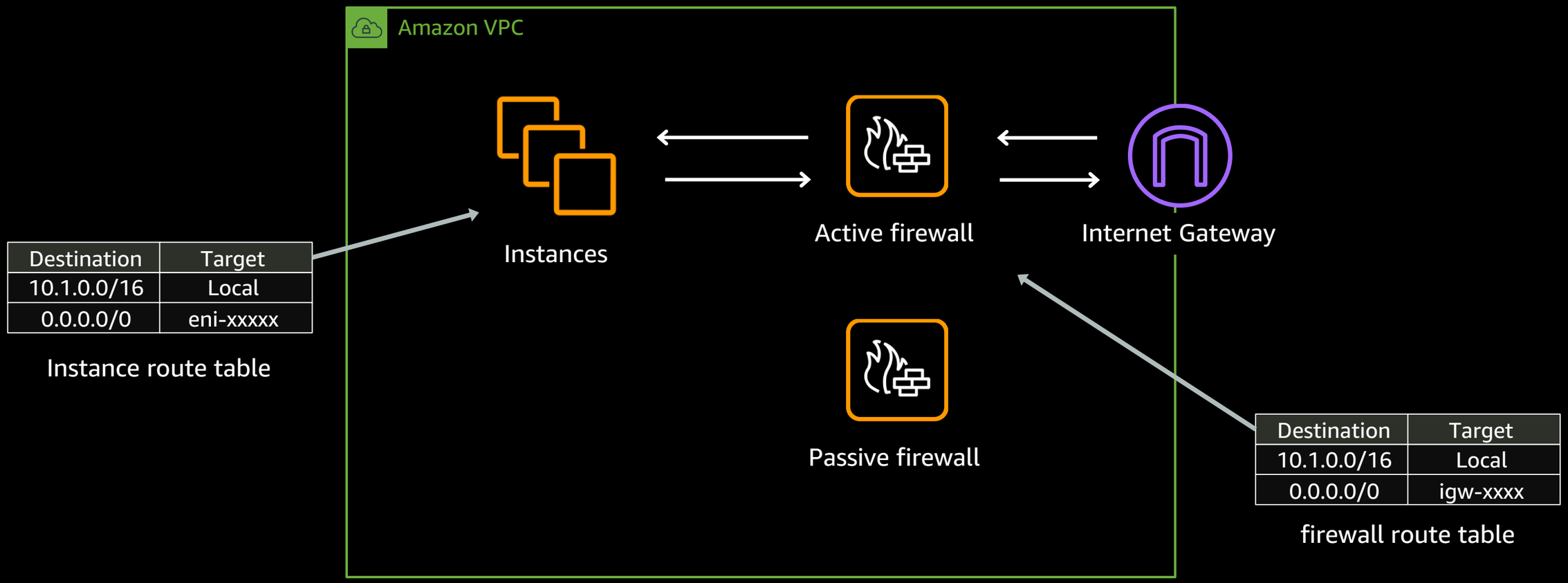
SCAN ME

https://amzn.to/38NvQv8

Introducing Gateway Load Balancer!

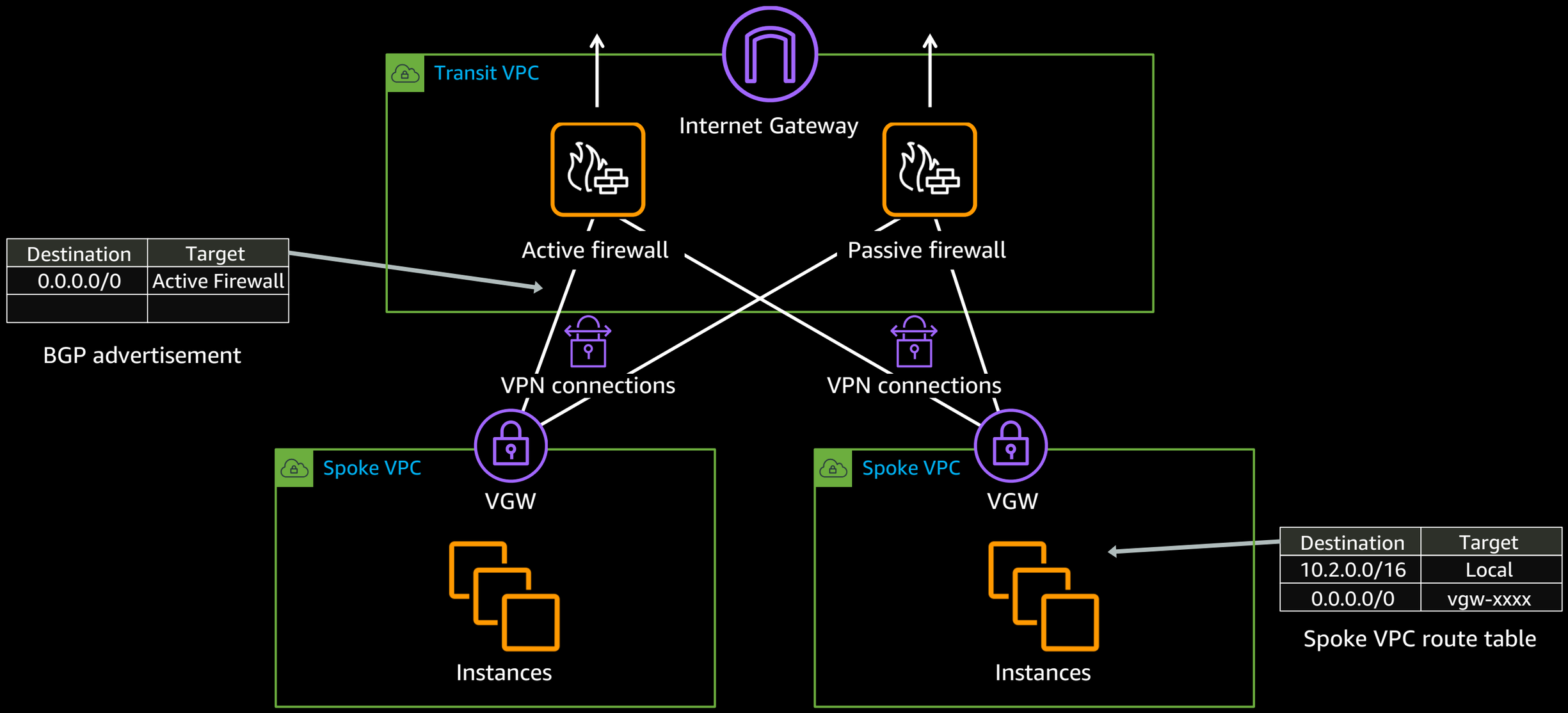
Gateway Load Balancer: Before

From the archives, inline appliances, single VPC



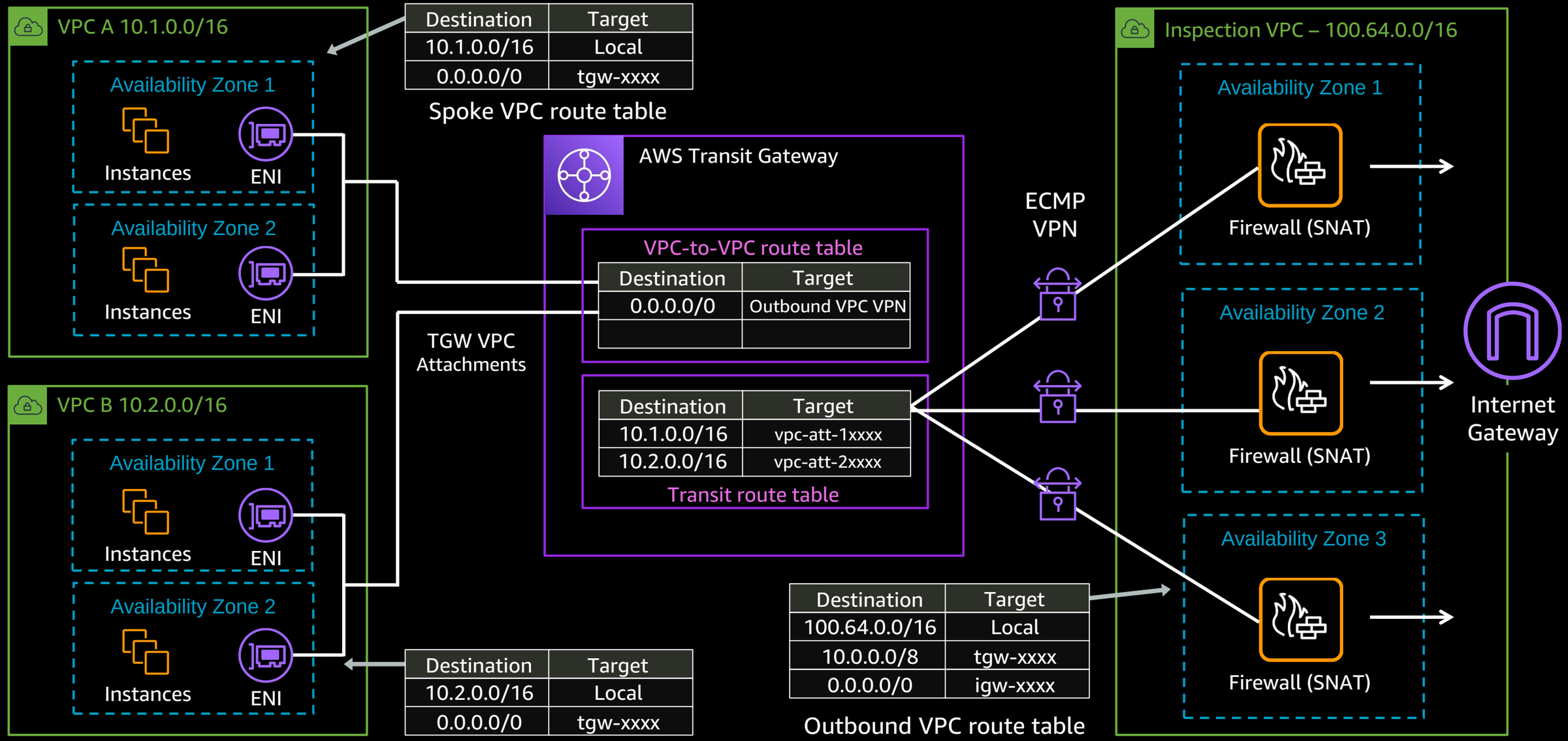
Gateway Load Balancer: Before

From the archives, inline appliances, Transit VPC



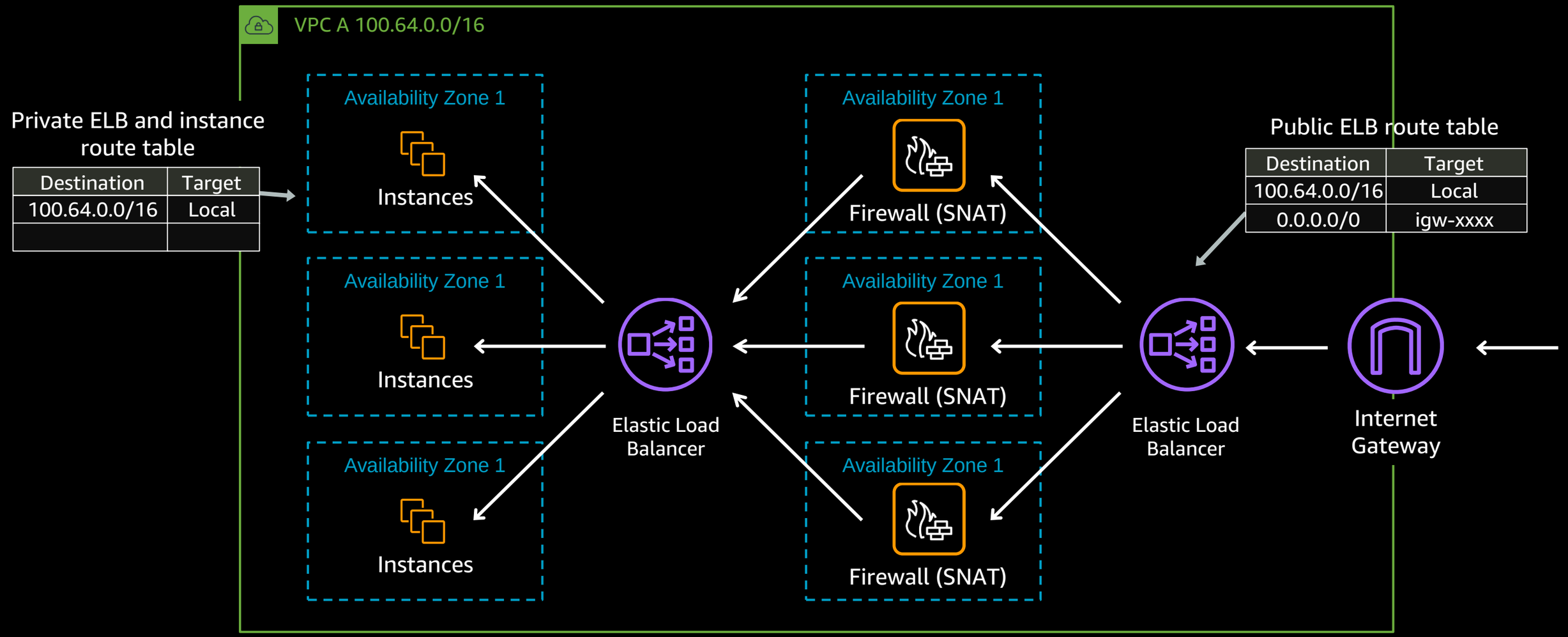
Gateway Load Balancer: Before

From the archives, inline appliances, Transit VPC with Transit Gateway

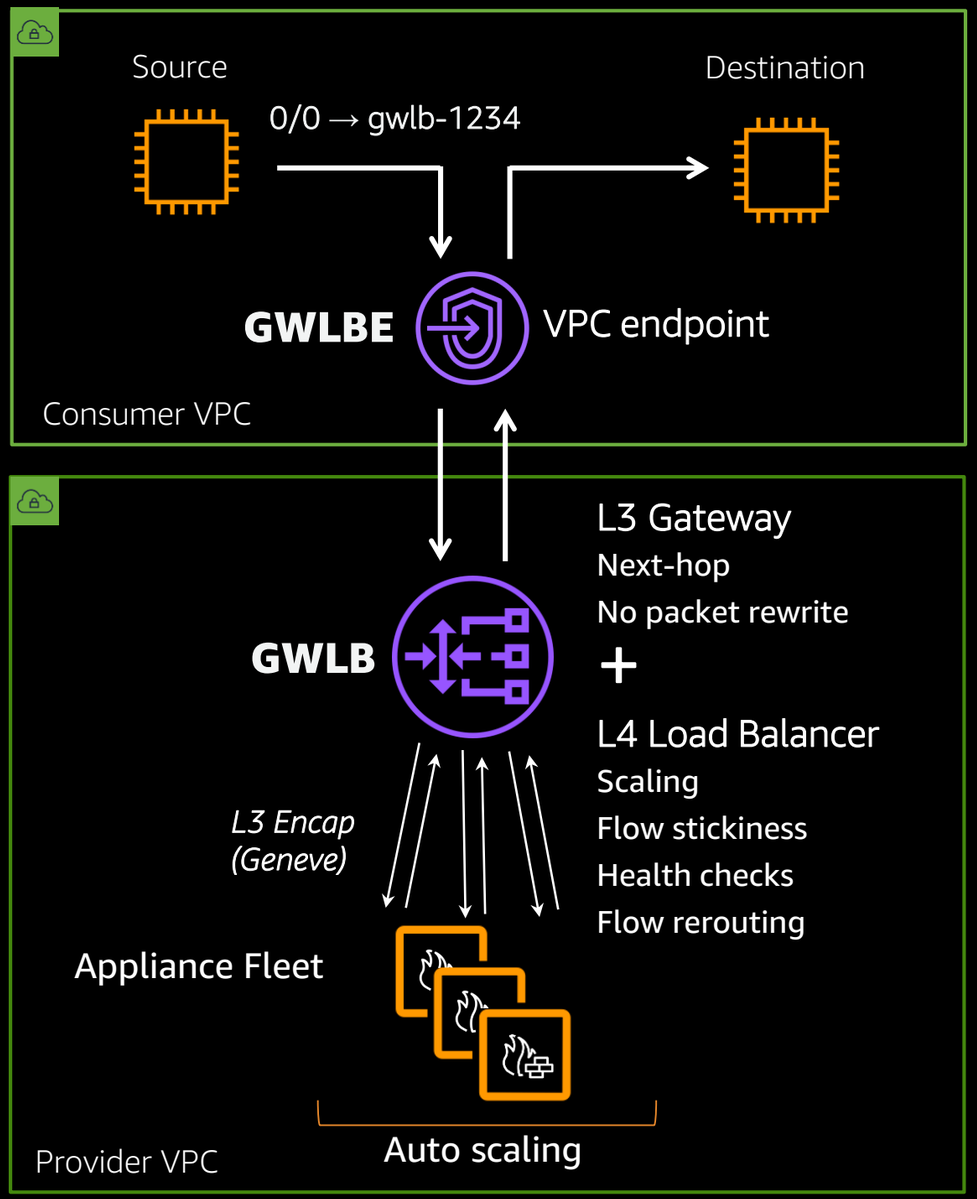


Gateway Load Balancer: Before

From the archives, inline appliances (inbound), the *famous* ELB sandwich



Gateway Load Balancer: After



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

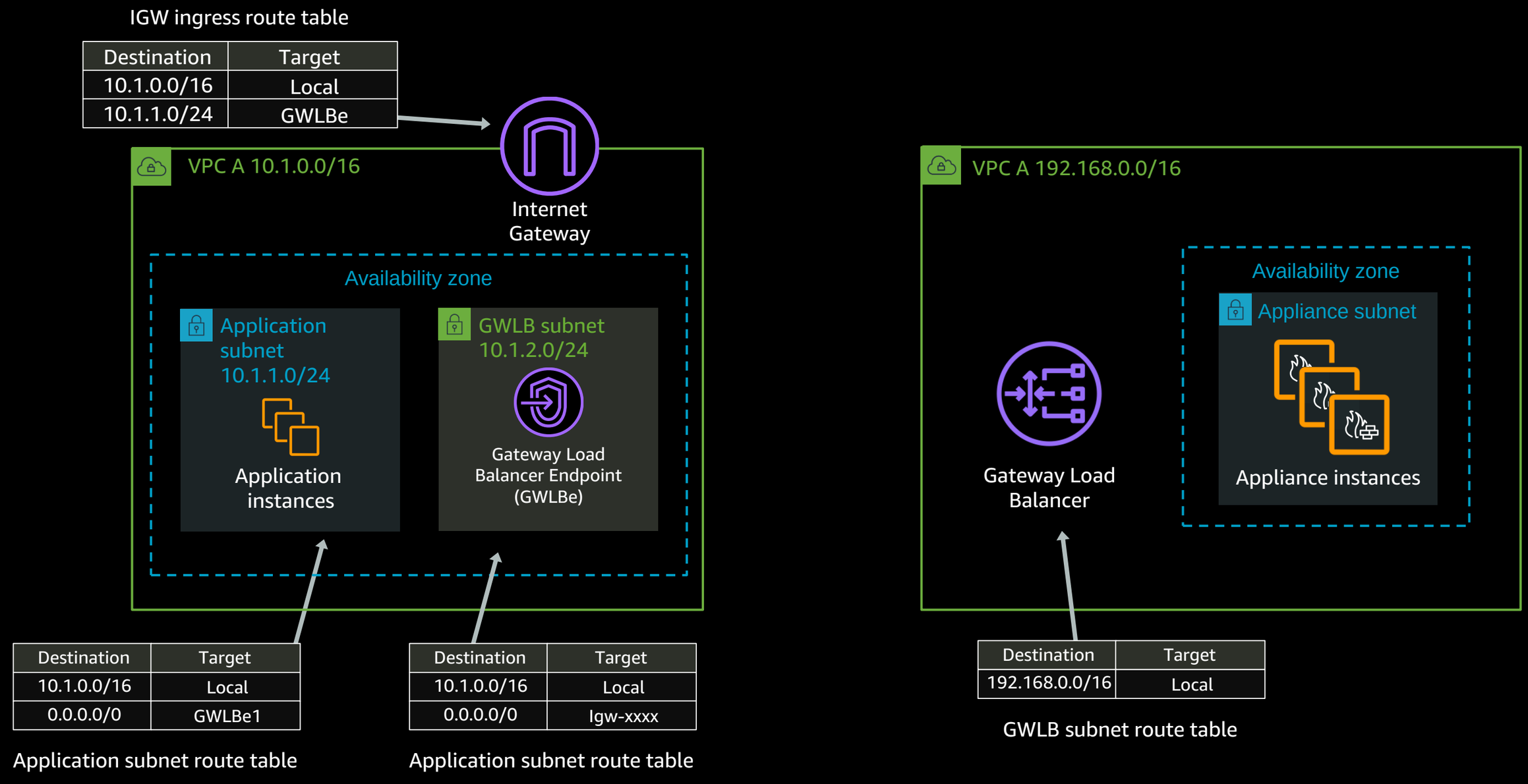
Benefits

- 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)

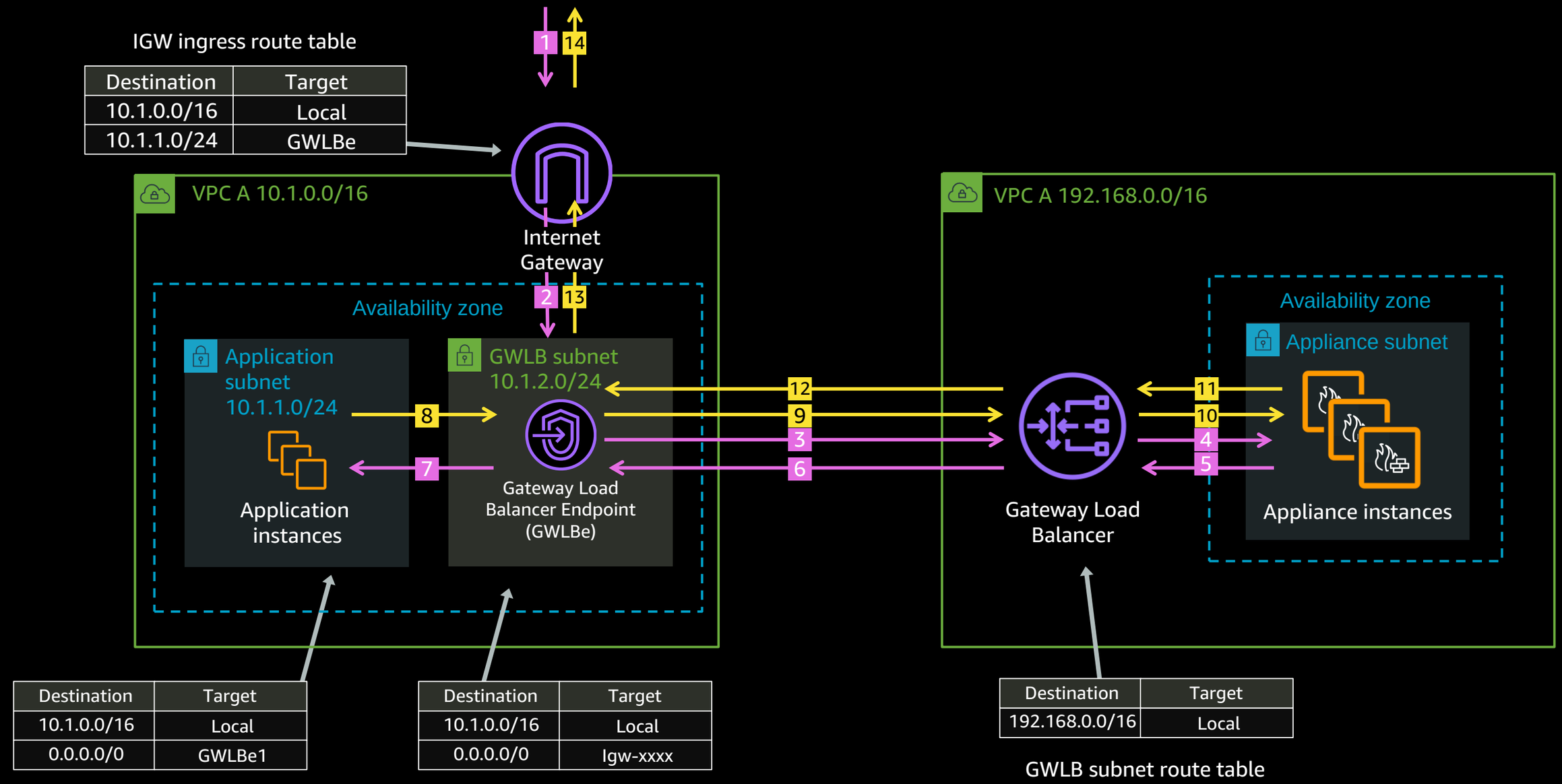
Deployment

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

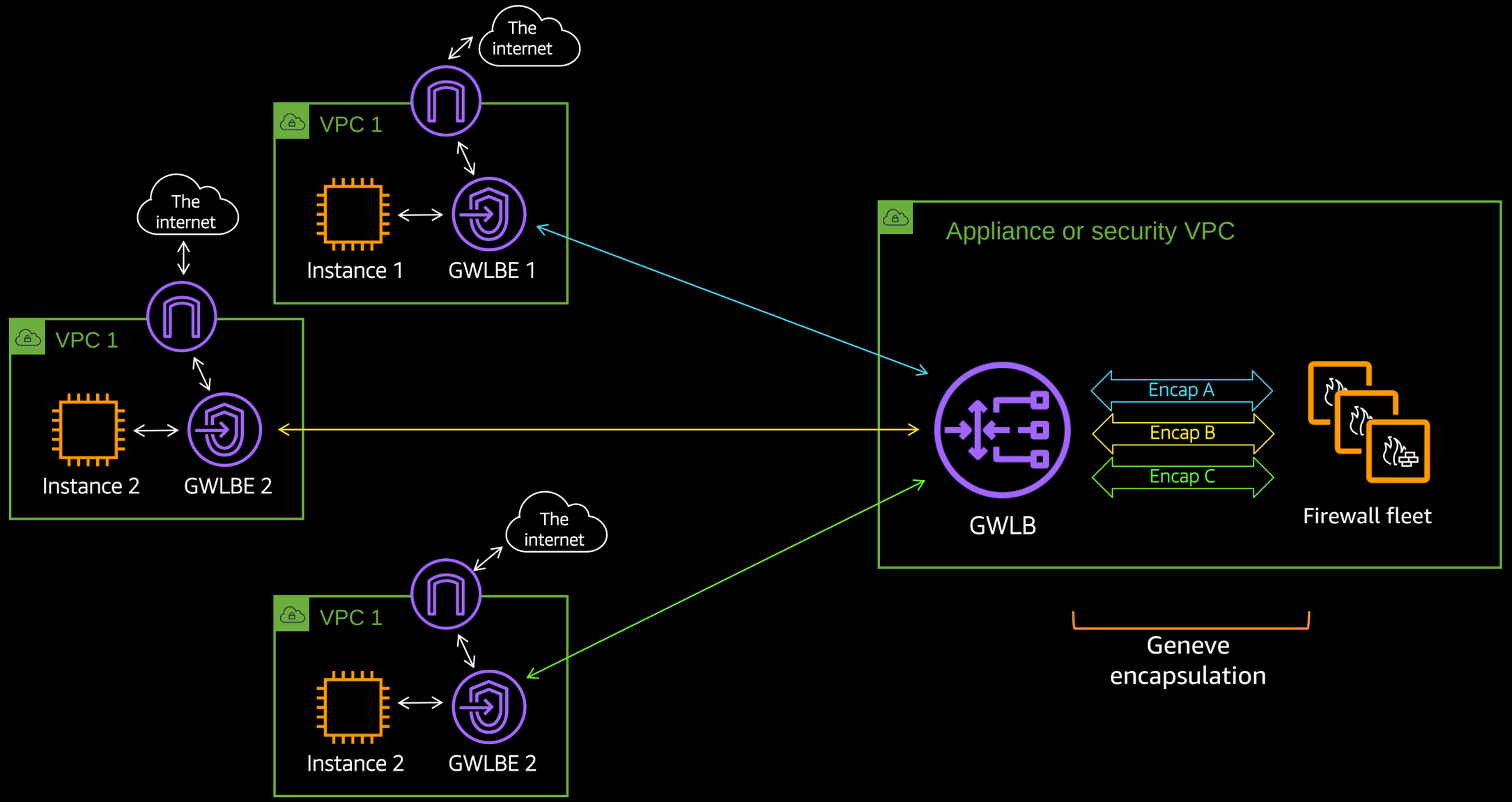
Gateway Load Balancer: After



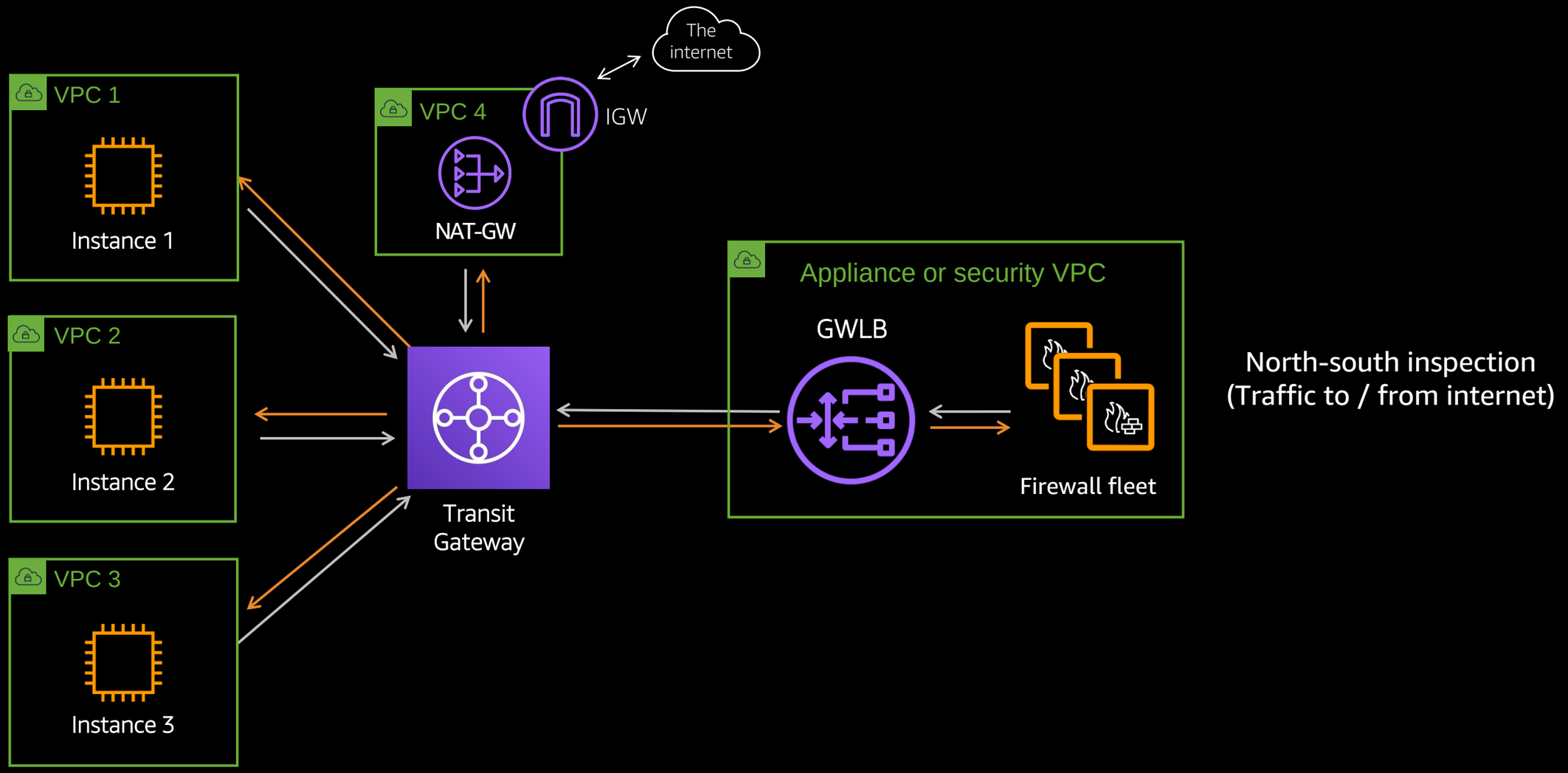
Gateway Load Balancer: After



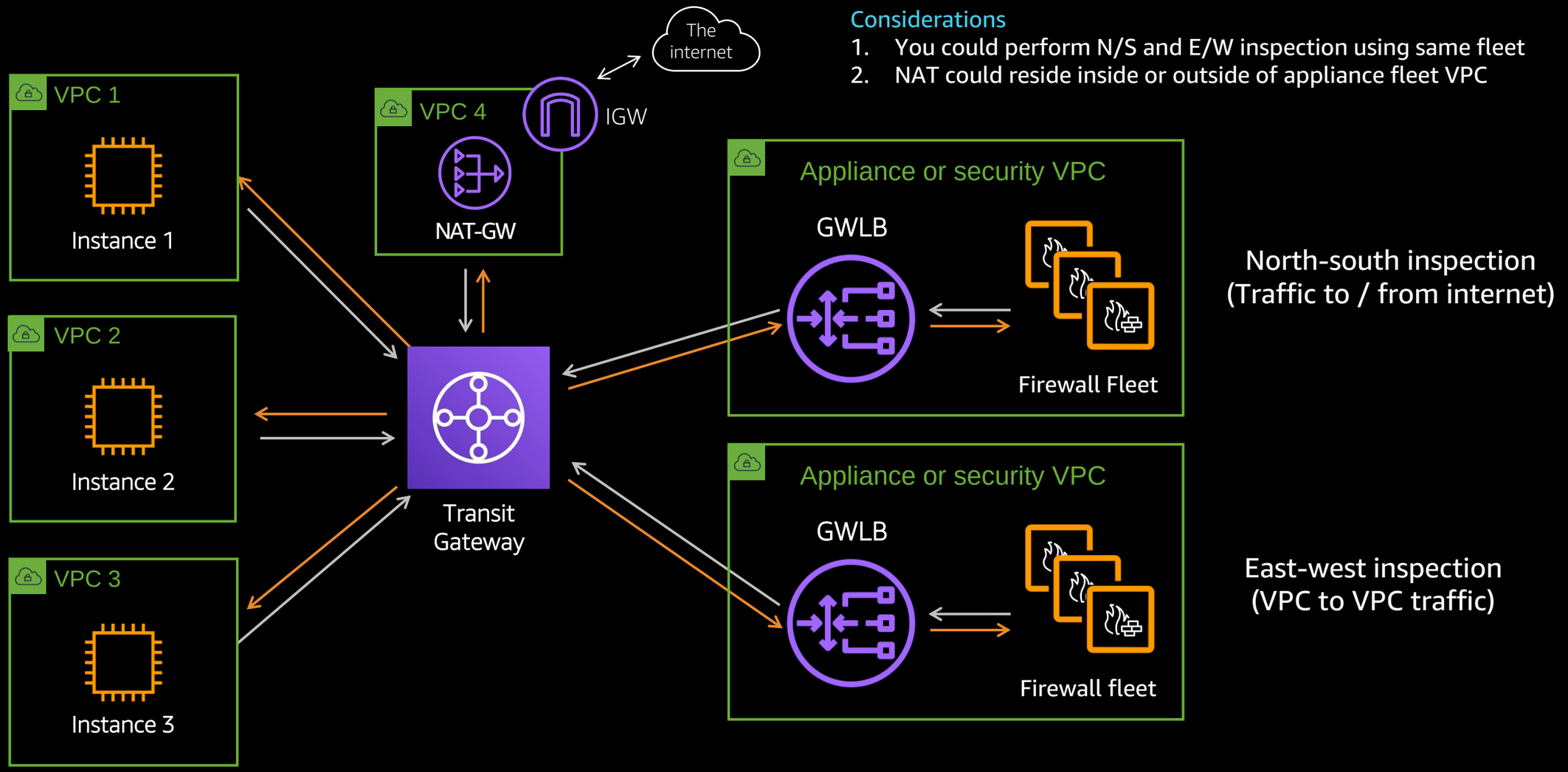
Gateway Load Balancer: After



Centralized security inspection with TGW



Centralized security inspection with TGW



Considerations

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

North-south inspection
(Traffic to / from internet)

East-west inspection
(VPC to VPC traffic)

GWLB launch partners and 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



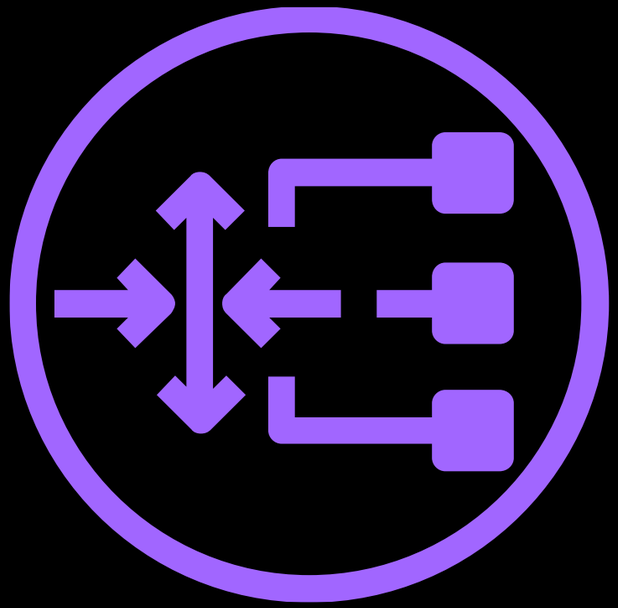




System integration partners:
Can implement architectures using GWLB



Gateway Load Balancer: Key takeaways



Reduce complexity and deploy faster

Elastically scale and reduce costs

Improve appliance availability

Supported by leading appliance vendors

AWS Network Firewall



SCAN ME

https://aws.amazon.com/network-firewall/

Introducing AWS Network Firewall!

AWS Network Firewall



AWS Network Firewall

Native firewall service from AWS that allows you to apply blanket protections for your entire VPC, regardless of the application type or protocol

Gives control and visibility across Layers 3-7 of the OSI model

Allows you to broadly inspect traffic flows to and from VPC, internet, and over direct connect and VPN

AWS Network Firewall



AWS Network Firewall

- Stateful and stateless rule options
- IP / port / protocol / FQDN-based filtering
- Regular expression matching
- ALLOW, DROP, or ALERT
- Rule-specific logging can be sent to Amazon S3, Amazon CloudWatch logs, and Amazon Kinesis Data Firehose

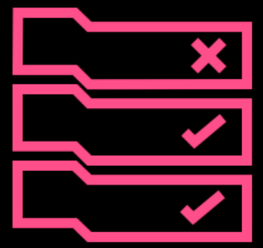
AWS Network Firewall: Key benefits



Fully managed



Flexible deployments



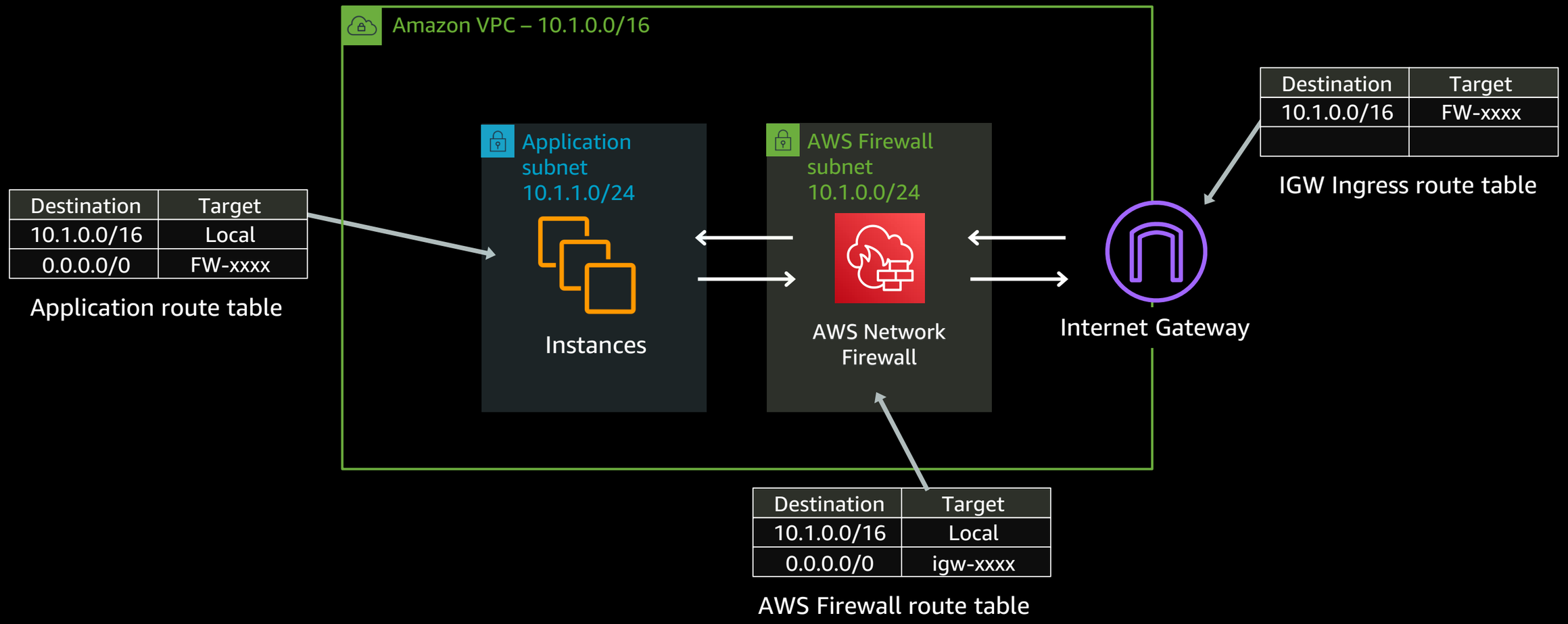
Fine-grained controls



Partner integrated

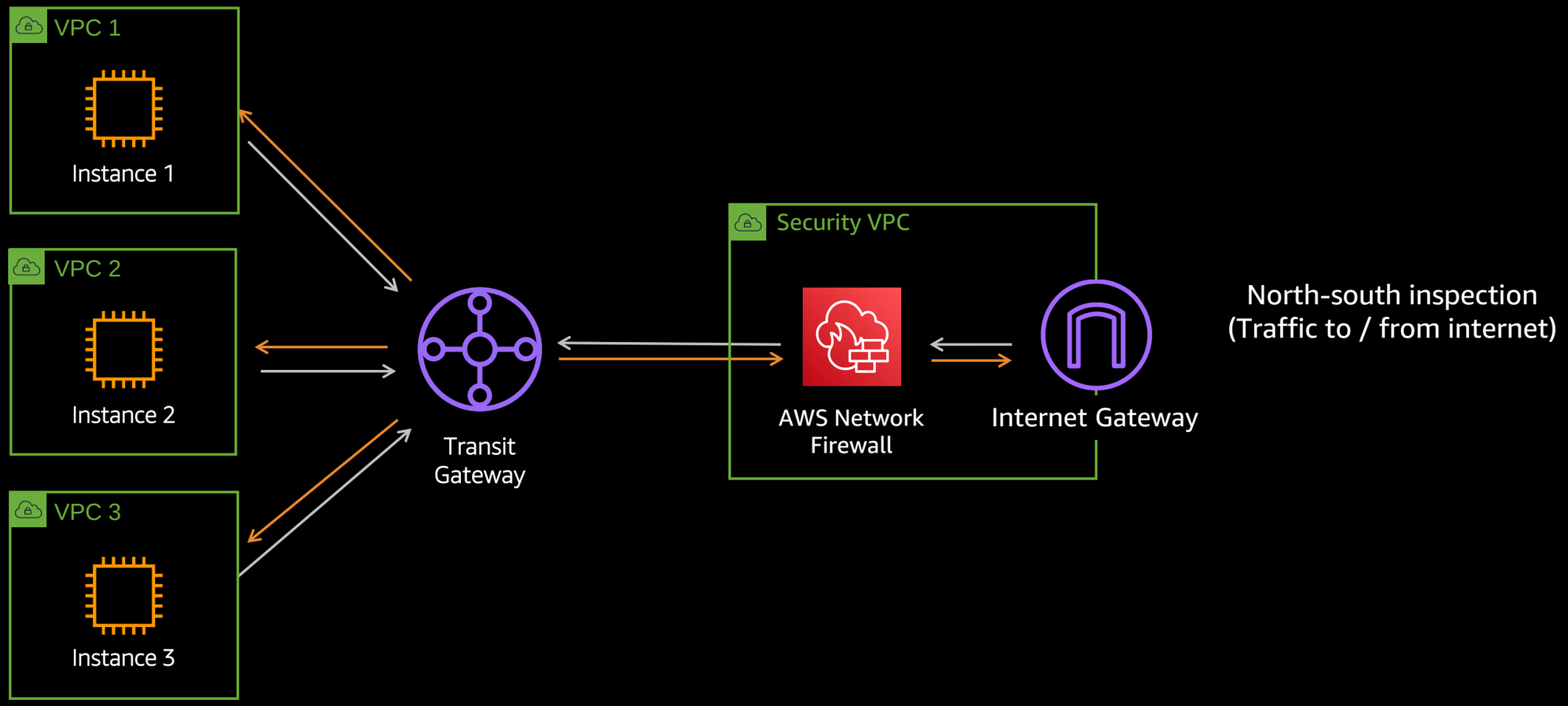
AWS Network Firewall

And Amazon VPC



AWS Network Firewall

And AWS Transit Gateway



SCAN ME

https://amzn.to/32P0BvM

What is AWS Client VPN?

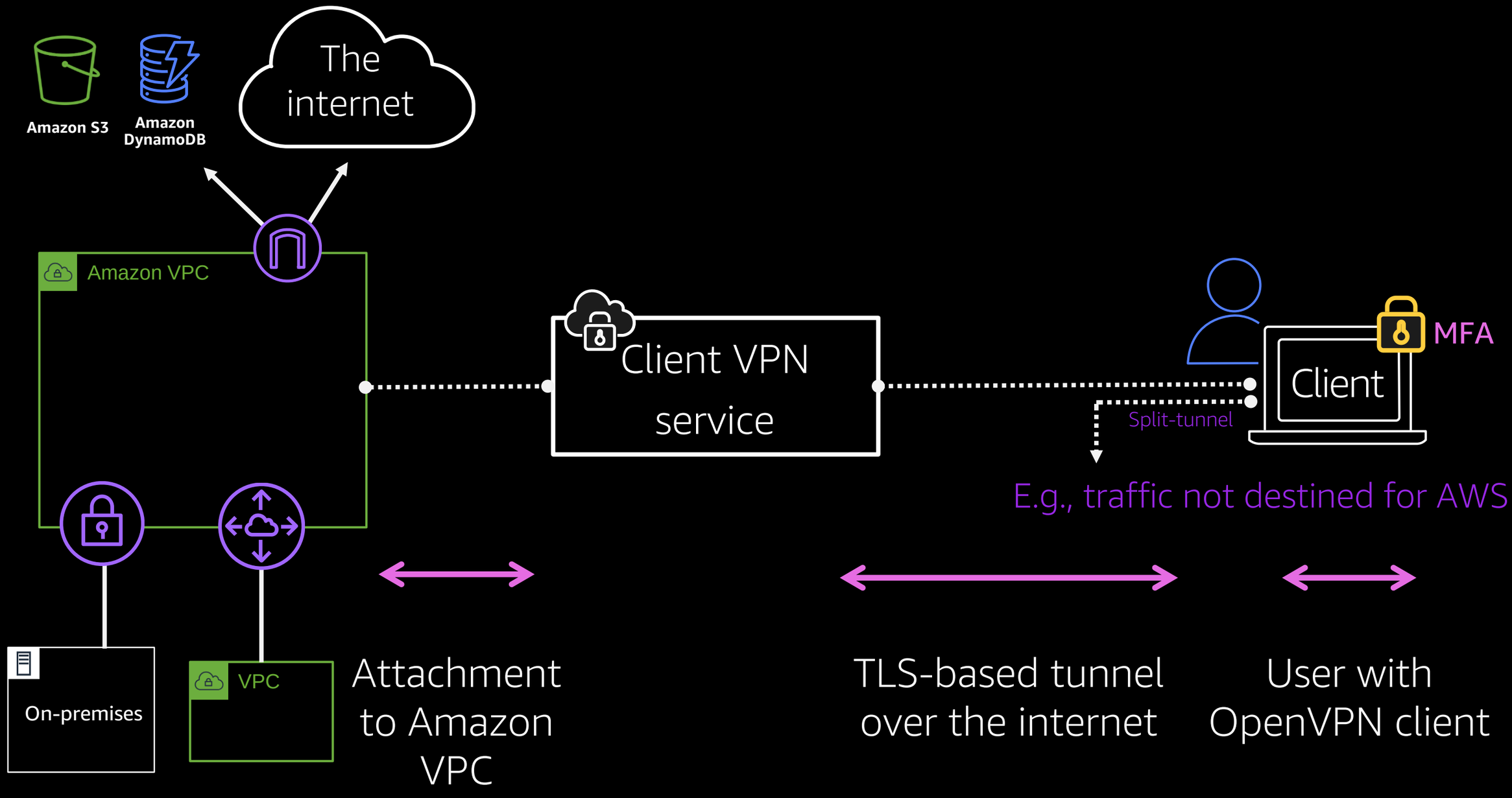
AWS VPN



AWS Client VPN

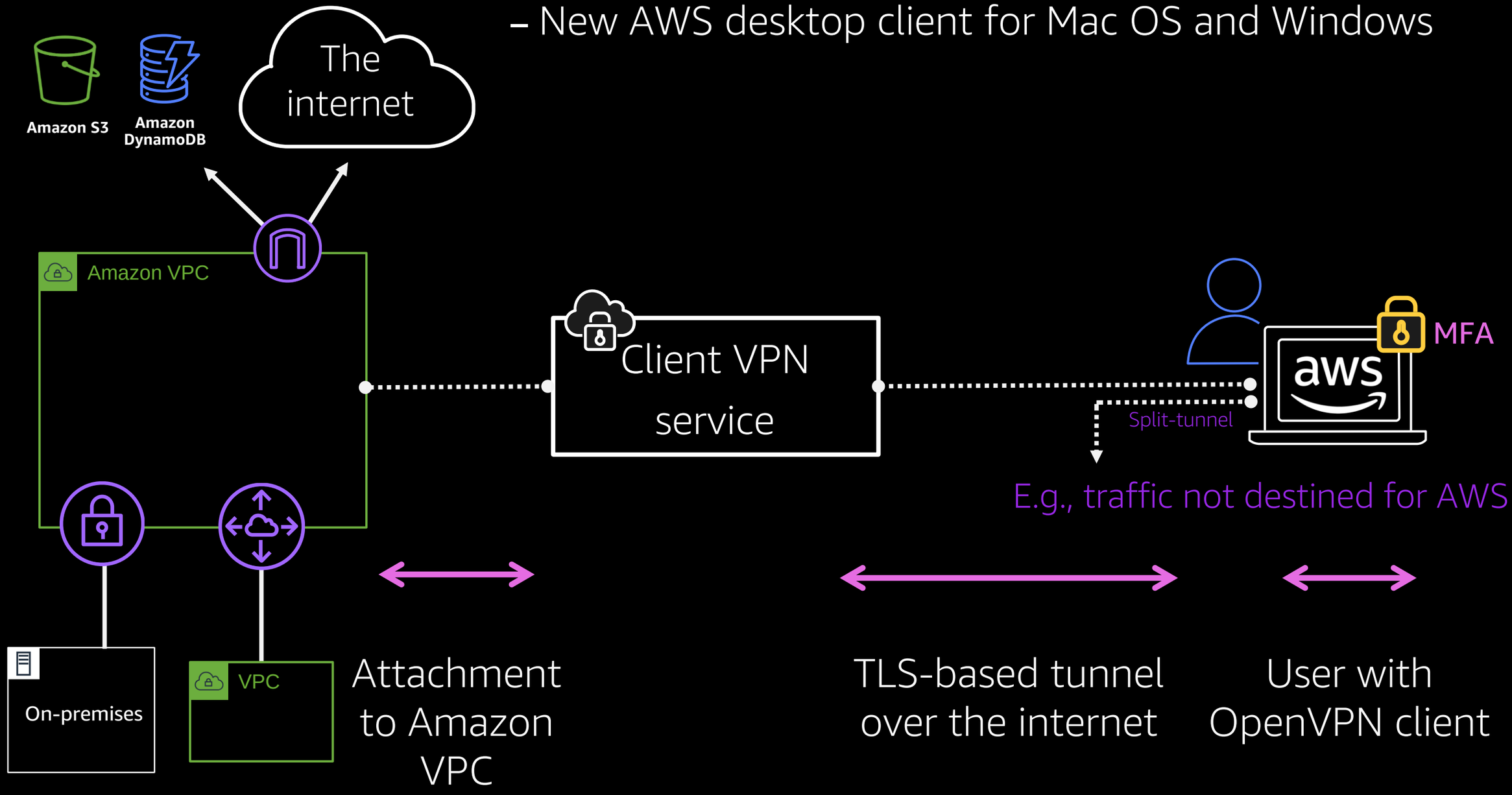
AWS Site-to-Site VPN

AWS Client VPN: Before



AWS Client VPN: After

– New AWS desktop client for Mac OS and Windows



AWS VPN



AWS Client VPN

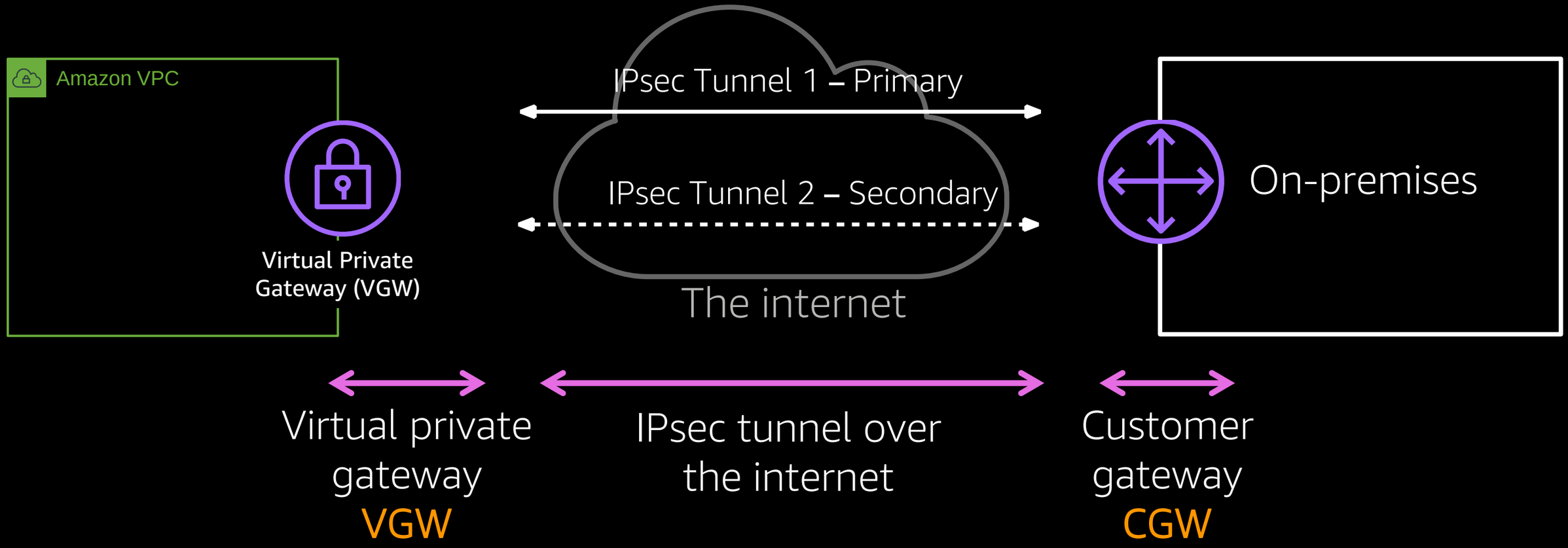
AWS Site-to-Site VPN

SCAN ME

https://amzn.to/3lz0ziQ

What is AWS Site-to-Site VPN?

AWS Site-to-Site VPN: Before



AWS Site-to-Site VPN: After

– Additional encryption, integrity, and key exchange algorithms

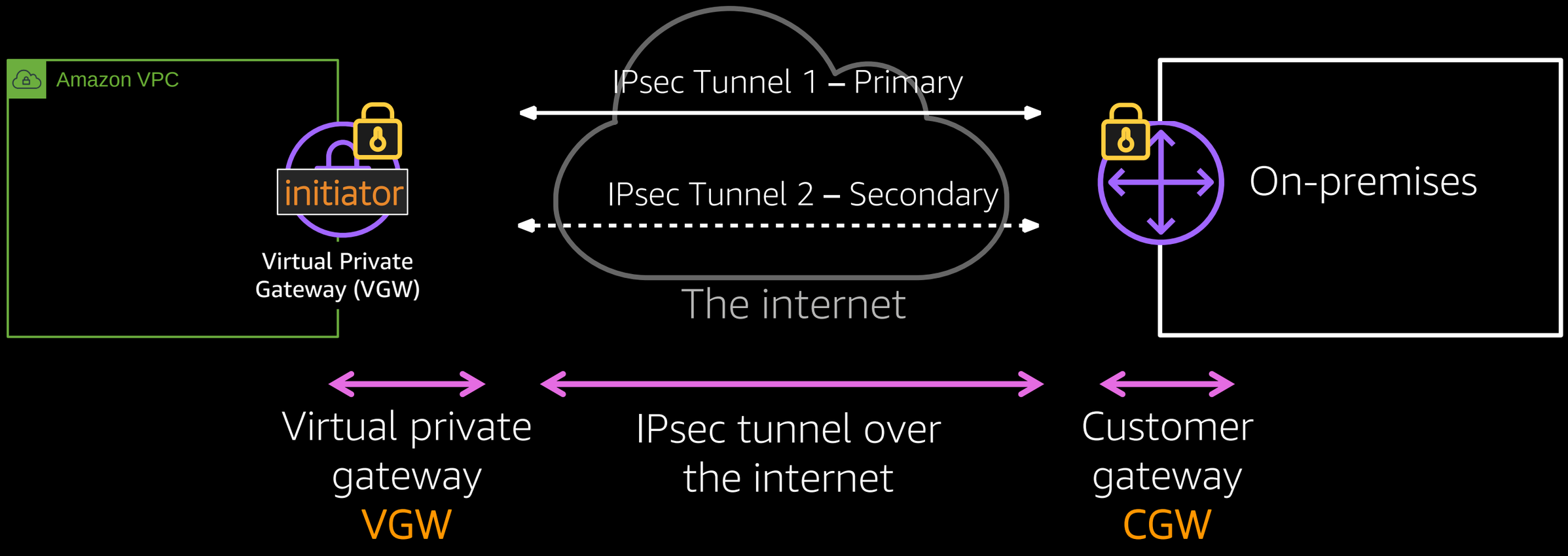
– Tunnel initiator mode

SCAN ME

Additional encryption, integrity, and key exchange:

Encryption: AES128-GCM-16, AES256-GCM-16.
Integrity:. SHA2-384, SHA2-512
Diffie-Hellman groups: 19, 20, 21.

https://amzn.to/3f4N9sI



AWS Site-to-Site VPN: After

– Additional encryption, integrity, and key exchange algorithms

– Tunnel initiator mode

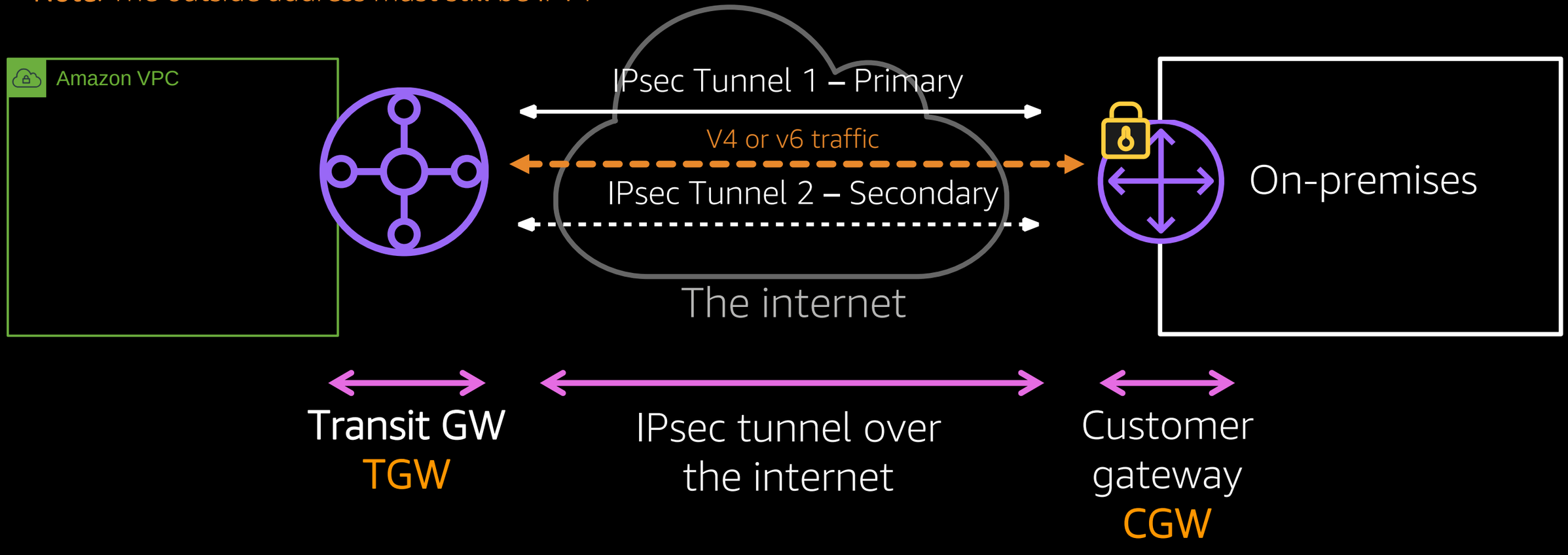
– IPv4 or IPv6 traffic inside the AWS site to site VPN tunnel
(/30 address range for v4 and /128 for v6)

Note: The outside address must still be IPv4

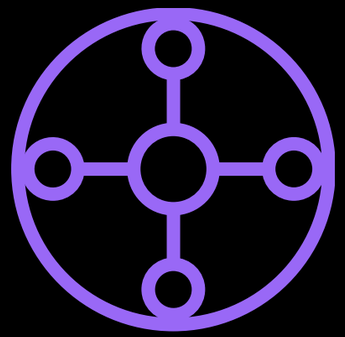
SCAN ME

IPv4 and IPv6 inside traffic for TGW Site to Site VPN

https://amzn.to/3f4N9sI



AWS Transit Gateway

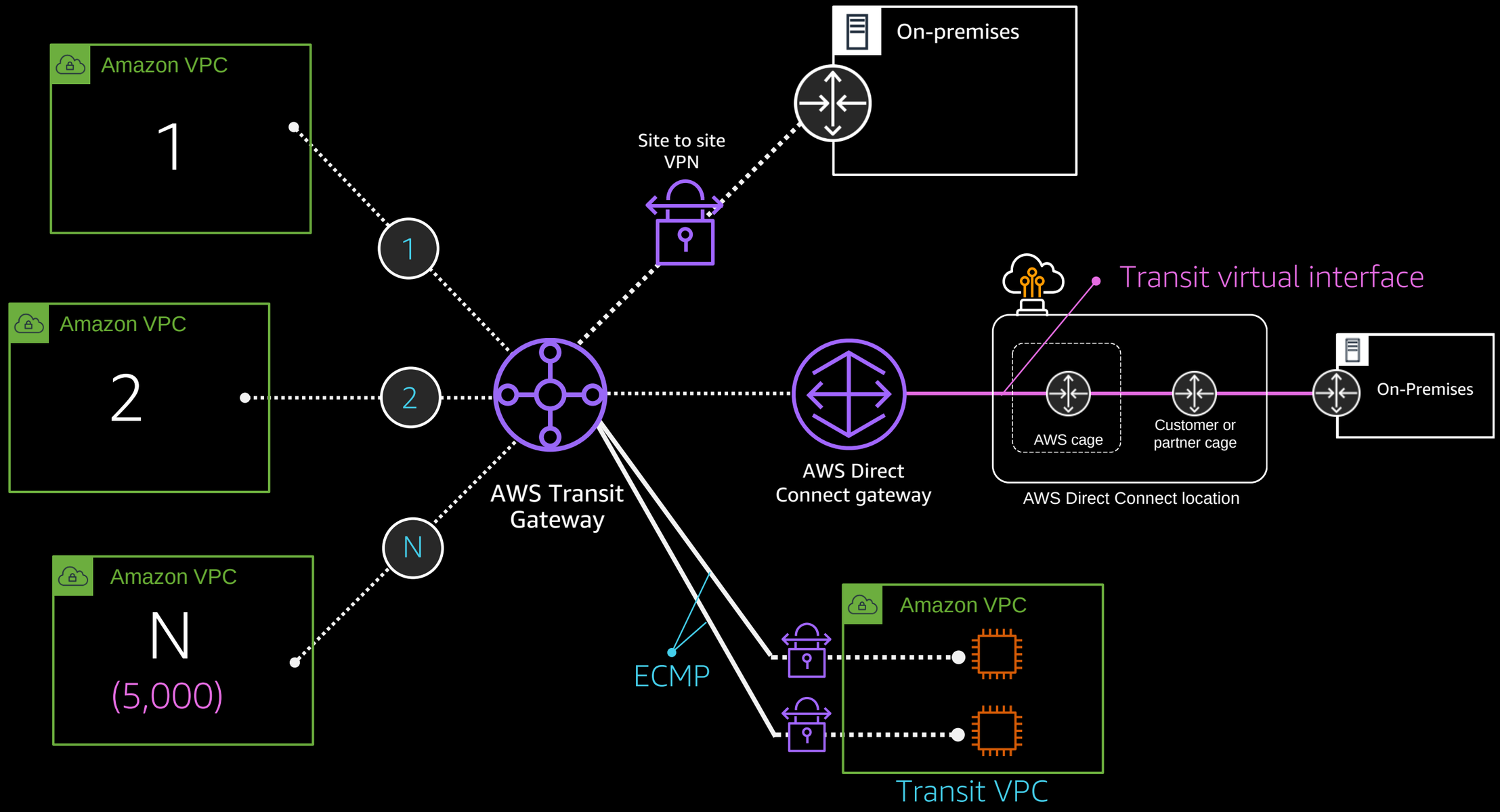


SCAN ME

https://amzn.to/35wUD4u

What is AWS Transit Gateway?

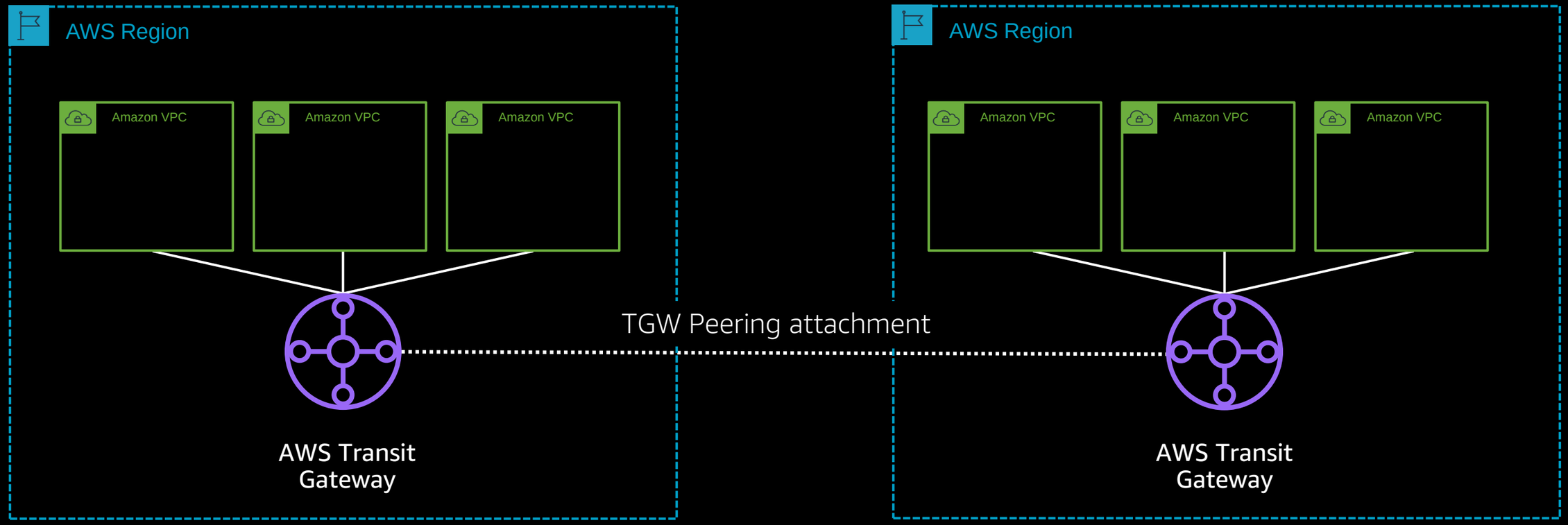
AWS Transit Gateway: Before



AWS Transit Gateway: Before

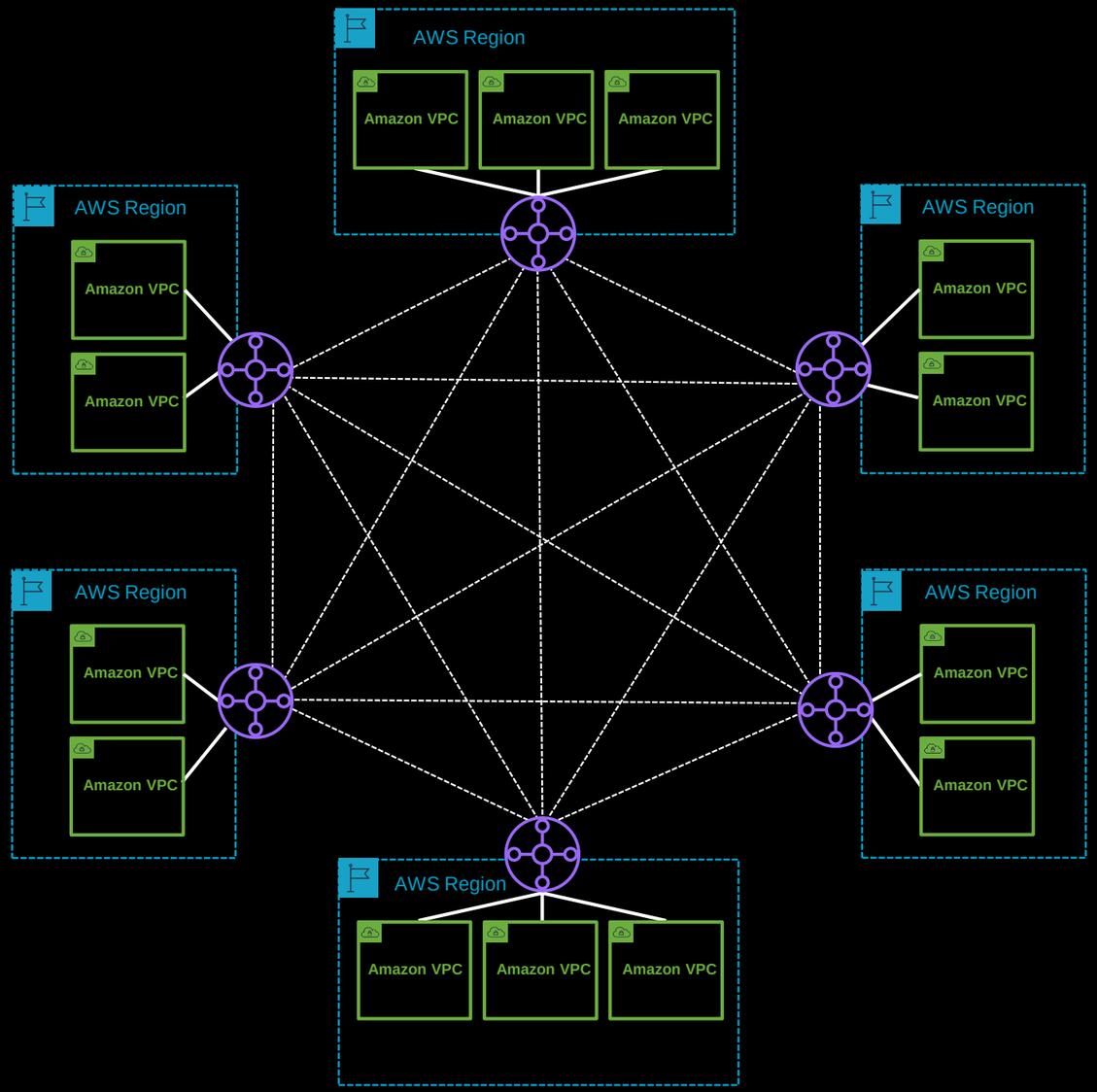
Cross-region transit gateway peering

– Static peering between regions (US only at launch)
– New attachment type
– Uses encrypted VPC peering across the AWS backbone
– No peering within the same region (designed for inter-region connectivity)



AWS Transit Gateway: Before

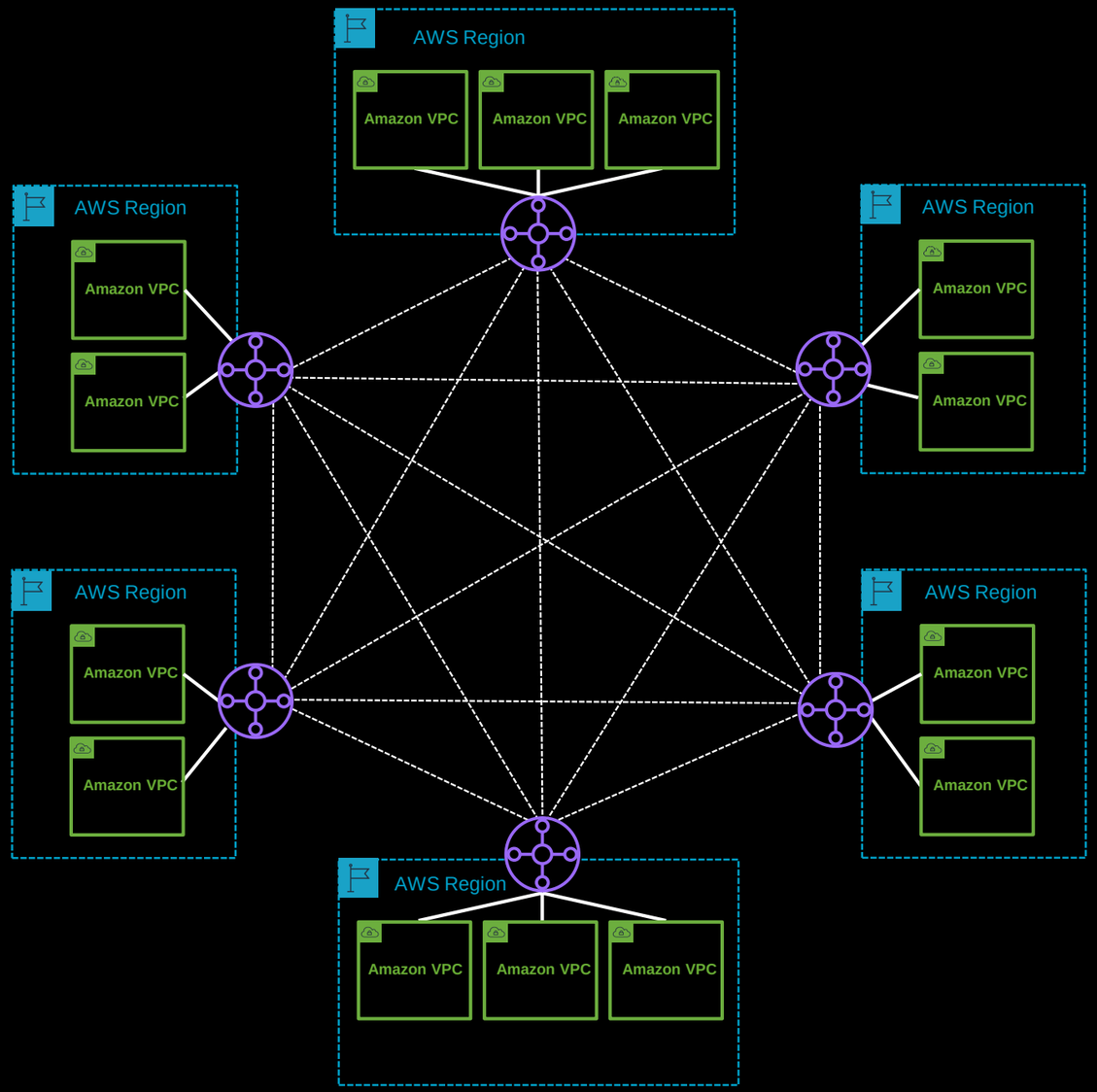
Multi-region transit gateway peering



- Suggested full-mesh peering
- Use unique ASNs for Transit Gateways across regions
- Supported in:
  - US East (Virginia)
  - US East (Ohio)
  - US West (Oregon)
  - US West (Northern California)
  - EU (Ireland) and
  - AsiaPacific (Mumbai)

AWS Transit Gateway: After

Multi-region transit gateway peering



- Attachment level metrics now available via Amazon CloudWatch
- Transit GW peering now supported in:
  - US East (N. Virginia)
  - US East (Ohio)
  - US West (Oregon)
  - US West (N. California)
  - AWS GovCloud (US-East)
  - AWS GovCloud (US-West)
  - Canada (Central)
  - EU (Ireland), EU (Frankfurt)
  - EU (Paris), EU (London)
  - EU (Stockholm)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Tokyo)
  - Asia Pacific (Seoul)
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney) and
  - South America (Sao Paulo)

AWS Transit Gateway: After

Route Analyzer

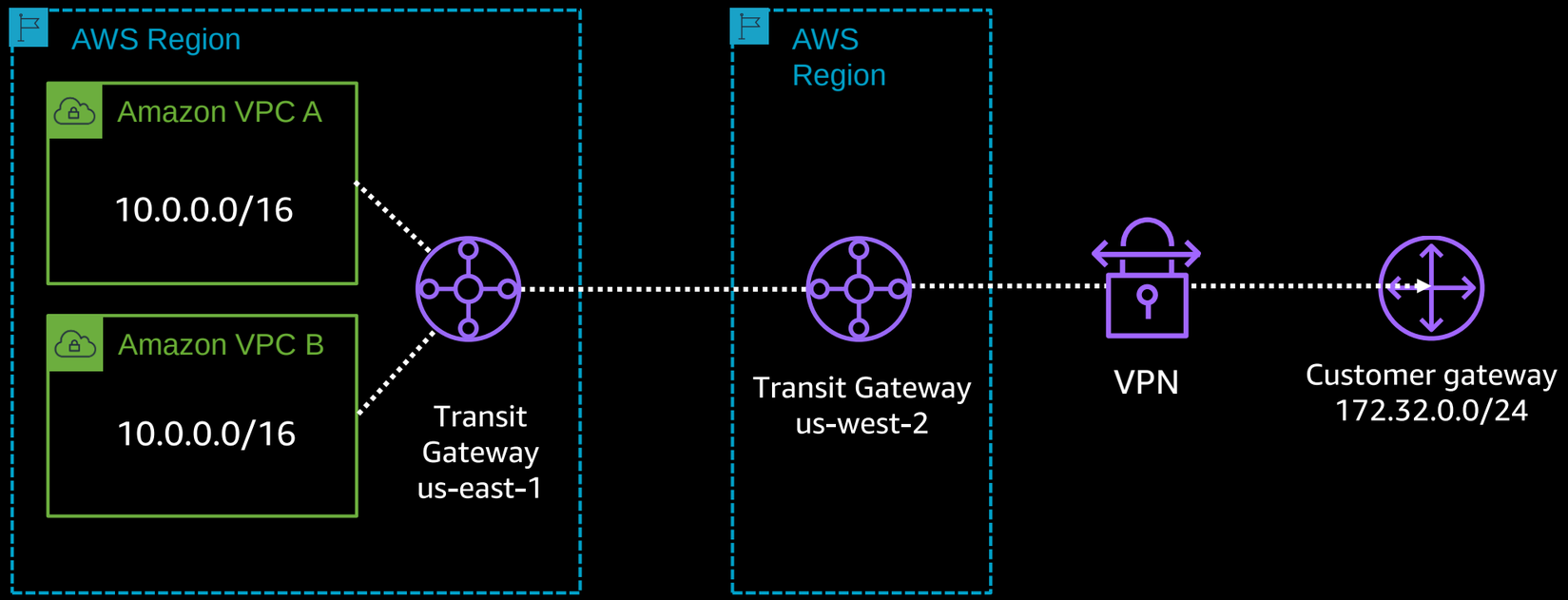
SCAN ME

https://amzn.to/2J8vDbi

Introducing Route Analyzer!

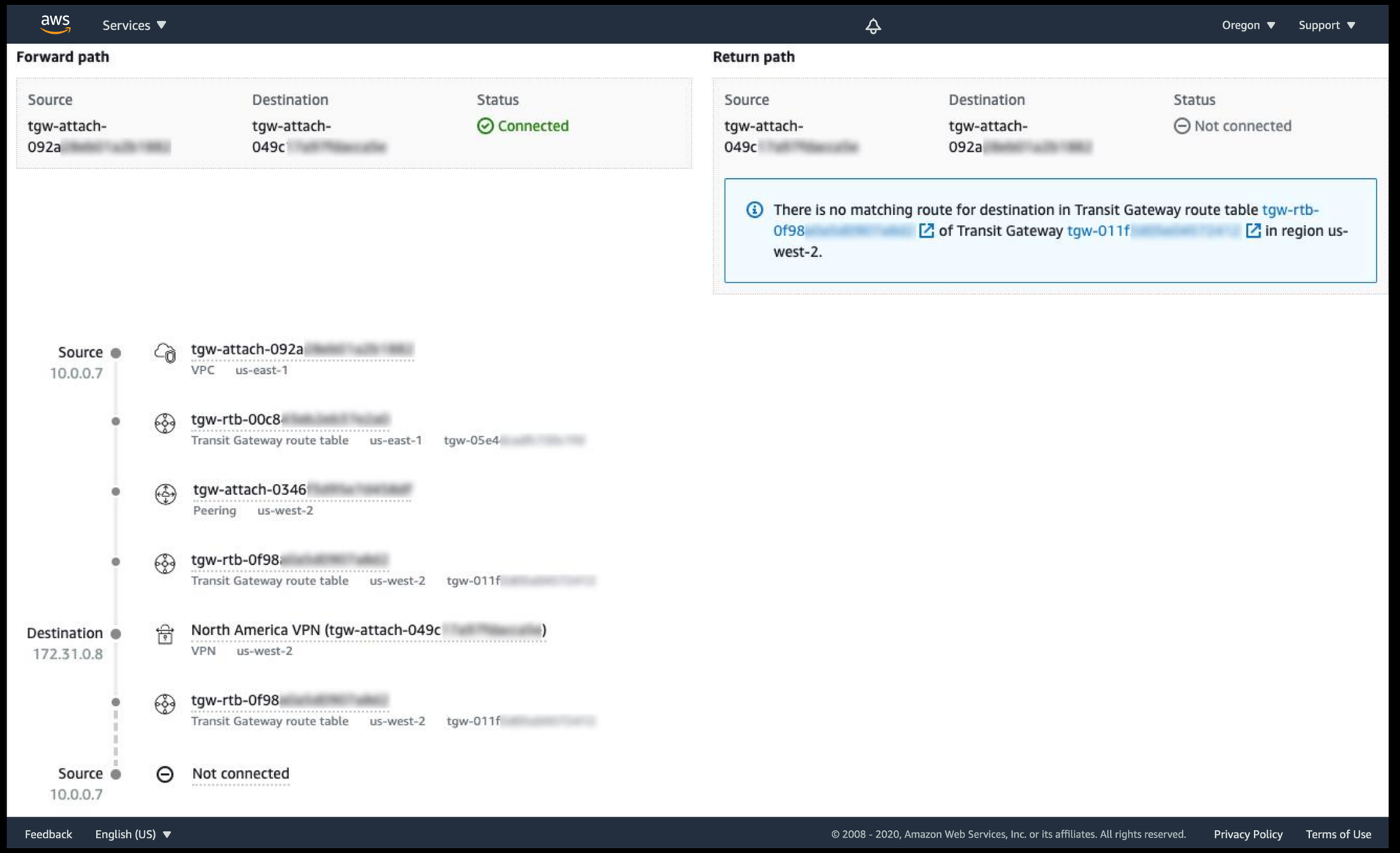
Route Analyzer can –

- Verify that the transit gateway route table configuration will work as expected before you start sending traffic
- Validate your existing route configuration
- Diagnose route-related issues that are causing traffic disruption in your global network



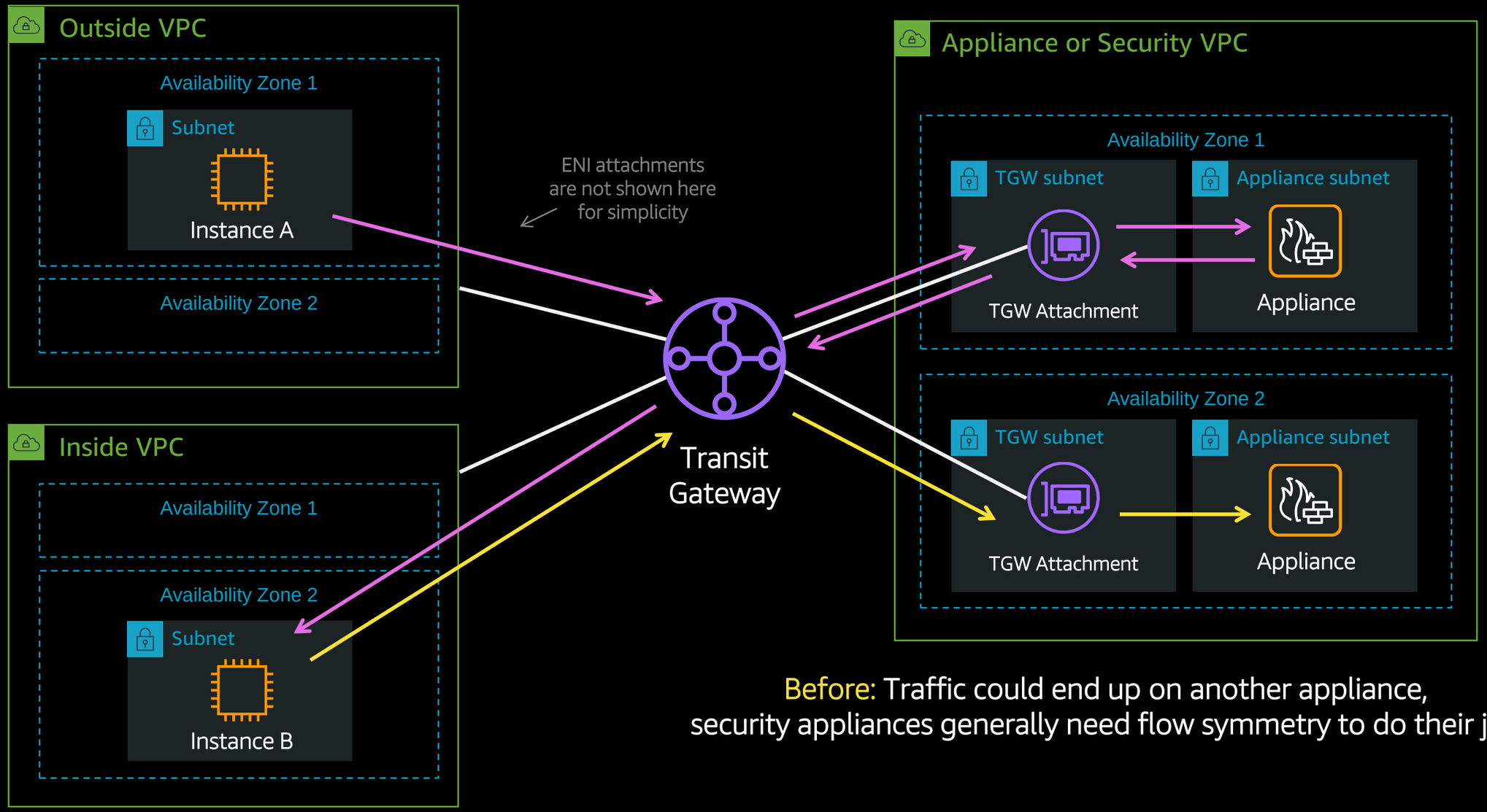
AWS Transit Gateway: After

Route Analyzer



AWS Transit Gateway: Before

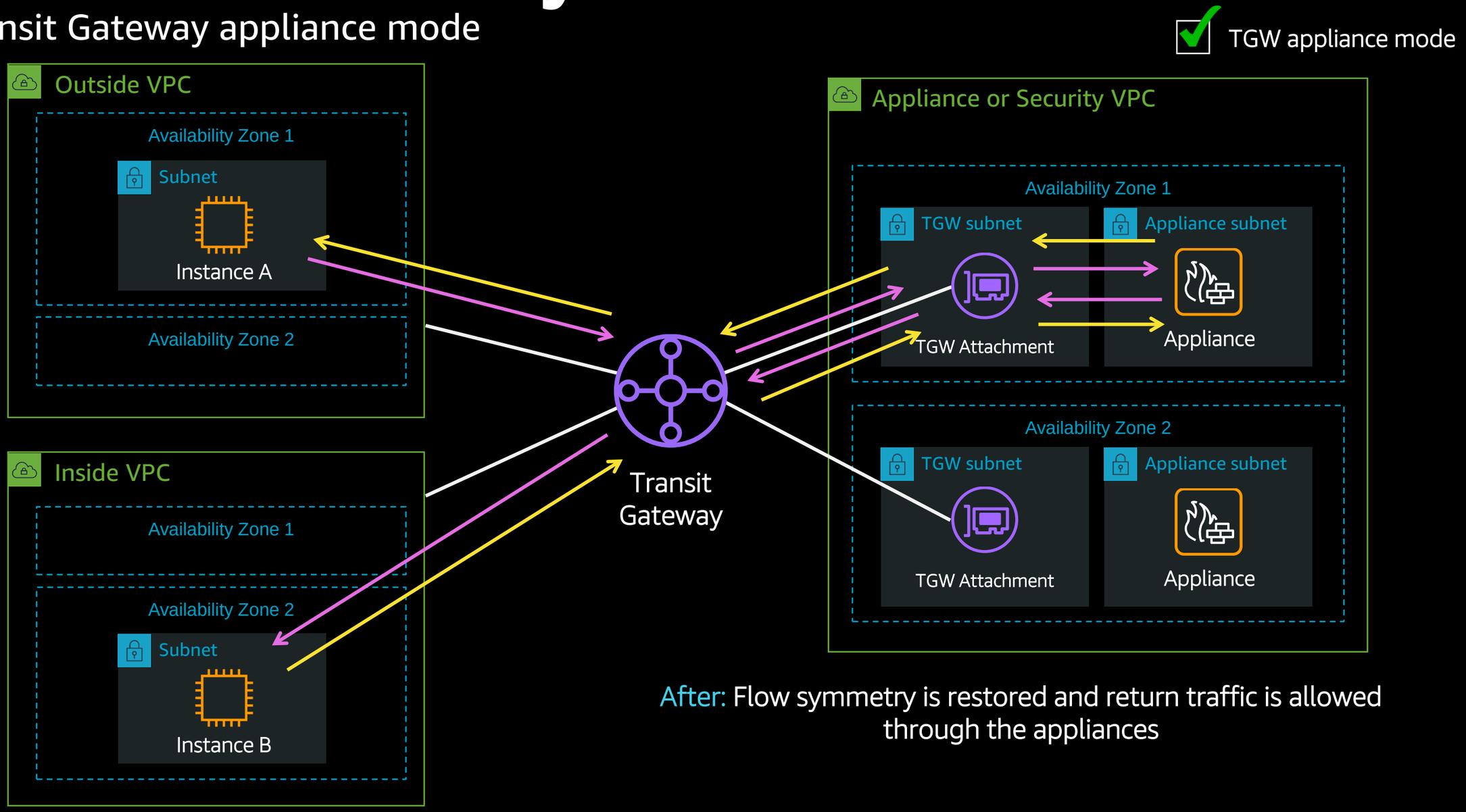
AWS Transit Gateway appliance mode



Before: Traffic could end up on another appliance, security appliances generally need flow symmetry to do their job

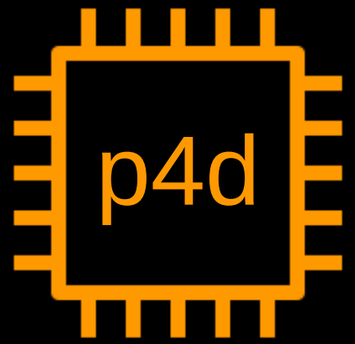
AWS Transit Gateway: After

AWS Transit Gateway appliance mode



After: Flow symmetry is restored and return traffic is allowed through the appliances

400 Gbps networking



SCAN ME

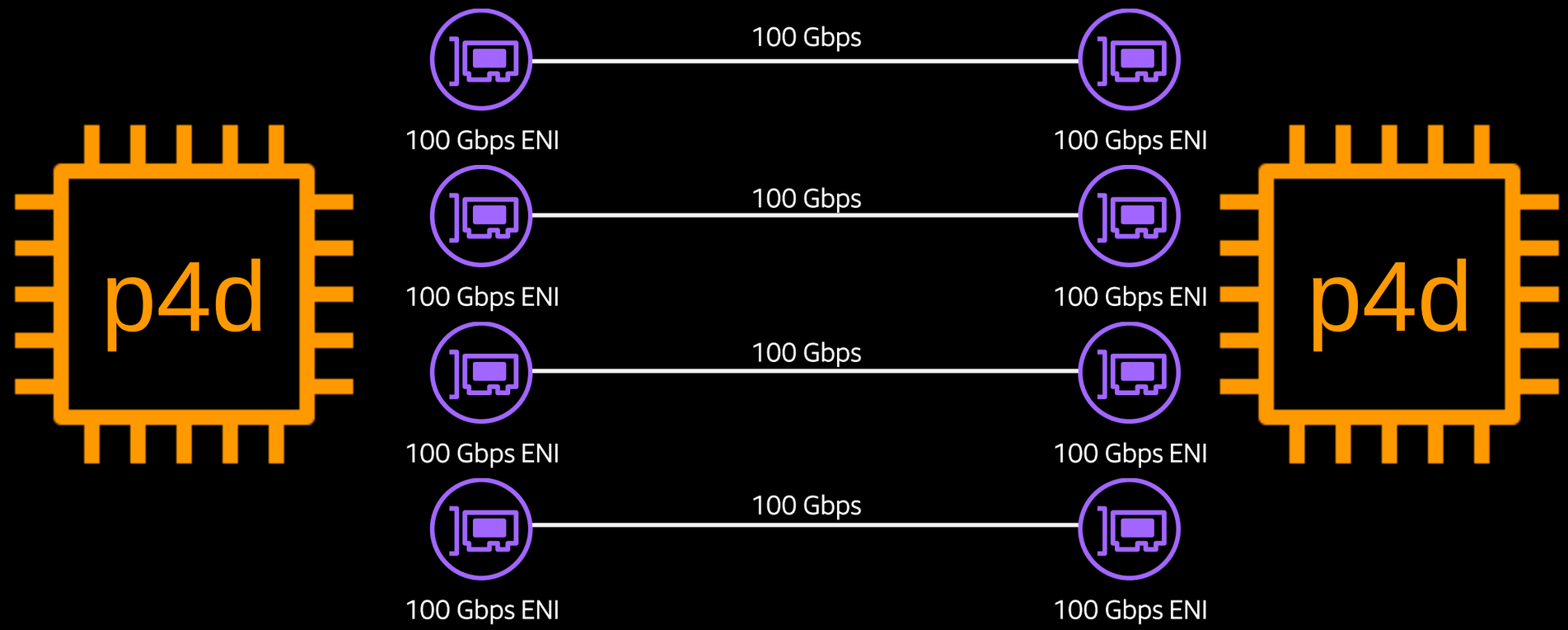
https://amzn.to/3lAkr5h

Amazon p4d instances with 400 Gbps!

400 Gbps instance networking: Cloud First!

Amazon EC2 P4d instances are deployed in hyperscale clusters

Multiple network cards (x4) allow for N-times throughput of Amazon EC2 instances



Honorable mentions



Bring your own IPv6

Create VPCs with your own IPv6 addresses

https://amzn.to/3kyeTH5



IPv6 for Network Load Balancer (NLB)

https://amzn.to/3lMQIG8



Amazon VPC prefix lists

Use your own prefix lists to simplify the configuration of security groups and route tables

https://amzn.to/3ntFiaO



Related sessions

NET201: AWS Outposts: Networking foundations

NET202: Go global with AWS multi-Region network services

NET205: Introducing GWLB for deploying and running virtual appliances

NET303: Shared VPCs, lessons learned, and best practices

NET308: Migrating your on-premises resources to the cloud

NET311: How AWS Global Accelerator improves performance

AWS PrivateLink

IPv6 for Network Load Balancer

Bring your own IPv6

400 Gbps networking

p4d

Amazon VPC Prefix Lists

Gateway Load Balancer (GWLB)

Monitoring and Visibility

VPC Flow Logs

VPC Traffic Mirroring

AWS Network Firewall

AWS VPN

AWS Client VPN

AWS Site to Site VPN

AWS Transit Gateway

Thank you!

Matt Lehwess
@mlehwess



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.