Access Your Cloud Workloads From Anywhere

Bruce Wang, Partner Solutions Architect

Amazon Web Services

What to expect from this session

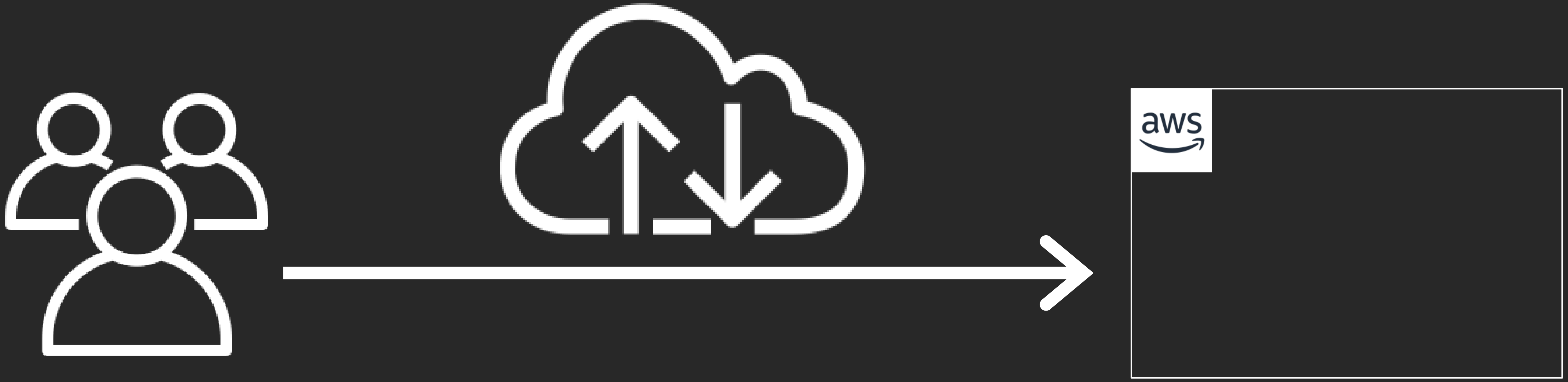
You will learn how to integrate variety of AWS networking services to build a reliable and scalable architecture in three common cloud access scenarios.

Access from internet

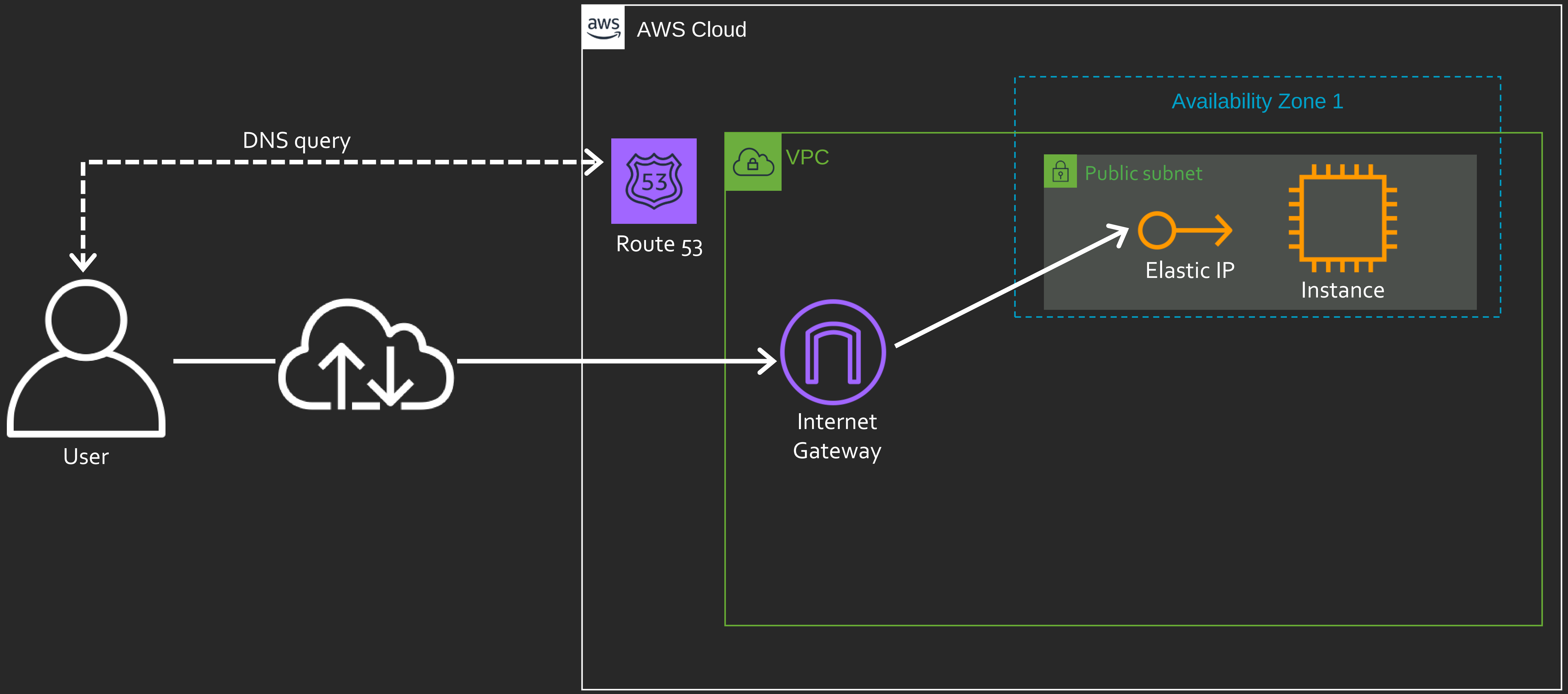
Access from other VPCs

Access from your on-premises

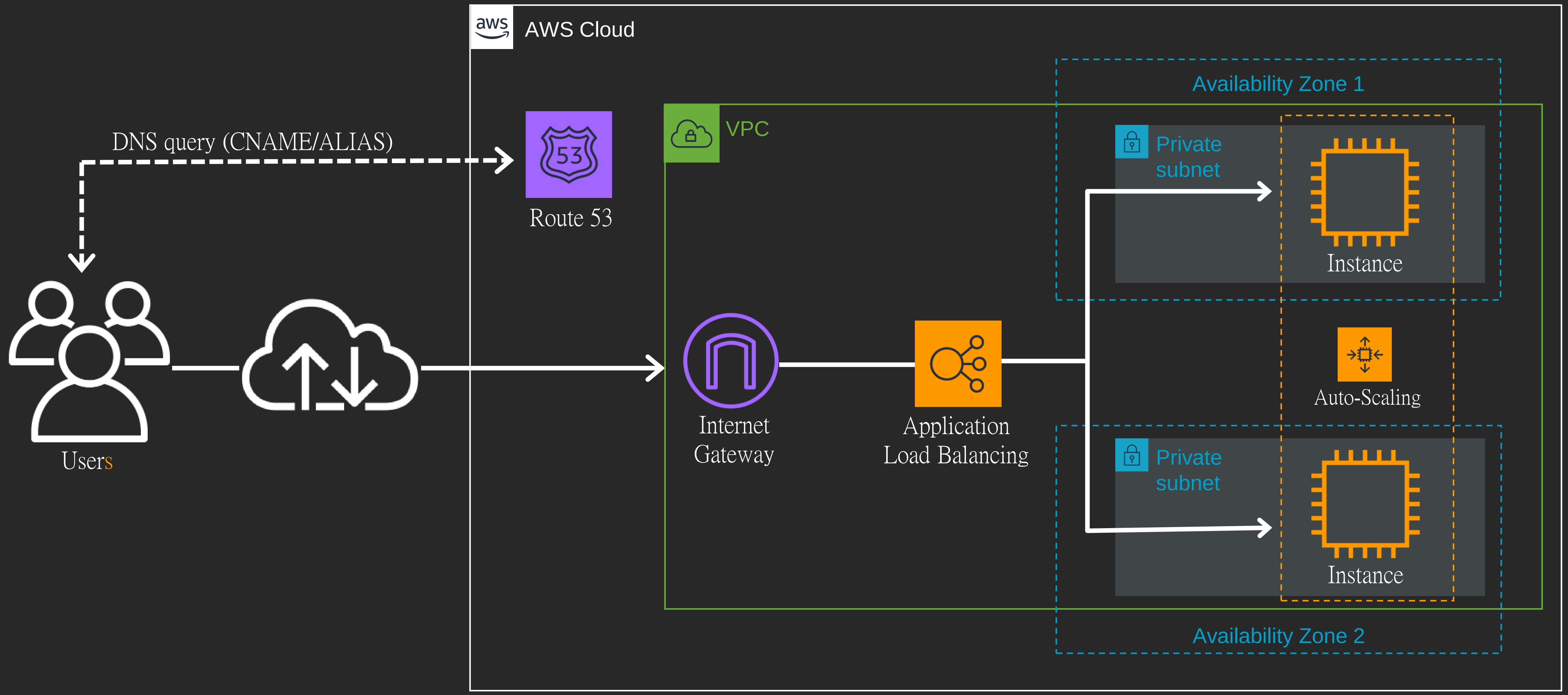
Access from Internet



Our starting point



Auto-Scaling and Load Balancing in VPC



Elastic Load Balancing security tools

TLS Offloading

Offload TLS processing to Application Load Balancer

SNI Support

Allows for multiple TLS certificates per load balancer

Access Logs

Request logging for all requests received by the load balancer

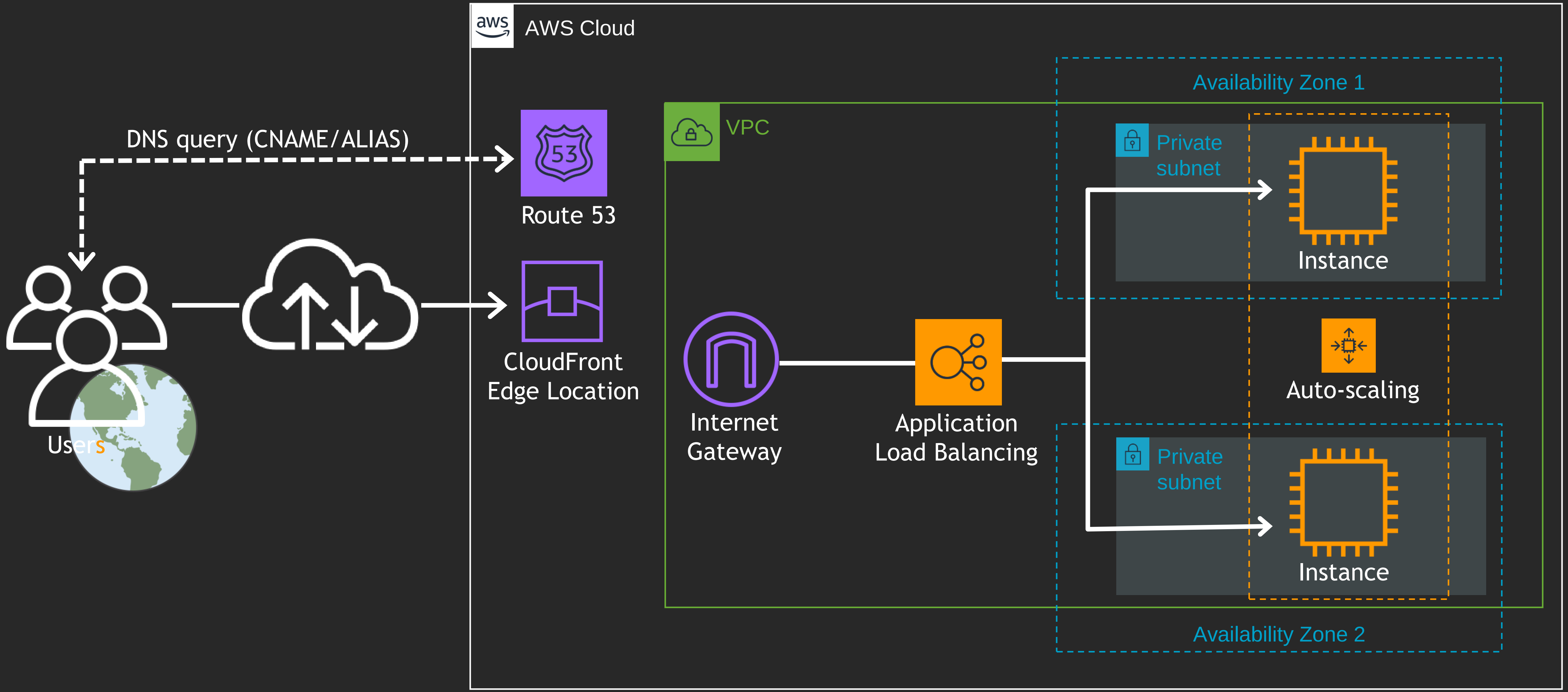
Application Firewall

Integrated with the Website Application Firewall (WAF)

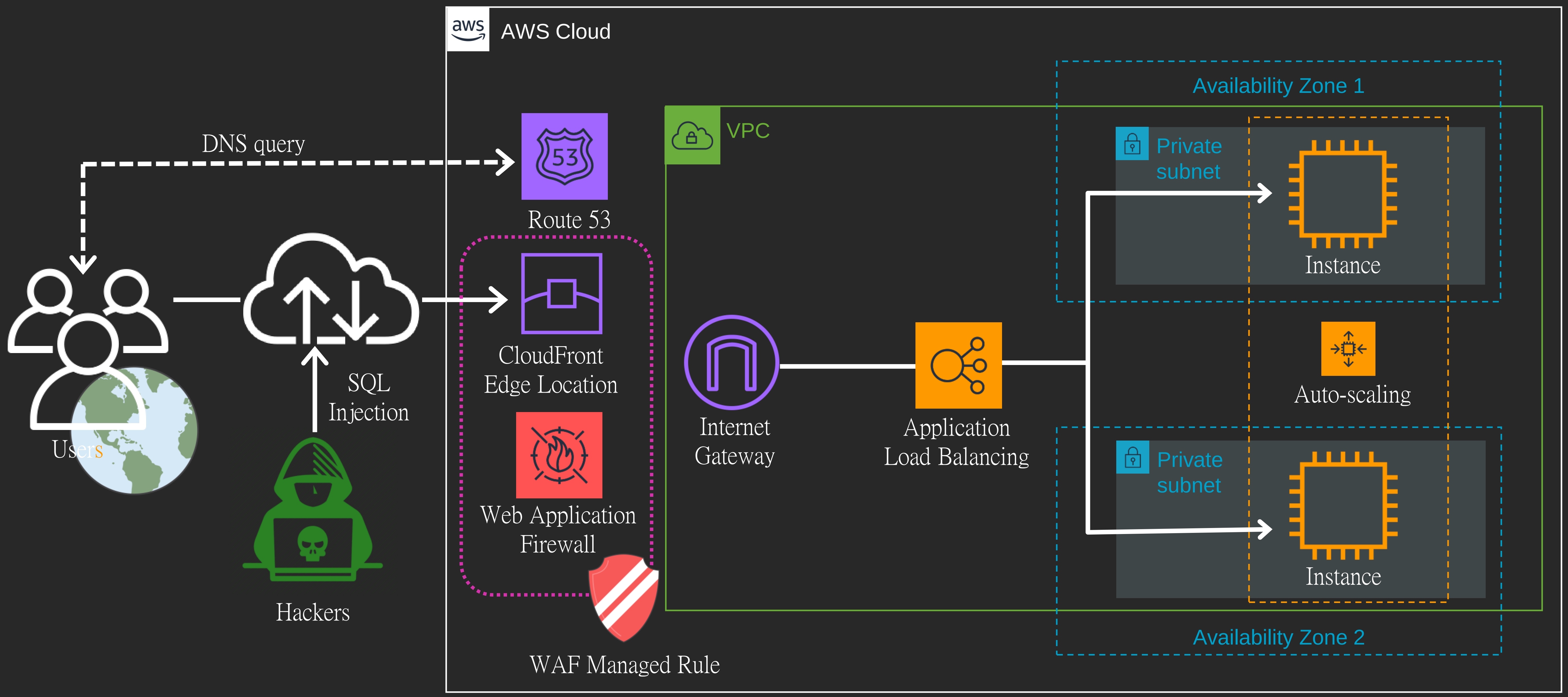
User Authentication

Secure your application by offloading user authentication to Application Load Balancer, including support for federated identities.

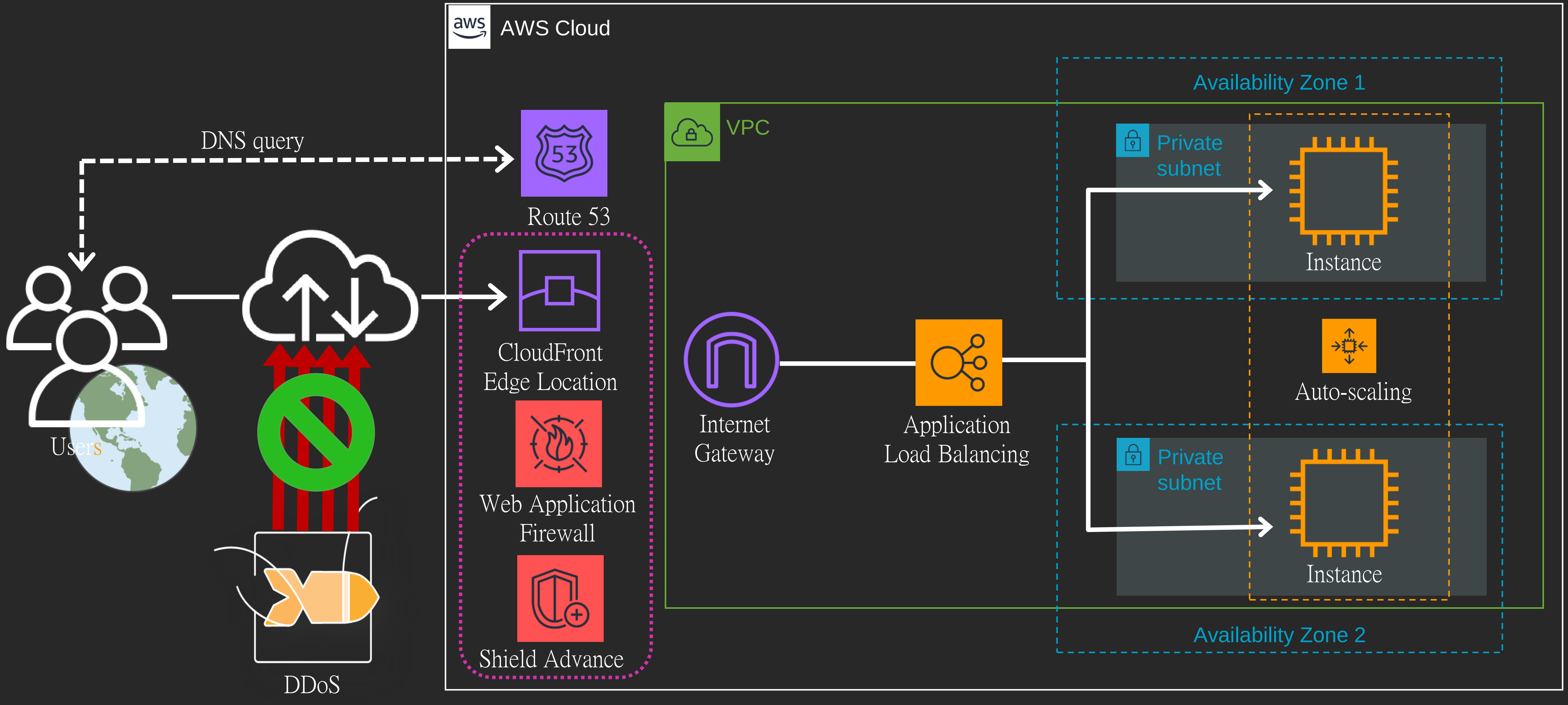
Global reachability



Secure your web applications



DDoS Mitigation



Content Distribution with Amazon CloudFront

Benefits

Fast, massively scaled and globally distributed

Highly Programmable

Network and application protection at the edge

Deep Integration with AWS

Key advancements

50 new Amazon CloudFront locations

Improved availability with origin failover

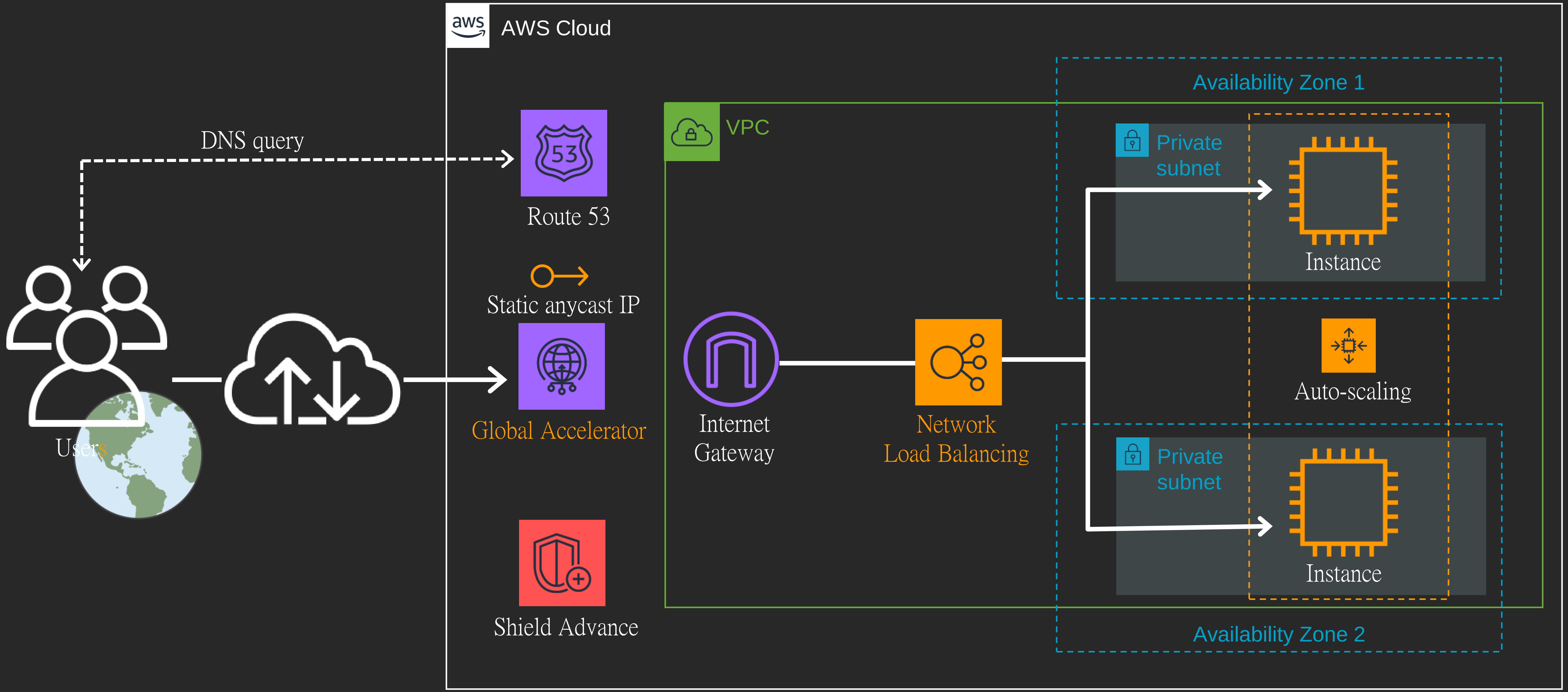
Improved performance and security via websockets

Support for ECDSA certificates

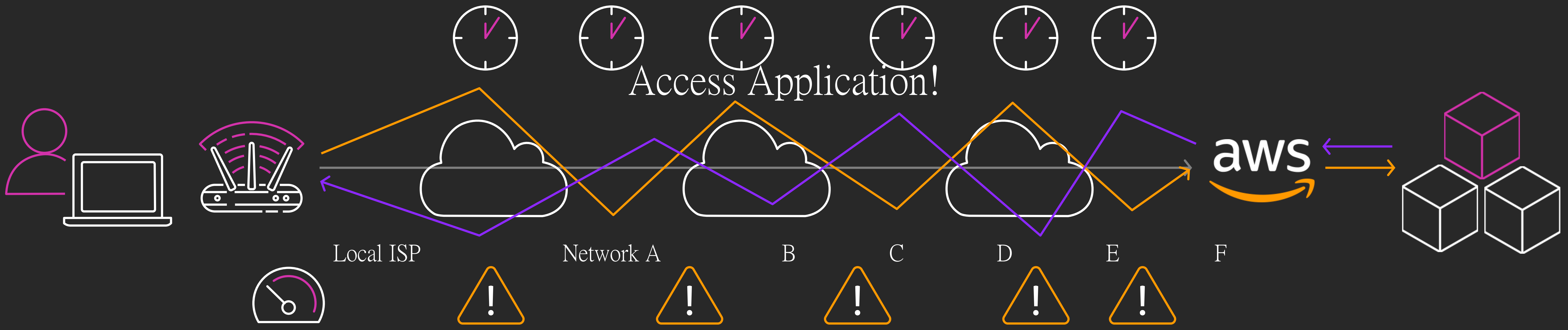
Request body access & S3 origin support for Lambda@Edge

reddit hulu prime video slack Spotify

I have a TCP service (non-http/s)



Introducing AWS Global Accelerator



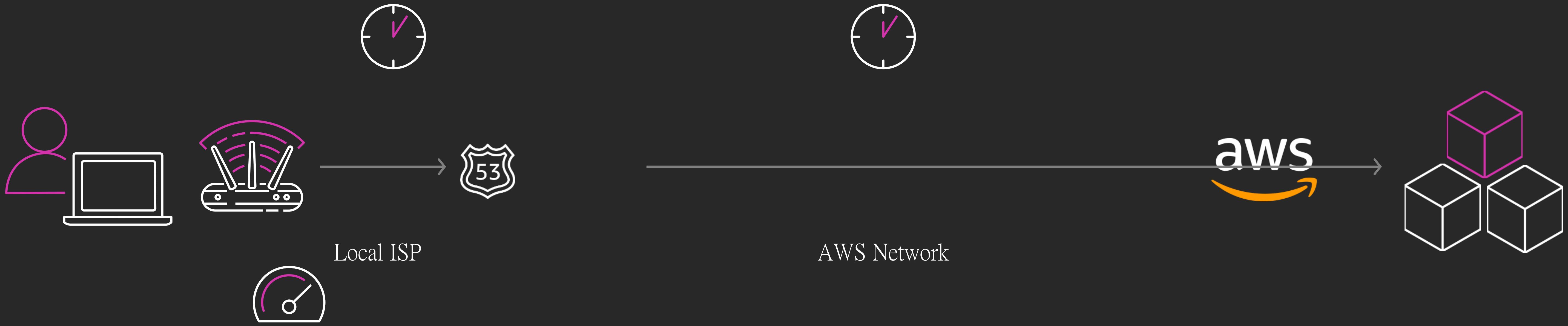
Accessing your application is not that straightforward!

It can take many networks to reach the application

Paths to and from the application may differ

Each hop impacts performance and can introduce risk

Accessing your web applications with AWS Global Accelerator

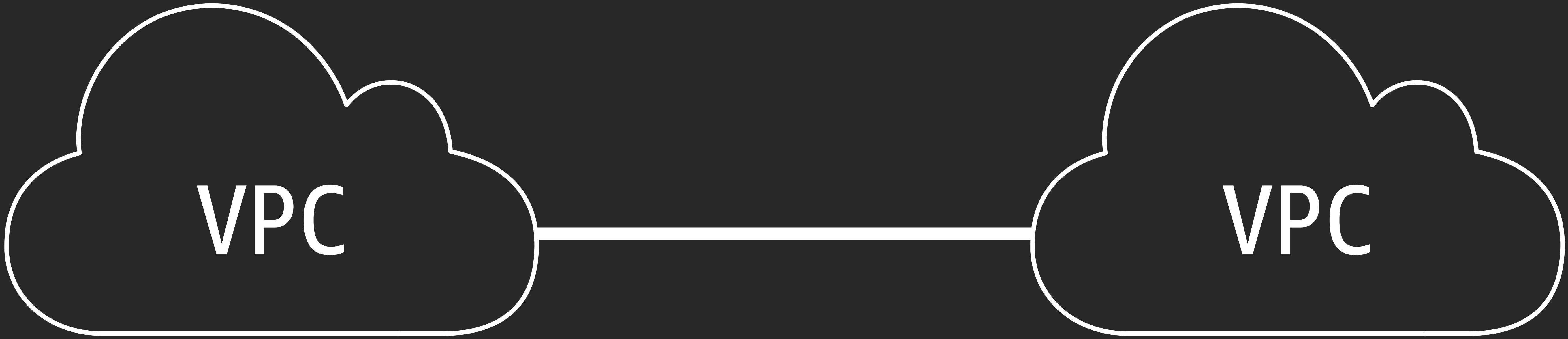


Adding AWS Global Accelerator removes these inefficiencies

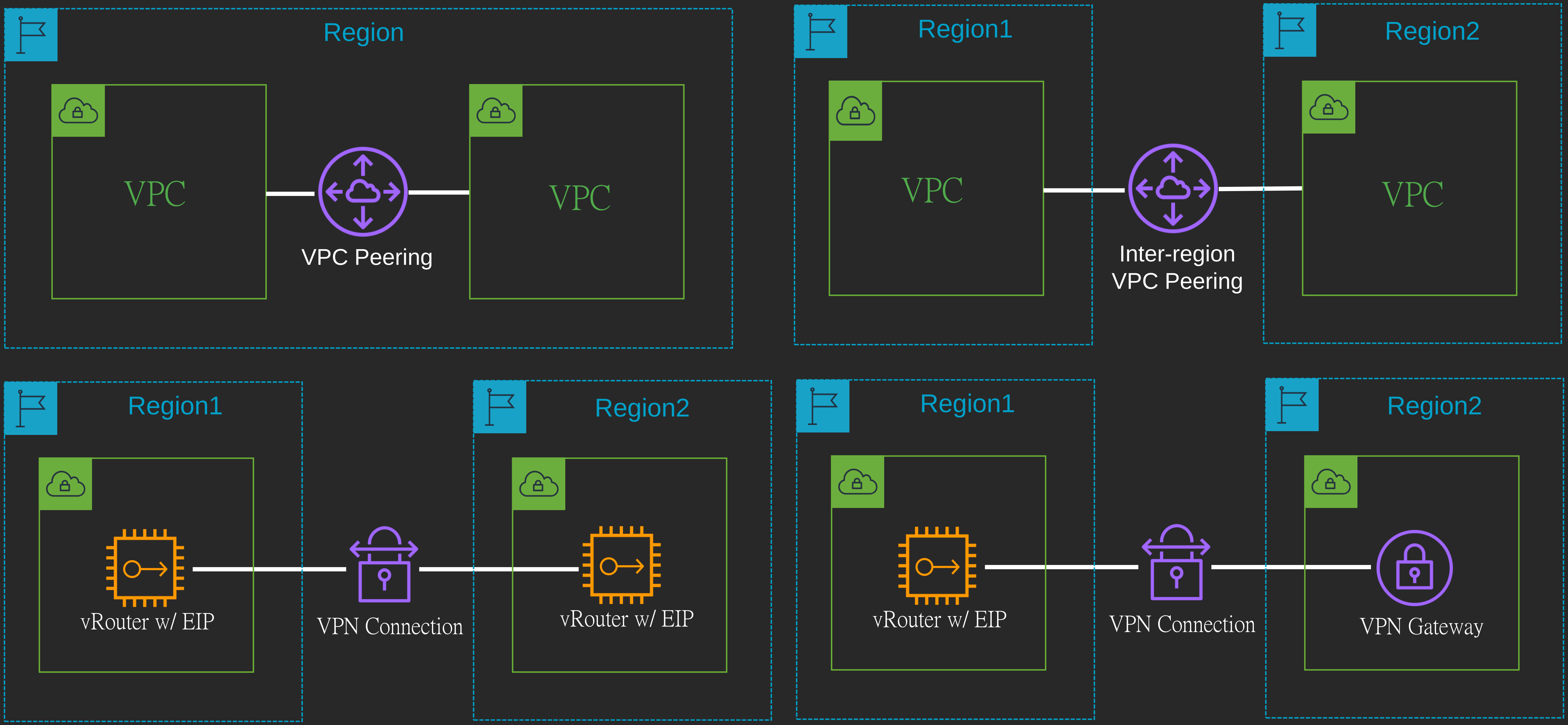
Leverages the Global AWS Network

Resulting in improved performance

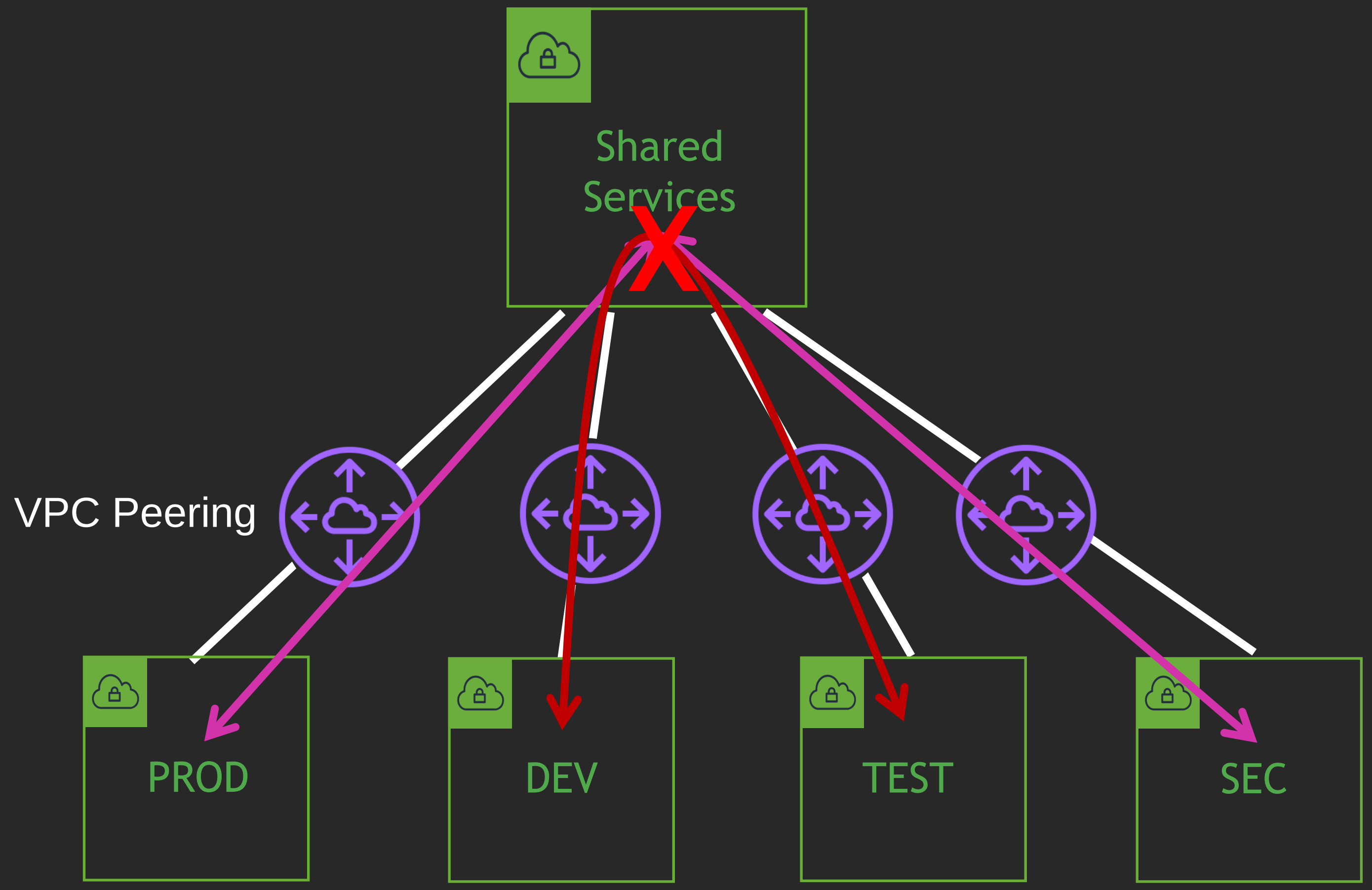
Access from other VPCs



VPC to VPC


Region
VPC
VPC Peering
VPC
Region1
VPC
Inter-region VPC Peering
Region2
VPC
Region1
vRouter w/ EIP
VPN Connection
Region2
vRouter w/ EIP
Region1
vRouter w/ EIP
VPN Connection
Region2
VPN Gateway

VPC to VPCs – VPC peering



Pros

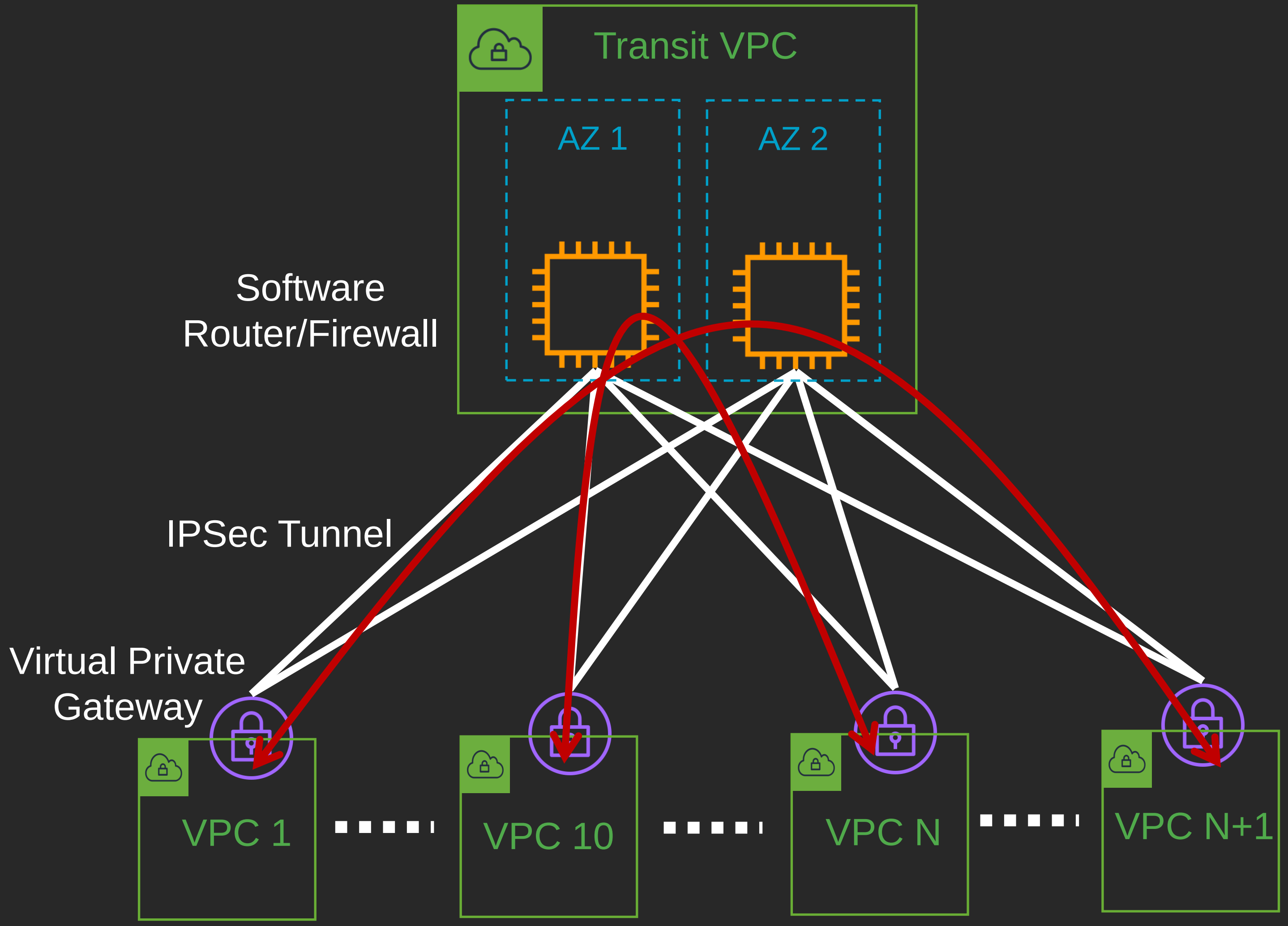
- AWS managed service
- Easy to deploy
- Inter-region support
- Security groups across VPCs
- Private DNS name support
- Encryption (inter-region)

Cons

- Do not support transitive routing
- 125 peering connection per VPC
- Max. full-mesh VPCs: 14 (limit of VPC route table)

VPC to VPCs – Transit VPC

I want to run full-mesh connectivity between all VPCs



Pros

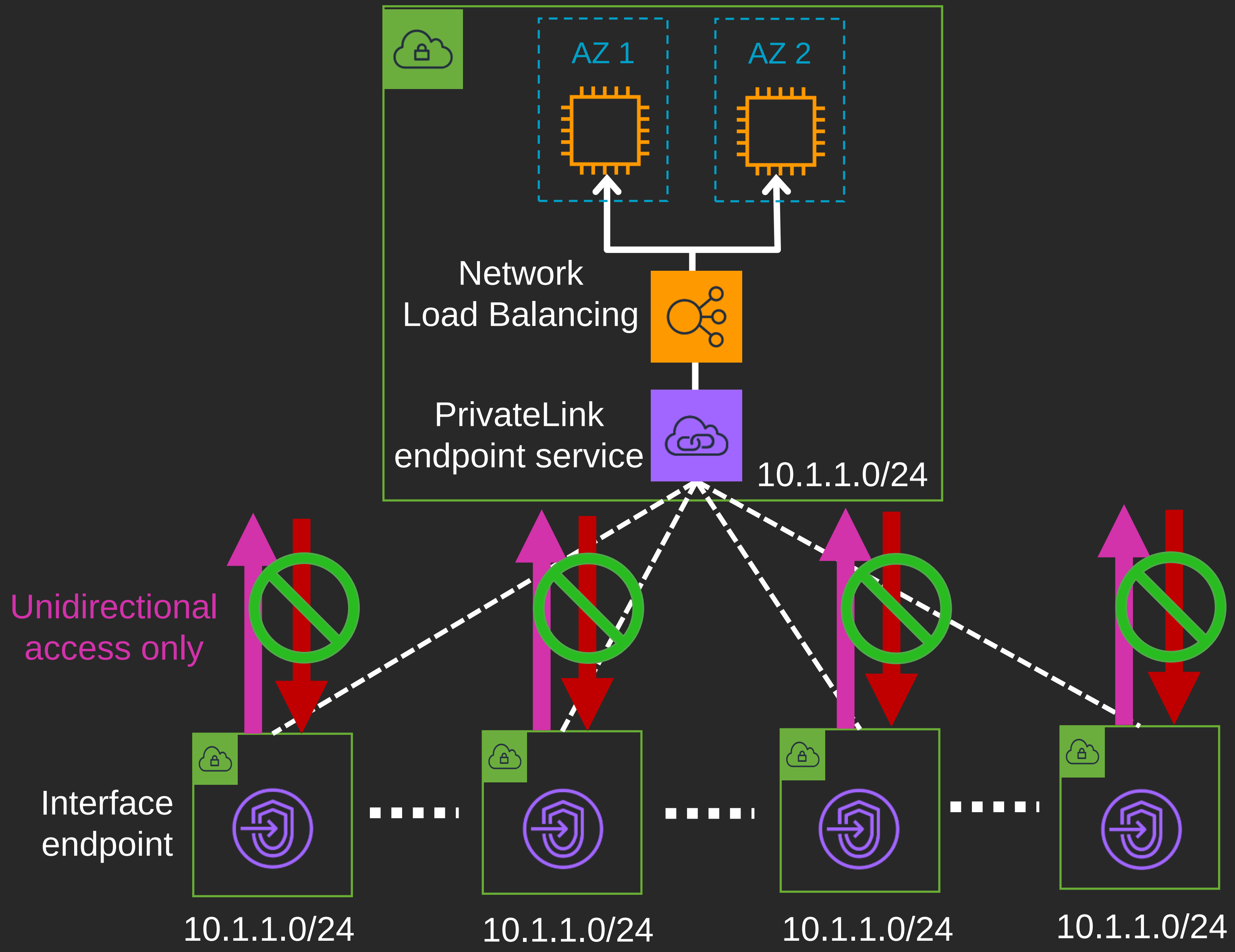
- Scalable for VPC expanding
- Central routing control
- East-west routing
- Automation with partners solution
- Cross account
- Encryption

Cons

- Bandwidth constrained
- Complex management
- Instance and licensing costs

VPC to VPCs – AWS PrivateLink

I need to solve the issue of IP overlap



Benefits

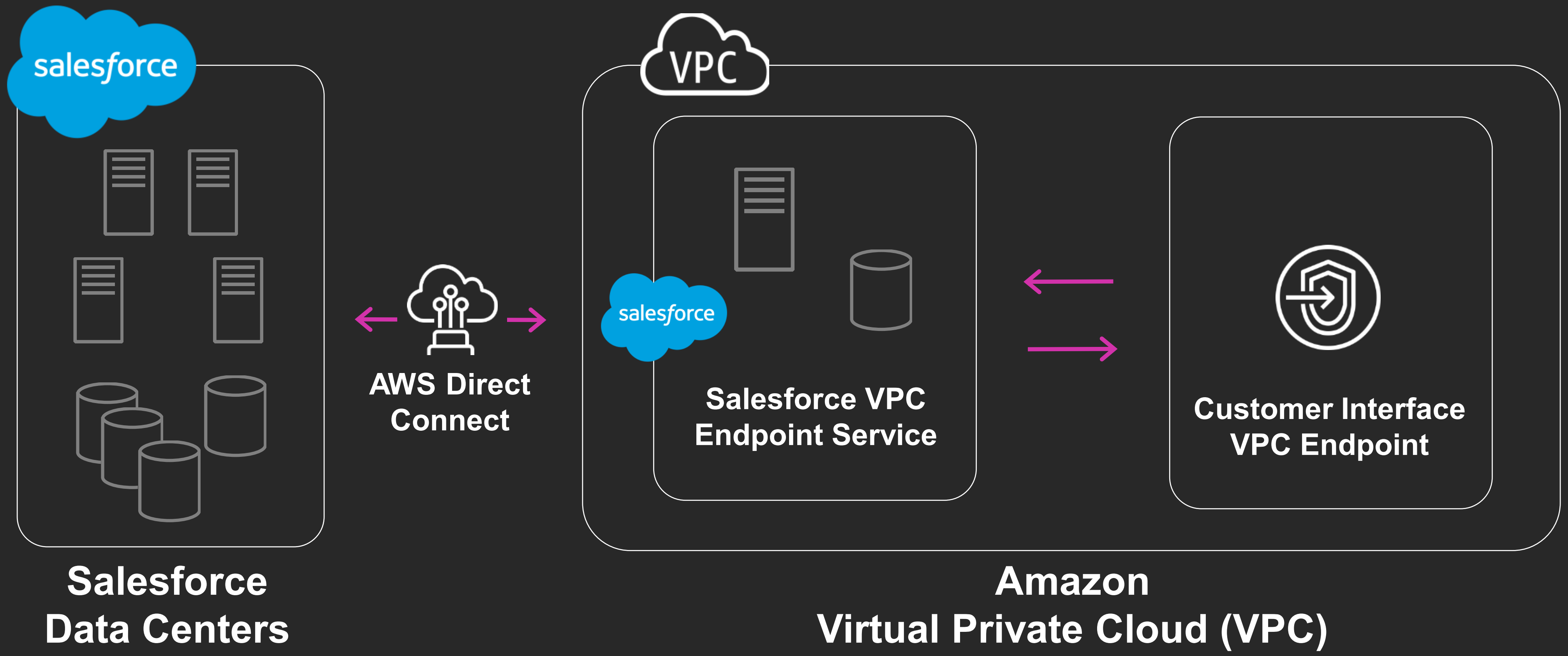
- Highly scalable
- Support overlapping CIDRs
- Support all TCP based services
- All traffic is transmitted privately
- Three types of services accessible over PrivateLink
  - AWS Services
  - Customer hosted internal services
  - 3rd Party services (SaaS)

AWS PrivateLink Momentum

Share services privately between VPCs and on-premises networks

Secure. Scalable. Reliable.

salesforce heroku

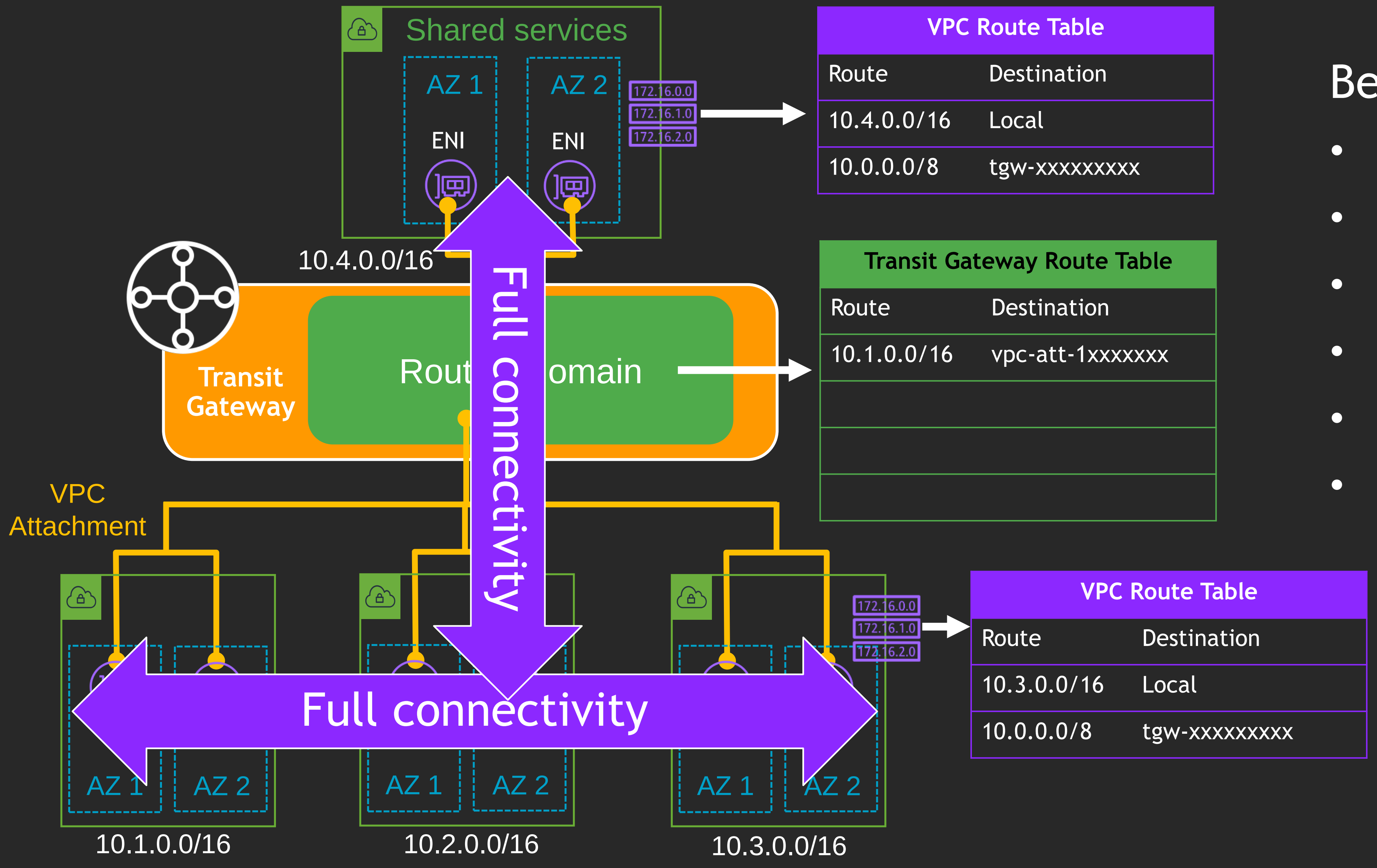


salesforce
VPC
salesforce
AWS Direct Connect
Salesforce VPC Endpoint Service
Customer Interface VPC Endpoint
Salesforce Data Centers
Amazon Virtual Private Cloud (VPC)

ca technologies · APPDYNAMICS · GE · Expedia · Vanguard · twilio · aqua · TIBCO · snowflake · cisco Stealthwatch Cloud · AUTODESK · dynatrace · Alfresco · SIGOPT

VPCs to VPCs – after AWS re:Invent 2018

AWS Transit Gateway



VPC Route Table

Route	Destination
10.4.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

Transit Gateway Route Table

Route	Destination
10.1.0.0/16	vpc-att-1xxxxxxx

VPC Route Table

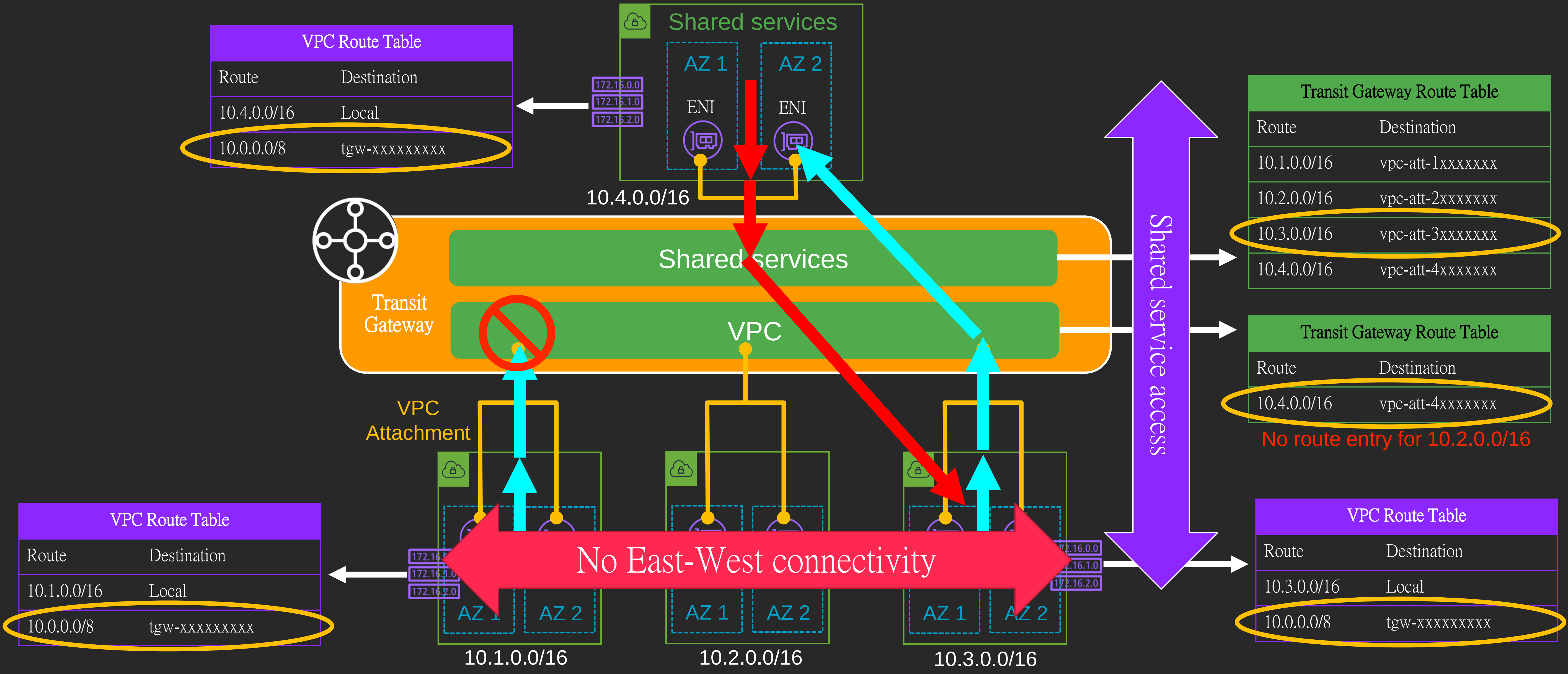
Route	Destination
10.3.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

Benefits

- Highly scalable ~ 5000 attachments
- High performance ~50Gbps per VPC
- Many-to-many or one-to-many
- Routing domain segmentation
- Site-to-site VPN with ECMP
- Direct Connect Gateway support

VPCs to VPCs – VPC Segmentation

AWS Transit Gateway



VPC Route Table	
Route	Destination
10.4.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

Transit Gateway Route Table	
Route	Destination
10.1.0.0/16	vpc-att-1xxxxxxx
10.2.0.0/16	vpc-att-2xxxxxxx
10.3.0.0/16	vpc-att-3xxxxxxx
10.4.0.0/16	vpc-att-4xxxxxxx

Transit Gateway Route Table	
Route	Destination
10.4.0.0/16	vpc-att-4xxxxxxx

No route entry for 10.2.0.0/16

VPC Route Table	
Route	Destination
10.1.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

VPC Route Table	
Route	Destination
10.3.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

AWS Transit Gateway

Regional Gateway

Simple regional gateway to easily manage VPC connectivity

Massive Scale

Attach thousands of VPCs, VPN and Direct Connect connections

Routing Domains

Support for routing domains, allowing per-attachment routing

Partner Integration

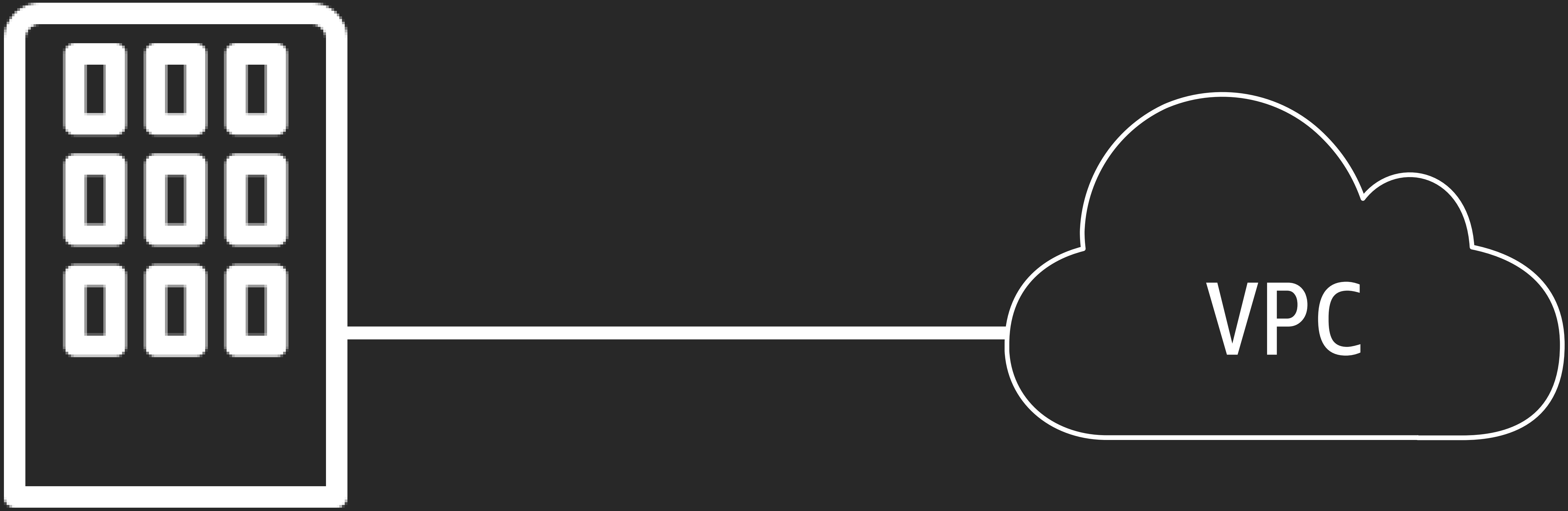
Support for middle-boxing of partner appliances

fuze

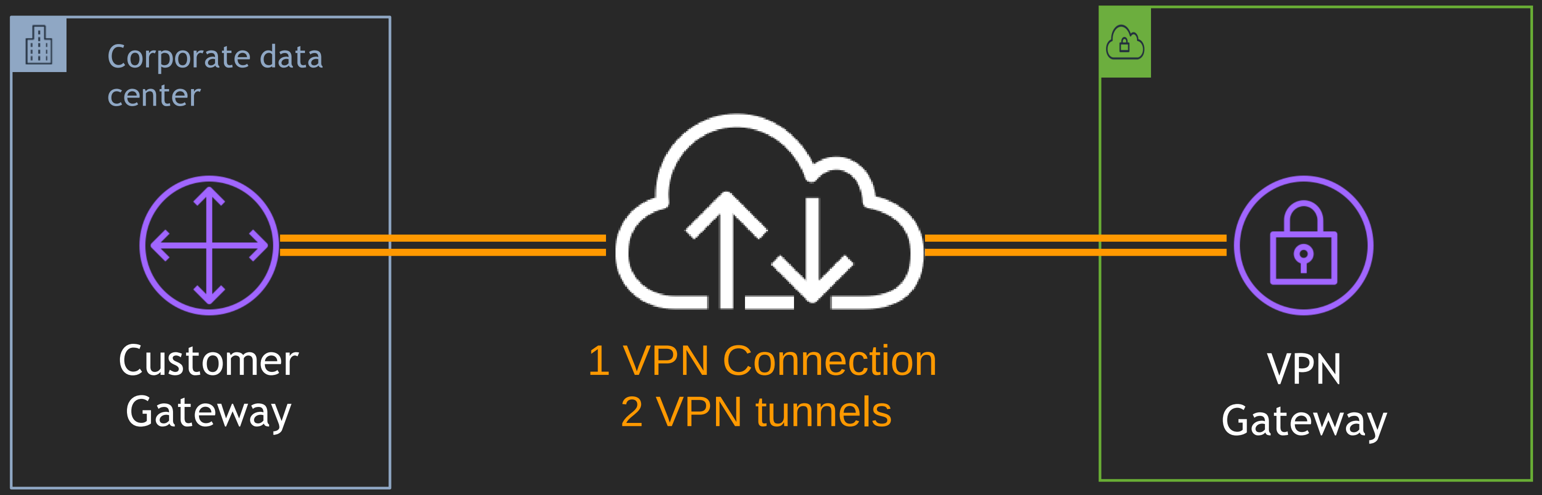
> “AWS Transit Gateway radically evolved and simplified cloud networking. Using Transit Gateway, we reduced the time to interconnect new VPCs and on-premise networks from weeks to minutes while attaining consistent and more reliable network performance!”

Khoder Shamy, Director, Cloud Platform and Infrastructure, Fuze

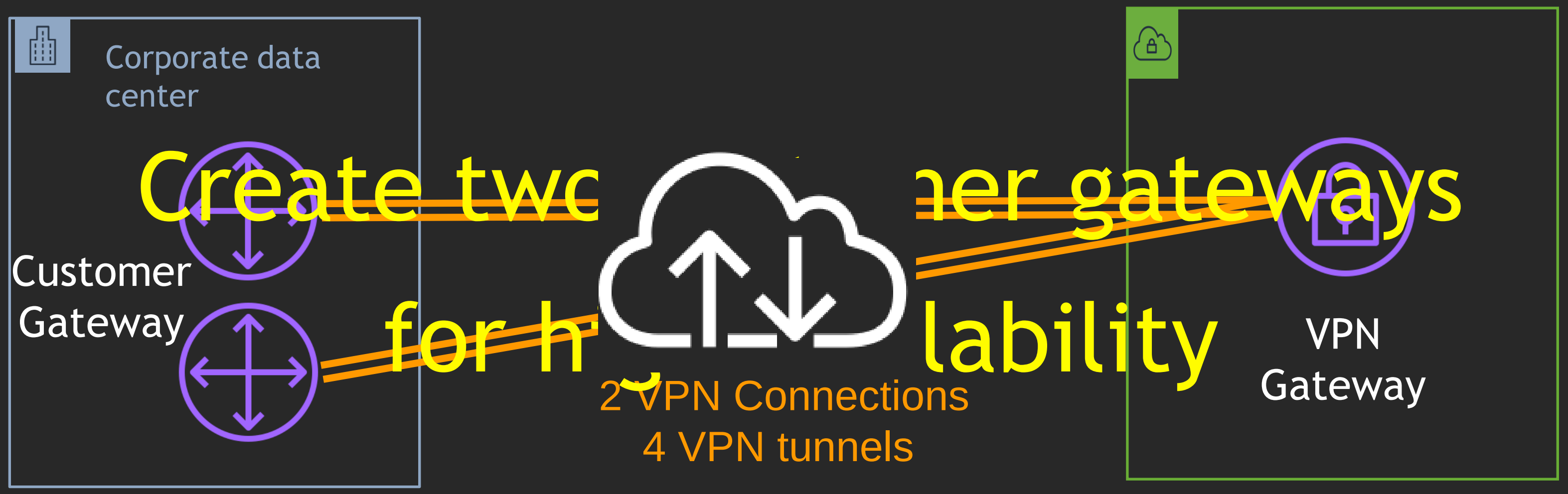
Access from on-premises



Site-to-Site VPN



The VPN tunnels are active/standby by default, you configure BGP attributes for active/active.



Create twc ner gateways for h lability

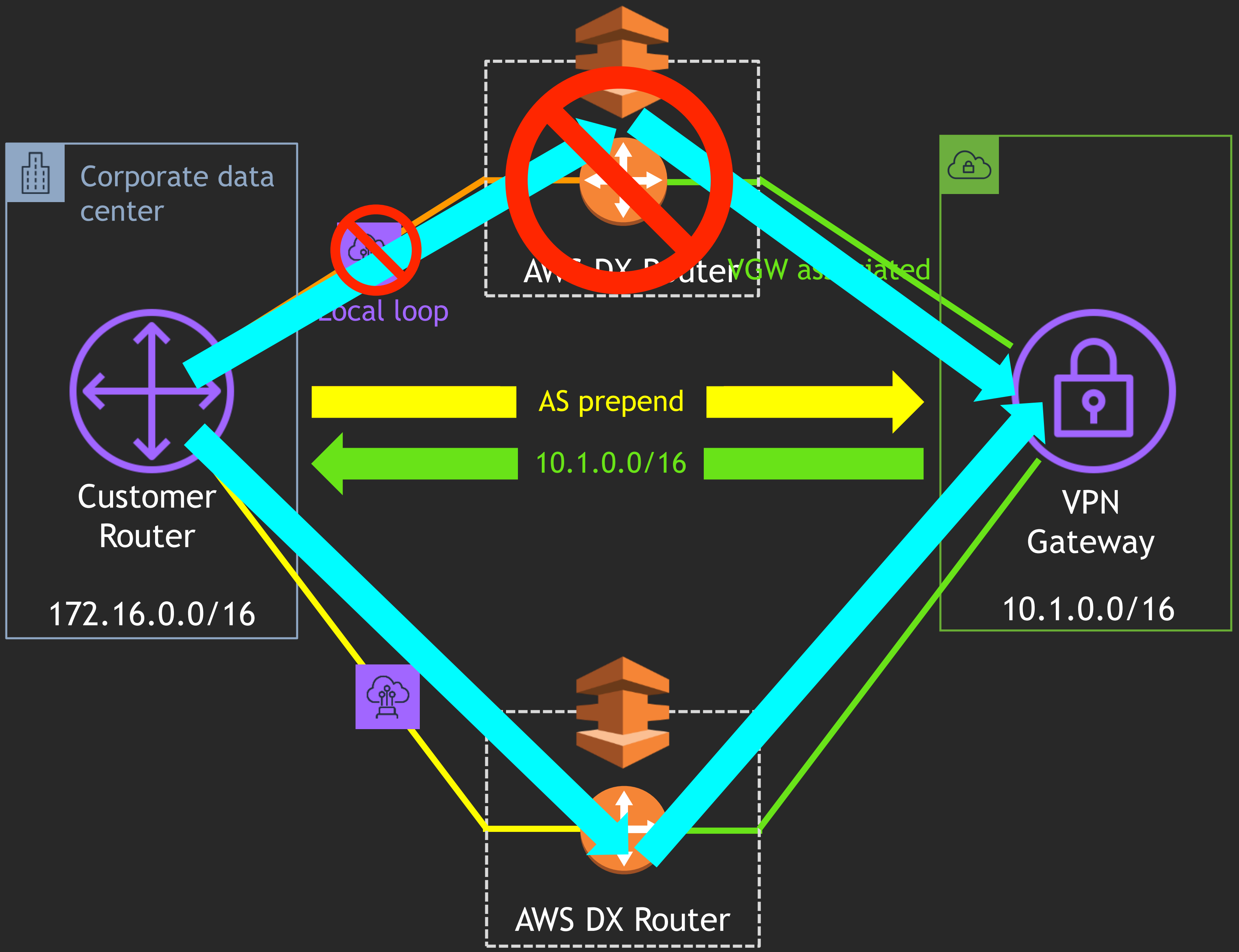
Pros

- Cost effective
- Easy install, minutes to set up
- Support static routing and BGP
- VPN Gateway is managed service

Cons

- Bandwidth constrained (up to 1.25G)
- Hard to manage
- Repeat for every VPC
- No ECMP support

AWS Direct Connect



Pros

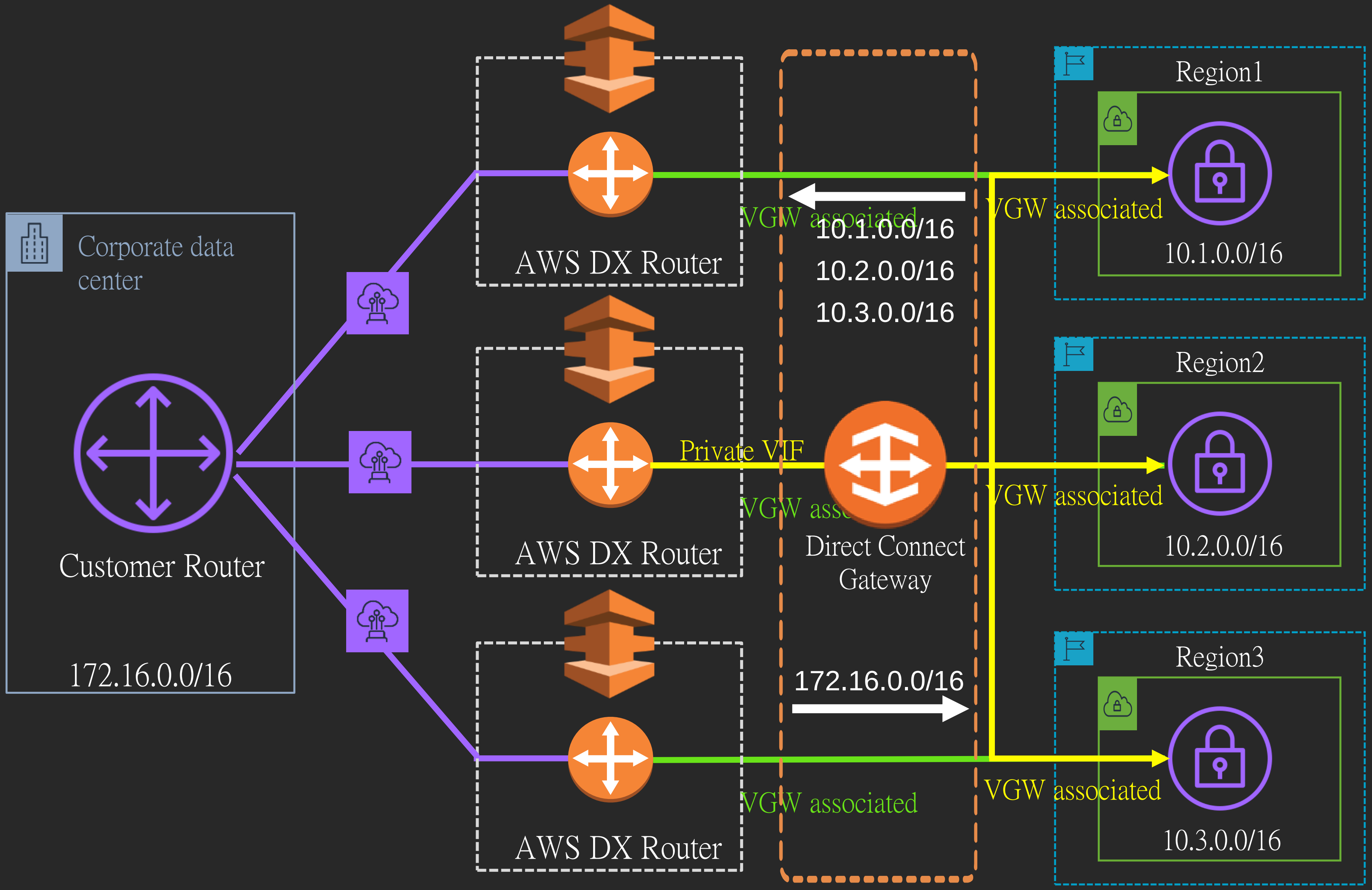
- Consistent networking performance
- LAG support(1Gbps * 4)
- Lower data transfer charges
- BGP routing policy (AS path, BGP communities)

Cons

- Lead time could take weeks
- Local loop monthly charges
- Single region only

Direct Connect Gateway

Access multiple VPCs in different regions



DX Gateway disallowed path

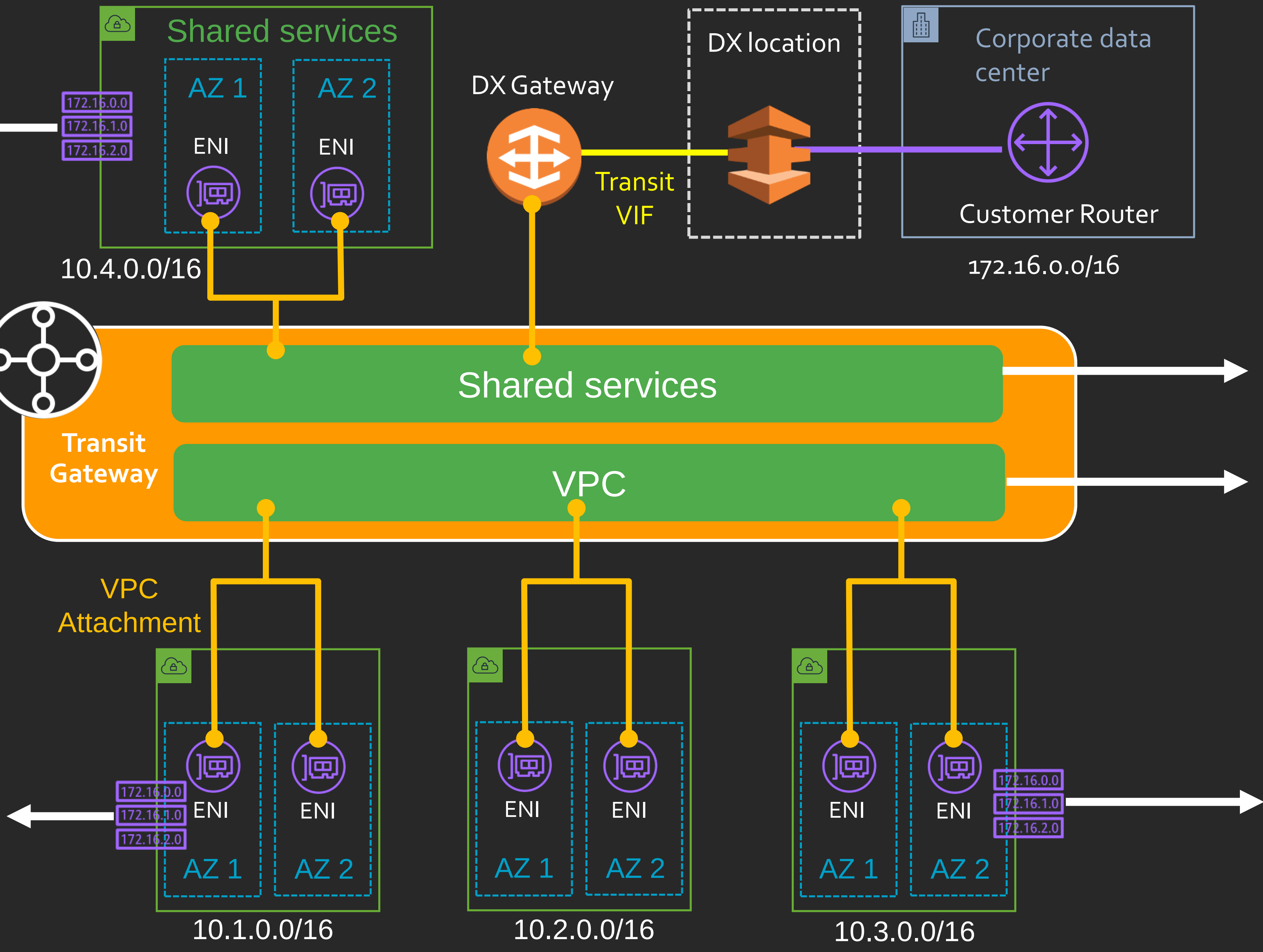
- Private VIF to Private VIF
- VGW to VGW
- Private VIF to VPN

DX Gateway limits

- 200 DX Gateways per account
- 30 VIF attachments per DXG
- 10 VGW associations per DXG

Direct Connect Gateway with TGW

VPC Route Table	
Route	Destination
10.3.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx



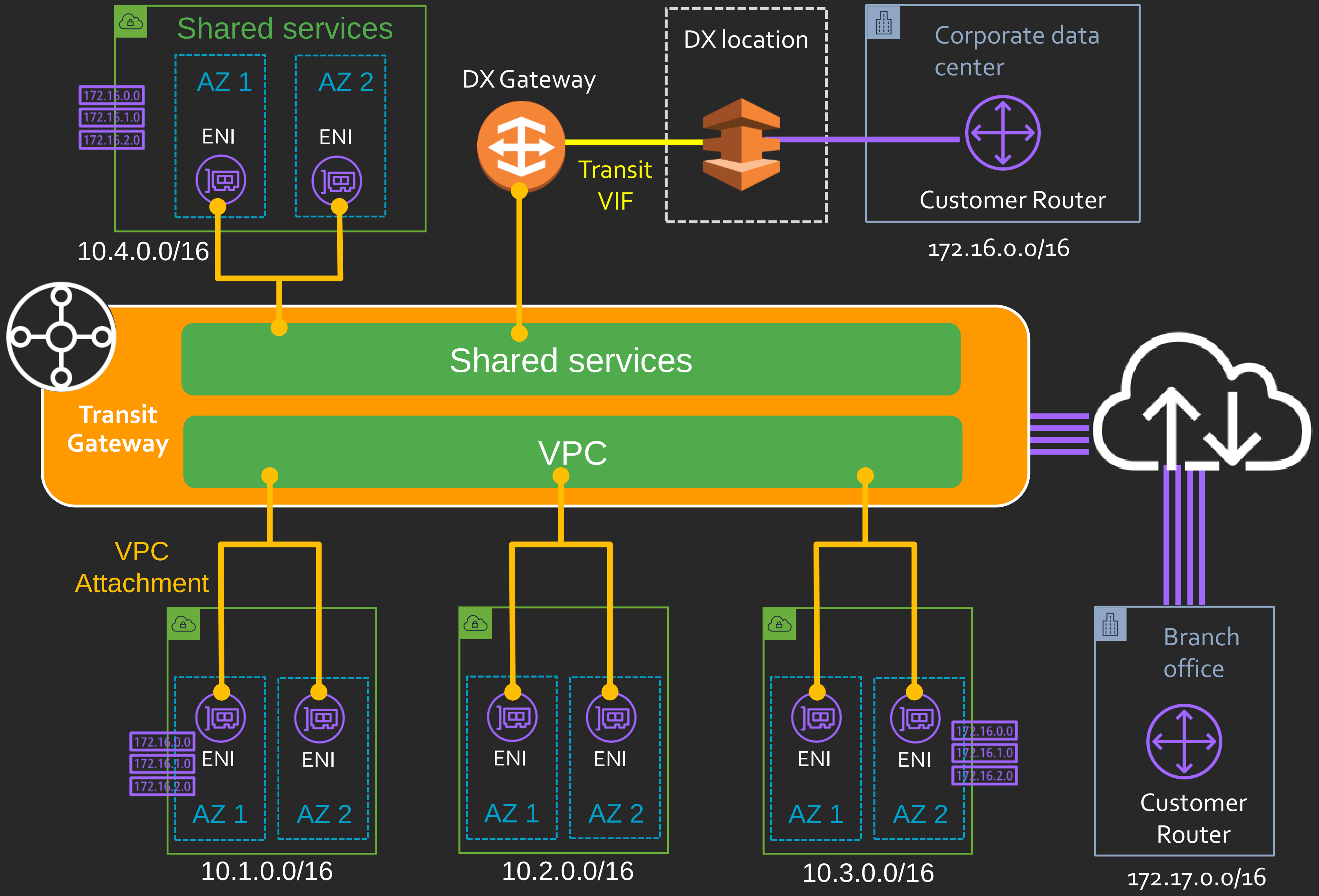
Transit Gateway Route Table	
Route	Destination
10.1.0.0/16	vpc-att-1xxxxxxx
10.2.0.0/16	vpc-att-2xxxxxxx
10.3.0.0/16	vpc-att-3xxxxxxx
10.4.0.0/16	vpc-att-4xxxxxxx

Transit Gateway Route Table	
Route	Destination
10.4.0.0/16	vpc-att-4xxxxxxx

VPC Route Table	
Route	Destination
10.3.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

VPC Route Table	
Route	Destination
10.3.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

Site–to-site VPN with TGW



Benefits

- Consolidate VPN at the Transit Gateway (TGW)
- ECMP support with BGP multi-path (1.25 * 8 = 10Gbps)
- 50Gbps throughput
- Support full-mesh between all attached networks (on-premises behind DX, on-premises behind VPN and VPC)

Client VPN

Client VPN

AWS managed TLS
Client-based VPN

Secure Access

Access resources within
AWS and on-premised via
Direct Connect or VPN

Any Device

Connection from any
device via an
OpenVPN client

Integrated

Seamless integrated with
other AWS resources, i.e.
VPC and Active Directory

Route 53 Resolver

Features

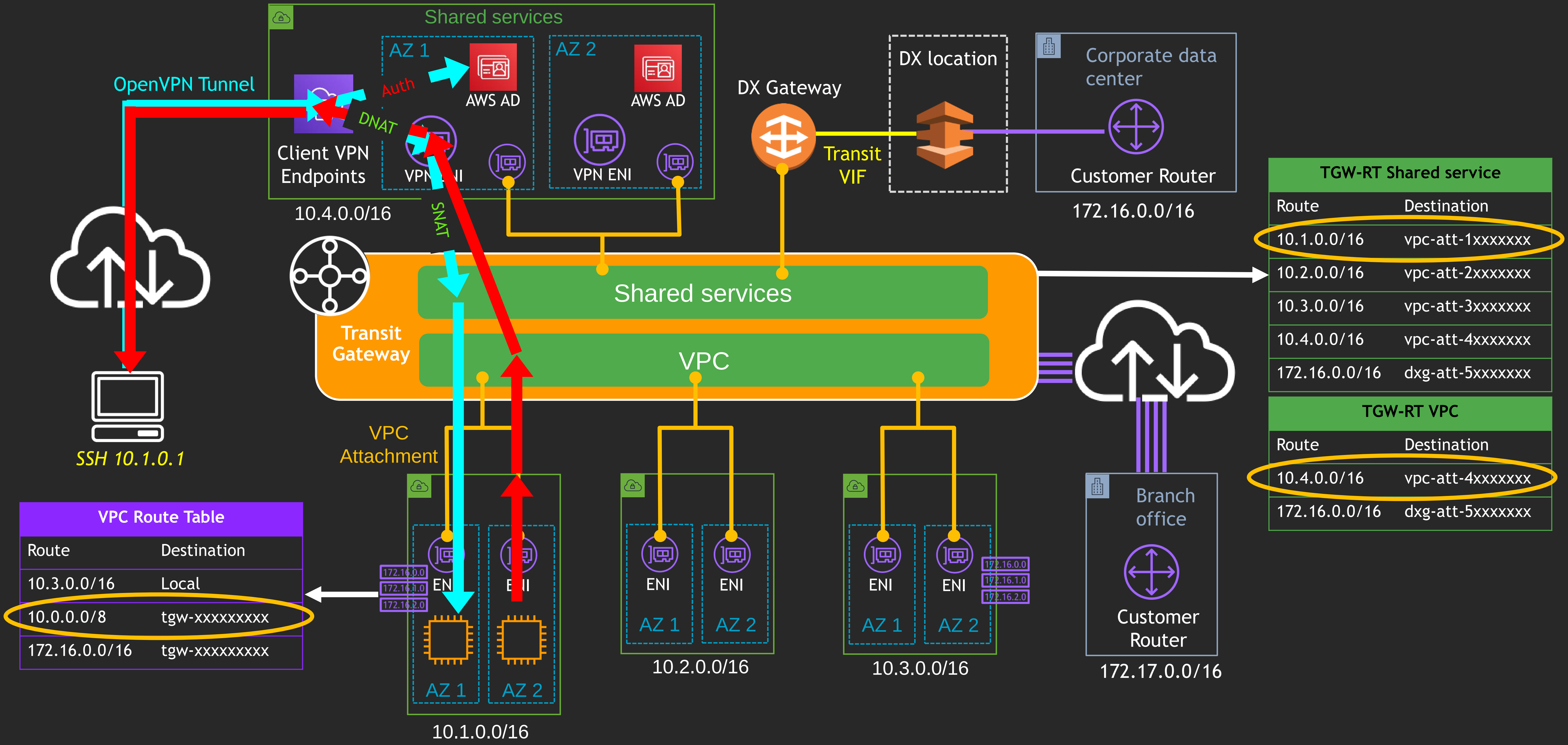
- Managed DNS resolver service from Route 53
- Enables hybrid DNS resolution over Direct Connect and VPN
- Create conditional forwarding rules to re-direct query traffic

Benefits

- Reduce complexity for DNS resolver management
- No single point of failure; highly available
- Ability to maintain VPC specific answers
- Eliminates DNS bottlenecks
- Share rules across multiple accounts

Fully managed DNS resolver for on-premises and AWS

Access your cloud workloads from anywhere



VPC Route Table

Route	Destination
10.3.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx
172.16.0.0/16	tgw-xxxxxxxxx

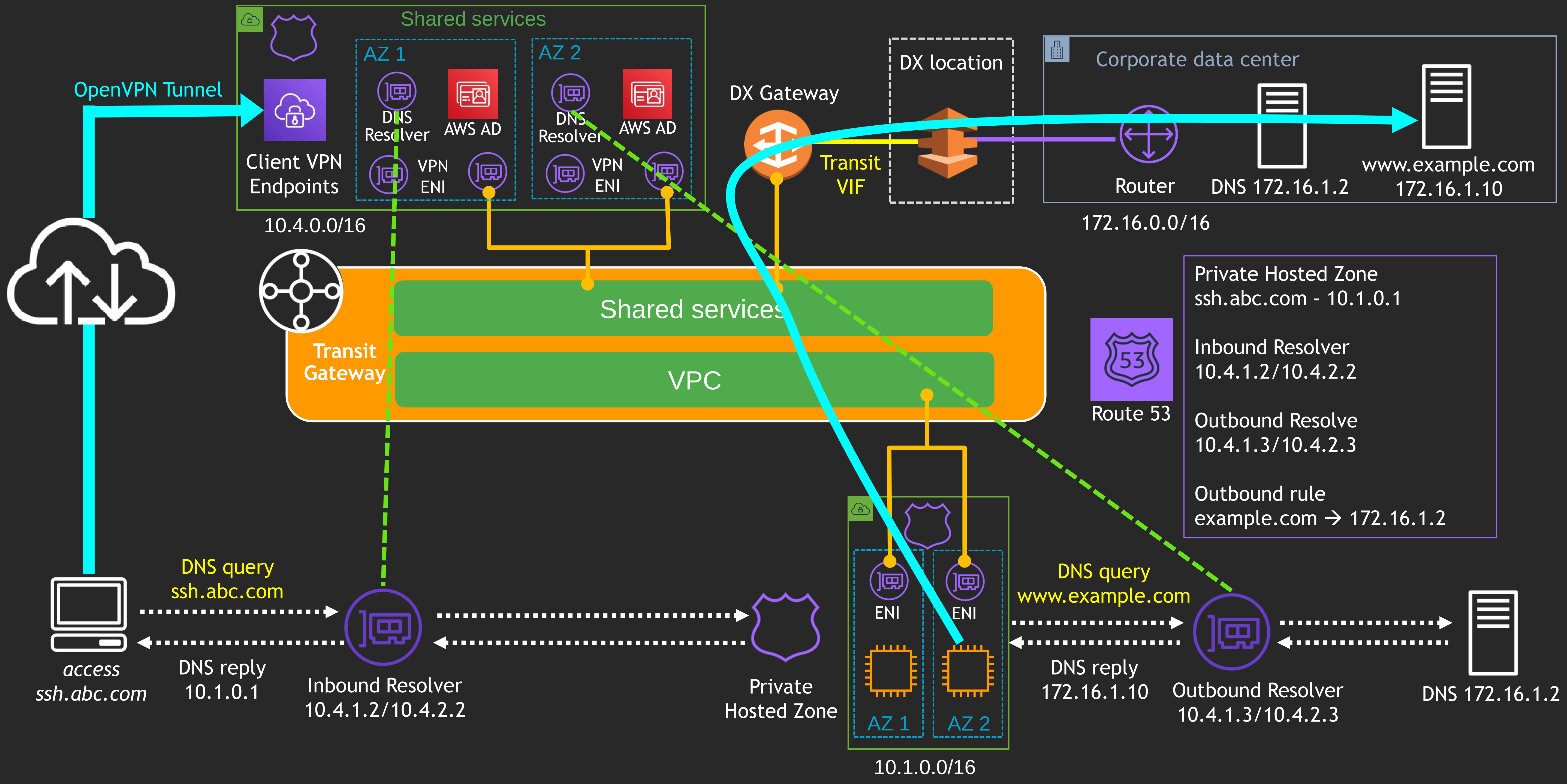
TGW-RT Shared service

Route	Destination
10.1.0.0/16	vpc-att-1xxxxxxx
10.2.0.0/16	vpc-att-2xxxxxxx
10.3.0.0/16	vpc-att-3xxxxxxx
10.4.0.0/16	vpc-att-4xxxxxxx
172.16.0.0/16	dxg-att-5xxxxxxx

TGW-RT VPC

Route	Destination
10.4.0.0/16	vpc-att-4xxxxxxx
172.16.0.0/16	dxg-att-5xxxxxxx

Hybrid DNS architecture



Hybrid connectivity solutions

Site-to-Site VPN

IPSEC connectivity between AWS and your on-premises network

AWS Direct Connect

Private connectivity between AWS and your on-premises network

Transit Gateway

Route 53 Resolver

Support for DNS resolution over Direct Connect and VPN connections

Client VPN

Secure access to AWS resources from any device, anywhere

Providing seamless connectivity between on-premises and AWS

Thank You